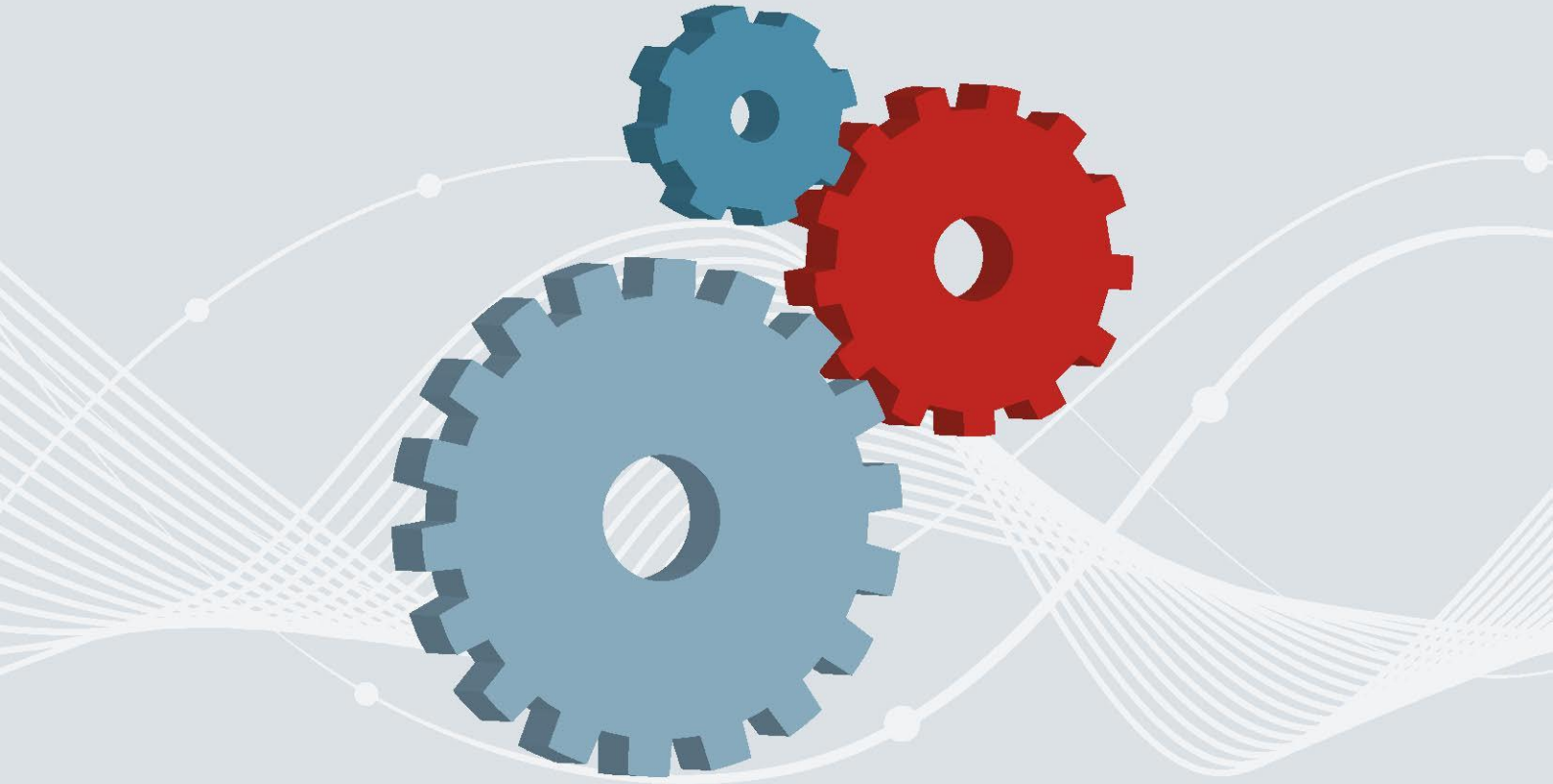
Bundesamt
für Sicherheit in der
Informationstechnik



IT-Grundschutz-Kompendium

Final Draft

Inhaltsverzeichnis

Inhaltsverzeichnis 2
Allgemeines 6
Neues im IT-Grundschutz-Kompendium 6
Dankesworte 9
Institutionen und Personen 10
Mäzene von Bausteinen 10
Bundesamt für Sicherheit in der Informationstechnik 10
1 IT-Grundschutz - Basis für Informationssicherheit 12
1.1 Warum ist Informationssicherheit wichtig? 12
1.2 IT-Grundschutz: Ziel, Idee und Konzeption 14
1.3 Aufbau des IT-Grundschutz-Kompendiums 16
1.4 Aufbau der Bausteine 17
1.5 Umsetzungshinweise 19
1.6 Mitwirkung der Anwender und Versionierung 20
1.7 Anwendungsweisen des IT-Grundschutz-Kompendiums 20
2 Schichtenmodell und Modellierung 24
2.1 Modellierung nach IT-Grundschutz 24
2.2 Zuordnung anhand Schichtenmodell 26
2.3 Bearbeitungsreihenfolge der Bausteine 35
Rollendefinition 37
Glossar 42
Elementare Gefährdungen 57
G 0.1 Feuer 59
G 0.2 Ungünstige klimatische Bedingungen 60
G 0.3 Wasser 61
G 0.4 Verschmutzung, Staub, Korrosion 62
G 0.5 Naturkatastrophen 63
G 0.6 Katastrophen im Umfeld 64
G 0.7 Großereignisse im Umfeld 65
G 0.8 Ausfall oder Störung der Stromversorgung 66
G 0.9 Ausfall oder Störung von Kommunikationsnetzen 67
G 0.10 Ausfall oder Störung von Versorgungsnetzen 68
G 0.11 Ausfall oder Störung von Dienstleistern 69
G 0.12 Elektromagnetische Störstrahlung 70
G 0.13 Abfangen kompromittierender Strahlung 71
G 0.14 Ausspähen von Informationen (Spionage) 72
G 0.15 Abhören 73
G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten 74
G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten 75
G 0.18 Fehlplanung oder fehlende Anpassung 76
G 0.19 Offenlegung schützenswerter Informationen 77
G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle 79

G 0.21 Manipulation von Hard- oder Software **80**
G 0.22 Manipulation von Informationen **81**
G 0.23 Unbefugtes Eindringen in IT-Systeme **82**
G 0.24 Zerstörung von Geräten oder Datenträgern **83**
G 0.25 Ausfall von Geräten oder Systemen **84**
G 0.26 Fehlfunktion von Geräten oder Systemen **85**
G 0.27 Ressourcenmangel **86**
G 0.28 Software-Schwachstellen oder -Fehler **87**
G 0.29 Verstoß gegen Gesetze oder Regelungen **88**
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen **89**
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen **90**
G 0.32 Missbrauch von Berechtigungen **91**
G 0.33 Personalausfall **92**
G 0.34 Anschlag **93**
G 0.35 Nötigung, Erpressung oder Korruption **94**
G 0.36 Identitätsdiebstahl **95**
G 0.37 Abstreiten von Handlungen **96**
G 0.38 Missbrauch personenbezogener Daten **97**
G 0.39 Schadprogramme **98**
G 0.40 Verhinderung von Diensten (Denial of Service) **99**
G 0.41 Sabotage **100**
G 0.42 Social Engineering **101**
G 0.43 Einspielen von Nachrichten **102**
G 0.44 Unbefugtes Eindringen in Räumlichkeiten **103**
G 0.45 Datenverlust **104**
G 0.46 Integritätsverlust schützenswerter Informationen **105**
G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe **107**
Bausteine **108**
ISMS: Sicherheitsmanagement **108**
ISMS.1 Sicherheitsmanagement **109**
ORP: Organisation und Personal **118**
ORP.1 Organisation **119**
ORP.2 Personal **126**
ORP.3 Sensibilisierung und Schulung **133**
ORP.4 Identitäts- und Berechtigungsmanagement **140**
ORP.5 Compliance Management (Anforderungsmanagement) **148**
CON: Konzeption und Vorgehensweisen **154**
CON.1 Kryptokonzept **155**
CON.2 Datenschutz **164**
CON.3 Datensicherungskonzept **169**
CON.4 Auswahl und Einsatz von Standardsoftware **175**
CON.5 Entwicklung und Einsatz von Fachanwendungen **182**
CON.6 Löschen und Vernichten **189**
CON.7 Informationssicherheit auf Auslandsreisen **195**
OPS: Betrieb **206**
OPS.1.1.2 Ordnungsgemäße IT-Administration **207**
OPS.1.1.3 Patch- und Änderungsmanagement **215**
OPS.1.1.4 Schutz vor Schadprogrammen **222**
OPS.1.1.5 Protokollierung **228**
OPS.1.1.6 Software-Tests und -Freigaben **235**
OPS.1.2.2 Archivierung **242**

OPS.1.2.3 Informations- und Datenträgeraustausch **251**
OPS.1.2.4 Telearbeit **259**
OPS.2.1 Outsourcing für Kunden **265**
OPS.2.4 Fernwartung **274**
OPS.3.1 Outsourcing für Dienstleister **284**
DER: Detektion und Reaktion **293**
DER.1 Detektion von sicherheitsrelevanten Ereignissen **294**
DER.2.1 Behandlung von Sicherheitsvorfällen **303**
DER.2.2 Vorsorge für die IT-Forensik **314**
DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle **320**
DER.3.1 Audits und Revisionen **327**
DER.3.2 IS-Revision für Bundesbehörden **335**
DER.4 Notfallmanagement **344**
APP: Anwendungen **352**
APP.1.1 Office-Produkte **353**
APP.1.2 Web-Browser **361**
APP.2.1 Allgemeiner Verzeichnisdienst **368**
APP.2.2 Active Directory **376**
APP.3.1 Webanwendungen **386**
APP.3.2 Webserver **397**
APP.3.3 Fileserver **406**
APP.3.4 Samba **414**
APP.3.6 DNS-Server **421**
APP.4.3 Relationale Datenbanksysteme **430**
APP.5.1 Allgemeine Groupware **440**
APP.5.2 Microsoft Exchange und Outlook **450**
SYS: IT-Systeme **458**
Übersicht **458**
SYS.1.1 Allgemeiner Server **459**
SYS.1.2.2 Windows Server 2012 **470**
SYS.1.3 Server unter Unix **478**
SYS.1.5 Virtualisierung **484**
SYS.1.8 Speicherlösungen **493**
SYS.2.1 Allgemeiner Client **503**
SYS.2.2.2 Clients unter Windows 8.1 **515**
SYS.2.2.3 Clients unter Windows 10 **524**
SYS.2.3 Clients unter Unix **533**
SYS.3.1 Laptops **540**
SYS.3.2.1 Allgemeine Smartphones und Tablets **547**
SYS.3.2.2 Mobile Device Management (MDM) **556**
SYS.3.2.3 iOS (for Enterprise) **565**
SYS.3.2.4 Android **577**
SYS.3.4 Mobile Datenträger **582**
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte **589**
SYS.4.4 Allgemeines IoT-Gerät **597**
IND: Industrielle IT **606**
IND.1 Betriebs- und Steuerungstechnik **607**
IND.2.1 Allgemeine ICS-Komponente **620**
IND.2.2 Speicherprogrammierbare Steuerung (SPS) **629**
IND.2.3 Sensoren und Aktoren **633**
IND.2.4 Maschine **637**

NET: Netze und Kommunikation **641**
NET.1.1 Netzarchitektur und -design **642**
NET.1.2 Netzmanagement **653**
NET.2.1 WLAN-Betrieb **663**
NET.2.2 WLAN-Nutzung **671**
NET.3.1 Router und Switches **676**
NET.3.2 Firewall **686**
NET.3.3 VPN **696**
INF: Infrastruktur **702**
INF.1 Allgemeines Gebäude **703**
INF.2 Rechenzentrum sowie Serverraum **713**
INF.3 Elektrotechnische Verkabelung **725**
INF.4 IT-Verkabelung **732**
INF.7 Büroarbeitsplatz **739**
INF.8 Häuslicher Arbeitsplatz **745**
INF.9 Mobiler Arbeitsplatz **751**
INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume **758**

Neues im IT-Grundschutz-Kompendium

Das IT-Grundschutz-Kompendium wird künftig immer zum 1. Februar eines jeden Jahres in einer neuen Edition erscheinen. Bausteine, die in der Zwischenzeit erstellt und nach einer Kommentierung durch die IT-Grundschutz-Anwender veröffentlicht werden, erscheinen zunächst online als neue Version, bevor sie in die nächste Edition einfließen.

Bei der Bearbeitung der Bausteine wurde vielfach auf die bestehenden Bausteine aufgesetzt, zu vielen Themen wurden Bausteine aber auch neu verfasst. Für die Anwender des IT-Grundschutzes bedeutet die behutsame Anpassung der Inhalte, dass sie einfach auf die neuen Bausteine umsteigen können. Als Hilfestellung hierfür gibt es zu jedem modernisierten Baustein eine entsprechende Migrationstabelle, in der die bisherigen Maßnahmen des klassischen IT-Grundschutzes den Anforderungen des modernisierten IT-Grundschutzes gegenübergestellt sind.

Für die erste Edition des IT-Grundschutz-Kompendiums wurden folgende Bausteine modernisiert und in die erste Edition übernommen:

- ISMS.1 Sicherheitsmanagement
- ORP.1 Organisation
- ORP.2 Personal
- ORP.3 Sensibilisierung und Schulung
- ORP.4 Identitäts- und Berechtigungsmanagement
- ORP.5 Compliance Management (Anforderungsmanagement)
- CON.1 Kryptokonzept
- CON.2 Datenschutz
- CON.3 Datensicherungskonzept
- CON.4 Auswahl und Einsatz von Standardsoftware
- CON.5 Entwicklung und Einsatz von Allgemeinen Anwendungen
- CON.6 Löschen und Vernichten
- OPS.1.1.3 Patch- und Änderungsmanagement
- OPS.1.1.4 Schutz vor Schadprogrammen
- OPS.1.1.5 Protokollierung
- OPS.1.1.6 Software-Tests und -Freigaben
- OPS.1.2.2 Archivierung
- OPS.1.2.3 Informations- und Datenträgeraustausch
- OPS.1.2.4 Telearbeit
- OPS.2.1 Outsourcing für Kunden
- OPS.3.1 Outsourcing für Dienstleister
- DER.4 Notfallmanagement
- APP.2.1 Allgemeiner Verzeichnisdienst
- APP.2.2 Active Directory
- APP.3.1 Webanwendungen
- APP.3.2 Webserver
- APP.3.4 Samba
- APP.3.6 DNS-Server
- APP.5.1 Allgemeine Groupware

- APP.5.2 Microsoft Exchange und Outlook
- SYS.1.1 Allgemeiner Server
- SYS.1.5 Virtualisierung
- SYS.1.8 Speicherlösungen
- SYS.2.1 Allgemeine Clients
- SYS.2.2.2 Clients unter Windows 8.1
- SYS.3.1 Laptops
- SYS.3.2.1 Allgemeine Smartphones und Tablets
- SYS.3.4 Mobile Datenträger
- SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte
- NET.2.1 WLAN-Betrieb
- NET.2.2 WLAN-Nutzung
- NET.3.1 Router und Switches
- NET.3.2 Firewall
- NET.3.3 VPN
- INF.1 Allgemeines Gebäude
- INF.3 Elektrotechnische Verkabelung
- INF.4 IT-Verkabelung
- INF.7 Büroarbeitsplatz
- INF.8 Häuslicher Arbeitsplatz
- INF.9 Mobiler Arbeitsplatz
- INF.10 Besprechungs-, Veranstaltungs- und Schulungsraum

Neben den modernisierten Bausteinen enthält die erste Edition des IT-Grundschutz-Kompendiums auch Bausteine zu neuen Themen sowie solche, die ausgehend von bereits vorhandenen Bausteinen grundlegend überarbeitet wurden:

- CON.7 Informationssicherheit auf Auslandsreisen
- OPS.1.1.2 Ordnungsgemäße IT-Administration
- OPS.2.4 Fernwartung
- DER.1 Detektion von sicherheitsrelevanten Ereignissen
- DER.2.1 Behandlung von Sicherheitsvorfällen
- DER.2.2 Vorsorge für die IT-Forensik
- DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle (APT-Responder)
- DER.3.1 Audits und Revisionen
- DER.3.2 IS-Revision für Bundesbehörden
- APP.1.1 Office-Produkte
- APP.1.2 Web-Browser
- APP.3.3 Fileserver
- APP.4.3 Relationale Datenbanksysteme
- SYS.1.2.2 Windows Server 2012
- SYS.1.3 Server unter Unix
- SYS.2.2.3 Clients unter Windows 10
- SYS.2.3 Clients unter Unix
- SYS.3.2.2 Mobile Device Management (MDM)
- SYS.3.2.3 iOS (for Enterprise)
- SYS.3.2.4 Android
- SYS.4.4 Allgemeines IoT-Gerät
- IND.1 Betriebs- und Steuerungstechnik
- IND.2.1 Allgemeine ICS-Komponente
- IND.2.2 Speicherprogrammierbare Steuerung (SPS)
- IND.2.3 Sensoren und Aktoren
- IND.2.4 Maschine
- NET.1.1 Netzarchitektur und -design
- NET.1.2 Netzmanagement
- INF.2 Rechenzentrum

Zu zahlreichen Bausteinen sind auf der IT-Grundschutz-Webseite auch entsprechende Umsetzungshinweise veröffentlicht. In den Umsetzungshinweisen wird konkret beschrieben, wie die Anforderungen der IT-Grundschutz-Bausteine erfüllt werden können.

Neue elementare Gefährdung zu Seiteneffekten IT-gestützter Angriffe

Ergänzend zu den 46 bereits vorhandenen elementaren Gefährdungen wurde eine weitere elementare Gefährdung identifiziert. Diese 47. elementare Gefährdung adressiert die "schädlichen Seiteneffekte IT-gestützter Angriffe". Diese zeichnen sich dadurch aus, dass sie von den Tätern nicht beabsichtigt sind, nicht die unmittelbar angegriffenen Zielobjekte betreffen oder unbeteiligte Dritte schädigen. Ursächlich hierfür sind die hohe Komplexität und Vernetzung moderner Informationstechnik sowie die Tatsache, dass die Abhängigkeiten der angegriffenen Zielobjekte und der zugehörigen Prozesse in der Regel nicht offenkundig sind.

Dankesworte

Mit der Edition 2018 des IT-Grundschutz-Kompendiums wurde der IT-Grundschutz grundlegend modernisiert und so auf aktuelle Entwicklungen angepasst. Für die Mitarbeit bei der Modernisierung des IT-Grundschutzes und die engagierte Unterstützung bei der Erstellung neuer Bausteine wird an dieser Stelle allen Beteiligten gedankt.

Strategische Ausrichtung und Gesamtverantwortung:

Frau Isabel Münch, BSI

Gesamtkoordination und Chefredaktion:

Herr Holger Schildt, BSI

Management und Controlling:

Herr Alex Essoh, BSI

Herr Florian Hillebrand, BSI

Redaktionelle Bearbeitung:

Herr Ehad Qorri, BSI

Frau Katharina Thönnes, BSI

Herr Christoph Wiemers, BSI

Qualitätssicherung:

Frau Katrin Alberts, BSI

Herr Sebastian Frank, SecuMedia Verlag

Herr Peter Hohl, SecuMedia Verlag

Herr Alexander Stanik, BSI

Leitung Bausteinerstellung:

Frau Petra Bottenberg, BSI

Herr Alex Essoh, BSI

Herr Florian Hillebrand, BSI

Herr Birger Klein, BSI

Frau Verena Lang, BSI

Herr Ehad Qorri, BSI

Herr Holger Schildt, BSI

Frau Katharina Thönnes, BSI

Herr Christoph Wiemers, BSI

Die Anwender des IT-Grundschutzes konnten vor der Veröffentlichung des IT-Grundschutz-Kompendiums die Bausteine kommentieren. Viele Anwender haben das BSI dabei unterstützt und ihr Fachwissen in die Modernisierung einfließen lassen. Auch hier sei den Mitwirkenden gedankt. Darüber hinaus sei allen gedankt, die sich durch konstruktive Kritik und praktische Verbesserungsvorschläge an der Verbesserung des IT-Grundschutzes beteiligt haben.

Institutionen und Personen

Folgende Anwender und Auftragnehmer haben durch die Erstellung von Bausteinen ihr Fachwissen in die Erstellung und Migration von Bausteinen für das IT-Grundschutz-Kompendium einfließen lassen. Ihnen gebührt ausdrücklicher Dank, da ihr Engagement die Entstehung, Modernisierung und Weiterentwicklung des IT-Grundschutz-Kompendiums erst ermöglicht hat.

Besonderer Dank gilt den Mitarbeitern der Firma HiSolutions AG für die Unterstützung bei der Modernisierung des IT-Grundschutzes.

Hierüber hinaus danken wir folgenden Personen:

Herrn Oliver Flüs (ComConsult Beratung und Planung GmbH), Frau Daniela Gies (ComConsult Beratung und Planung GmbH), Herrn Dr. Simon Hoff (ComConsult Beratung und Planung GmbH), Frau Dietlind Hübner (ComConsult Beratung und Planung GmbH), Herrn Dr. Sönke Maseberg (datenschutz cert GmbH), Herrn Christian Merz (chm-software.com), Herrn Christoph Möhring (ITZBund), Herrn Simon Oberem (ComConsult Beratung und Planung GmbH), Herrn Jan Schirrmacher (datenschutz cert GmbH), Herrn Steffen Schwalm (BearingPoint GmbH), Herrn Thomas Simon (ComConsult Beratung und Planung GmbH), Herrn Andreas F. Scholtz (mc-2 management consulting GmbH), Herrn Roland Schwarz (Bundesdruckerei GmbH), Herrn Martin Stolle, (mc-2 management consulting GmbH), Herrn Dr. Gerhard Weck (INFODAS GmbH)

sowie den Mitgliedern der Arbeitsgruppe Informationssicherheit (AG InfoSic) des IT-Planungsrats und des AK Technik der Datenschutzbeauftragten des Bundes und der Länder für die zahlreichen konstruktiven Kommentare.

Mäzene von Bausteinen

Der IT-Grundschutz wird nicht nur vom BSI oder im Auftrag des BSI weiterentwickelt, sondern auch durch die Unterstützung der Anwender. Viele Themen genießen bei den Anwendern des IT-Grundschutzes so eine hohe Priorität, dass sie Bausteine erstellen und kostenlos zur Verfügung stellen oder vorhandene Bausteine maßgebend kostenlos verbessern. Den folgenden Anwendern, die die genannten Bausteine entwickelt oder umfangreich aktualisiert haben, gilt der größte Dank:

- Herrn Dr. Martin Meints (Dataport) für CON.5 Entwicklung und Einsatz von Allgemeinen Anwendungen
- Herrn Reiner Meisriemler (Oracle) für APP.4.3 Relationale Datenbanksysteme

Bundesamt für Sicherheit in der Informationstechnik

Das IT-Grundschutz-Kompendium wurde mit dem fachlichen Wissen folgender Kollegen des Bundesamtes für Sicherheit in der Informationstechnik bereichert:

Herr Heinrich Altengarten, Herr Dr. Stephan Arlt, Herr Kirsten Beiss, Herr Thomas Caspers, Herr Armin Cordel, Herr Markus de Brün, Herr Thorsten Dietrich, Herr Dr. Clemens Doubrava, Herr Michael Dwucet, Herr Dr. Lothar Eßer, Herr Jürgen Förster, Herr Dr. Kai Fuhrberg, Herr Dr. Patrick Grete, Herr Carl-Daniel Hailfinger, Herr Dr. Dirk Häger, Frau Veselina Hensel, Herr Dr. Hartmut Isselhorst, Herr Holger Junker, Herr Wilfried Kister, Herr Jens Kluge, Frau Dr. Ulrike Korte, Herr Dr. Robert Krawczyk, Herr Dr. Helge Kreutzmann, Herr Daniel Loevenich, Herr Jens Mehrfeld, Herr Marc Meyer, Herr Michael Mehrhoff, Herr Dr. Frank Niedermeyer, Herr Dr. Harald Niggemann, Herr Michael Nosbüsch, Herr Detlef Nuß,

Herr Michael Otter, Herr Rudolf Schick, Herr Karl Hubert Schmitz, Herr Arndt Schneider, Herr Carsten Schulz, Herr Jens Sieberg, Herr Dr. Timo Steffens, Frau Anne-Kathrin Walter, Herr Frank Weber, Herr Maximilian Winkler, Herr Dr. Dietmar Wippig

sowie Herr Michael Förtsch, Herr Thomas Häberlen, Herr Kevin Mosser

1 IT-Grundschutz – Basis für Informationssicherheit

1.1 Warum ist Informationssicherheit wichtig?

Informationen sind ein wesentlicher Wert für Unternehmen und Behörden und müssen daher angemessen geschützt werden. Die meisten Geschäftsprozesse sind heute in Wirtschaft und Verwaltung ohne IT-Unterstützung längst nicht mehr vorstellbar. Eine zuverlässig funktionierende Informationsverarbeitung ist ebenso wie die zugehörige Technik für die Aufrechterhaltung des Betriebes unerlässlich. Unzureichend geschützte Informationen stellen einen häufig unterschätzten Risikofaktor dar, der sogar existenzbedrohend werden kann. Dabei ist ein vernünftiger Informationsschutz ebenso wie eine Grundsicherung der IT schon mit verhältnismäßig geringen Mitteln zu erreichen: Mit dem IT-Grundschutz bietet das BSI eine praktikable Methode an, um die Informationen einer Institution angemessenen zu schützen. Die Kombination aus den IT-Grundschutz-Vorgehensweisen Basis-, Kern- und Standard-Absicherung sowie dem IT-Grundschutz-Kompendium beinhaltet für unterschiedliche Einsatzumgebungen sowohl Sicherheitsanforderungen als auch Maßnahmen zum sicheren Umgang mit Informationen.

Aufgrund der skizzierten Abhängigkeit steigt bei Cyber-Sicherheitsvorfällen auch die Gefahr für Institutionen, einen Imageschaden zu erleiden. Die verarbeiteten Daten und Informationen müssen adäquat geschützt, Sicherheitsmaßnahmen sorgfältig geplant, umgesetzt und kontrolliert werden. Hierbei ist es aber wichtig, sich nicht nur auf die Sicherheit von IT-Systemen zu konzentrieren, da Informationssicherheit nicht nur eine Frage der Technik ist. Sie hängt auch stark von infrastrukturellen, organisatorischen und personellen Rahmenbedingungen ab. Die Sicherheit der Betriebsumgebung, die ausreichende Schulung der Mitarbeiter, die Verlässlichkeit von Dienstleistungen, der richtige Umgang mit zu schützenden Informationen und viele andere wichtige Aspekte dürfen auf keinen Fall vernachlässigt werden.

Mängel im Bereich der Informationssicherheit können zu erheblichen Problemen führen. Die potentiellen Schäden lassen sich verschiedenen Kategorien zuordnen.

- **Verlust der Verfügbarkeit**
  Wenn grundlegende Informationen nicht vorhanden sind, fällt dies meistens schnell auf, vor allem, wenn Aufgaben ohne diese nicht weitergeführt werden können. Läuft ein IT-System nicht, können beispielsweise keine Geldtransaktionen durchgeführt werden, Online-Bestellungen sind nicht möglich, Produktionsprozesse stehen still. Auch wenn die Verfügbarkeit von bestimmten Informationen lediglich eingeschränkt ist, kann es zu Arbeitsbeeinträchtigungen in den Prozessen einer Institution kommen.
- **Verlust der Vertraulichkeit von Informationen**
  Jeder Bürger und jeder Kunde möchte, dass mit seinen personenbezogenen Daten vertraulich umgegangen wird. Jedes Unternehmen sollte wissen, dass interne, vertrauliche Daten über Umsatz, Marketing, Forschung und Entwicklung die Konkurrenz interessieren. Die ungewollte Offenlegung von Informationen kann in vielen Bereichen schwere Schäden nach sich ziehen.
- **Verlust der Integrität (Korrektheit von Informationen)**

Gefälschte oder verfälschte Daten können beispielsweise zu Fehlbuchungen, falschen Lieferungen oder fehlerhaften Produkten führen. Auch der Verlust der Authentizität (Echtheit und Überprüfbarkeit) hat, als ein Teilbereich der Integrität, eine hohe Bedeutung: Daten werden beispielsweise einer falschen Person zugeordnet. So können Zahlungsanweisungen oder Bestellungen zu Lasten einer dritten Person verarbeitet werden, ungesicherte digitale Willenserklärungen können falschen Personen zugerechnet werden, die "digitale Identität" wird gefälscht.

Informations- und Kommunikationstechnik spielt in fast allen Bereichen des täglichen Lebens eine bedeutende Rolle, dabei ist das Innovationstempo seit Jahren unverändert hoch. Besonders erwähnenswert sind dabei folgende Entwicklungen:

- **Steigender Vernetzungsgrad**
  Menschen, aber auch IT-Systeme arbeiten heutzutage nicht mehr isoliert voneinander, sondern immer stärker vernetzt. Dies ermöglicht es, auf gemeinsame Datenbestände zuzugreifen und intensive Formen der Kooperation über geographische, politische oder institutionelle Grenzen hinweg zu nutzen. Damit entsteht nicht nur eine Abhängigkeit von einzelnen IT-Systemen, sondern in starkem Maße auch von Datennetzen. Sicherheitsmängel können dadurch schnell globale Auswirkungen haben.
- **IT-Verbreitung und Durchdringung**
  Immer mehr Bereiche werden durch Informationstechnik unterstützt, häufig ohne dass dies dem Benutzer auffällt. Die erforderliche Hardware wird zunehmend kleiner und günstiger, so dass kleine und kleinste IT-Einheiten in alle Bereiche des Alltags integriert werden können. So gibt es beispielsweise Bekleidung mit integrierten Gesundheitssensoren, mit dem Internet vernetzte Glühbirnen sowie IT-gestützte Sensorik in Autos, um automatisch auf veränderte Umgebungsverhältnisse reagieren zu können oder sogar selbstfahrende Fahrzeuge zu ermöglichen. Die Kommunikation der verschiedenen IT-Komponenten untereinander findet dabei zunehmend drahtlos statt. Alltagsgegenstände werden dadurch über das Internet lokalisierbar und steuerbar.
- **Verschwinden der Netzgrenzen**
  Bis vor kurzem ließen sich Geschäftsprozesse und Anwendungen eindeutig auf IT-Systeme und Kommunikationsstrecken lokalisieren. Ebenso ließ sich sagen, an welchen Standorten und bei welcher Institution diese angesiedelt waren. Durch die zunehmende Verbreitung von Clouddiensten sowie der Kommunikation über das Internet verschwinden diese Grenzen zunehmend.
- **Kürzere Angriffszyklen**
  Die beste Vorbeugung gegen Schadprogramme oder andere Angriffe auf IT-Systeme, Anwendungsprogramme und Protokolle ist, sich frühzeitige über Sicherheitslücken und deren Beseitigung, z. B. durch Einspielen von Patches und Updates, zu informieren. Die Zeitspanne zwischen dem Bekanntwerden einer Sicherheitslücke und den ersten Angriffen in der Breite ist mittlerweile sehr kurz, so dass es immer wichtiger wird, ein gut aufgestelltes Informationssicherheitsmanagement und Warnsystem zu haben.
- **Höhere Interaktivität von Anwendungen**
  Bereits vorhandene Techniken werden immer stärker miteinander kombiniert, um so neue Anwendungs- und Nutzungsmodelle zu erschaffen. Darunter finden sich unterschiedliche Anwendungsbereiche wie soziale Kommunikationsplattformen, Portale für die gemeinsame Nutzung von Informationen, Bildern und Videos oder interaktive Web-Anwendungen. Dies führt aber auch zu einer höheren Verquickung unterschiedlicher Geschäftsprozess und höherer Komplexität, wodurch die Systeme insgesamt schwieriger abzusichern sind.
- **Verantwortung der Benutzer**
  Die beste Technik und solide Sicherheitsmaßnahmen können keine ausreichende Informationssicherheit gewährleisten, wenn der Mensch als Akteur nicht angemessen berücksichtigt wird. Dabei geht es vor allem um das verantwortungsvolle Handeln des Einzelnen. Dazu ist es notwendig, aktuelle Informationen über Sicherheitsrisiken und Verhaltensregeln im Umgang mit der IT zu beachten.

Angesichts der vorgestellten Gefährdungspotenziale und der steigenden Abhängigkeit stellen sich damit für jede Institution, sei es ein Unternehmen oder eine Behörde, bezüglich Informationssicherheit mehrere zentrale Fragen:

- Wie sorgfältig wird mit geschäftsrelevanten Informationen umgegangen?
- Wie sicher ist die Informationstechnik einer Institution?
- Welche Anforderungen müssen erfüllt und welche Sicherheitsmaßnahmen müssen hierfür ergriffen werden?
- Wie müssen diese Maßnahmen konkret umgesetzt werden?
- Wie hält bzw. verbessert eine Institution das erreichte Sicherheitsniveau?
- Werden die personellen Aspekte der Informationssicherheit angemessen berücksichtigt?
- Wie hoch ist das Sicherheitsniveau anderer Institutionen, mit denen eine Kooperation stattfindet?
- Sind Notfallvorkehrungen getroffen, um im Gefährdungsfall schnell reagieren zu können?

Bei der Beantwortung dieser Fragen für die eigene Institution ist zu beachten, dass Informationssicherheit eine Kombination aus technischen, organisatorischen, personellen und infrastrukturellen Aspekten ist. Es ist sinnvoll, ein Informationssicherheitsmanagement einzuführen, mit dem die mit Informationssicherheit verbundenen Aufgaben konzipiert, koordiniert und überwacht werden können.

Die Erfahrung zeigt, dass es ohne ein funktionierendes Informationssicherheitsmanagement praktisch nicht möglich ist, kontinuierlich ein angemessenes Sicherheitsniveau zu erzielen und zu erhalten. Daher wird im BSI-Standard 200-1 *Managementsysteme für Informationssicherheit (ISMS)* beschrieben, was ein solches Managementsystem leisten sollte und welche Aufgaben damit verbunden sind.

Werden die Geschäftsprozesse, Anwendungen und IT-Systeme typischer Institutionen im Hinblick auf obige Fragen verglichen, so kristallisiert sich eine Gruppe mit gemeinsamen Eigenschaften heraus. Die Vorgehensweisen und IT-Systeme in dieser Gruppe lassen sich wie folgt charakterisieren:

- Es sind typische Vorgehensweisen und IT-Systeme, d. h. es sind keine Individuallösungen, sondern sie sind weit verbreitet im Einsatz.
- Der Schutzbedarf der Informationen bezüglich Vertraulichkeit, Integrität und Verfügbarkeit liegt im Rahmen des Normalen.
- Die Geschäftsprozesse, Anwendungen und IT-Systeme sind den üblichen Rahmenbedingungen unterworfen und unterliegen somit typischen Bedrohungen und Gefahren.

Gelingt es, für diese Gruppe der "typischen" Geschäftsprozesse, Anwendungen und IT-Systeme den gemeinsamen Nenner aller erforderlichen Sicherheitsanforderungen zu beschreiben, so erleichtert dies die Beantwortung obiger Fragen für diese "typischen" Anwendungsfälle erheblich. Bereiche, die außerhalb dieser Gruppe liegen, seien es seltenere Individuallösungen oder IT-Systeme mit hohem Schutzbedarf, können sich dann zwar an den Anforderungen orientieren, bedürfen letztlich aber einer besonderen Betrachtung.

Die Bausteine des IT-Grundschutz-Kompendiums beschreiben detailliert standardisierte Sicherheitsanforderungen, die für jedes Objekt im Informationsverbund zu beachten sind. Eine ausführliche Beschreibung des Prozesses zum Erreichen und Aufrechterhalten eines angemessenen Sicherheitsniveaus sowie eine einfache Verfahrensweise zur Ermittlung des erreichten Sicherheitsniveaus in Form eines Soll-Ist-Vergleichs finden sich in den BSI-Standards 200-1, 200-2 und 200-3 zum IT-Grundschutz.

1.2 IT-Grundschutz: Ziel, Idee und Konzeption

Im IT-Grundschutz-Kompendium werden standardisierte Sicherheitsanforderungen für typische Geschäftsprozesse, Anwendungen und IT-Systeme in einzelnen Bausteinen beschrieben. Ziel des IT-Grundschutzes ist es, einen angemessenen Schutz für alle Informationen einer Institution zu erreichen. Die IT-Grundschutz-Methodik zeichnet sich dabei durch den ganzheitlichen Ansatz aus. Durch die geeignete Kombination von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsanforderungen wird ein Sicherheitsniveau erreicht, das für den jeweiligen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen. Darüber hinaus bilden die Anforderungen des IT-Grundschutz-Kompendiums nicht nur eine Basis für hochschutzbedürftige IT-Systeme und Anwendungen, sondern erläutern an vielen Stellen, wie ein höheres Sicherheitslevel erreichbar ist.

Die IT-Grundschutz-Methodik nutzt das Baukastenprinzip, um den heterogenen Bereich der Informationstechnik einschließlich der Einsatzumgebung besser strukturieren und planen zu können. Die einzelnen Bausteine thematisieren typische Abläufe von Geschäftsprozessen und Bereiche des IT-Einsatzes, wie beispielsweise Notfall-Management, Client-Server-Netze, bauliche Einrichtungen sowie Kommunikations- und Applikationskomponenten.

Die Bausteine des IT-Grundschutz-Kompendiums bilden den Stand der Technik ab, basierend auf den Erkenntnissen zum Zeitpunkt der Veröffentlichung. Die dort formulierten Anforderungen beschreiben, was generell umzusetzen ist, um mit geeigneten Sicherheitsmaßnahmen den Stand der Technik zu erreichen. Anforderungen bzw. Maßnahmen, die den Stand der Technik abbilden, entsprechen dem, was zum jeweiligen Zeitpunkt einerseits technisch fortschrittlich und andererseits in der Praxis bewährt ist.

Analyseaufwand reduzieren

Die Methodik nach IT-Grundschutz ermöglicht es, Sicherheitskonzepte einfach und arbeitsökonomisch zu erstellen. Bei der traditionellen Risikoanalyse werden zunächst die Bedrohungen ermittelt und mit Eintrittswahrscheinlichkeiten bewertet, um dann die geeigneten Sicherheitsmaßnahmen auszuwählen und anschließend das noch verbleibende Restrisiko bewerten zu können. Diese Schritte sind beim IT-Grundschutz bereits für jeden Baustein durchgeführt worden. Es wurden die für typische Einsatzszenarien passenden standardisierten Sicherheitsanforderungen ausgewählt, die dann von den Anwendern in Sicherheitsmaßnahmen überführt werden können, die zu den individuellen Rahmenbedingungen passen. Bei der IT-Grundschutz-Methodik reduziert sich die Analyse auf einen Soll-Ist-Vergleich zwischen den im IT-Grundschutz-Kompendium empfohlenen und den bereits umgesetzten Sicherheitsanforderungen. Die noch offenen Anforderungen zeigen die Sicherheitsdefizite auf, die es zu beheben gilt. Erst bei einem signifikant höheren Schutzbedarf muss zusätzlich zu den Anforderungen aus den IT-Grundschutz-Bausteinen eine indiviuelle Risikoanalyse unter Beachtung von Kosten- und Wirksamkeitsaspekten durchgeführt werden. Hierbei reicht es dann aber in der Regel aus, die auf Basis des IT-Grundschutz-Kompendiums ausgewählten Maßnahmen durch entsprechende individuelle, qualitativ höherwertige Maßnahmen zu ergänzen. Eine einfache Vorgehensweise hierzu ist im BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* beschrieben.

Auch wenn besondere Komponenten oder Einsatzumgebungen vorliegen, die im IT-Grundschutz-Kompendium nicht hinreichend behandelt werden, bietet das IT-Grundschutz-Kompendium dennoch eine wertvolle Arbeitshilfe. Bei der erforderlichen individuellen Risikoanalyse kann der Fokus auf die spezifischen Gefährdungen und Sicherheitsmaßnahmen gelegt werden.

Anforderungen für jedes Sicherheitsbedürfnis

Die im IT-Grundschutz-Kompendium aufgeführten Anforderungen sollten erfüllt werden, um ein angemessenes Sicherheitsniveau zu erreichen. Die Anforderungen sind in Basis- und Standard-Anforderungen sowie Anforderungen für erhöhten Schutzbedarf unterteilt. Die Basis-Anforderungen stellen das Minimum dessen dar, was vernünftigerweise an Sicherheitsvorkehrungen umzusetzen ist. Als Einstieg können sich die Anwender auf die Basis-Anforderungen beschränken, um so zeitnah die wirkungsvollsten Anforderungen zu erfüllen. Eine angemessene Sicherheit wird allerdings erst mit der Umsetzung der Standard-Anforderungen erreicht. Die exemplarischen Anforderungen für einen erhöhten Schutzbedarf haben sich ebenfalls in der Praxis bewährt und zeigen auf, wie eine Institution sich bei erhöhten Sicherheitsanforderungen zusätzlich absichern kann. Zudem enthalten die Umsetzungshinweise, die ergänzend zu den meisten Bausteinen veröffentlicht werden, Best Practices sowie ergänzende Hinweise, wie die Anforderungen erfüllt werden können. Für eine Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz müssen für den ausgewählten Geltungsbereich die Basis- und Standard-Anforderungen erfüllt werden.

Die IT-Grundschutz-Bausteine und die zugehörigen Umsetzungshinweise werden ebenso wie die meisten Informationen rund um IT-Grundschutz auch in elektronischer Form zur Verfügung gestellt. Die IT-Grundschutz-Texte können daher auch als Grundlage benutzt werden, um Sicherheitskonzepte zu erstellen. Den Anwendern stehen zudem Hilfsmittel und Musterlösungen zur Verfügung, die dabei unterstützen können, die Anforderungen geeignet umzusetzen.

Da der IT-Grundschutz auch international großen Anklang findet, werden das IT-Grundschutz-Kompendium und weitere Veröffentlichungen auch in englischer Sprache online zur Verfügung gestellt.

Weiterentwicklung des IT-Grundschutz-Kompendiums

Die Inhalte des IT-Grundschutz-Kompendiums sind aufgrund der rasanten Entwicklungen in der Informationstechnik sowie immer kürzer werdender Produktzyklen ständigen Veränderungen ausgesetzt. Struktur und Inhalt des BSI-Standardwerks zur Informationssicherheit sind daher danach angelegt, dass einzelne Veröffentlichungen wie Bausteine zügig aktualisiert und neue Themen aufgenommen werden können. Neben dem BSI können auch IT-Grundschutz-Anwender ihren Beitrag leisten, indem sie Texte bis hin zu ganzen Bausteinen für den IT-Grundschutz erstellen, Bausteine kommentieren oder neue Themen anregen. Ziel ist es, das IT-Grundschutz-Kompendium auf einem aktuellen Stand zu halten.

Aktuelle Informationen zum IT-Grundschutz liefert der IT-Grundschutz-Newsletter, für den Interessierte sich auf der BSI-Webseite kostenfrei anmelden können. Über den Newsletter werden Anwender auch immer wieder auf Mitwirkungsmöglichkeiten hingewiesen, wie beispielsweise auf Anwenderbefragungen zu einzelnen aktuellen Themen. Die Rückmeldungen der Anwender liefern wertvolle Anregungen und Hinweise für die Weiterentwicklung des IT-Grundschutzes. Die Erfahrungen der Anwender aus der Alltagspraxis sind sehr wichtig, damit Anforderungen und Maßnahmenempfehlungen stets auf den Prüfstand gestellt und an den aktuellen Bedarf angepasst werden.

1.3 Aufbau des IT-Grundschutz-Kompendiums

Das IT-Grundschutz-Kompendium lässt sich in unterschiedliche Bereiche untergliedern, die zum besseren Verständnis hier kurz erläutert werden sollen:

Einstieg und Methodik

In diesem einleitenden Teil wird die Konzeption und die Vorgehensweise zur Erstellung eines Sicherheitskonzepts nach IT-Grundschutz vorgestellt. Zudem wird die Struktur des IT-Grundschutz-Kompendiums erläutert und beschrieben, wie es anzuwenden ist. Eine ausführliche Beschreibung der IT-Grundschutz-Methodik ist im BSI-Standard 200-1 nachzulesen.

Hinweise zum Schichtenmodell und zur Modellierung

Um einen komplexen Informationsverbund nach IT-Grundschutz zu modellieren, müssen die passenden Bausteine des IT-Grundschutz-Kompendiums ausgewählt und umgesetzt werden. Um die Auswahl zu erleichtern, sind die Bausteine im IT-Grundschutz-Kompendium zunächst in prozess- und systemorientierte Bausteine aufgeteilt. Prozess-Bausteine gelten in der Regel für sämtliche oder große Teile des Informationsverbunds gleichermaßen, System-Bausteine lassen sich in der Regel auf einzelne Objekte oder Gruppen von Objekten anwenden. Die Prozess- und System-Bausteine bestehen wiederum aus weiteren Teilschichten.

In den Hinweisen zum Schichtenmodell und zur Modellierung wird beschrieben, wann ein einzelner Baustein sinnvollerweise eingesetzt werden soll und auf welche Zielobjekte er anzuwenden ist. Außerdem sind die Bausteine danach gekennzeichnet, ob sie vor- oder nachrangig umgesetzt werden sollten.

Beschreibung der Rollen

In den Anforderungen der Bausteine werden die Rollen genannt, die für die jeweilige Umsetzung zuständig sind. Hieraus können die geeigneten Ansprechpartner für die jeweilige Thematik in der Institution identifiziert werden. Da die Bezeichnungen der im IT-Grundschutz-Kompendium als Verantwortliche genannten Personen oder Rollen nicht in allen Institutionen einheitlich sind, wird für eine leichtere Zuordnung eine kurze Beschreibung der wesentlichen Rollen dargestellt.

Glossar und Begriffsdefinitionen

Im Glossar zum IT-Grundschutz-Kompendium werden die wichtigsten Begriffe rund um Informationssicherheit und IT-Grundschutz erläutert. Ein hierzu ergänzendes Glossar zur Cyber-Sicherheit ist auf den Webseiten des BSI zu finden.

Elementare Gefährdungen

Das BSI hat aus den vielen spezifischen Einzelgefährdungen der Bausteine der früheren IT-Grundschutz-Kataloge die generellen Aspekte herausgearbeitet und in 47 elementare Gefährdungen überführt. Diese sind im IT-Grundschutz-Kompendium aufgeführt. Bei der Erstellung der Übersicht der elementaren Gefährdungen wurden die im Folgenden beschriebenen Ziele verfolgt. Elementare Gefährdungen sind

- für die Verwendung bei der Risikoanalyse optimiert,
- produktneutral (immer), technikneutral (möglichst, bestimmte Techniken prägen so stark den Markt, dass sie auch die abstrahierten Gefährdungen beeinflussen),
- kompatibel mit vergleichbaren internationalen Katalogen und Standards und
- nahtlos in den IT-Grundschutz integriert.

Bausteine

Die Bausteine des IT-Grundschutz-Kompendiums enthalten jeweils eine Beschreibung der betrachteten Komponente, Vorgehensweisen und IT-Systeme, gefolgt von einem kurzen Überblick über spezifische Gefährdungen sowie konkreter Anforderungen, um die Komponente abzusichern. Die Bausteine sind in die folgenden Schichten gruppiert:

- Prozess-Bausteine
  - ISMS (implementierte Anforderungen)
  - ORP (Organisation und Personal)
  - CON (Konzepte und Vorgehensweisen)
  - OPS (Betrieb)
  - DER (Detektion & Reaktion)
- System-Bausteine
  - APP (Anwendungen)
  - SYS (IT-Systeme)
  - IND (Industrielle IT)
  - NET (Netze und Kommunikation)
  - INF (Infrastruktur)

1.4 Aufbau der Bausteine

Die zentrale Rolle des IT-Grundschutz-Kompendiums spielen die Bausteine, deren Aufbau jeweils gleich ist. Zunächst ist jeweils das betrachtete Zielobjekt beschrieben. Die folgende Zielsetzung formuliert, welcher Sicherheitsgewinn mit der Umsetzung des IT-Grundschutz-Bausteins erreicht werden soll. Danach folgt eine Abgrenzung der Aspekte, die nicht in diesem Baustein behandelt werden, sowie Verweise auf andere Bausteine, die diese aufgreifen.

Im Anschluss werden spezifische Gefährdungen aufgeführt. Sie erheben keinen Anspruch auf Vollständigkeit, liefern aber ein Bild über die Sicherheitsprobleme, die ohne Gegenmaßnahmen beim Einsatz der betrachteten Komponente, Vorgehensweise oder des IT-Systems entstehen können. Die Erläuterung der möglichen Risiken kann den Anwender noch stärker für das Thema sensibilisieren. Bei der Risikoanalyse, die jedem Baustein zugrunde liegt, wurden diese spezifischen Gefährdungen aus den elementaren Gefährdungen abgeleitet.

Auf die spezifischen Gefährdungen folgen in der Bausteinstruktur die Anforderungen. Diese sind in drei Kategorien gegliedert: Basis- und Standard-Anforderungen sowie Anforderungen bei erhöhtem Schutzbedarf. Basis-Anforderungen müssen vorrangig umgesetzt werden, da sie mit geringem Aufwand den größtmöglichen Nutzen erzielen. Gemeinsam mit den Basis-Anforderungen erfüllen die Standard-Anforderungen dem Stand der Technik und adressieren den normalen Schutzbedarf. Ergänzend dazu bieten die Bausteine des IT-Grundschutz-Kompendiums Vorschläge für Anforderungen bei erhöhtem Schutzbedarf. Zur Referenzierung sind die Anforderungen bausteinübergreifend eindeutig nummeriert, z. B. SYS.3.4.A2. Über dieses Schema wird zunächst die Schicht (im Beispiel "SYS") benannt, dann die Nummern der jeweiligen Teilschichten und des Bausteins (im Beispiel "3.4") und schließlich die Anforderung

selbst (im Beispiel "A2"). Gibt es passende Umsetzungshinweise, trägt die dort aufgeführte Maßnahme zu einer Anforderung "A" die gleiche Nummer mit einem vorangestellten Buchstaben "M", im Beispiel also "SYS.3.4.M2".

In jedem Baustein ist beschrieben, wer für dessen Umsetzung zuständig ist. Es ist immer ein Haupt-Verantwortlicher benannt. Daneben kann es weitere Rollen geben, die für die Umsetzung von Anforderungen verantwortlich sind. Diese werden dann jeweils im Titel der Anforderung in eckigen Klammern genannt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Am Ende des Bausteins sind weiterführende Informationen und Verweise aufgeführt. Ergänzt werden die Bausteine zudem in einem Anhang um eine Tabelle, in der den Anforderungen die betreffenden elementaren Gefährdungen zugeordnet werden. Diese Zuordnung kann für eine Risikoanalyse genutzt werden.

Modalverben

In den Bausteinen des IT-Grundschutz-Kompendiums werden die Prüfaspekte in den Anforderungen mit den in Versalien geschriebenen Modalverben MUSS und SOLLTE sowie den zugehörigen Verneinungen formuliert, um die jeweiligen Anforderungen eindeutig zu kennzeichnen.

Die hier genutzte Definition basiert auf RFC 2119 (Key words for use in RFCs to Indicate Requirement Levels), Stand 1997 sowie DIN 820-2:2012, Anhang H.

MUSS/DARF NUR:

bedeutet, dass eine Anforderung unbedingt erfüllt werden muss (eine solche Anforderung kann beispielsweise nicht im Rahmen der Risikoanalyse ohne Weiteres ignoriert werden).

DARF NICHT/SOLLTE KEIN:

bedeutet, dass etwas in keinem Fall getan werden darf.

SOLLTE:

bedeutet, dass etwas normalerweise getan werden sollte, es aber Gründe geben kann, dies nicht zu tun. Dies muss aber sorgfältig abgewogen und begründet werden und die Begründung muss bei einem Audit vom Auditor auf ihre Stichhaltigkeit geprüft werden.

SOLLTE NICHT/SOLLTE KEIN:

bedeutet, dass etwas normalerweise nicht getan werden sollte, es aber Gründe gibt, dies doch zu tun. Dies muss aber sorgfältig abgewogen und begründet werden und und die Begründung muss bei einem Audit vom Auditor auf ihre Stichhaltigkeit geprüft werden.

Basis-Anforderungen sind wie folgt formuliert:

Es MUSS xyz getan werden. Es DARF NICHT xyz gemacht werden.

Standard-Anforderungen sowie Anforderungen bei erhöhtem Schutzbedarf haben die folgende Form:

Es SOLLTE xyz getan werden. Es SOLLTE NICHT xyz gemacht werden.

Einzelne Aussagen in den Basis-Anforderungen können mit "SOLLTE" gekennzeichnet sein. Diese Teilanforderungen in den Basis-Anforderungen müssen nicht zwingend erfüllt werden, sie treten aber in Verbindung mit verbindlichen MUSS-Anforderungen auf und ergänzen diese um zusätzliche Aspekte. Bei den Anforderungen für erhöhten Schutzbedarf wird hauptsächlich das Modalverb SOLLTE verwendet. Diese Anforderungen resultieren aus Best Practices und müssen bei erhöhtem Schutzbedarf im Rahmen einer Risikoanalyse bewertet werden.

Kreuzreferenztabellen

Jeder Baustein enthält einen Anhang mit einer Übersicht zu den relevanten elementaren Gefährdungen. Wie die elementaren Gefährdungen des IT-Grundschutzes und die Anforderungen des Bausteins zueinander stehen, kann den Kreuzreferenztabellen entnommen werden. Diese finden sich ebenfalls im Anhang des Bausteins.

Alle Kreuzreferenztabellen haben einen einheitlichen Aufbau. In der Kopfzeile sind die im dazugehörigen Baustein aufgelisteten elementaren Gefährdungen mit ihren Nummern eingetragen. In der ersten Spalte finden sich entsprechend die Nummern der Anforderungen wieder.

Die übrigen Spalten beschreiben, wie die Anforderung des Bausteins und die elementaren Gefährdungen konkret zueinander stehen. Ist in einem Feld ein "X" eingetragen, so bedeutet dies, dass die korrespondierende Anforderung gegen die entsprechende Gefährdung wirksam ist. Diese Wirkung kann schadensvorbeugender oder schadensmindernder Natur sein.

Zu beachten ist, dass eine Anforderung nicht automatisch hinfällig wird, wenn alle in der Tabelle zugeordneten Gefährdungen in einem bestimmten Anwendungsfall nicht relevant sind. Ob auf eine Anforderung verzichtet werden kann, muss immer im Einzelfall anhand der vollständigen Sicherheitskonzeption und nicht nur anhand der Kreuzreferenztabelle geprüft und dokumentiert werden.

1.5 Umsetzungshinweise

Zu vielen Bausteinen des IT-Grundschutz-Kompendiums gibt es detaillierte Umsetzungshinweise. Diese beschreiben, wie die Anforderungen der Bausteine umgesetzt werden können und erläutern im Detail geeignete Sicherheitsmaßnahmen. Die Sicherheitsmaßnahmen können als Grundlage für Sicherheitskonzeptionen verwendet werden, sie sollten aber an die Rahmenbedingungen der jeweiligen Institution angepasst werden. Daneben enthalten die Umsetzungshinweise eine exemplarische Abbildung der Maßnahmen auf einen Lebenszyklus, der aus den Schritten "Planung und Konzeption", "Beschaffung", "Umsetzung", "Betrieb" und "Aussonderung" und "Notfallvorsorge" besteht.

Für die Phasen des Lebenszyklus sind folgende typische Arbeiten angegeben, die im Rahmen einzelner Maßnahmen durchgeführt werden sollten. Phasenübergreifend wirken dabei das Sicherheitsmanagement und die Revision, die den gesamten Lebenszyklus begleiten und kontrollieren.

- Planung und Konzeption
  - Definition des Einsatzzwecks
  - Festlegung von Einsatzszenarien
  - Abwägung des Risikopotentials
  - Dokumentation der Einsatzentscheidung
  - Erstellung des Sicherheitskonzepts
  - Festlegung von Richtlinien für den Einsatz
- Beschaffung (sofern erforderlich)
  - Festlegung der Anforderungen an zu beschaffende Produkte (nach Möglichkeit auf Basis der Einsatzszenarien der Planungsphase)
  - Auswahl der geeigneten Produkte
- Umsetzung
  - Konzeption und Durchführung des Testbetriebs
  - Installation und Konfiguration entsprechend Sicherheitsrichtlinie
  - Schulung und Sensibilisierung aller Betroffenen
- Betrieb
  - Sicherheitsmaßnahmen für den laufenden Betrieb (z. B. Protokollierung)
  - Kontinuierliche Pflege und Weiterentwicklung
  - Änderungsmanagement
  - Organisation und Durchführung von Wartungsarbeiten
  - Audit
- Aussonderung (sofern erforderlich)
  - Entzug von Berechtigungen
  - Entfernen von Datenbeständen und Referenzen auf diese Daten
  - Sichere Entsorgung von Datenträgern

- Notfallvorsorge
  - Konzeption und Organisation der Datensicherung
  - Nutzung von Redundanz zur Erhöhung der Verfügbarkeit
  - Umgang mit Sicherheitsvorfällen
  - Erstellen eines Notfallplans

Es finden sich in den Umsetzungshinweisen nicht für jede Phase entsprechende Maßnahmen. Da sich alle Geschäftsprozesse, IT-Systeme und Einsatzbedingungen ständig ändern und weiterentwickelt werden, müssen die Phasen erfahrungsgemäß immer wieder durchlaufen werden. Dies sicherzustellen ist Aufgabe des Informationssicherheitsmanagements.

Die Umsetzungshinweise adressieren jeweils die Personengruppen, die für die Umsetzung der Baustein-Anforderungen zuständig sind, beispielsweise den IT-Betrieb oder die Haustechnik. Die Umsetzungshinweise sind nicht Bestandteil des IT-Grundschutz-Kompendiums, sondern werden als Hilfsmittel zu den Bausteinen veröffentlicht.

1.6 Mitwirkung der Anwender und Versionierung

Die Anwender des IT-Grundschutzes werden bei der Erstellung und Überarbeitung von Bausteinen sowie weiterer Veröffentlichungen wie den BSI-Standards beteiligt. Alle Anwender sind aufgerufen, ihre Wünsche für neue Themenbereiche im IT-Grundschutz sowie für Änderungen an bestehenden Texten dem IT-Grundschutz-Team des BSI mitzuteilen. Das BSI sichtet die Anregungen und stößt, abhängig von der Nachfrage und den Ressourcen, die entsprechenden Aktualisierungen an. Anwender können aber Bausteine, Umsetzungshinweise oder einzelne Ergänzungen der IT-Grundschutz-Texte selber erstellen und auch dem BSI zur Veröffentlichung zur Verfügung stellen.

Neue IT-Grundschutz-Dokumente werden auf der IT-Grundschutz-Webseite zunächst zur Kommentierung veröffentlicht. Die Rückmeldungen aus der Praxis tragen dazu bei, dass die Inhalte einzelner Bausteine noch aktueller und praxisnäher werden, bis sie finalisiert und als jährliche Edition publiziert werden. Der Veröffentlichtungsprozess sieht unterschiedliche Bearbeitungsstufen vor, die wie folgt gekennzeichnet sind:

- Working Draft (WD): interne Arbeitspapiere
- Community Draft (CD): Entwurfsfassung zur Diskussion mit der IT-Grundschutz-Community (Anwender)
- Final Draft (FD): finale Entwürfe, in die alle relevanten Kommentare der Community eingeflossen sind und die eine hohe Stabilität erreicht haben, so dass keine inhaltlichen Änderungen mehr zu erwarten sind
- Edition (E): Dies bezeichnet den Stand eines IT-Grundschutz-Dokuments, das als die offizielle Fassung veröffentlicht wurde und auch als Basis für die Zertifizierung genutzt wird.

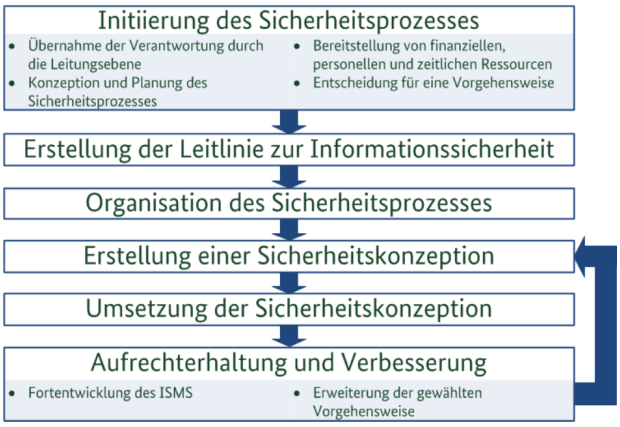
Von jedem dieser Redaktionsprozessstände kann es unterschiedliche Versionsstände x und Unterversionsstände y geben. So kann aus einem CD 1.0 nach der schnellen Einarbeitung erster Anwenderkommentare ein CD 1.1 (kleinere Änderungen) oder ein CD 2.0 (größere Änderungen) werden.

1.7 Anwendungsweisen des IT-Grundschutz-Kompendiums

Für den erfolgreichen Aufbau eines kontinuierlichen und effektiven Sicherheitsprozesses müssen zahlreiche Aufgaben durchgeführt werden. Hierfür bietet die IT-Grundschutz-Methodik (siehe BSI-Standard 200-2) mit dem IT-Grundschutz-Kompendium viele Hinweise zu den Vorgehensweisen Basis-, Kern- und Standard-Absicherung sowie praktische Umsetzungshilfen. Hinzu kommen Lösungsansätze für verschiedene, die Informationssicherheit betreffende Aufgabenstellungen, beispielsweise Sicherheitskonzeption, Revision und Zertifizierung. Je nach vorliegender Aufgabenstellung sind dabei unterschiedliche Anwendungsweisen des IT-Grundschutzes zweckmäßig. Die folgenden Anwendungshinweise dienen dazu, durch Querverweise auf die entsprechenden Kapitel der IT-Grundschutz-Methodik im BSI-Standard 200-2 den direkten Einstieg in die einzelnen Anwendungsweisen zu erleichtern.

Sicherheitsprozess und Management der Informationssicherheit

Informationssicherheit ist für alle Geschäftsprozesse und Fachaufgabe relevant und daher als originäre Aufgabe anzusehen. Die folgende Abbildung beinhaltet alle wesentlichen Schritte, die für einen kontinuierlichen Sicherheitsprozess notwendig sind:



Phasen des Sicherheitsprozesses

Im BSI-Standard 200-2 wird der Ablauf für die Vorgehensweisen zur Basis-, Kern- und Standard-Absicherung ausführlich beschrieben. Außerdem wird im Baustein ISMS.1 *Sicherheitsmanagement* der Sicherheitsprozess im Überblick dargestellt. Zusätzlich werden in diesem Baustein die einzelnen Aktionen und Schritte im Rahmen des Sicherheitsprozesses in Form von Anforderungen beschrieben.

Zur Erstellung der Sicherheitskonzeption sind nach IT-Grundschutz einige Schritte notwendig, die für die Standard-Absicherung im Folgenden kurz dargestellt werden. Die Standard-Absicherung wurde hierbei als Beispiel gewählt, da hiermit ein vollständiges Sicherheitskonzept nach IT-Grundschutz erstellt werden kann. Bei der Basis- und der Kernabsicherung handelt es sich um Vorgehensweisen zum Einstieg in den IT-Grundschutz, diese werden ebenfalls detailliert im BSI-Standard 200-2 *IT-Grundschutz-Methodik* beschrieben.

Strukturanalyse

Unter einem Informationsverbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann die gesamte Institution, aber auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungen) oder gemeinsame Geschäftsprozesse bzw. -anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.

Für die Erstellung eines Sicherheitskonzepts nach IT-Grundschutz ist es erforderlich, die Struktur des vorliegenden Informationsverbundes zu analysieren und zu dokumentieren. Bei der Strukturanalyse werden daher die Informationen, Anwendungen, IT-Systeme, Räume und Kommunikationsnetze als Zielobjekte erfasst.

Die einzelnen Schritte der Strukturanalyse für die Standard-Absicherung werden detailliert in Kapitel 8.1 der IT-Grundschutz-Methodik (BSI-Standard 200-2) beschrieben.

Schutzbedarfsfeststellung

Zweck der Schutzbedarfsfeststellung ist es zu ermitteln, welcher Schutz für die Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die erwartbaren Schäden betrachtet, die bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Eine Einteilung in die drei Schutzbedarfskategorien "normal", "hoch" und "sehr hoch" hat sich bislang bewährt. Im Kapitel 8.2 der IT-Grundschutz-Methodik (BSI-Standard 200-2) sind Erläuterungen und praktische Hinweise zum Thema zu finden.

Modellierung

Als nächstes müssen die Bausteine des IT-Grundschutz-Kompendiums in einem Modellierungsschritt auf die Zielobjekte des vorliegenden Informationsverbunds abgebildet werden.

In Kapitel 8.3 der IT-Grundschutz-Methodik im BSI-Standard 200-2 wird beschrieben, wie die Modellierung eines Informationsverbunds durch Bausteine aus dem IT-Grundschutz-Kompendium für die Standard-Absicherung vorgenommen werden sollte. Detaillierte Hinweise für die Verwendung der Prozess- und System-Bausteine bei der Modellierung sind im Kapitel 2 des IT-Grundschutz-Kompendiums enthalten. Außerdem sind an dieser Stelle die Bausteine danach gekennzeichnet, in welcher Reihenfolge sie für die Basis-Absicherung sinnvollerweise umgesetzt werden sollten. Das Ergebnis der Modellierung ist ein erster grober Entwurf des Sicherheitskonzepts.

IT-Grundschutz-Check

Der IT-Grundschutz-Check ist ein Organisationsinstrument, mit dem sich ein Überblick über das vorhandene Sicherheitsniveau erstellen lässt. Mit Hilfe von Interviews wird der Status Quo eines bestehenden (nach IT-Grundschutz modellierten) Informationsverbunds ermittelt. Als Ergebnis liegt eine Übersicht vor, in der für jede relevante Anforderung der Erfüllungsstatus "entbehrlich", "ja", "teilweise" oder "nein" erfasst ist. Durch die Identifizierung von noch nicht oder nur teilweise erfüllten Anforderungen werden Verbesserungsmöglichkeiten für die Sicherheit der betrachteten Zielobjekte aufgezeigt. Kapitel 8.5 des BSI-Standards 200-2 beschreibt einen Aktionsplan für die Durchführung eines IT-Grundschutz-Sicherheitschecks. Dabei wird sowohl den organisatorischen Aspekten als auch den fachlichen Anforderungen Rechnung getragen.

Weiterführende Sicherheitsmaßnahmen

Die Anforderungen und Sicherheitsmaßnahmen nach IT-Grundschutz bieten im Normalfall einen angemessenen und ausreichenden Schutz. Insbesondere bei hohem oder sehr hohem Schutzbedarf ist jedoch zu prüfen, ob weitere Sicherheitsmaßnahmen erforderlich sind. Hierfür sollte eine Risikoanalyse durchgeführt werden, ein mögliches Vorgehen hierfür ist im BSI-Standard 200-3 beschrieben. Eine Risikoanalyse ist auch dann erforderlich, wenn Teile des Informationsverbunds nicht hinreichend mit den existierenden Bausteinen des IT-Grundschutz-Kompendiums abgebildet werden können oder wenn besondere Einsatzszenarien vorliegen, die im IT-Grundschutz nicht vorgesehen sind.

Umsetzung von Sicherheitskonzepten

Damit das angestrebte Informationssicherheitsniveau erreicht wird, müssen bestehende Schwachstellen ermittelt und alle erforderlichen Maßnahmen identifiziert werden. Vor allem müssen alle Maßnahmen, die im Sicherheitskonzept vorgesehen sind, auch konsequent anhand eines Realisierungsplans umgesetzt werden. In Kapitel 9 des BSI-Standards 200-2 zur IT-Grundschutz-Methodik wird beschrieben, was bei der Umsetzungsplanung von Sicherheitsmaßnahmen zu beachten ist.

Sicherheitsrevision

Die im IT-Grundschutz-Kompendium enthaltenen Anforderungen können auch für die Sicherheitsrevision genutzt werden. Hierzu wird die gleiche Vorgehensweise wie beim IT-Grundschutz-Check empfohlen. Hilfreich und arbeitsökonomisch ist es, für jeden Baustein anhand der Anforderungen eine speziell auf die eigene Institution angepasste Checkliste zu erstellen. Dies erleichtert die Revision und die Ergebnisse können besser reproduziert werden.

Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz

Die Vorgehensweisen nach IT-Grundschutz und das IT-Grundschutz-Kompendium werden nicht nur für die Erstellung von Sicherheitskonzeptionen, sondern auch als Referenz im Sinne eines Sicherheitsstandards verwendet. Durch eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz kann eine Institution dokumentieren, dass sie sowohl ISO 27001 als auch IT-Grundschutz erfolgreich umgesetzt hat.

Dokumentation des Sicherheitsprozesses

Bei den vielfältigen Aufgaben des Informationssicherheitsmanagements entstehen Konzepte, Richtlinien, Berichte und weitere Dokumente. Nur durch eine ausreichende Dokumentation werden getroffene Entscheidungen nachvollziehbar, Handlungen wiederholbar und Schwächen erkannt, so dass sie in Zukunft vermieden werden können.

Hinweis zur Dokumentation im IT-Grundschutz: Es muss nicht jedes Mal ein neues Dokument erstellt werden, wenn laut der IT-Grundschutz-Methodik etwas dokumentiert werden muss. Häufig reichen Notizen oder informelle Informationssammlungen, solange diese auffindbar und nachvollziehbar sind. Einige Dokumentationen sind für das Sicherheitsmanagement erforderlich, vor allem, wenn eine Zertifizierung angestrebt wird.

2 Schichtenmodell und Modellierung

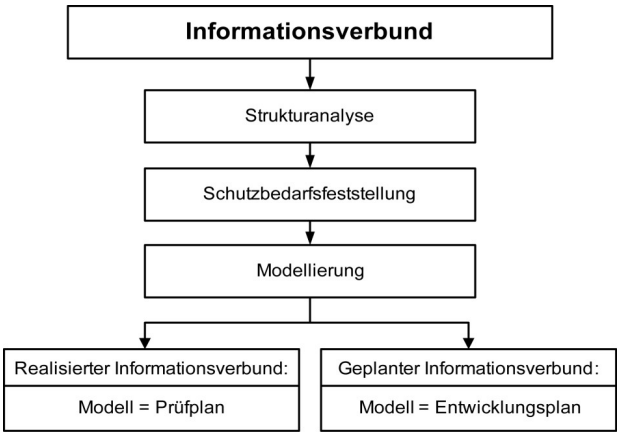
2.1 Modellierung nach IT-Grundschutz

Bei der Umsetzung von IT-Grundschutz muss der betrachtete Informationsverbund mit Hilfe der vorhandenen Bausteine nachgebildet werden, es müssen also die relevanten Sicherheitsanforderungen aus dem IT-Grundschutz-Kompendium zusammengetragen werden. Dafür müssen alle relevanten Prozesse, Anwendungen und IT-Systeme erfasst sein beziehungsweise es müssen die Strukturanalyse und in der Regel eine Schutzbedarfsfeststellung vorliegen. Darauf aufbauend wird ein IT-Grundschutz-Modell des Informationsverbunds erstellt, das aus verschiedenen, gegebenenfalls auch mehrfach verwendeten IT-Grundschutz-Bausteinen besteht und eine Abbildung zwischen den Bausteinen und den sicherheitsrelevanten Aspekten des Informationsverbunds beinhaltet.

Das erstellte IT-Grundschutz-Modell ist unabhängig davon, ob der Informationsverbund aus bereits im Einsatz befindlichen IT-Systemen besteht oder ob es sich um einen Informationsverbund handelt, der sich erst im Planungsstadium befindet. Das Modell kann daher unterschiedlich verwendet werden:

- Das IT-Grundschutz-Modell eines bereits realisierten Informationsverbunds identifiziert über die verwendeten Bausteine die relevanten Sicherheitsanforderungen. Es kann in Form eines Prüfplans benutzt werden, um einen Soll-Ist-Vergleich durchzuführen.
- Das IT-Grundschutz-Modell eines geplanten Informationsverbunds stellt hingegen ein Entwicklungskonzept dar. Es beschreibt über die ausgewählten Bausteine, welche Sicherheitsanforderungen bei der Realisierung des Informationsverbunds erfüllt werden müssen.

Die Einordnung der Modellierung und die möglichen Ergebnisse verdeutlicht das folgende Bild:

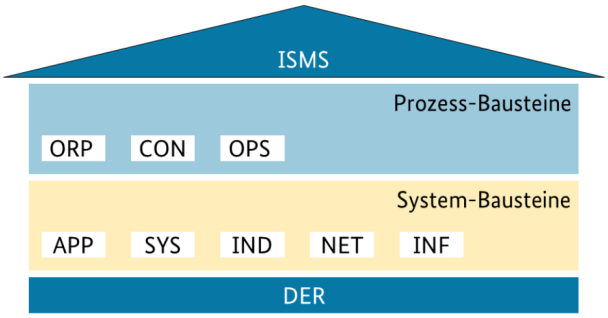


Ergebnis der Modellierung nach IT-Grundschutz

Typischerweise wird ein im Einsatz befindlicher Informationsverbund sowohl realisierte als auch in Planung befindliche Anteile umfassen. Das resultierende IT-Grundschutz-Modell beinhaltet dann sowohl einen Prüfplan wie auch Anteile eines Entwicklungskonzepts. Alle im Prüfplan bzw. im Entwicklungskonzept vorgesehenen Sicherheitsanforderungen bilden dann gemeinsam die Basis für die Erstellung des Sicherheitskonzepts.

Um einen im Allgemeinen komplexen Informationsverbund nach IT-Grundschutz zu modellieren, müssen die passenden Bausteine des IT-Grundschutz-Kompendiums ausgewählt und umgesetzt werden. Um die Auswahl zu erleichtern, sind die Bausteine im IT-Grundschutz-Kompendium zunächst in prozess- und systemorientierte Bausteine aufgeteilt und diese jeweils in einzelne Schichten untergliedert.

Die Sicherheitsaspekte eines Informationsverbunds werden wie folgt den einzelnen Schichten zugeordnet:



Das Schichtenmodell des IT-Grundschutzes

Prozessorientierte Bausteine:

Die Prozess-Bausteine, die in der Regel für sämtliche oder große Teile des Informationsverbunds gleichermaßen gelten, unterteilen sich in die folgenden Schichten, die wiederum aus weiteren Teilschichten bestehen können.

- Die Schicht ISMS enthält als Grundlage für alle weiteren Aktivitäten im Sicherheitsprozess den Baustein *Sicherheitsmanagement.*
- Die Schicht ORP befasst sich mit organisatorischen und personellen Sicherheitsaspekten. In diese Schicht fallen beispielsweise die Bausteine *Organisation* und *Personal.*
- Die Schicht CON enthält Bausteine, die sich mit Konzepten und Vorgehensweisen befassen. Typische Bausteine der Schicht CON sind unter anderem *Kryptokonzept* und *Datenschutz.*
- Die Schicht OPS umfasst alle Sicherheitsaspekte betrieblicher Art. Insbesondere sind dies die Sicherheitsaspekte des operativen IT-Betriebs, sowohl bei einem Betrieb im Haus, als auch bei einem IT-Betrieb, der in Teilen oder komplett durch Dritte betrieben wird. Ebenso enthält er die Sicherheitsaspekte, die bei einem IT-Betrieb für Dritte zu beachten sind. Beispiele für die Schicht OPS sind die Bausteine *Schutz vor Schadprogrammen* und *Outsourcing für Kunden.*
- In der Schicht DER finden sich alle Bausteine, die für die Überprüfung der umgesetzten Sicherheitsmaßnahmen, die Detektion von Sicherheitsvorfällen sowie die geeigneten Reaktionen darauf relevant sind. Typische Bausteine der Schicht DER sind *Behandlung von Sicherheitsvorfällen* und *Vorsorge für IT-Forensik*.

Neben den Prozess-Bausteinen beinhaltet das IT-Grundschutz-Kompendium auch System-Bausteine. Diese werden in der Regel auf einzelne Zielobjekte oder Gruppen von Zielobjekten angewendet. Die System-Bausteine unterteilen sich in die folgenden Schichten. Ähnlich wie bei prozessorientierten Bausteinen können systemorientierte Bausteine auch aus weiteren Teilschichten bestehen.

System-Bausteine:

- Die Schicht APP beschäftigt sich mit der Absicherung von Anwendungen und Diensten, unter anderem in den Bereichen Kommunikation, Verzeichnisdienste, netzbasierte Dienste sowie Business- und Client-Anwendungen. Typische Bausteine der Schicht APP sind *Allgemeine Groupware*, *Office-Produkte*, *Webserver* und *Relationale Datenbanksysteme*.

- Die Schicht SYS betrifft die einzelnen IT-Systeme des Informationsverbunds, die ggf. in Gruppen zusammengefasst wurden. Hier werden die Sicherheitsaspekte von Servern, Desktop-Systemen, Mobile Devices und sonstigen IT-Systemen wie Druckern und TK-Anlagen behandelt. Zur Schicht SYS gehören beispielsweise Bausteine zu konkreten Betriebssystemen, *Allgemeine Smartphones und Tablets* sowie *Drucker, Kopierer und Multifunktionsgeräte*.
- Die Schicht IND befasst sich mit Sicherheitsaspekten industrieller IT. In diese Schicht fallen beispielsweise die Bausteine *Betriebs- und Steuerungstechnik*, *Allgemeine ICS-Komponente* und *Speicherprogrammierbare Steuerung (SPS)*.
- Die Schicht NET betrachtet die Vernetzungsaspekte, die sich nicht primär auf bestimmte IT-Systeme, sondern auf die Netzverbindungen und die Kommunikation beziehen. Dazu gehören zum Beispiel die Bausteine *Netz-Management*, *Firewall* und *WLAN-Betrieb*.
- Die Schicht INF befasst sich mit den baulich-technischen Gegebenheiten, hier werden Aspekte der infrastrukturellen Sicherheit zusammengeführt. Dies betrifft unter anderem die Bausteine *Allgemeines Gebäude* und *Rechenzentrum*.

Die Einteilung in diese Schichten hat folgende Vorteile:

- Die Komplexität der Informationssicherheit wird reduziert, indem eine sinnvolle Aufteilung der Einzelaspekte vorgenommen wird.
- Da übergeordnete Aspekte und gemeinsame infrastrukturelle Fragestellungen getrennt von den IT-Systemen betrachtet werden, werden Redundanzen vermieden, weil diese Aspekte nur einmal bearbeitet werden müssen und nicht wiederholt für jedes IT-System.
- Die einzelnen Schichten sind so gewählt, dass auch die Zuständigkeiten für die betrachteten Aspekte gebündelt sind. So betreffen beispielsweise die Schichten ISMS und ORP Grundsatzfragen des sicheren Umgangs mit Informationen, Schicht INF den Bereich Haustechnik, Schicht SYS die Zuständigen für die IT-Systeme, Schicht NET die Ebene der Netzadministratoren und Schicht APP schließlich die Anwendungsverantwortlichen und -betreiber.
- Aufgrund der Aufteilung der Sicherheitsaspekte in Schichten können Einzelaspekte in resultierenden Sicherheitskonzepten leichter aktualisiert und erweitert werden, ohne dass andere Schichten umfangreich tangiert werden.

Die Modellierung nach IT-Grundschutz besteht nun darin, für die Bausteine einer jeden Schicht zu entscheiden, ob und wie sie zur Abbildung des Informationsverbunds herangezogen werden können. Je nach betrachtetem Baustein können die Zielobjekte dieser Abbildung von unterschiedlicher Art sein: einzelne Geschäftsprozesse oder Komponenten, Gruppen von Komponenten, Gebäude, Liegenschaften, Organisationseinheiten usw.

Nachfolgend wird die Vorgehensweise der Modellierung für einen Informationsverbund detailliert beschrieben. Dabei wird besonderer Wert auf die Randbedingungen gelegt, wann ein einzelner Baustein sinnvollerweise eingesetzt werden soll und auf welche Zielobjekte er anzuwenden ist.

Bei der Modellierung eines Informationsverbunds nach IT-Grundschutz kann das Problem auftreten, dass es Zielobjekte gibt, die mit den existierenden Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet werden können. In diesem Fall sollte eine Risikoanalyse durchgeführt werden, wie in der IT-Grundschutz-Methodik beschrieben.

Hinweis:

Mit der Veröffentlichung der ersten Edition des IT-Grundschutz-Kompendiums wurden zunächst die wesentlichen bzw. die am häufigsten genutzten Bausteine der 15. Ergänzungslieferung der IT-Grundschutz-Kataloge migriert. Mit der zweiten Edition wird das IT-Grundschutz-Kompendium mit neuen Bausteinen sowie mit weiteren migrierten Bausteinen ergänzt werden. An einigen Stellen im IT-Grundschutz-Kompendium wird bereits auf Bausteine verwiesen, die nicht Bestandteil der ersten Edition sind, aber spätestens mit der zweiten Edition nachgeliefert werden. Für Zielobjekte, für die es im IT-Grundschutz-Kompendium noch keine Bausteine gibt, sollten soweit vorhanden zwischenzeitlich die bestehenden Bausteine der IT-Grundschutz-Kataloge genutzt werden.

2.2 Zuordnung anhand Schichtenmodell

Bei der Modellierung eines Informationsverbunds ist es zweckmäßig, die Zuordnung der Bausteine anhand des Schichtenmodells vorzunehmen. Daran anschließend folgt schließlich die Vollständigkeitsprüfung.

Hinter jedem Bausteintitel der folgenden Auflistung ist mit R1, R2 und R3 die vorgeschlagene Reihenfolge für die Bearbeitung der Bausteine angegeben. Eine detaillierte Beschreibung hierzu findet sich in Kapitel 2.3 *Bearbeitungsreihenfolge der Bausteine*.

Prozessbausteine

Mit prozessorientierten Bausteinen werden alle Aspekte des Informationsverbunds modelliert, die den technischen Komponenten übergeordnet sind. Diese Aspekte sollten für den gesamten Informationsverbund einheitlich geregelt sein, so dass die entsprechenden Bausteine in den meisten Fällen nur einmal für den gesamten Informationsverbund anzuwenden sind. Dem Informationssicherheitsmanagement, der Organisation des IT-Betriebs, der Schulung und Sensibilisierung des Personals sowie der Detektion und Reaktion auf Sicherheitsvorfälle kommt dabei eine besondere Bedeutung zu. Die Umsetzung der diesbezüglichen Anforderungen ist von grundlegender Bedeutung für den sicheren Umgang mit geschäftsrelevanten Informationen und die sichere Nutzung von Informations- und Kommunikationstechnik.

ISMS (Sicherheitsmanagement)

Diese Schicht beschäftigt sich mit dem Aufbau, der Aufrechterhaltung und kontinuierlichen Verbesserung eines Managementmentsystems für Informationssicherheit und enthält den gleichnamigen Baustein ISMS.1.

- ISMS.1 Sicherheitsmanagement (R1)
  Der Baustein ISMS.1 *Sicherheitsmanagement* ist für den gesamten Informationsverbund einmal anzuwenden. Ein funktionierendes Informationssicherheitsmanagement ist die wesentliche Grundlage für die Erreichung eines angemessenen Sicherheitsniveaus.

ORP (Organisation und Personal)

In dieser Schicht befinden sich Bausteine, die Sicherheitsanforderungen für organisatorische Prozesse innerhalb einer Institution enthalten. Dies deckt insbesondere auch personalbezogene Aspekte wie Identitätsmanagement und Schulungen mit ab.

- ORP.1 Organisation (R1)
  Der Baustein ORP.1 *Organisation* muss für jeden Informationsverbund mindestens einmal herangezogen werden. Wenn Teile des vorliegenden Informationsverbunds einer anderen Organisation(-seinheit) zugeordnet sind und daher anderen Rahmenbedingungen unterliegen, sollte der Baustein auf jede Organisation(-seinheit) getrennt angewandt werden.
- ORP.2 Personal (R1)
  Der Baustein ORP.2 *Personal* muss für jeden Informationsverbund mindestens einmal herangezogen werden. Wenn Teile des vorliegenden Informationsverbunds einer anderen Organisation(-seinheit) zugeordnet sind und daher anderen Rahmenbedingungen unterliegen, sollte der Baustein auf jede Organisation(-seinheit) getrennt angewandt werden.
- ORP.3 Sensibilisierung und Schulung (R1)
  Der Baustein ORP.3 *Sensibilisierung und Schulung* ist für den gesamten Informationsverbund einmal anzuwenden.
- ORP.4 Identitäts- und Berechtigungsmanagement (R1)
  Der Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* ist für den gesamten Informationsverbund einmal anzuwenden.
- ORP.5 Compliance Management (Anforderungsmanagement) (R3)
  Der Baustein ORP.5 *Compliance Management (Anforderungsmanagement)* ist für den gesamten Informationsverbund einmal anzuwenden.

CON (Konzepte und Vorgehensweisen)

Die Schicht CON befasst sich mit grundlegenden Konzepten und Vorgehensweisen, welche die Basis für Informationssicherheit in einer Institution bilden. Die Bausteine sind daher in der Regel bereichsübergreifend für den gesamten Informationsverbund anzuwenden.

- CON.1 Kryptokonzept (R3)
  Der Baustein CON.1 *Kryptokonzept* ist für den gesamten Informationsverbund einmal anzuwenden.
- CON.2 Datenschutz (R2)
  Der Baustein CON.2 *Datenschutz* ist einmal für den gesamten Informationsverbund anzuwenden, wenn personenbezogene oder personenbeziehbare Daten im Informationsverbund verarbeitet werden.
- CON.3 Datensicherungskonzept (R1)
  Der Baustein CON.3 *Datensicherungskonzept* ist für den gesamten Informationsverbund einmal anzuwenden.
- CON.4 Auswahl und Einsatz von Standardsoftware (R2)
  Der Baustein CON.4 *Auswahl und Einsatz von Standardsoftware* ist zumindest einmal für den gesamten Informationsverbund anzuwenden. Gibt es innerhalb des Informationsverbunds Teilbereiche mit unterschiedlichen Anforderungen oder Regelungen für die Nutzung von Standardsoftware, sollte CON.4 *Auswahl und Einsatz von Standardsoftware* auf diese Teilbereiche jeweils getrennt angewandt werden.
- CON.5 Entwicklung und Einsatz von Allgemeinen Anwendungen (R3)
  Der Baustein CON.5 *Entwicklung und Einsatz von Allgemeinen Anwendungen* ist auf den Informationsverbund anzuwenden, wenn spezialisierte Anwendungssoftware eingesetzt wird. Hierzu gehört Individualsoftware und Standardsoftware mit eigenen Anpassungen.
- CON.6 Löschen und Vernichten (R1)
  Der Baustein CON.6 *Löschen und Vernichten* ist für den gesamten Informationsverbund einmal anzuwenden.
- CON.7 Informationssicherheit auf Auslandsreisen (R3)
  Der Baustein CON.7 *Informationssicherheit auf Auslandsreisen* ist einmal für den gesamten Informationsverbund anzuwenden, wenn Mitarbeiter auf Auslandsreisen gehen oder zeitweise im Ausland tätig sind und dabei besonders schutzbedürftige Informationen mitgeführt oder verarbeitet werden sollen.

OPS (Betrieb)

Sicherheitsaspekte, die sich auf den Betrieb beziehen, werden in dieser Schicht abgedeckt. Dabei werden neben dem eigenem Betrieb auch Aspekte des Outsourcings, sowohl als Dienstleister als auch Kunde betrachtet. Die Schicht OPS ist zur Übersichtlichkeit in die Teilschichten *Eigener IT-Betrieb*, *Betrieb von Dritten*, *Betrieb für Dritte* und *Betriebliche Aspekte* aufgeteilt. Im Themenbereich *Kern-IT-Betrieb* werden Anforderungen für die wesentlichen Kernbereiche eines selbst erbrachten IT-Betriebs aufgestellt. Die entsprechenden Bausteine decken die grundlegenden Aspekte ab und sind mit hoher Priorität zu betrachten.

Kern-IT-Betrieb

- OPS.1.1.2 Ordnungsgemäße IT-Administration (R1)
  Der Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* ist einmal für den gesamten Informationsverbund anzuwenden, wenn die IT von der Institution selber administriert wird. Wird die IT von externen Auftragnehmern administriert, so muss der Bautein entsprechend für die Outsourcing-Dienstleister geprüft werden.
- OPS.1.1.3 Patch- und Änderungsmanagement (R1)
  Der Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* ist einmal für den gesamten Informationsverbund anzuwenden. Das Patchmanagement stellt einen Teilbereich bzw. speziellen Prozess innerhalb des Änderungsmanagements dar, der auf die Aktualisierung von Software zielt und in jedem Fall anzuwenden ist. Aspekte des Änderungsmanagements sind den Gegebenheiten der Institution entsprechend zu betrachten.

- OPS.1.1.4 Schutz vor Schadprogrammen (R1)
  Der Baustein OPS.1.1.4 *Schutz vor Schadprogrammen* ist mindestens einmal für alle IT-Systeme im gesamten Informationsverbund anzuwenden.
- OPS.1.1.5 Protokollierung (R1)
  Der Baustein OPS.1.1.5 *Protokollierung* ist für den gesamten Informationsverbund einmal anzuwenden.
- OPS.1.1.6 Software-Tests und -Freigaben (R1)
  Der Baustein OPS.1.1.6 *Software-Tests und -Freigaben* ist einmal für den gesamten Informationsverbund anzuwenden.

Weiterführende Aufgaben

- OPS.1.2.2 Archivierung (R3)
  Der Baustein OPS.1.2.2 *Archivierung* ist auf den Informationsverbund anzuwenden, wenn aufgrund interner oder externer Vorgaben eine Langzeitarchivierung elektronischer Dokumente erforderlich ist oder bereits ein System zur Langzeitarchivierung elektronischer Dokumente betrieben wird.
- OPS.1.2.3 Informations- und Datenträgeraustausch (R3)
  Der Baustein OPS.1.2.3 *Informations- und Datenträgeraustausch* ist für jede Anwendung einmal heranzuziehen, die als Datenquelle für einen Datenträgeraustausch dient oder auf diesem Wege eingegangene Daten weiterverarbeitet.
- OPS.1.2.4 Telearbeit (R3)
  Der Baustein OPS.1.2.4 *Telearbeit* ist bei jedem Telearbeitsplatz bzw. auf jede entsprechende Gruppe anzuwenden.

Betrieb von Dritten

- OPS.2.1 Outsourcing für Kunden (R2)
  Der Baustein OPS.2.1 *Outsourcing für Kunden* ist für jede Outsourcing-Dienstleistung aus Sicht des Anwenders separat anzuwenden.
- OPS.2.4 Fernwartung (R3)
  Der Baustein OPS.2.4 *Fernwartung* ist einmal für den gesamten Informationsverbund anzuwenden.

Betrieb für Dritte

- OPS.3.1 Outsourcing für Dienstleister (R3)
  Der Baustein OPS.3.1 *Outsourcing für Dienstleister* ist einmal für den Outsourcing-Dienstleister anzuwenden.

Betriebliche Aspekte

In dieser Schicht werden betriebliche Aspekte behandelt, die über die zuvor genannten hinausgehen.

Hinweis: Die Erstellung entsprechender Bausteine ist für die zweite Edition des IT-Grundschutz-Kompendiums geplant.

DER (Detektion und Reaktion)

In dieser Schicht finden sich Bausteine, die Vorgehensweisen beschreiben, um Sicherheitsvorfälle zu erkennen und geeignet mit diesen umzugehen. Auch das Thema Sicherheitsüberprüfungen wird geeignet mit entsprechenden Bausteinen adressiert. Die Schicht DER umfasst die Teilschichten *Detektion von Sicherheitsvorfällen*, *Security Incident Management*, *Sicherheitsüberprüfungen* und *Notfallmanagement*.

Detektion von Sicherheitsvorfällen

- DER.1 Detektion von sicherheitsrelevanten Ereignissen (R2)
  Der Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen* ist für den gesamten Informationsverbund einmal anzuwenden.

Security Incident Management

- DER.2.1 Behandlung von Sicherheitsvorfällen (R2)
  Der Baustein DER.2.1 *Behandlung von Sicherheitsvorfällen* ist für den gesamten Informationsverbund einmal anzuwenden.
- DER.2.2 Vorsorge für die IT-Forensik (R3)
  Der Baustein DER.2.2 *Vorsorge für die IT-Forensik* ist für den gesamten Informationsverbund einmal anzuwenden.
- DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle (APT-Responder) (R3)
  Der Baustein DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle (APT-Responder)* ist immer dann anzuwenden, wenn der reguläre und sichere Betriebszustand eines Informationsverbunds nach einem APT-Vorfall wiederhergestellt werden soll und hierfür IT-Systeme bereinigt werden sollen.

Sicherheitsüberprüfungen

- DER 3.1 Audits und Revisionen (R3)
  Der Baustein DER.3.1 *Audits und Revisionen* ist einmal für den gesamten Informationsverbund anzuwenden.
- DER 3.4 IS-Revision für Bundesbehörden (R3)
  Der Bautein DER.3.4 *IS-Revision für Bundesbehörden* ist einmal für den gesamten Informationsverbund anzuwenden, sofern die IS-Revision erforderlich ist.

Notfallmanagement

- DER.4 Notfallmanagement (R3)
  Der Baustein DER.4 *Notfallmanagement* ist einmal für den gesamten Informationsverbund anzuwenden.

System-Bausteine

System-Bausteine adressieren Sicherheitsaspekte von spezifischen Komponenten und können somit auf relevante Zielobjekte des Informationsverbunds modelliert werden. Beispiele hierfür sind IT-Systeme, ICS-Komponenten, Gebäude, Anwendungen etc.

APP (Anwendungen)

In der Schicht APP (Anwendungen) des zu modellierenden Informationsverbunds erfolgt die Nachbildung der Anwendungen. Moderne Anwendungen beschränken sich nur selten auf ein einzelnes IT-System. Insbesondere behörden- bzw. unternehmensweite Kernanwendungen sind in der Regel als Client-Server-Applikationen realisiert. In vielen Fällen greifen Server selbst wieder auf andere, nachgeschaltete Server, z. B. Datenbanksysteme, zu. Die Sicherheit der Anwendungen muss daher unabhängig von den IT-Systemen und Netzen betrachtet werden.

Die Schicht APP umfasst die Teilschichten *Client-Anwendungen*, *Verzeichnisdienste*, *Netzbasierte Anwendungen*, *Business-Anwendungen* und *Groupware bzw. Kommunikation*.

Client-Anwendungen

- APP.1.1 Office-Produkte (R2)
  Der Baustein APP.1.1 *Office-Produkte* ist einmal für den gesamten Informationsverbund anzuwenden, wenn auf den eigenen IT-Systemen, z. B. auf Clients oder Terminalservern Office-Produkte wie Textverarbeitung oder Tabellenkalkulation eingesetzt werden.
- APP.1.2 Web-Browser (R2)
  Der Baustein APP.1.2 *Web-Browser* ist für alle IT-Systeme innerhalb des Informationsverbundes anzuwenden, auf denen Web-Browser eingesetzt werden.

Verzeichnisdienste

- APP.2.1 Allgemeiner Verzeichnisdienst (R2)

Der Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* sollte, unabhängig vom gewählten Produkt, auf jeden Verzeichnisdienst einmal angewandt werden.

- APP.2.2 Active Directory (R2)
  Der Baustein APP.2.2 *Active Directory* ist für den Informationsverbund anzuwenden, wenn in der Institution Microsofts Active Directory, etwa innerhalb einer Windows-Domäne, eingesetzt wird. Gibt es mehrere getrennte Instanzen von Active Directory, so ist der Baustein entsprechend mehrfach anzuwenden. In der Regel ist der Baustein gemeinsam mit den Bausteinen zu Windows Server sowie zum APP.2.1 *Allgemeiner Verzeichnisdienst* anzuwenden.

Netzbasierte Dienste

- APP.3.1 Webanwendungen (R2)
  Der Baustein APP.3.1 *Webanwendungen* ist auf jeden als Webanwendung ausgelegten Web-Dienst (z. B. Intranet oder Internet) des betrachteten Informationsverbunds anzuwenden.
- APP.3.2 Webserver (R2)
  Der Baustein APP.3.2 *Webserver* ist auf jeden WWW-Dienst (z. B. Intranet oder Internet) des betrachteten Informationsverbunds anzuwenden.
- APP.3.3 Fileserver (R2)
  Der Baustein APP.3.3 *Fileserver* ist auf jeden Fileserver des betrachteten Informationsverbunds anzuwenden.
- APP.3.4 Samba (R2)
  Der Baustein APP.3.4 *Samba* ist auf jeden Samba-Server des betrachteten Informationsverbunds anzuwenden.
- APP 3.6 DNS-Server (R2)
  Der Baustein APP.3.6 *DNS-Server* ist auf jeden im Informationsverbund betriebenen DNS-Server bzw. auf jede Gruppe von DNS-Servern anzuwenden.

Business-Anwendungen

- APP.4.3 Relationale Datenbanksysteme (R2)
  Der Baustein APP.4.3 *Relationale Datenbanksysteme* ist auf jedes relationale Datenbanksystem bzw. auf jede Gruppe von relationalen Datenbanksystemen einmal anzuwenden.

Groupware und Kommunikation

- APP.5.1 Allgemeine Groupware (R2)
  Der Baustein APP.5.1 *Allgemeine Groupware* ist auf jedes E-Mail-System (intern oder extern) des betrachteten Informationsverbunds anzuwenden.
- APP.5.2 Microsoft Exchange und Outlook (R2)
  Der Baustein APP.5.2 *Microsoft Exchange und Outlook* ist, zusätzlich zum Baustein APP.5.1 *Allgemeine Groupware,* auf jedes Workgroup- oder E-Mail-System anzuwenden, das auf Microsoft Exchange bzw. Outlook basiert.

SYS (IT-Systeme)

Sicherheitsaspekte, die sich auf IT-Systeme beziehen, werden in dieser Schicht abgedeckt. Diese Schicht SYS ist zur Übersichtlichkeit nach Servern, Deskop-Systemen, Mobile Devices und sonstigen Systemen sortiert. Bei letzteren handelt es sich in der Regel um IT-Systeme mit besonderen Funktionen, auf denen kein gängiges Betriebssystem installiert werden kann. Entsprechend den Einsatzumne nachgebildet werden, es müssen also die relevanten Sicherheitsanforderungen aus dem IT-Grundschutz-Kompendium zusammengetragen werden. Dafür müssen alle relevanten Prozesse, Anwendungen und IT-Systeme erfasst sein beziehungsweise es müssen die Strukturanalyse und in der Regel eine Schutzbedarfsfeststellung vorliegen. Darauf aufbauend wird ein IT-Grundschutz-Modell des Informationsverbunds erstellt, das aus verschiedenen, gegebenenfalls auch mehrfach verwendeten IT-Grundschutz-Bausteinen besteht und eine Abbildung zwischen den Bausteinen ugebungen sind die Bausteine auf die jeweiligen IT-Systeme im Informationsverbund anzuwenden.

Die Bausteine des Bereichs *IT-Systeme* können sowohl auf einzelne IT-Systeme als auch auf Gruppen solcher IT-Systeme angewandt werden. Dies wird im Folgenden nicht mehr gesondert hervorgehoben.

Server

- SYS.1.1 Allgemeiner Server (R2)
  Der Baustein SYS.1.1 *Allgemeiner Server* ist auf jedes IT-System anzuwenden, das Dienste (z. B. Datei- oder Druckdienste) als Server im Netz anbietet.
- SYS.1.3 Server unter Unix (R2)
  Der Baustein SYS.1.3 *Server unter Unix* ist auf jeden Server anzuwenden, der mit diesem Betriebssystem arbeitet.Hinweis: Für jeden Server muss neben dem Betriebssystem-spezifischen Baustein immer auch der Baustein SYS.1.1 *Allgemeiner Server* angewendet werden, da in diesem Baustein die plattformunabhängigen Sicherheitsaspekte für Server zusammengefasst sind.
- SYS.1.5 Virtualisierung (R2)
  Der Baustein SYS.1.5 *Virtualisierung* ist auf jeden Virtualisierungsserver bzw. auf jede Gruppe von Virtualisierungsservern anzuwenden.
- SYS.1.8 Speicherlösungen (R2)
  Der Baustein SYS.1.8 *Speicherlösungen* ist immer dann anzuwenden, wenn zentrale Speicherlösungen eingesetzt werden. Typische Zielobjekte für diesen Baustein sind NAS-Systeme (Network Attached Storage), SAN-Systeme (Storage Area Networks), Hybrid Storage, Objekt Storage und Cloud Storage.

Desktop-Systeme

- SYS.2.1 Allgemeine Client (R2)
  Der Baustein SYS.2.1 *Allgemeine Clients*ist auf jeden Client anzuwenden. Clients sind Arbeitsplatz-Computer die regelmäßig oder zumindest zeitweise in einem Netz betrieben werden (im Gegensatz zu Einzeplatz-Systemen).
- SYS.2.2.2 Clients unter Windows 8.1 (R2)
  Der Baustein SYS.2.2.2 *Clients unter Windows 8.1* ist für jeden Client bzw. jede Gruppe von Clients im Informationsverbund anzuwenden, auf denen das Betriebsystem Windows 8.1 von Microsoft eingesetzt wird.
  Hinweis: Für jeden Client muss neben dem Betriebsystem-spezifischen Baustein immer auch der Baustein SYS.2.1 *Allgemeine Clients*angewendet werden, da in diesem Baustein die plattformunabhängigen Sicherheitsaspekte für Clients zusammengefasst sind.
- SYS.2.2.3 Clients unter Windows 10 (R2)
  Der Baustein SYS.2.2.3 *Clients unter Windows 10* ist für jeden Client bzw. jede Gruppe von Clients im Informationsverbund anzuwenden, auf denen das Betriebsystem Windows 10 von Microsoft eingesetzt wird.
  Hinweis: Für jeden Client muss neben dem Betriebsystem-spezifischen Baustein immer auch der Baustein SYS.2.1 *Allgemeine Clients*angewendet werden, da in diesem Baustein die plattformunabhängigen Sicherheitsaspekte für Clients zusammengefasst sind.
- SYS.2.3 Clients unter Unix (R2)
  Der Baustein SYS.2.3 *Clients unter Unix* ist für jeden Client bzw. jede Gruppe von Clients im Informationsverbund anzuwenden, auf denen das Betriebsystem Unix eingesetzt wird.
  Hinweis: Für jeden Client muss neben dem Betriebsystem-spezifischen Baustein immer auch der Baustein SYS.2.1 *Allgemeine Clients*angewendet werden, da in diesem Baustein die plattformunabhängigen Sicherheitsaspekte für Clients zusammengefasst sind.

Mobile Devices

- SYS.3.1 Laptops (R2)
  Der Baustein SYS.3.1 *Laptops* ist auf jeden mobilen Computer (Laptop) anzuwenden.
- SYS.3.2.1 Allgemeine Smartphones und Tablets (R2)
  Der Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* ist immer dann anzuwenden, wenn in der Institution Endgeräte dienstlich eingesetzt werden, die auf mobilen Betriebssystemen wie z. B. Android oder iOS basieren. Der Baustein fasst die plattformunabhängigen Sicherheitsaspekte für die spezifischen Bausteine für solche mobilen Endgeräte zusammen.
- SYS.3.2.2 Mobile Device Management (MDM) (R2)

Der Baustein SYS.3.2.2 *Mobile Device Management (MDM)* ist immer dann anzuwenden, wenn in der Institution mobile Endgeräte wie Smartphones und Tablets zentral mithilfe eines Mobile Device Managements (MDM) verwaltet werden.

- SYS.3.2.3 iOS (for Enterprise) (R2)
  Der Baustein SYS.3.2.3 *iOS (for Enterprise)* ist für alle Endgeräte anzuwenden, auf denen in der Institution das Betriebssystem iOS von Apple dienstlich eingesetzt wird. Zu diesen Geräten gehören vorwiegend iPhones und iPads.
  Hinweis: Für jedes iOS-basierende Endgerät muss neben dem Betriebssystem-spezifischen Baustein immer auch der Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* angewendet werden, da in diesem Baustein die plattformunabhängigen Sicherheitsaspekte zusammengefasst sind.
- SYS.3.2.4 Android (R2)
  Der Baustein SYS.3.2.4 *Android* ist in Ergänzung zum Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* für jedes Zielobjekt oder jede Zielobjektgruppe mit dem Betriebssystem Android anzuwenden.
- SYS.3.4 Mobile Datenträger (R2)
  Der Baustein SYS.3.4 *Mobile Datenträger* ist für jeden mobilen Datenträger des Informationsverbundes bzw. von jeder Gruppe hiervon anzuwenden.

Sonstige Systeme

- SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte (R2)
  Der Baustein SYS.4.1 *Drucker, Kopierer und Multifunktionsgeräte* ist für jeden Drucker, Kopierer oder Multifunktionsgerät im Informationsverbund bzw. in jeder Gruppe hiervon anzuwenden. Als Multifunktionsgeräte werden dabei Geräte bezeichnet, die mehrere verschiedene papierverarbeitende Funktionen bieten, etwa Drucken, Kopieren und Scannen oder auch Fax-Dienste.
- SYS.4.4 Allgemeines IoT-Gerät (R2)
  Der Baustein SYS.4.4 *Allgemeines IoT-Gerät* ist auf jedes Gerät mit Funktionalitäten aus dem Bereich Internet of Things (IoT) bzw. auf jede entsprechende Gruppe anzuwenden. Dies sind im Gegensatz zu "klassischen" IT-Systemen "intelligente" Gegenstände, die zusätzliche "smarte" Funktionen enthalten.

IND (Industrielle IT)

Die Bausteine dieser Schicht enthalten Anforderungen für IT-Systeme und ICS-Komponenten, die in industriellen und Produktionsbereichen eingesetzt werden. Die Schicht IND ist in die drei Teilschichten *Betriebs- und Steuerungstechnik*, *ICS-Komponenten* und *Produktionsnetze* eingeteilt.

Betriebs- und Steuerungstechnik

- IND.1 Betriebs- und Steuerungstechnik (R2)
  Der Baustein IND.1 *Betriebs- und Steuerungstechnik* ist einmal für den industriellen Teil innerhalb des Informationsverbundes anzuwenden.

ICS-Komponenten

- IND.2.1 Allgemeine ICS-Komponente (R2)
  Der Baustein IND.2.1 *Allgemeine ICS-Komponente* ist für alle Komponenten der industriellen Steuerung anzuwenden. Hinzu kommen die spezifischen Bausteine für die einzelnen Zielobjekte bzw. Zielobjektgruppen.
- IND.2.2 Speicherprogrammierbare Steuerung (SPS) (R2)
  Der Baustein IND.2.2 *Speicherprogrammierbare Steuerung (SPS)* ist auf jede SPS-Komponente bzw. jede Gruppe hiervon anzuwenden.
- IND.2.3 Sensoren und Aktoren (R2)
  Der Baustein IND.2.3 *Sensoren und Aktoren* ist auf Sensoren und Aktoren bzw. jede Gruppe hiervon anzuwenden.
- IND 2.4 Maschine (R2)
  Der Baustein IND.2.4 *Maschine* ist auf jede Maschine bzw. jede Gruppe von Maschinen anzuwenden.

Produktionsnetze

Hinweis: Die Erstellung entsprechender Bausteine ist für künftige Editionen des IT-Grundschutz-Kompendiums geplant.

NET (Netze und Kommunikation)

In dieser Schicht werden Sicherheitsaspekte in Netzen behandelt, die nicht primär an bestimmten IT-Systemen (z. B. Servern) festgemacht werden können. Vielmehr geht es im Wesentlichen um Sicherheitsaspekte, die sich auf die Netzverbindungen und die Kommunikation zwischen den IT-Systemen beziehen.

Um die Komplexität zu verringern, kann es sich als sinnvoll erweisen, bei der Modellierung statt des Gesamtnetzes Teilbereiche jeweils einzeln zu betrachten. Die hierzu erforderliche Aufteilung des Gesamtnetzes in Teilnetze sollte anhand der Kriterien erfolgen, die im Baustein NET.1.1 *Netzarchitektur und -design* definiert worden sind.

Die Schicht Netze und Kommunikation ist zur Übersichtlichkeit nach Netzen, Funknetzen, Netzkomponenten und Telekommunikation sortiert.

Netze

- NET.1.1 Netzarchitektur und -design (R2)
  Der Baustein *NET.1.1 Netzarchitektur und -design* ist auf das Gesamtnetz einer Institution (inklusive Teilnetze) anzuwenden.
- NET.1.2 Netzmanagement (R2)
  Der Baustein NET.1.2 *Netzmanagement* ist auf jedes Netzmanagement-System anzuwenden, das im vorliegenden Informationsverbund eingesetzt wird.

Funknetze

- NET.2.1 WLAN-Betrieb (R2)
  Der Baustein NET.2.1 *WLAN-Betrieb* ist auf alle Kommunikationsnetze anzuwenden, die gemäß der Standard-Reihe 802.11 und deren Erweiterungen aufgebaut und betrieben werden.
- NET.2.2 WLAN-Nutzung (R2)
  Der Baustein NET.2.2 *WLAN-Nutzung* ist immer dann anzuwenden, wenn WLANs genutzt werden.

Netzkomponenten

- NET.3.1 Router und Switches (R2)
  Der Baustein NET.3.1 *Router und Switches* ist in jedem aktiven Netz, das im vorliegenden Informationsverbund eingesetzt wird, anzuwenden.
- NET.3.2 Firewall (R2)
  Der Baustein NET.3.2 *Firewall* ist immer anzuwenden, wenn unterschiedlich vertrauenswürdige Netze gekoppelt werden. Ein typischer Anwendungsfall ist die Absicherung einer Außenverbindung (z. B. beim Übergang eines internen Netzes zum Internet oder bei Anbindungen zu Netzen von Geschäftspartnern). Aber auch bei einer Kopplung von zwei organisationsinternen Netzen mit unterschiedlich hohem Schutzbedarf ist der Baustein anzuwenden, z. B. bei der Trennung des Bürokommunikationsnetzes vom Netz der Entwicklungsabteilung, wenn dort besonders vertrauliche Daten verarbeitet werden.
- NET.3.3 VPN (R2)
  Der Baustein NET.3.3 *VPN* ist für jede Art von Fernzugriffen auf den Informationsverbund, also interne Netze oder IT-Systeme, einmal anzuwenden. Hierzu gehören Verbindungen über Datennetze, wie z. B. Site-to-Site-, End-to-End- oder Remote-Access-VPNs, und über Telekommunikationsverbindungen, wie z. B. über analoge Wählleitungen, ISDN- oder Mobiltelefonie.

Telekommunikation

Hinweis: Die Erstellung entsprechender Bausteine (z. B. NET.4.1 *TK-Anlagen* oder NET.4.2 *VoIP*) ist für die zweite Edition des IT-Grundschutz-Kompendiums geplant.

INF (Infrastruktur)

Die für den vorliegenden Informationsverbund relevanten baulichen Gegebenheiten werden mit Hilfe der Bausteine aus der Schicht *Infrastruktur* modelliert. Jedem Gebäude, Raum oder Schutzschrank (bzw. Gruppen dieser Komponenten) wird dabei der entsprechende Baustein aus dem IT-Grundschutz-Kompendium zugeordnet.

- INF.1 Allgemeines Gebäude (R2)
  Der Baustein INF.1 *Allgemeines Gebäude* ist für jedes Gebäude bzw. jede Gebäudegruppe einmal anzuwenden.
- INF.2 Rechenzentrum (R2)
  Der Baustein INF.2 *Rechenzentrum* ist auf jedes Rechenzentrum und jeden Serverraum anzuwenden.
  Hinweis: Das BSI hat die Begriffe "Rechenzentrum" und "Serverraum" neu gefasst. Dabei ist auf den bisherigen Ansatz verzichtet worden, Rechenzentren und Serverräume über die getroffenen Maßnahmen, Organisationsformen oder Betriebsgrößen zu unterscheiden. Die neue Definition für Rechenzentren orientiert sich ausschließlich an der Bedeutung der IT-Struktur für die Aufgabenerfüllung der nutzenden Institution und steht damit im methodischen Einklang mit der DIN EN 50600. Details zur Unterscheidung finden sich im Baustein INF.2 *Rechenzentrum*.
- INF.3 Elektrotechnische Verkabelung (R2)
  Der Baustein INF.3 *Elektrotechnische Verkabelung* ist in der Regel einmal pro Gebäude bzw. Gebäudegruppe anzuwenden (zusätzlich zum Baustein INF.1 *Allgemeines Gebäude*). Darüber hinaus kann der Baustein INF.3 *Elektrotechnische Verkabelung* auch für einzelne Räume bzw. Raumgruppen, wie beispielsweise Rechenzentren, angewendet werden, wenn diese Besonderheiten im Bezug auf die elektrotechnische Verkabelung aufweisen. Für die IT-Verkabelung ist zusätzlich der Baustein INF.4 *IT-Verkabelung* anzuwenden.
- INF.4 IT-Verkabelung (R2)
  Der Baustein INF.4 *IT-Verkabelung* ist in der Regel einmal pro Gebäude bzw. Gebäudegruppe anzuwenden (zusätzlich zum Baustein INF.1 *Allgemeines Gebäude*). Darüber hinaus kann der Baustein INF.4 *IT-Verkabelung* auch für einzelne Räume bzw. Raumgruppen, wie beispielsweise Rechenzentren, angewendet werden, wenn diese Besonderheiten im Bezug auf die IT-Verkabelung aufweisen. Für die elektrotechnische Verkablung ist zusätzlich der Baustein INF.3 *Elektrotechnische Verkabelung* anzuwenden.
- INF.7 Büroarbeitsplatz (R2)
  Der Baustein INF.7 *Büroarbeitsplatz* ist auf jeden Raum bzw. jede Gruppe von Räumen anzuwenden, in denen sich Mitarbeiter aufhalten, um dort ihre Aufgaben zu erledigen.
- INF.8 Häuslicher Arbeitsplatz (R2)
  Der Baustein INF.8 *Häuslicher Arbeitsplatz* ist auf jeden häuslichen Arbeitsplatz bzw. jede Gruppe einmal anzuwenden.
- INF.9 Mobiler Arbeitsplatz (R2)
  Der Baustein INF.9 *Mobiler Arbeitsplatz* ist immer dann anzuwenden, wenn Mitarbeiter häufig nicht mehr nur innerhalb der Räumlichkeiten der Institution arbeiten, sondern an wechselnden (mobilen) Arbeitsplätzen außerhalb. Typische Zielobjekte für den Baustein sind Laptops.
- INF.10 Besprechungs-, Veranstaltungs- und Schulungsraum (R2)
  Der Baustein INF.10 *Besprechungs-, Veranstaltungs- und Schulungsräume* ist auf jeden solchen Raum bzw. jede Gruppe (falls entsprechende Gruppen definiert wurden) einmal anzuwenden.

2.3 Bearbeitungsreihenfolge der Bausteine

Um grundlegende Risiken abzudecken und eine ganzheitliche Informationssicherheit aufzubauen, müssen die essentiellen Sicherheitsanforderungen frühzeitig erfüllt und entsprechende Sicherheitsmaßnahmen umgesetzt werden. Daher wird im IT-Grundschutz mit R1, R2 und R3 eine Reihenfolge für die umzusetzenden Bausteine vorgeschlagen (siehe Kapitel 2.2 *Zuordnung anhand Schichtenmodell).*

- R1: Diese Bausteine sollten vorrangig umgesetzt werden, da sie die Grundlage für einen effektiven Sicherheitsprozess bilden.

- R2: Diese Bausteine sollten als nächstes umgesetzt werden, da sie in wesentlichen Teilen des Informationsverbundes für nachhaltige Sicherheit erforderlich sind.
- R3: Diese Bausteine werden zur Erreichung des angestrebten Sicherheitsniveaus ebenfalls benötigt und müssen umgesetzt werden, es wird aber empfohlen, diese erst nach den anderen Bausteinen zu betrachten.

Mit R1 sind die Bausteine gekennzeichnet, die notwendig sind, um ein grundlegendes Sicherheitsgerüst zu erreichen. Es handelt sich um die Bausteine der Bereiche

- ISMS *Sicherheitsmanagement*
- ORP *Organisation und Personal*
- OPS.1 *Kernaufgaben* der Schicht *Eigener IT-Betrieb*

Die im zweiten und dritten Schritt umzusetzenden Bausteine (R2 und R3) finden sich in allen anderen Schichten des IT-Grundschutz-Kompendiums.

Diese Kennzeichnung zeigt nur die sinnvolle zeitliche Reihenfolge für die Umsetzung der Anforderungen des jeweiligen Bausteins auf und stellt keine Gewichtung der Bausteine untereinander dar. Grundsätzlich müssen alle für den jeweiligen Informationsverbund relevanten Bausteine des IT-Grundschutz-Kompendiums umgesetzt werden.

Die Kennzeichnung der Bausteine stellt außerdem nur eine Empfehlung dar, in welcher Reihenfolge die verschiedenen Bausteine sinnvoll umgesetzt werden könnten. Jede Institution kann hier eine abweichende, für sich sinnvolle Reihenfolge festlegen.

Rollen

In den Maßnahmen werden neben der eigentlichen Empfehlung, wie die einzelnen Maßnahmen umzusetzen sind, Verantwortliche für die Initiierung bzw. für die Umsetzung dieser Maßnahmen beispielhaft genannt. Da die Bezeichnungen der hier als Verantwortliche genannten Personen oder Rollen nicht in allen Organisationen einheitlich sind, wird für eine leichtere Zuordnung in diesem Kapitel eine kurze Beschreibung der wesentlichen Rollen dargestellt.

Verantwortliche	**Rollenbeschreibung**
Administrator	Ein Administrator ist zuständig für Einrichtung, Betrieb, Überwachung und Wartung eines IT-Systems.
Änderungsmanager	Der Änderungsmanager (Change Manager) hat die Aufgabe, ein effizientes und effektives Patch- und Änderungsmanagement zu betreiben. Aufgabe des Änderungsmanager ist es, verändernde Eingriffe in Anwendungen, Infrastruktur, Dokumentationen, Prozesse und Verfahren steuer- und kontrollierbar zu gestalten.
Anforderungsmanager (Compliance Manager)	Der Anforderungsmanager (Compliance Manager) ist verantwortlich dafür, die für die Institution relevanten gesetzlichen, vertraglichen und sonstigen Vorgaben zu identifizieren und deren Einhaltung zu prüfen.
Archivverwalter	Der Archivverwalter hat die Aufgaben Einrichtung, Betrieb, Überwachung und Wartung eines Archivsystems auf fachlicher Ebene.
Auditteam	Das Auditteam besteht aus Auditoren und Fachexperten, die den Auditteamleiter insbesondere fachlich während eines Audits unterstützen.
Auditteamleiter	Der Auditteamleiter ist für die korrekte Durchführung deines Audits verantwortlich. Der Auditteamleiter ist der Hauptansprechpartner seitens der Institution und der Zertifizierungsstelle des BSI.
Bauleiter	Ein Bauleiter ist für die Umsetzung von Baumaßnahmen zuständig.
Benutzer	Ein Benutzer ist ein Mitarbeiter des Unternehmens bzw. der Behörde, der informationstechnische Systeme im Rahmen der Erledigung seiner Aufgaben benutzt. IT-Benutzer und Benutzer sind hierbei als Synonyme zu betrachten, da heutzutage nahezu jeder Mitarbeiter eines Unternehmens bzw. einer Behörde informationstechnische Systeme während der Erledigung seiner Aufgaben benutzt.
Bereichs-Sicherheitsbeauftragter	Der Bereichs-Sicherheitsbeauftragte ist für alle Sicherheitsbelange der Geschäftsprozesse, Anwendungen und IT-Systeme in seinem Bereich (zum Beispiel Abteilung oder Außenstelle) verantwortlich. Je nach Größe des zu betreuenden Bereichs kann die Aufgabe des Bereichs-Sicherheitsbeauftragten von einer Person übernommen werden, die bereits mit ähnlichen Aufgaben betreut ist.

Verantwortliche	Rollenbeschreibung
Beschaffer	Dies bezeichnet einen Mitarbeiter der Beschaffungsstelle, dessen Aufgabe die Beschaffung von Betriebsmitteln oder IT-Systemen ist.
Beschaffungsstelle	Die Beschaffungsstelle initiiert und überwacht Beschaffungen. Öffentliche Einrichtungen wickeln ihre Beschaffungen nach vorgeschriebenen Verfahren ab.
Brandschutzbeauftragter	Ein Brandschutzbeauftragter ist Ansprechpartner und Verantwortlicher in allen Fragen des Brandschutzes. Er ist u. a. zuständig für die Erstellung von Brandrisikoanalysen, Aus- und Fortbildung der Beschäftigten, teilweise auch für Wartung und Instandhaltung der Brandschutzeinrichtungen.
Datenschutzbeauftragter	Ein Datenschutzbeauftragter ist eine von der Behörden- bzw. Unternehmensleitung bestellte Person, die auf den datenschutzrechtlich korrekten bzw. gesetzeskonformen Umgang mit personenbezogenen Daten im Unternehmen bzw. in der Behörde hinwirkt.
Entwickler	Mit Entwickler wird im Kontext des IT-Grundschutzes eine Person bezeichnet, die bei Planung, Entwicklung, Test oder Pflege von Software, Hardware oder ganzen Systemen mitarbeitet. Im IT-Grundschutz werden unter der Rolle Entwickler verschiedene weitere Rollen zusammengefasst, wie z. B. Software-Architekt, Software-Designer, Software-Entwickler, Programmierer und Tester.
Ermittler	Bezeichnet die Person, die alle Tätigkeiten in einem Ermittlungsverfahren durchführt, wie zum Beispiel Vorbereitungen, Analysen und Dokumentationen.
Ermittlungsleiter	Hiermit ist die Person gemeint, die für die Planung der Vorgehensweise und alle Tätigkeiten in einem Ermittlungsverfahren verantwortlich ist, wie z. B. Vorbereitungen, Analysen und Dokumentation.
Errichterfirma	Es handelt sich hierbei um ein Unternehmen, das Gewerke oder aber auch Gebäude erstellt.
Fachabteilung	Eine Fachabteilung ist ein Teil einer Behörde bzw. eines Unternehmens, welche fachspezifische Aufgaben zu erledigen hat. Bei Bundes- und Landesbehörden ist eine Abteilung die übergeordnete Organisationsform mehrerer Referate, die inhaltlich zusammengehören.
Fachverantwortliche	Der Fachverantwortliche ist inhaltlich für ein oder mehrere Geschäftsprozesse oder Fachverfahren verantwortlich (so ist z. B. der Leiter des Referats "Vertrieb" der Fachverantwortliche für die Anwendung "automatisierter Vertrieb").
Haustechnik	Haustechnik bezeichnet die Organisationseinheit, die sich um die Einrichtungen der Infrastruktur in einem Gebäude oder in einer Liegenschaft kümmert. Betreute Gewerke können dabei z. B. sein: Elektrotechnik, Melde- und Steuerungstechnik, Sicherungstechnik, IT-Netze (Physikalischer Teil), Heizungs- und Sanitärtechnik, Aufzüge etc.
ICS-Administrator	Ein Administrator-ICS ist für Einrichtung, Betrieb, Überwachung und Wartung der ICS-Systeme zuständig.

Verantwortliche	Rollenbeschreibung
ICS-Informationssicherheitsbeauftragter	Ein ICS-Informationssicherheitsbeauftragter (oft auch Industrial Security Officer genannt) ist eine von der Institutionsleitung benannte Person, die Im Auftrag der Leitungsebene dafür sorgt, dass die speziellen Anforderungen im Bereich der industriellen Steuerung abgedeckt sind und die Sicherheitsorganisation aus dem Bereich ICS in das Gesamt-ISMS eingebunden ist.
Informationssicherheitsbeauftragter (ISB)	Ein ISB ist eine von der Behörden- bzw. Unternehmensleitung ernannte Person, die im Auftrag der Leitungsebene die Aufgabe Informationssicherheit koordiniert und innerhalb der Behörde bzw. des Unternehmens vorantreibt.
Innerer Dienst	Der Innere Dienst ist eine Organisationseinheit, die alle zentralen Dienste für die Mitarbeiter koordiniert, z. B. Poststelle, Kopierer, Fahrdienst, Botendienst, Beseitigung technischer Störungen, Gebäudereinigung, Bereitstellung von Betriebsmitteln etc.
Institutionsleitung	Dies bezeichnet die Leitungsebene der Institution bzw. der betrachteten Organisationseinheit.
ISB Outsourcing-Dienstleister	Der ISB Outsourcing-Dienstleister ist der ISB des beautragten Outsourcing-Dienstleisters. Er ist eine von der Institutionsleitung des Outsourcing-Dienstleisters ernannte Person, die im Auftrag unter anderem die Informationssicherheit mit dem ISB des Outsourcing-Kunden vorantreibt.
ISB Outsourcing-Kunde	Der ISB Outsourcing-Kunde ist der ISB der eigenen Institution, die Outsourcing nutzt. Er steht bei Outsourcing in Kontakt mit dem ISB des Outsourcing-Dienstleisters
IS-Management-Team	Das IS-Management-Team unterstützt den IT-Sicherheitsbeauftragten, indem es übergreifende Maßnahmen in der Gesamtorganisation koordiniert, Informationen zusammenträgt und Kontrollaufgaben durchführt.
IS-Revisionsteam	Das IS-Revisionsteam besteht aus IS-Revisoren und Fachexperten, die den Verantwortlichen für die IS-Revision insbesondere fachlich während der IS-Revision unterstützen.
IT-Betreuer	Zu den Aufgaben von IT-Betreuern zählen u. a. die Entgegennahme und Bearbeitung von Benutzeranfragen zu Problemen rund um die IT-Ausstattung.
IT-Betrieb	Als IT-Betrieb wird die Organisationseinheit bezeichnet, die die interne IT einrichtet, betreibt überwacht und wartet.
Leiter Beschaffung	Hiermit ist der Leiter der Beschaffungsstelle oder der Organisationseinheit gemeint, die für die Beschaffung zuständig ist.
Leiter Entwicklung	Dies bezeichnet den Leiter einer Entwicklungsabteilung für Hard- bzw. Software oder den Projektleiter eines Entwicklerteams.
Leiter Fachabteilung	Dies bezeichnet den Leiter einer Fachabteilung.
Leiter Haustechnik	Hiermit ist der Verantwortliche für die Haustechnik gemeint.
Leiter Innerer Dienst	Dies bezeichnet den Leiter des Inneren Dienstes bzw. den Verantwortlichen für die Bereitstellung zentraler Dienste.
Leiter IT	Hiermit ist der Leiter der IT-Abteilung bzw. das für die Informationstechnik zuständige Management gemeint.
Leiter Netze	Der Leiter Netze ist dafür verantwortlich, dass Datennetze sicher entworfen, geplant und aufgebaut werden.

Verantwortliche	Rollenbeschreibung
Leiter Organisation	Dies bezeichnet den Leiter der Organisationseinheit, die u. a. für Regelung und Überwachung des allgemeinen Betriebs sowie für Planung, Organisation und Durchführung aller Verwaltungsdienstleistungen verantwortlich ist.
Leiter Personal	Hiermit ist der Leiter der Personalabteilung bzw. der für Personalfragen zuständigen Organisationseinheit gemeint.
Leiter Produktion und Fertigung	Dies bezeichnet den Leiter des Bereichs Produktion und Fertigung bzw. den Verantwortlichen für die Industriellen Steuerungssysteme (ICS), die von der Institution eingesetzt werden.
Leitstellen-Operator	Mit Leitstellen-Operator wird im Kontext der industriellen Steuerung eine Person bezeichnet, die die Gesamteinsatzlage überwacht, die Betriebsabläufe steuert und Maßnahmen einleitet, um Gefahren abzuwehren.
Mitarbeiter	Ein Mitarbeiter ist Mitglied einer Fachabteilung, einer Behörde oder eines Unternehmens.
Notfallbeauftragter	Der Notfallbeauftragte steuert alle Aktivitäten rund um das Notfallmanagement. Er ist für die Erstellung, Umsetzung, Pflege und Betreuung des institutionsweiten Notfallmanagements und der zugehörigen Dokumente, Regelungen und Maßnahmen zuständig. Er analysiert den Gesamtablauf der Notfallbewältigung nach einem Schadensereignis.
Personalabteilung	Die Personalabteilung ist unter Anderem für folgende Aufgaben zuständig: • Personalwirtschaftliche Grundfragen • Personalbedarfsplanung • Personalangelegenheiten der Mitarbeiter • Soziale Betreuung der Mitarbeiter • Allgemeine Zusammenarbeit mit der Personalvertretung
Personalrat / Betriebsrat	Der Personal- bzw. Betriebsrat (Personalvertretung) ist für die Interessenvertretung der Mitarbeiter gegenüber der Behörden- bzw. Unternehmensleitung zuständig.
Planer	Mit dem allgemeinen Begriff "Planer" werden Rollen wie "Netzplaner" und "Bauplaner" zusammengefasst. Gemeint sind also Personen, die für die Planung und Konzeption bestimmter Aufgaben zuständig sind.
Poststelle	Die Poststelle ist die Sammelstelle einer Behörde oder eines Unternehmens für ankommende und ausgehende Post. Zu den Aufgabengebieten können auch Fax- und E-Mail-Dienstleistungen sowie das Scannen eingehender Dokumente im Rahmen eines elektronischen Workflows gehören.
Pressestelle	Die Pressestelle ist zuständig für alle ein- und ausgehenden Kontakte zu Presse und Medien. In vielen Fällen werden dort auch Anfragen von Privatpersonen und Firmen bearbeitet.
Telearbeiter	Ein Telearbeiter nimmt seine Tätigkeiten außerhalb der Büroräume des Unternehmens oder der Behörde wahr und verfügt über eine kommunikationstechnische Anbindung an die IT des Arbeit- bzw. Auftraggebers.
Tester	Tester sind Personen, die gemäß eines Testplans nach vorher festgelegten Verfahren und Kriterien eine neue oder veränderte Software bzw. Hardware testen und die Testergebnisse mit den erwarteten Ergebnissen vergleichen.

TK-Anlagen-Verantwortlicher	Der TK-Anlagen-Verantwortliche ist für den ordnungsgemäßen Betrieb der Telekommunikationsanlagen und für entsprechende Regelungen zuständig.
Verantwortliche der einzelnen Anwendungen	Der Verantwortliche für die einzelne Anwendung ist nicht nur für den reibungslosen Betrieb der Anwendung zuständig, sondern auch für die Initiierung und Umsetzung von Sicherheitsmaßnahmen für diese Anwendung.
Verantwortliche für die Datensicherung	Der Verantwortliche für die Datensicherung ist zuständig für die Erstellung, Pflege, regelmäßige Aktualisierung und Umsetzung eines Datensicherungskonzeptes.
Verantwortlicher für die IS-Revision	Der Verantwortliche für die IS-Revision ist für die korrekte Durchführung der IS-Revision zuständig.
Vertragsmanagement	Vertragsmanagement ist die gemeinsame Fachaufgabe der Beschaffungsstelle und des Vertriebs und beinhaltet die Planung, Steuerung und Fortentwicklung aller Verträge mit Dienstleistern, Lieferanten und sonstigen Stellen, die zur Beschaffung oder zum Vertrieb von Gütern und Dienstleistungen der Institution notwendig sind.
Vertrieb	Der Vertrieb ist die zuständige Stelle für alle Aktivitäten, die für das Vertreiben von Gütern und Dienstleistungen einer Institution notwendig sind.
Vorgesetzte	Als Vorgesetzte werden die Mitarbeiter einer Institution bezeichnet, die gegenüber anderen, ihnen zugeordneten Mitarbeitern weisungsbefugt sind.
Wartungspersonal	Beim Wartungspersonal handelt es sich um Mitarbeiter von externen Dienstleistern, die mit der Wartung von technischen Systemen (Z. B. ICS- oder IT-Systeme) im Informati-

Glossar

In diesem Glossar werden die wichtigsten Begriffe rund um Informationssicherheit und IT-Grundschutz erläutert. Ein hierzu ergänzendes Glossar zur Cyber-Sicherheit ist auf den Webseiten des BSI zu finden.
https://www.bsi.bund.de/cyberglossar

Advanced Persistent Threats (APT)

Bei Advanced Persistent Threats (APT) handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netz verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind in der Regel schwierig zu detektieren.

Anforderung bei erhöhtem Schutzbedarf

Siehe Sicherheitsanforderung.

Angriff

Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.

Application-Level-Gateway (ALG)

Die Funktionen eines Sicherheitsgateways auf Anwendungsebene werden von den so genannten Application-Level-Gateways (ALG) übernommen. Implizit nehmen ALGs auch Funktionen auf den ISO-/OSI-Schichten 1 bis 3 wahr. ALGs, auch Sicherheitsproxies genannt, unterbrechen den direkten Datenstrom zwischen Quelle und Ziel. Bei einer Kommunikationsbeziehung zwischen Client und Server über einen Proxy hinweg nimmt der Proxy die Anfragen des Clients entgegen und leitet sie an den Server weiter. Bei einem Verbindungsaufbau in umgekehrter Richtung, also vom Server zum Client, verfährt der Proxy analog.

Sämtliche Kommunikationsbeziehungen zwischen den beiden Rechnern verlaufen in diesem Fall also mittelbar über den Proxy. Diese Kommunikationsform ermöglicht es einem Proxy beispielsweise bestimmte Protokollbefehle zu filtern.

Assets

Als Assets werden Bestände von Objekten bezeichnet, die für einen bestimmten Zweck, besonders zur Erreichung von Geschäftszielen, benötigt werden. Der englische Begriff "asset" wird häufig mit "Wert" übersetzt. "Wert" ist allerdings im Deutschen ein mit vielen Bedeutungen belegter Begriff – von der gesellschaftlichen Bedeutung, die einer Sache zukommt, bis hin zur inneren Qualität eines Objekts. Im IT-Grundschutz wird der Begriff "Assets" in der Bedeutung von "werthaltigen bzw. wertvollen Zielobjekten" verwendet.

Authentisierung (englisch "authentication")

Authentisierung bezeichnet den Nachweis oder die Überprüfung der Authentizität. Die Authentisierung einer Identität kann u.a. durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen, die Authentisierung von Daten z. B. durch kryptographische Signaturen.

Authentizität

Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.

Autorisierung

Bei einer Autorisierung wird geprüft, ob eine Person, IT-Komponente oder Anwendung zur Durchführung einer bestimmten Aktion berechtigt ist.

Basis-Absicherung

Die Basis-Absicherung ermöglicht es, als Einstieg in den IT-Grundschutz zunächst eine breite, grundlegende Erst-Absicherung über alle Geschäftsprozesse bzw. Fachverfahren einer Institution vorzunehmen.

Basis-Anforderung

Siehe Sicherheitsanforderung.

Bausteine

Das IT-Grundschutz-Kompendium enthält für unterschiedliche Vorgehensweisen, Komponenten und IT-Systeme Erläuterungen zur Gefährdungslage, Sicherheitsanforderungen und weiterführende Informationen, die jeweils in einem Baustein zusammengefasst sind. Das IT-Grundschutz-Kompendium ist aufgrund der Baustein-Struktur modular aufgebaut und legt einen Fokus auf die Darstellung der wesentlichen Sicherheitsanforderungen in den Bausteinen. Die grundlegende Struktur des IT-Grundschutz-Kompendiums sieht eine Unterteilung in prozess- und systemorientierte Bausteine vor, zudem sind sie nach Themen in ein Schichtenmodell einsortiert.

Beauftragter für IT-Sicherheit

Person mit Fachkompetenz zur IT-Sicherheit, die in großen Institutionen für Aspekte rund um die IT-Sicherheit zuständig ist, in enger Abstimmung mit dem IT-Betrieb. Der ISB gestaltet das Informationssicherheitsmanagement und erstellt die generellen Sicherheitsziele und -vorgaben, ein Beauftragter für die IT-Sicherheit sorgt dafür, dass diese technisch umgesetzt werden. Ein Beauftragter für die IT-Sicherheit ist somit typischerweise im IT-Betrieb tätig, während der ISB unmittelbar der Leitungsebene zuarbeitet.

Bedrohung (englisch "threat")

Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann. Beispiele für Bedrohungen sind höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen. Trifft eine Bedrohung auf eine Schwachstelle (insbesondere technische oder organisatorische Mängel), so entsteht eine Gefährdung.

Benutzerkennung (häufig auch Benutzerkonto)

Die Benutzerkennung ist der Name, mit dem sich der Benutzer einem IT-System gegenüber identifiziert. Dies kann der tatsächliche Name sein, ein Pseudonym, eine Abkürzung oder eine Kombination aus Buchstaben und/oder Ziffern.

BIA (Business Impact Analyse)

Eine Business Impact Analyse (Folgeschädenabschätzung) ist eine Analyse zur Ermittlung von potentiellen direkten und indirekten Folgeschäden für eine Institution, die durch das Auftreten eines Notfalls oder einer Krise und Ausfall eines oder mehrerer Geschäftsprozesse verursacht werden. Es ist ein Verfahren, um kritische Ressourcen und Wiederanlaufanforderungen sowie die Auswirkungen von ungeplanten Geschäftsunterbrechungen zu identifizieren.

Biometrie

Unter Biometrie ist die automatisierte Erkennung von Personen anhand ihrer körperlichen Merkmale zu verstehen. Diese kann genutzt werden, um Benutzer auf Grundlage besonderer Merkmale eindeutig zu authentisieren. Ein oder mehrere der folgenden biometrischen Merkmale können beispielsweise für eine Authentisierung verwendet werden:

- Iris
- Fingerabdruck
- Gesichtsproportionen
- Stimme und Sprachverhalten
- Handschrift
- Tippverhalten am Rechner

Blackbox-Test

Bei Blackbox-Tests wird das Verhalten von Außentätern simuliert, wobei vorausgesetzt wird, dass der Angreifer keine oder nur oberflächliche Informationen über sein Angriffsziel hat.

Browser

Mit Browser (von "to browse", auf deutsch: schmökern, blättern, umherstreifen) wird Software zum Zugriff auf das World Wide Web bezeichnet. Das Programm interpretiert die ankommenden Daten und stellt sie als Text und Bild auf dem Bildschirm dar.

Business Continuity Management

Business Continuity Management (BCM) bezeichnet alle organisatorischen, technischen und personellen Maßnahmen, die zur Fortführung des Kerngeschäfts einer Behörde oder eines Unternehmens nach Eintritt eines Notfalls bzw. eines Sicherheitsvorfalls dienen. Weiterhin unterstützt BCM die sukzessive Fortführung der Geschäftsprozesse bei länger anhaltenden Ausfällen oder Störungen.

Client

Als Client wird Soft- oder Hardware bezeichnet, die bestimmte Dienste von einem Server in Anspruch nehmen kann. Häufig steht der Begriff Client für einen Arbeitsplatzrechner, der in einem Netz auf Daten und Programme von Servern zugreift.

Cyber-Raum

Der Cyber-Raum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Dem Cyber-Raum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, welches durch beliebige andere Datennetze erweitert werden kann.

Cyber-Sicherheit

Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Häufig wird bei der Betrachtung von Cyber-Sicherheit auch ein spezieller Fokus auf Angriffe aus dem Cyber-Raum gelegt.

Datenschutz

Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Mit Datenschutz wird daher der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet (nicht zu verwechseln mit Datensicherheit).

Für den Begriff "Datenschutz" existieren zwei englische Übersetzungen: Dabei bezeichnet "Data Protection" den Datenschutz als Rechtsbegriff. "Privacy" zielt dagegen auf die gesellschaftliche Lebensweise ab (Schutz der Privatsphäre) und wird überwiegend im amerikanischen Sprachumfeld und mittlerweile auch im EU-Raum vermehrt genutzt.

Datenschutz-Management

Mit Datenschutz-Management werden die Prozesse bezeichnet, die notwendig sind, um die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von Verfahren zur Informationsverarbeitung sicher zu stellen.

Datensicherheit

Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein modernerer Begriff dafür ist "Informationssicherheit".

Datensicherung (englisch "Backup")

Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen erstellt. Datensicherung umfasst alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der Systeme einschließlich der auf diesen Systemen gespeicherten und für Verarbeitungszwecke genutzten Daten, Programme und Prozeduren.

Ordnungsgemäße Datensicherung bedeutet, dass die getroffenen Maßnahmen in Abhängigkeit von der Datensensitivität eine sofortige oder kurzfristige Wiederherstellung des Zustandes von Systemen, Daten, Programmen oder Prozeduren nach erkannter Beeinträchtigung der Verfügbarkeit, Integrität oder Konsistenz aufgrund eines schadenswirkenden Ereignisses ermöglichen. Die Maßnahmen umfassen dabei mindestens die Herstellung und Erprobung der Rekonstruktionsfähigkeit von Kopien der Software, Daten und Prozeduren in definierten Zyklen und Generationen.

Demilitarisierte Zone (DMZ)

Eine DMZ ist ein Zwischennetz, das an Netzübergängen gebildet wird, aber weder zu dem einen, noch zu dem anderen Netz gehört. Sie stellt ein eigenes Netz dar, das nicht so stark gesichert ist wie das eigentlich zu schützende Netz.

DMZ werden bei einfachen Sicherheitsgateways üblicherweise an einer dritten Schnittstelle des Paketfilters erzeugt. Besteht das Sicherheitsgateway aus Paketfilter - Application-Level-Gateway - Paketfilter, dient in der Regel eine weitere Schnittstelle des Application-Level-Gateways (ALG) als DMZ-Schnittstelle. Verfügen Paketfilter oder ALG über mehr als drei Schnittstellen, können weitere DMZ gebildet werden.

Digitale Signatur

Eine digitale Signatur ist eine Kontrollinformation, die an eine Nachricht oder Datei angehängt wird, mit der folgende Eigenschaften verbunden sind:

- Anhand einer digitalen Signatur kann eindeutig festgestellt werden, wer diese erzeugt hat, und
- es ist authentisch überprüfbar, ob die Datei, an die die digitale Signatur angehängt wurde, identisch ist mit der Datei, die tatsächlich signiert wurde.

Fachaufgabe

Fachaufgaben sind Aufgaben, die aus der Zweckbestimmung einer Institution bzw. deren Auftrag folgen. Als Fachaufgaben werden im IT-Grundschutz Geschäftsprozesse in Behörden bezeichnet.

Firewall

Eine Firewall (oft auch als Sicherheitsgateway bezeichnet) ist ein System aus soft- und hardwaretechnischen Komponenten, um IP-Netze sicher zu koppeln (siehe Sicherheitsgateway).

Gefahr

"Gefahr" wird oft als übergeordneter Begriff gesehen, wohingegen unter "Gefährdung" eine genauer beschriebene Gefahr (räumlich und zeitlich nach Art, Größe und Richtung bestimmt) verstanden wird. Beispiel: Die Gefahr ist ein Datenverlust. Datenverlust kann unter anderem durch eine defekte Festplatte oder einen Dieb entstehen, der die Festplatte stiehlt. Die Gefährdungen sind dann "defekter Datenträger" und "Diebstahl von Datenträgern". Diese Unterscheidung wird aber in der Literatur nicht durchgängig gemacht und ist eher von akademischer Bedeutung, so dass es sinnvoll ist, "Gefahr" und "Gefährdung" als gleichbedeutend aufzufassen.

Gefährdung (englisch "applied threat")

Eine Gefährdung ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt.

Sind beispielsweise Schadprogramme eine Bedrohung oder eine Gefährdung für Anwender, die im Internet surfen? Nach der oben gegebenen Definition lässt sich feststellen, dass alle Anwender prinzipiell durch Schadprogramme im Internet bedroht sind. Der Anwender, der eine virenverseuchte Datei herunterlädt, wird von dem Schadprogramm gefährdet, wenn sein IT-System anfällig für diesen Typ des Schadprogramms ist. Für Anwender mit einem wirksamen Virenschutz, einer Konfiguration, die das Funktionieren des Schadprogramms verhindert, oder einem Betriebssystem, das den Code des Schadprogramms nicht ausführen kann, bedeutet das geladene Schadprogramm hingegen keine Gefährdung.

Geschäftsprozess

Ein Geschäftsprozess ist eine Menge logisch verknüpfter Einzeltätigkeiten (Aufgaben, Arbeitsabläufe), die ausgeführt werden, um ein bestimmtes geschäftliches oder betriebliches Ziel zu erreichen.

Grundwerte der Informationssicherheit

Der IT-Grundschutz betrachtet die drei Grundwerte der Informationssicherheit:

- Vertraulichkeit,
- Verfügbarkeit und
- Integrität.

Jedem Anwender steht es natürlich frei, bei der Schutzbedarfsfeststellung weitere Grundwerte zu betrachten, wenn dies in seinem individuellem Anwendungsfall hilfreich ist. Weitere generische Oberbegriffe der Informationssicherheit sind zum Beispiel:

- Authentizität,

- Verbindlichkeit,
- Zuverlässigkeit und
- Nichtabstreitbarkeit.

Hintertür (englisch "backdoor")

Hintertüren sind Schadprogramme, die dazu dienen, einen unbefugten Zugang zu einem IT-System offen zu halten, der einen unbemerkten Einbruch in das System ermöglicht und dabei möglichst weitgehende Zugriffsrechte besitzt, beispielsweise um Angriffsspuren zu verstecken.

Industrial Control System (ICS)

ICS ist ein Oberbegriff für Automatisierungslösungen zur Steuerung technischer Prozesse.

Informationssicherheit

Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Die Schutzziele oder auch Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Viele Anwender ziehen in ihre Betrachtungen weitere Grundwerte mit ein.

Informationssicherheitsbeauftragter (ISB)

Ein Informationssicherheitsbeauftragter (kurz IS-Beauftragter oder ISB) ist für die operative Erfüllung der Aufgabe "Informationssicherheit" zuständig. Andere Bezeichnungen sind CISO (Chief Information Security Officer) oder Informationssicherheitsmanager (ISM). Die Rolle des ISB sollte von einer Person mit eigener Fachkompetenz zur Informationssicherheit in einer Stabsstelle eines Unternehmens oder einer Behörde wahrgenommen werden.

Informationssicherheitsmanagement (IS-Management)

Die Planungs-, Lenkungs- und Kontrollaufgabe, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen, wird als Informationssicherheitsmanagement bezeichnet. Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.

Informationstechnik (IT)

Informationstechnik (IT) umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen.

Informationsverbund

Unter einem Informationsverbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei als Ausprägung die gesamte Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungen) oder gemeinsame Geschäftsprozesse bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.

Infrastruktur

Beim IT-Grundschutz werden unter Infrastruktur die für die Informationsverarbeitung und die IT genutzten Gebäude, Räume, Energieversorgung, Klimatisierung und die Verkabelung verstanden. Die IT-Systeme und Netzkoppelelemente gehören nicht dazu.

Institutionen

Mit dem Begriff Institutionen werden in diesem Dokument Unternehmen, Behörden und sonstige öffentliche oder private Organisationen bezeichnet.

Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. Der Begriff "Information" wird dabei für "Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

Intranet

Ein Intranet ist ein internes Netz, das sich unter vollständiger Kontrolle des Netzbetreibers (also der jeweiligen Behörde oder des Unternehmens) befindet. Meist werden Zugriffe aus anderen Netzen (wie dem Internet) durch eine Firewall abgesichert.

IS-Management-Team

In größeren Institutionen ist es sinnvoll, ein IS-Management-Team (häufig auch IT-Sicherheitsmanagement-Team) aufzubauen, das den ISB unterstützt, beispielsweise indem es übergreifende Maßnahmen in der Gesamtorganisation koordiniert, Informationen zusammenträgt und Kontrollaufgaben durchführt.

IT-Grundschutz-Check

Der Begriff bezeichnet im IT-Grundschutz die Überprüfung, ob die nach IT-Grundschutz empfohlenen Anforderungen in einer Institution bereits erfüllt sind und welche grundlegenden Sicherheitsanforderungen noch fehlen (früher: Basis-Sicherheitscheck).

IT-Grundschutz-Kompendium

Die Bausteine des IT-Grundschutzes sind im IT-Grundschutz-Kompendium zusammengefasst. Es stellt den Nachfolger der bis zur 15. Ergänzungslieferung verfügbaren IT-Grundschutz-Kataloge dar.

IT-System

IT-Systeme sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Einzelplatz-Computer, Mobiltelefone, Router, Switches und Sicherheitsgateways.

Kern-Absicherung

Im Fokus der Kern-Absicherung stehen zunächst die besonders gefährdeten Geschäftsprozesse und Assets.

Komponenten

Als Komponenten werden im IT-Grundschutz technische Zielobjekte (siehe dort) oder Teile von Zielobjekten bezeichnet.

Kronjuwelen

Als Kronjuwelen werden solche Assets bezeichnet, deren Diebstahl, Zerstörung oder Kompromittierung einen existenzbedrohenden Schaden für die Institution bedeuten würde.

Kumulationseffekt

Der Kumulationseffekt beschreibt, dass sich der Schutzbedarf eines IT-Systems erhöhen kann, wenn durch Kumulation mehrerer (z. B. kleinerer) Schäden auf einem IT-System ein insgesamt höherer Gesamtschaden entstehen kann. Ein Auslöser kann auch sein, dass mehrere IT-Anwendungen bzw. eine Vielzahl sensitiver Informationen auf einem IT-System verarbeitet werden, so dass durch Kumulation von Schäden der Gesamtschaden höher sein kann.

Leitlinie zur Informationssicherheit

Die Leitlinie ist ein zentrales Dokument für die Informationssicherheit einer Institution. In ihr wird beschrieben, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Institution hergestellt werden soll. Sie beinhaltet die von der Institution angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Die Sicherheitsleitlinie beschreibt damit auch über die Sicherheitsziele das angestrebte Sicherheitsniveau in einer Behörde oder einem Unternehmen.

Mandantenfähigkeit

Als mandantenfähig werden Anwendungen, IT-Systeme oder auch Dienstleistungen bezeichnet, bei denen die Prozesse, Informationen und Anwendungen eines Mandanten strikt von denen anderer Kunden getrennt sind, also keine Zugriffe oder Störungen von dem einen in den anderen Bereich möglich sind und somit auch deren Vertraulichkeit, Integrität oder Verfügbarkeit nicht beeinträchtigt werden kann.

Maximum-Prinzip

Nach dem Maximum-Prinzip bestimmt der Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen den Schutzbedarf eines Geschäftsprozesses, einer Anwendung bzw. eines IT-Systems.

Modellierung

Bei den Vorgehensweisen nach IT-Grundschutz wird bei der Modellierung der betrachtete Informationsverbund eines Unternehmens oder einer Behörde mit Hilfe der Bausteine aus dem IT-Grundschutz-Kompendium nachgebildet. Hierzu enthält Kapitel 2.2 des IT-Grundschutz-Kompendiums für jeden Baustein einen Hinweis, auf welche Zielobjekte er anzuwenden ist und welche Voraussetzungen dabei gegebenenfalls zu beachten sind.

Netzplan

Ein Netzplan ist eine graphische Übersicht über die Komponenten eines Netzes und ihrer Verbindungen.

Nichtabstreitbarkeit (englisch "non repudiation")

Hierbei liegt der Schwerpunkt auf der Nachweisbarkeit gegenüber Dritten. Ziel ist es zu gewährleisten, dass der Versand und Empfang von Daten und Informationen nicht in Abrede gestellt werden kann. Es wird unterschieden zwischen

- Nichtabstreitbarkeit der Herkunft: Es soll einem Absender einer Nachricht unmöglich sein, das Absenden einer bestimmten Nachricht nachträglich zu bestreiten.
- Nichtabstreitbarkeit des Erhalts: Es soll einem Empfänger einer Nachricht unmöglich sein, den Erhalt einer gesendeten Nachricht nachträglich zu bestreiten.

Paketfilter

Paketfilter sind IT-Systeme mit spezieller Software, die den ein- und ausgehenden Datenverkehr in einem Netz anhand spezieller Regeln filtern. Aufgabe eines Paketfilters ist es, Datenpakete anhand der Informationen in den Header-Daten der UDP/IP- bzw. TCP/IP-Schicht (z. B. IP-Adresse und Portnummer) weiterzuleiten oder zu verwerfen. Diese Entscheidung treffen Paketfilter anhand der vom Anwen-

der vorgegebenen Filterregeln. Vielfach bieten die Paketfilter auch eine Möglichkeit zur "Network Address Translation" (NAT), bei der die Absender-Adressen von IP-Paketen durch eine IP-Adresse des Paketfilters ersetzt wird. Dadurch wird die Netzstruktur des zu schützenden Netzes verdeckt.

Patch

Ein Patch (vom englischen "patch", auf deutsch: Flicken) ist ein kleines Programm, das Softwarefehler wie z. B. Sicherheitslücken in Anwendungsprogrammen oder Betriebssystemen behebt.

Penetrationstest

Ein Penetrationstest ist ein gezielter, in der Regel simulierter, Angriffsversuch auf ein IT-System. Er wird als Wirksamkeitsprüfung vorhandener Sicherheitsmaßnahmen eingesetzt.

Privilegierte Berechtigungen

Privilegierte oder administrative Berechtigungen umfassen weitergehende Zugriffsmöglichkeiten auf IT-Systeme oder Software-Komponenten, als für normale Benutzer erforderlich sind. In der Regel werden privilegierte Berechtigungen nur solchen Rollen, Gruppen oder Personen zugewiesen, die überwiegend mit der Administration von Informationstechnik betraut sind. Dazu gehört unter anderem die betriebliche und/oder sicherheitstechnische Konfiguration.

Proxy

Ein Proxy ist eine Art Stellvertreter in Netzen. Er nimmt Daten von einer Seite an und leitet sie an eine andere Stelle im Netz weiter. Mittels eines Proxys lassen sich Datenströme filtern und gezielt weiterleiten.

Revision

Revision ist die systematische Überprüfung der Eignung und Einhaltung vorgegebener (Sicherheits-)Richtlinien. Die Revision sollte unabhängig und neutral sein.

Risiko

Risiko wird häufig definiert als die Kombination (also dem Produkt) aus der Häufigkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens. Der Schaden wird häufig als Differenz zwischen einem geplanten und ungeplanten Ergebnis dargestellt. Risiko ist eine spezielle Form der Unsicherheit oder besser Unwägbarkeit.

In der ISO wird Risiko auch als das Ergebnis von Unwägbarkeiten auf Zielobjekte definiert. In diesem Sinne wird daher auch von Konsequenzen statt von Schaden gesprochen, wenn Ereignisse anders eintreten als erwartet. Hierbei kann eine Konsequenz negativ (Schaden) oder positiv (Chance) sein. Die obige Definition hat sich allerdings als gängiger in der Praxis durchgesetzt.

Im Unterschied zu "Gefährdung" umfasst der Begriff "Risiko" bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.

Risikoanalyse

Als Risikoanalyse wird der komplette Prozess bezeichnet, um Risiken zu beurteilen (identifizieren, einschätzen und bewerten) sowie zu behandeln. Risikoanalyse bezeichnet nach den einschlägigen ISO-Normen ISO 31000 und ISO 27005 nur einen Schritt im Rahmen der Risikobeurteilung, die aus den folgenden Schritten besteht:

- Identifikation von Risiken (Risk Identification)
- Analyse von Risiken (Risk Analysis)
- Evaluation oder Bewertung von Risiken (Risk Evaluation)

Im deutschen Sprachgebrauch hat sich allerdings der Begriff Risikoanalyse für den kompletten Prozess der Risikobeurteilung und Risikobehandlung etabliert. Daher wird auch in diesem Dokument weiter der Begriff Risikoanalyse für den umfassenden Prozess benutzt.

Risikoappetit (Risikoneigung / Risikobereitschaft)

Risikoappetit bezeichnet die durch kulturelle, interne, externe oder wirtschaftliche Einflüsse entstandene Neigung einer Institution, wie sie Risiken bewertet und mit ihnen umgeht.

Risikobehandlungsplan

Die vollständige Erfüllung der im IT-Grundschutz geforderten Basis- und Standard-Anforderungen und gegebenenfalls die Anforderungen bei erhöhtem Schutzbedarf ist ein hoher Anspruch an jede Institution. In der Praxis lassen sich nicht alle Anforderungen erfüllen, sei es, dass Umstände vorliegen, die eine Erfüllung nicht sinnvoll erscheinen lassen (Neubeschaffung von Informationstechnik, Umzugspläne oder Ähnliches) oder dass eine Anforderung aus organisatorischen oder technischen Rahmenbedingungen nicht möglich ist (IT-System oder Anwendung werden nicht eingesetzt oder Ähnliches). Bestehende Defizite bei der Umsetzung von Sicherheitsmaßnahmen, die aus den Sicherheitsanforderungen resultieren und die damit verbundenen Risiken müssen in Form eines Managementberichtes dokumentiert werden, einschließlich einer Umsetzungsplanung für die weitere Behandlung der bestehenden Risiken. Der Risikobehandlungsplan sollte eine Beschreibung der geplanten Ressourcen und zeitliche Vorgaben enthalten. Er wird durch Unterschrift der Institutionsleitung genehmigt.

Die einzelnen Anforderungen aus dem Risikobehandlungsplan sollten mindestens einmal pro Jahr überprüft werden. Eine dauerhafte und unbefristete Übernahme von Risiken durch die Institutionsleitung muss vermieden werden, da sich im Bereich der Informationssicherheit die Risiken in kurzer Zeit verändern können. Eine unbefristete Übernahme von Risiken birgt die Gefahr, dass diese Risiken nur zu einem Stichtag geprüft und bewertet werden und eine erneute Betrachtung ausgeschlossen bleibt.

Risikomanagement

Als Risikomanagement werden alle Aktivitäten mit Bezug auf die strategische und operative Behandlung von Risiken bezeichnet, also alle Tätigkeiten, um Risiken für eine Institution zu identifizieren, zu steuern und zu kontrollieren.

Das strategische Risikomanagement beschreibt die wesentlichen Rahmenbedingungen, wie die Behandlung von Risiken innerhalb einer Institution, die Kultur zum Umgang mit Risiken und die Methodik ausgestaltet sind. Diese Grundsätze für die Behandlung von Risiken innerhalb eines ISMS müssen mit den Rahmenbedingungen des organisationsweiten Risikomanagements übereinstimmen bzw. aufeinander abgestimmt sein.

Die Rahmenbedingungen des operativen Risikomanagements umfassen den Regelprozess aus

- Identifikation von Risiken,
- Einschätzung und Bewertung von Risiken,
- Behandlung von Risiken,
- Überwachung von Risiken und
- Risikokommunikation.

Schaden / Konsequenz

Eine Abweichung von einem erwarteten Ergebnis führt zu einer Konsequenz (häufig "Schaden" genannt). Hierbei kann es sich grundsätzlich um eine positive oder negative Abweichung handeln.

Eine positive Konsequenz / positiver Schaden im Sinne der Chancen- und Risikoanalyse wird auch als Chance bezeichnet. Meistens werden in der Risikoanalyse jedoch die negativen Konsequenzen, also die Schäden, betrachtet.

Das Ausmaß eines Schadens wird als Schadenshöhe definiert und kann als bezifferbar oder nicht direkt bezifferbar betitelt werden. Die bezifferbaren Schäden können in der Regel mit direkten Aufwänden (z. B. finanzieller Art) dargestellt werden. Zu den nicht direkt bezifferbaren Schäden gehören z. B. Imageschäden oder Opportunitätskosten. Bei diesen lässt sich die tatsächliche Schadenshöhe häufig nur vermuten oder schätzen. Alle Angaben werden in der Regel aufgrund von Erfahrungs- oder Branchenwerten in Kategorien klassifiziert.

Schadfunktion

Mit Schadfunktion wird eine vom Anwender ungewünschte Funktion bezeichnet, die die Informationssicherheit unbeabsichtigt oder bewusst gesteuert gefährden kann.

Schadprogramm / Schadsoftware / Malware

Die Begriffe Schadfunktion, Schadprogramm, Schadsoftware und Malware werden häufig synonym benutzt. Malware ist ein Kunstwort, abgeleitet aus "Malicious software" und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Beispiele sind Computer-Viren, Würmer und Trojanische Pferde. Schadsoftware ist üblicherweise für eine bestimmte Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.

Schutzbedarf

Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.

Schutzbedarfsfeststellung

Bei der Schutzbedarfsfeststellung wird der Schutzbedarf der Geschäftsprozesse, der verarbeiteten Informationen und der IT-Komponenten bestimmt. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung der Grundwerte der Informationssicherheit – Vertraulichkeit, Integrität oder Verfügbarkeit – entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien "normal", "hoch" und "sehr hoch".

Schwachstelle (englisch "vulnerability")

Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.

Server

Als Server wird Soft- oder Hardware bezeichnet, die bestimmte Dienste anderen (nämlich Clients) anbietet. Typischerweise wird damit ein Rechner bezeichnet, der seine Hardware- und Software-Ressourcen in einem Netz anderen Rechnern zugänglich macht. Beispiele sind Applikations-, Daten-, Web- oder E-Mail-Server.

Sicherheitsgateway

Ein Sicherheitsgateway (oft auch Firewall genannt) ist ein System aus soft- und hardware-technischen Komponenten. Es gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer Sicherheitsrichtlinie als ordnungsgemäß definierte Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei im Wesentlichen, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen und die übertragenen Daten kontrolliert werden.

Sicherheitsanforderung

Als Sicherheitsanforderung werden Anforderungen für den organisatorischen, personellen, infrastrukturellen und technischen Bereich bezeichnet, deren Erfüllung zur Erhöhung der Informationssicherheit notwendig ist bzw. dazu beiträgt. Eine Sicherheitsanforderung beschreibt also, was getan werden muss, um ein bestimmtes Niveau bezüglich der Informationssicherheit zu erreichen. Wie die Anforderungen im konkreten Fall erfüllt werden können, ist in entsprechenden Sicherheitsmaßnahmen beschrieben (siehe dort). Im englischen Sprachraum wird für Sicherheitsanforderungen häufig der Begriff "control" verwendet.

Der IT-Grundschutz unterscheidet zwischen Basis-Anforderungen, Standard-Anforderungen und Anforderungen bei erhöhtem Schutzbedarf. Basis-Anforderungen sind fundamental und stets umzusetzen, sofern nicht gravierende Gründe dagegen sprechen. Standard-Anforderungen sind für den normalen Schutzbedarf grundsätzlich umzusetzen, sofern sie nicht durch mindestens gleichwertige Alternativen oder die bewusste Akzeptanz des Restrisikos ersetzt werden. Anforderungen bei erhöhtem Schutzbedarf sind exemplarische Vorschläge, was bei entsprechendem Schutzbedarf zur Absicherung sinnvoll umzusetzen ist.

Sicherheitskonzept

Ein Sicherheitskonzept dient zur Umsetzung der Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Institution zu erreichen. Das Sicherheitskonzept ist das zentrale Dokument im Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete Sicherheitsmaßnahme muss sich letztlich darauf zurückführen lassen.

Sicherheitskonzeption

Die Erstellung einer Sicherheitskonzeption ist eine der zentralen Aufgaben des Informationssicherheitsmanagements. Aufbauend auf den Ergebnissen von Strukturanalyse und Schutzbedarfsfeststellung werden hier die erforderlichen Sicherheitsmaßnahmen identifiziert und im Sicherheitskonzept dokumentiert.

Sicherheitsmaßnahme

Mit Sicherheitsmaßnahme (kurz Maßnahme) werden alle Aktionen bezeichnet, die dazu dienen, um Sicherheitsrisiken zu steuern und um diesen entgegenzuwirken. Dies schließt sowohl organisatorische, als auch personelle, technische oder infrastrukturelle Sicherheitsmaßnahmen ein. Sicherheitsmaßnahmen dienen zur Erfüllung von Sicherheitsanforderungen (siehe dort). Synonym werden auch die Begriffe Sicherheitsvorkehrung oder Schutzmaßnahme benutzt. Als englische Übersetzung wurde "safeguard", "security measure" oder "measure" gewählt.

Sicherheitsrichtlinie (englisch "Security Policy")

In einer Sicherheitsrichtlinie werden Schutzziele und allgemeine Sicherheitsanforderungen im Sinne offizieller Vorgaben eines Unternehmens oder einer Behörde formuliert. Detaillierte Sicherheitsmaßnahmen sind in einem umfangreicheren Sicherheitskonzept enthalten.

Spyware

Als Spyware werden Programme bezeichnet, die heimlich, also ohne darauf hinzuweisen, Informationen über einen Benutzer bzw. die Nutzung eines Rechners sammeln und an den Urheber der Spyware weiterleiten. Spyware gilt häufig nur als lästig, es sollte aber nicht übersehen werden, dass durch Spyware auch sicherheitsrelevante Informationen wie Passwörter ausgeforscht werden können.

Standard-Absicherung

Die Standard-Absicherung entspricht im Wesentlichen der klassischen IT-Grundschutz-Vorgehensweise. Mit der Standard-Absicherung kann ein ISB die Assets und Prozesse einer Institution sowohl umfassend als auch in der Tiefe absichern.

Standard-Anforderung

Siehe Sicherheitsanforderung.

Standardsoftware

Unter Standardsoftware wird Software (Programme, Programm-Module, Tools etc.) verstanden, die für die Bedürfnisse einer Mehrzahl von Kunden am Markt und nicht speziell vom Auftragnehmer für den Auftraggeber entwickelt wurde, einschließlich der zugehörigen Dokumentation. Sie zeichnet sich außerdem dadurch aus, dass sie vom Anwender selbst installiert werden soll und dass nur geringer Aufwand für die anwenderspezifische Anpassung notwendig ist.

Starke Authentisierung

Starke Authentisierung bezeichnet die Kombination von zwei oder mehr Authentisierungstechniken, wie Passwort plus Transaktionsnummern (Einmalpasswörter) oder plus Chipkarte. Daher wird dies auch häufig als Zwei- oder Mehr-Faktor-Authentisierung bezeichnet.

Strukturanalyse

In einer Strukturanalyse werden die erforderlichen Informationen über den ausgewählten Informationsverbund, die Geschäftsprozesse, Anwendungen, IT-Systeme, Netze, Räume, Gebäude und Verbindungen erfasst und so aufbereitet, dass sie die weiteren Schritte gemäß IT-Grundschutz unterstützen.

Trojanisches Pferd

Ein Trojanisches Pferd, oft auch (fälschlicherweise) kurz Trojaner genannt, ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.

Verbindlichkeit

Unter Verbindlichkeit werden die Sicherheitsziele Authentizität und Nichtabstreitbarkeit zusammengefasst. Bei der Übertragung von Informationen bedeutet dies, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann.

Verfügbarkeit

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

Verschlüsselung

Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation - die Zurückgewinnung des Klartextes aus dem Geheimtext - wird Entschlüsselung genannt.

Verteilungseffekt

Der Verteilungseffekt kann sich auf den Schutzbedarf relativierend auswirken, wenn zwar eine Anwendung einen hohen Schutzbedarf besitzt, ihn aber deshalb nicht auf ein betrachtetes IT-System überträgt, weil auf diesem IT-System nur unwesentliche Teilbereiche der Anwendung laufen.

Vertraulichkeit

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

VLAN

Virtuelle lokale Netze (Virtual LANs, VLANs) werden zur logischen Strukturierung von Netzen verwendet. Dabei wird innerhalb eines physikalischen Netzes eine logische Netzstruktur abgebildet, indem funktionell zusammengehörende Arbeitsstationen und Server zu einem virtuellen Netz verbunden werden.

VPN

Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes (oft des Internet) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In VPNs können unter Zuhilfenahme kryptographischer Verfahren die Integrität und Vertraulichkeit von Daten geschützt und die Kommunikationspartner sicher authentisiert werden, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.

Der Begriff VPN wird oft als Bezeichnung für verschlüsselte Verbindungen verwendet, zur Absicherung des Transportkanals können jedoch auch andere Methoden eingesetzt werden, beispielsweise spezielle Funktionen des genutzten Transportprotokolls.

Wert (englisch "asset")

Werte sind alles, was wichtig für eine Institution ist (Vermögen, Wissen, Gegenstände, Gesundheit).

WLAN

Mit WLAN werden drahtlose Netze bezeichnet, die auf der als IEEE 802.11 bezeichneten Gruppe von Standards basieren, die vom Institute of Electrical and Electronics Engineers (IEEE) spezifiziert wurden.

Wurm

Bei (Computer-, Internet-, E-Mail-)Würmern handelt es sich um Schadsoftware, ähnlich einem Virus, die sich selbst reproduziert und sich durch Ausnutzung der Kommunikationsschnittstellen selbstständig verbreitet.

Zertifikat

Der Begriff Zertifikat wird in der Informationssicherheit in verschiedenen Bereichen mit unterschiedlichen Bedeutungen verwendet. Zu unterscheiden sind vor allem:

- ISO 27001-Zertifikate: Der ISO-Standard 27001 "Information technology - Security techniques - Information security management systems requirements specification" ermöglicht eine Zertifizierung des Informationssicherheitsmanagements.
- ISO 27001-Zertifikate auf der Basis von IT-Grundschutz: Damit kann dokumentiert werden, dass für den betrachteten Informationsverbund alle relevanten Sicherheitsanforderungen gemäß IT-Grundschutz realisiert wurden. Voraussetzung für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist eine Überprüfung durch einen vom BSI zertifizierten ISO 27001-IT-Grundschutz-Auditor. Zu den Aufgaben eines ISO 27001-IT-Grundschutz-Auditors gehören eine Sichtung der von der Institution erstellten Referenzdokumente, die Durchführung einer Vor-Ort-Prüfung und die Erstellung eines Audit-Reports. Die Zertifizierungsstelle BSI stellt aufgrund des Audit-Reports fest, ob die notwendigen Sicherheitsanforderungen umgesetzt sind, erteilt im positiven Falle ein Zertifikat und veröffentlicht es.
- Schlüsselzertifikat: Ein Schlüsselzertifikat ist eine elektronische Bescheinigung, mit der Signaturprüfschlüssel einer Person zugeordnet werden. Bei digitalen Signaturen wird ein Zertifikat als Bestätigung einer vertrauenswürdigen dritten Partei benötigt, um nachzuweisen, dass die zur Erzeugung der Digitalen Signatur eingesetzten kryptographischen Schlüssel wirklich zu dem Unterzeichnenden gehören.

- Zertifikate für IT-Produktsicherheit: Zertifiziert wird nach international anerkannten Sicherheitskriterien, wie z. B. den Common Criteria (ISO/IEC 15408). Auf dieser Basis können Produkte und Systeme unterschiedlichster Art evaluiert werden. Eine wesentliche Voraussetzung ist jedoch, dass die am Ende des Verfahrens im Zertifikat zu bestätigenden Sicherheitseigenschaften im Zusammenhang mit der Wahrung von Vertraulichkeit, Verfügbarkeit und Integrität stehen.

Zielobjekt

Zielobjekte sind Teile des Informationsverbunds, denen im Rahmen der Modellierung ein oder mehrere Bausteine aus dem IT-Grundschutz-Kompendium zugeordnet werden können. Zielobjekte können dabei physische Objekte sein, wie beispielsweise Netze oder IT-Systeme. Häufig sind Zielobjekte jedoch logische Objekte, wie beispielsweise Organisationseinheiten, Anwendungen oder der gesamte Informationsverbund.

Zugang

Mit Zugang wird die Nutzung von IT-Systemen, System-Komponenten und Netzen bezeichnet. Zugangsberechtigungen erlauben somit einer Person, bestimmte Ressourcen wie IT-Systeme bzw. System-Komponenten und Netze zu nutzen.

Zugriff

Mit Zugriff wird die Nutzung von Informationen bzw. Daten bezeichnet. Über Zugriffsberechtigungen wird geregelt, welche Personen im Rahmen ihrer Funktionen oder welche IT-Anwendungen bevollmächtigt sind, Informationen, Daten oder auch IT-Anwendungen, zu nutzen oder Transaktionen auszuführen.

Zutritt

Mit Zutritt wird das Betreten von abgegrenzten Bereichen wie z. B. Räumen oder geschützten Arealen in einem Gelände bezeichnet. Zutrittsberechtigungen erlauben somit Personen, bestimmte Umgebungen zu betreten, also beispielsweise ein Gelände, ein Gebäude oder definierte Räume eines Gebäudes.

Gefährdungsübersicht

G 0.01	Feuer	59
G 0.02	Ungünstige klimatische Bedingungen	60
G 0.03	Wasser	61
G 0.04	Verschmutzung, Staub, Korrosion	62
G 0.05	Naturkatastrophen	63
G 0.06	Katastrophen im Umfeld	64
G 0.07	Großereignisse im Umfeld	65
G 0.08	Ausfall oder Störung der Stromversorgung	66
G 0.09	Ausfall oder Störung von Kommunikationsnetzen	67
G 0.10	Ausfall oder Störung von Versorgungsnetzen	68
G 0.11	Ausfall oder Störung von Dienstleistern	69
G 0.12	Elektromagnetische Störstrahlung	70
G 0.13	Abfangen kompromittierender Strahlung	71
G 0.14	Ausspähen von Informationen (Spionage)	72
G 0.15	Abhören	73
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	74
G 0.17	Verlust von Geräten, Datenträgern oder Dokumenten	75
G 0.18	Fehlplanung oder fehlende Anpassung	76
G 0.19	Offenlegung schützenswerter Informationen	77
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle	79
G 0.21	Manipulation von Hard- oder Software	80
G 0.22	Manipulation von Informationen	81
G 0.23	Unbefugtes Eindringen in IT-Systeme	82
G 0.24	Zerstörung von Geräten oder Datenträgern	83
G 0.25	Ausfall von Geräten oder Systemen	84
G 0.26	Fehlfunktion von Geräten oder Systemen	85
G 0.27	Ressourcenmangel	86
G 0.28	Software-Schwachstellen oder -Fehler	87
G 0.29	Verstoß gegen Gesetze oder Regelungen	88
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	89

G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	**90**
G 0.32	Missbrauch von Berechtigungen	**91**
G 0.33	Personalausfall	**92**
G 0.34	Anschlag	**93**
G 0.35	Nötigung, Erpressung oder Korruption	**94**
G 0.36	Identitätsdiebstahl	**95**
G 0.37	Abstreiten von Handlungen	**96**
G 0.38	Missbrauch personenbezogener Daten	**97**
G 0.39	Schadprogramme	**98**
G 0.40	Verhinderung von Diensten (Denial of Service)	**99**
G 0.41	Sabotage	**100**
G 0.42	Social Engineering	**101**
G 0.43	Einspielen von Nachrichten	**102**
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	**103**
G 0.45	Datenverlust	**104**
G 0.46	Integritätsverlust schützenswerter Informationen	**105**
G 0.47	Schädliche Seiteneffekte IT-gestützter Angriffe	**107**

Elementare Gefährdungen

G 0.01 Feuer

Feuer können schwere Schäden an Menschen, Gebäuden und deren Einrichtung verursachen. Neben direkten durch Feuer verursachten Schäden lassen sich Folgeschäden aufzeigen, die insbesondere für die Informationstechnik in ihrer Schadenswirkung ein katastrophales Ausmaß erreichen können. Löschwasserschäden treten beispielsweise nicht nur an der Brandstelle auf. Sie können auch in tiefer liegenden Gebäudeteilen entstehen. Bei der Verbrennung von PVC entstehen Chlorgase, die zusammen mit der Luftfeuchtigkeit und dem Löschwasser Salzsäure bilden. Werden die Salzsäuredämpfe über die Klimaanlage verteilt, können auf diese Weise Schäden an empfindlichen elektronischen Geräten entstehen, die in einem vom Brandort weit entfernten Teil des Gebäudes stehen. Aber auch "normaler" Brandrauch kann auf diesem Weg beschädigend auf die IT-Einrichtung einwirken.

Ein Brand entsteht nicht nur durch den fahrlässigen Umgang mit Feuer (z. B. durch unbeaufsichtigte offene Flammen, Schweiß- und Lötarbeiten), sondern auch durch unsachgemäße Benutzung elektrischer Einrichtungen (z. B. unbeaufsichtigte Kaffeemaschine, Überlastung von Mehrfachsteckdosen). Technische Defekte an elektrischen Geräten können ebenfalls zu einem Brand führen.

Die Ausbreitung eines Brandes kann unter anderem begünstigt werden durch:

- Aufhalten von Brandabschnittstüren durch Keile,
- unsachgemäße Lagerung brennbarer Materialien (z. B. Altpapier),
- Nichtbeachtung der einschlägigen Normen und Vorschriften zur Brandvermeidung,
- fehlende Brandmeldeeinrichtungen (z. B. Rauchmelder),
- fehlende oder nicht einsatzbereite Handfeuerlöscher oder automatische Löscheinrichtungen (z. B. Gaslöschanlagen),
- mangelhaften vorbeugenden Brandschutz (z. B. Fehlen von Brandabschottungen auf Kabeltrassen oder Verwendung ungeeigneter Dämmmaterialien zur Wärme- und Schallisolierung).

Beispiele:

- Anfang der 90er Jahre erlitt im Frankfurter Raum ein Großrechenzentrum einen katastrophalen Brandschaden, der zu einem kompletten Ausfall führte.
- Immer wieder kommt es vor, dass elektrische Kleingeräte, wie z. B. Kaffeemaschinen oder Tischleuchten, unsachgemäß installiert oder aufgestellt sind und dadurch Brände verursachen.

Elementare Gefährdungen

G 0.02 Ungünstige klimatische Bedingungen

Ungünstige klimatische Bedingungen wie Hitze, Frost oder hohe Luftfeuchtigkeit können zu Schäden verschiedenster Art führen, beispielsweise zu Fehlfunktionen in technischen Komponenten oder zur Beschädigung von Speichermedien. Häufige Schwankungen der klimatischen Bedingungen verstärken diesen Effekt. Ungünstige klimatische Bedingungen können auch dazu führen, dass Menschen nicht mehr arbeiten können oder sogar verletzt oder getötet werden.

Jeder Mensch und jedes technische Gerät hat einen Temperaturbereich, innerhalb dessen seine normale Arbeitsweise bzw. ordnungsgemäße Funktion gewährleistet ist. Überschreitet die Umgebungstemperatur die Grenzen dieses Bereiches nach oben oder unten, kann es zu Arbeitsausfällen, Betriebsstörungen oder zu Geräteausfällen kommen.

Zu Lüftungszwecken werden oft unerlaubt Fenster von Serverräumen geöffnet. In der Übergangszeit (Frühjahr, Herbst) kann das bei großen Temperaturschwankungen dazu führen, dass durch starke Abkühlung die zulässige Luftfeuchte überschritten wird.

Beispiele:

- Bei hochsommerlichen Temperaturen und unzureichender Kühlung kann es bei IT-Geräten zu temperaturbedingten Ausfällen kommen.
- Zu viel Staub in IT-Systemen kann zu einem Hitzestau führen.
- Durch zu hohe Temperaturen können magnetische Datenträger entmagnetisiert werden.

Elementare Gefährdungen

G 0.03 Wasser

Durch Wasser kann die Integrität und Verfügbarkeit von Informationen beeinträchtigt werden, die auf analogen und digitalen Datenträgern gespeichert sind. Auch Informationen im Arbeitsspeicher von IT-Systemen sind gefährdet. Der unkontrollierte Eintritt von Wasser in Gebäude oder Räume kann beispielsweise bedingt sein durch:

- Störungen in der Wasser-Versorgung oder Abwasser-Entsorgung,
- Defekte der Heizungsanlage,
- Defekte an Klimaanlagen mit Wasseranschluss,
- Defekte in Sprinkleranlagen,
- Löschwasser bei der Brandbekämpfung und
- Wassersabotage z. B. durch Öffnen der Wasserhähne und Verstopfen der Abflüsse.

Unabhängig davon, auf welche Weise Wasser in Gebäude oder Räume gelangt, besteht die Gefahr, dass Versorgungseinrichtungen oder IT-Komponenten beschädigt oder außer Betrieb gesetzt werden (Kurzschluss, mechanische Beschädigung, Rost etc.). Besonders wenn zentrale Einrichtungen der Gebäudeversorgung (Hauptverteiler für Strom, Telefon, Daten) in Kellerräumen ohne selbsttätige Entwässerung untergebracht sind, kann eindringendes Wasser sehr hohe Schäden verursachen.

Probleme können außerdem durch Frost entstehen. Beispielsweise können Rohre in frostgefährdeten Bereichen undicht werden, wenn darin Wasser bei anhaltendem Frost stillsteht. Auch eine vorhandene Wärmedämmung wird mit der Zeit vom Frost überwunden.

Beispiel:

- In einem Serverraum verlief eine Wasserleitung unterhalb der Decke, die mit Gipskartonelementen verkleidet war. Als eine Verbindung der Wasserleitung undicht wurde, wurde dies nicht rechtzeitig erkannt. Das austretende Wasser sammelte sich zunächst an der tiefsten Stelle der Verkleidung, bevor es dort austrat und im darunter angebrachten Stromverteiler einen Kurzschluss verursachte. Dies führte dazu, dass bis zur endgültigen Reparatur sowohl die Wasser- als auch die Stromversorgung des betroffenen Gebäudeteils komplett abgeschaltet werden musste.

Elementare Gefährdungen

G 0.04 Verschmutzung, Staub, Korrosion

Viele IT-Geräte enthalten neben der Elektronik auch mechanisch arbeitende Komponenten, wie z. B. bei Fest- und Wechselplatten, DVD-Laufwerken, Druckern, Scannern etc., aber auch Lüftern von Prozessoren und Netzteilen. Mit steigenden Anforderungen an die Qualität und die Schnelligkeit müssen diese Geräte immer präziser arbeiten. Bereits geringfügige Verunreinigungen können zu einer Störung eines Gerätes führen. Staub und Verschmutzungen können beispielsweise durch folgende Tätigkeiten in größerem Maße entstehen:

- Arbeiten an Wänden, Doppelböden oder anderen Gebäudeteilen,
- Umrüstungsarbeiten an der Hardware bzw.
- Entpackungsaktionen von Geräten (z. B. aufwirbelndes Styropor).

Vorhandene Sicherheitsschaltungen in den Geräten führen meist zu einem rechtzeitigen Abschalten. Das hält zwar den direkten Schaden am Gerät, die Instandsetzungskosten und die Ausfallzeiten klein, führt aber dazu, dass das betroffene Gerät nicht verfügbar ist.

Die Geräte und die Infrastruktur können außerdem durch Korrosion angegriffen werden. Dies kann sich nicht nur auf die IT, sondern sogar auf die Sicherheit von Gebäuden negativ auswirken.

Durch Korrosion können auch indirekt weitere Gefährdungen entstehen. So kann beispielsweise Wasser aus korrodierten Stellen austreten (siehe G 0.3 Wasser).

Insgesamt können Verschmutzung, Staub oder Korrosion somit zu Ausfällen oder Beschädigungen von IT-Komponenten und Versorgungseinrichtungen führen. Als Folge kann die ordnungsgemäße Informationsverarbeitung beeinträchtigt werden.

Beispiele:

- Bei der Aufstellung eines Servers in einem Medienraum, zusammen mit einem Kopierer und einem Faxgerät, traten nacheinander die Lähmung des Prozessor-Lüfters und des Netzteil-Lüfters aufgrund der hohen Staubbelastung des Raumes auf. Der Ausfall des Prozessor-Lüfters führte zu sporadischen Server-Abstürzen. Der Ausfall des Netzteil-Lüfters führte schließlich zu einer Überhitzung des Netzteils mit der Folge eines Kurzschlusses, was schließlich einen Totalausfall des Servers nach sich zog.
- Um eine Wandtafel in einem Büro aufzuhängen, wurden von der Haustechnik Löcher in die Wand gebohrt. Der Mitarbeiter hatte hierzu sein Büro für kurze Zeit verlassen. Nach Rückkehr an seinen Arbeitsplatz stellte er fest, dass sein PC nicht mehr funktionierte. Ursache hierfür war Bohrstaub, der durch die Lüftungsschlitze in das PC-Netzteil eingedrungen war.

Elementare Gefährdungen

G 0.05 Naturkatastrophen

Unter Naturkatastrophen werden natürliche Veränderungen verstanden, die verheerende Auswirkungen auf Menschen und Infrastrukturen haben. Ursachen für eine Naturkatastrophe können seismische, klimatische oder vulkanische Phänomene sein, wie beispielsweise Erdbeben, Hochwasser, Erdrutsche, Tsunamis, Lawinen und Vulkanausbrüche. Beispiele für extreme meteorologische Phänomene sind Unwetter, Orkane oder Zyklone. Je nach Standort der Institution ist diese den Risiken durch die verschiedenen Arten von Naturkatastrophen unterschiedlich stark ausgesetzt.

Beispiele:

- Für Rechenzentren in Hochwasser-gefährdeten Gebieten besteht oft in besonderem Maße die Gefahr, dass unkontrolliert Wasser in das Gebäude eindringt (Überschwemmungen oder Anstieg des Grundwasserspiegels).
- Die Häufigkeit von Erdbeben und somit auch das damit verbundene Risiko hängen stark von der geografischen Lage ab.
- Extrem erhöhte Solar-Aktivität hat in der Vergangenheit bereits mehrfach zu Beeinträchtigungen von Telekommunikationsinfrastrukturen und der Energieversorgung geführt.

Unabhängig von der Art der Naturkatastrophe besteht auch in nicht unmittelbar betroffenen Gebieten die Gefahr, dass Versorgungseinrichtungen, Kommunikationsverbindungen oder IT-Komponenten beschädigt oder außer Betrieb gesetzt werden. Besonders der Ausfall zentraler Einrichtungen der Gebäudeversorgung (Hauptverteiler für Strom, Telefon, Daten) kann sehr hohe Schäden nach sich ziehen. Betriebs- und Service-Personal kann aufgrund von großflächig eingerichteten Sperrbereichen der Zutritt zur Infrastruktur verwehrt werden.

Beispiele:

- Viele Gewerbebetriebe, auch große Unternehmen, tragen der Hochwassergefährdung nicht hinreichend Rechnung. So wurde ein Unternehmen bereits mehrere Male durch Hochwasserschäden am Rechenzentrum "überrascht". Das Rechenzentrum schwamm im wahrsten Sinne des Wortes innerhalb von 14 Monaten zum zweiten Mal davon. Der entstandene Schaden belief sich auf mehrere hunderttausend Euro und ist von keiner Versicherung gedeckt.
- Ein IT-System wird an einem Standort untergebracht, dessen geografische Lage für vulkanische Aktivität bekannt ist (zeitweilig aussetzendes Phänomen, bei dem die Emissionsphasen mit zum Teil langen Ruhephasen abwechseln).

Elementare Gefährdungen

G 0.06 Katastrophen im Umfeld

Eine Behörde bzw. ein Unternehmen kann Schaden nehmen, wenn sich im Umfeld ein schwerer Unglücksfall ereignet, zum Beispiel ein Brand, eine Explosion, die Freisetzung giftiger Substanzen oder das Austreten gefährlicher Strahlung. Gefahr besteht dabei nicht nur durch das Ereignis selbst, sondern auch durch die häufig daraus resultierenden Aktivitäten, beispielsweise Sperrungen oder Rettungsmaßnahmen.

Die Liegenschaften einer Institution können verschiedenen Gefährdungen aus dem Umfeld ausgesetzt sein, unter anderem durch Verkehr (Straßen, Schiene, Luft, Wasser), Nachbarbetriebe oder Wohngebiete.

Vorbeugungs- oder Rettungsmaßnahmen können die Liegenschaften dabei direkt betreffen. Solche Maßnahmen können auch dazu führen, dass Mitarbeiter ihre Arbeitsplätze nicht erreichen können oder Personal evakuiert werden muss. Durch die Komplexität der Haustechnik und der IT-Einrichtungen kann es aber auch zu indirekten Problemen kommen.

Beispiel:

- Bei einem Brand in einem chemischen Betrieb in unmittelbarer Nähe eines Rechenzentrums (ca. 1000 m Luftlinie) entstand eine mächtige Rauchwolke. Das Rechenzentrum besaß eine Klima- und Lüftungsanlage, die über keine Außenluftüberwachung verfügte. Nur durch die Aufmerksamkeit eines Mitarbeiters (der Unfall geschah während der Arbeitszeit), der die Entstehung und Ausbreitung verfolgte, konnte die Außenluftzufuhr rechtzeitig manuell abgeschaltet werden.

Elementare Gefährdungen

G 0.07 Großereignisse im Umfeld

Großveranstaltungen aller Art können zu Behinderungen des ordnungsgemäßen Betriebs einer Behörde bzw. eines Unternehmens führen. Hierzu gehören unter anderem Straßenfeste, Konzerte, Sportveranstaltungen, Arbeitskämpfe oder Demonstrationen. Ausschreitungen im Zusammenhang mit solchen Veranstaltungen können zusätzliche Auswirkungen, wie die Einschüchterung von Mitarbeitern bis hin zur Gewaltanwendung gegen das Personal oder das Gebäude, nach sich ziehen.

Beispiele:

- Während der heißen Sommermonate fand eine Demonstration in der Nähe eines Rechenzentrums statt. Die Situation eskalierte und es kam zu Gewalttätigkeiten. In einer Nebenstraße stand noch ein Fenster des Rechenzentrumsbereiches auf, durch das ein Demonstrant eindrang und die Gelegenheit nutzte, Hardware mit wichtigen Daten zu entwenden.
- Beim Aufbau einer Großkirmes wurde aus Versehen eine Stromleitung gekappt. Dies führte in einem hierdurch versorgten Rechenzentrum zu einem Ausfall, der jedoch durch die vorhandene Netzersatzanlage abgefangen werden konnte.

Elementare Gefährdungen

G 0.08 Ausfall oder Störung der Stromversorgung

Trotz hoher Versorgungssicherheit kommt es immer wieder zu Unterbrechungen der Stromversorgung seitens der Verteilungsnetzbetreiber (VNB) bzw. Energieversorgungsunternehmen (EVU). Die größte Zahl dieser Störungen ist mit Zeiten unter einer Sekunde so kurz, dass der Mensch sie nicht bemerkt. Aber schon Unterbrechungen von mehr als 10 ms sind geeignet, den IT-Betrieb zu stören. Neben Störungen im Versorgungsnetz können jedoch auch Abschaltungen bei nicht angekündigten Arbeiten oder Kabelbeschädigungen bei Tiefbauarbeiten dazu führen, dass die Stromversorgung ausfällt.

Von der Stromversorgung sind nicht nur die offensichtlichen, direkten Stromverbraucher (PC, Beleuchtung usw.) abhängig. Viele Infrastruktur-Einrichtungen sind heute vom Strom abhängig, z.B. Aufzüge, Klimatechnik, Gefahrenmeldeanlagen, Sicherheitsschleusen, automatische Türschließanlagen und Sprinkleranlagen. Selbst die Wasserversorgung in Hochhäusern ist wegen der zur Druck-Erzeugung in den oberen Etagen erforderlichen Pumpen stromabhängig. Bei längeren Stromausfällen kann der Ausfall der Infrastruktur-Einrichtungen dazu führen, dass keinerlei Tätigkeiten mehr in den betroffenen Räumlichkeiten durchgeführt werden können.

Neben Ausfällen können auch andere Störungen der Stromversorgung den Betrieb beeinträchtigen. Überspannung kann beispielsweise zu Fehlfunktionen oder sogar zu Beschädigungen von elektrischen Geräten führen.

Zu beachten ist außerdem, dass durch Ausfälle oder Störungen der Stromversorgung in der Nachbarschaft unter Umständen auch die eigenen Geschäftsprozesse betroffen sein können, beispielsweise wenn Zufahrtswege blockiert werden.

Beispiele:

- Durch einen Fehler in der USV eines Rechenzentrums schaltete diese nach einem kurzen Stromausfall nicht auf Normalbetrieb zurück. Nach Entladung der Batterien (nach etwa 40 Minuten) fielen alle Rechner im betroffenen Server-Saal aus.
- Anfang 2001 gab es über 40 Tage einen Strom-Notstand in Kalifornien. Die Stromversorgungslage war dort so angespannt, dass die Kalifornische Netzüberwachungsbehörde rotierende Stromabschaltungen anordnete. Von diesen Stromabschaltungen, die bis zu 90 Minuten andauerten, waren nicht nur Haushalte, sondern auch die High-Tech-Industrie betroffen. Weil mit dem Stromausfall auch Alarmanlagen und Überwachungskameras ausgeschaltet wurden, hielten die Energieversorger ihre Abschaltpläne geheim.
- Im November 2005 waren nach heftigen Schneefällen in Niedersachsen und Nordrhein-Westfalen viele Gemeinden tagelang ohne Stromversorgung, weil viele Hochspannungsmasten unter der Schnee- und Eislast umgestürzt waren. Die Wiederherstellung der Stromversorgung dauerte einige Tage.

Elementare Gefährdungen

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

Für viele Geschäftsprozesse werden heutzutage zumindest zeitweise intakte Kommunikationsverbindungen benötigt, sei es über Telefon, Fax, E-Mail oder andere Dienste über Nah- oder Weitverkehrsnetze. Fallen einige oder mehrere dieser Kommunikationsverbindungen über einen längeren Zeitraum aus, kann dies beispielsweise dazu führen, dass

- Geschäftsprozesse nicht mehr weiterbearbeitet werden können, weil benötigte Informationen nicht abgerufen werden können,
- Kunden die Institution nicht mehr für Rückfragen erreichen können,
- Aufträge nicht abgegeben oder beendet werden können.

Werden auf IT-Systemen, die über Weitverkehrsnetze verbunden sind, zeitkritische Anwendungen betrieben, sind die durch einen Netzausfall möglichen Schäden und Folgeschäden entsprechend hoch, wenn keine Ausweichmöglichkeiten (z. B. Anbindung an ein zweites Kommunikationsnetz) vorhanden sind.

Zu ähnlichen Problemen kann es kommen, wenn die benötigten Kommunikationsnetze gestört sind, ohne jedoch vollständig auszufallen. Kommunikationsverbindungen können beispielsweise eine erhöhte Fehlerrate oder andere Qualitätsmängel aufweisen. Falsche Betriebsparameter können ebenfalls zu Beeinträchtigungen führen.

Beispiele:

- Das Internet ist heute für viele Institutionen zu einem unverzichtbaren Kommunikationsmedium geworden, unter anderem zum Abruf wichtiger Informationen, zur Außendarstellung sowie zur Kommunikation mit Kunden und Partnern. Unternehmen, die sich auf Internet-basierte Dienstleistungen spezialisiert haben, sind natürlich in besonderem Maße von einer funktionierenden Internet-Anbindung abhängig.
- Im Zuge der Konvergenz der Netze werden Sprach- und Datendienste häufig über die gleichen technischen Komponenten transportiert (z. B. VoIP). Dadurch steigt jedoch die Gefahr, dass bei einer Störung der Kommunikationstechnik die Sprachdienste und die Datendienste gleichzeitig ausfallen.

Elementare Gefährdungen

G 0.10 Ausfall oder Störung von Versorgungsnetzen

Es gibt in einem Gebäude eine Vielzahl von Netzen, die der grundlegenden Ver- und Entsorgung und somit als Basis für alle Geschäftsprozesse einer Institution einschließlich der IT dienen. Beispiele für solche Versorgungsnetze sind:

- Strom,
- Telefon,
- Kühlung,
- Heizung bzw. Lüftung,
- Wasser und Abwasser,
- Löschwasserspeisungen,
- Gas,
- Melde- und Steueranlagen (z. B. für Einbruch, Brand, Hausleittechnik) und
- Sprechanlagen.

Der Ausfall oder die Störung eines Versorgungsnetzes kann unter anderem dazu führen, dass Menschen nicht mehr im Gebäude arbeiten können oder dass der IT-Betrieb und somit die Informationsverarbeitung beeinträchtigt wird.

Die Netze sind in unterschiedlich starker Weise voneinander abhängig, so dass sich Betriebsstörungen in jedem einzelnen Netz auch auf andere auswirken können.

Beispiele:

- Ein Ausfall von Heizung oder Lüftung kann zur Folge haben, dass alle Mitarbeiter die betroffenen Gebäude verlassen müssen. Dies kann unter Umständen hohe Schäden nach sich ziehen.
- Der Ausfall der Stromversorgung wirkt nicht nur auf die IT direkt, sondern auch auf alle anderen Netze, die mit elektrisch betriebener Steuer- und Regeltechnik ausgestattet sind. Selbst in Abwasserleitungen sind unter Umständen elektrische Hebepumpen vorhanden.
- Der Ausfall der Wasserversorgung beeinträchtigt eventuell die Funktion von Klimaanlagen.

Elementare Gefährdungen

G 0.11 Ausfall oder Störung von Dienstleistern

Kaum eine Institution arbeitet heute noch ohne Dienstleister wie Zulieferer oder Outsourcing-Anbieter. Wenn Organisationseinheiten von Dienstleistern abhängig sind, kann durch Ausfälle externer Dienstleistungen die Aufgabenbewältigung beeinträchtigt werden. Der teilweise oder vollständige Ausfall eines Outsourcing-Dienstleisters oder eines Zulieferers kann sich erheblich auf die betriebliche Kontinuität auswirken, insbesondere bei kritischen Geschäftsprozessen. Es gibt verschiedene Ursachen für solche Ausfälle, beispielsweise Insolvenz, einseitige Kündigung des Vertrags durch den Dienstleister oder Zulieferer, betriebliche Probleme beispielsweise durch Naturgewalten oder Personalausfall. Probleme können auch entstehen, wenn die vom Dienstleister erbrachten Leistungen nicht den Qualitätsanforderungen des Auftraggebers entsprechen.

Zu beachten ist außerdem, dass Dienstleister ebenfalls häufig auf Unterauftragnehmer zurückgreifen, um ihre Leistungen gegenüber dem Auftraggeber zu erbringen. Störungen, Qualitätsmängel und Ausfälle seitens der Unterauftragnehmer können dadurch indirekt zu Beeinträchtigungen beim Auftraggeber führen.

Auch durch Ausfälle von IT-Systemen beim Dienstleister oder der Kommunikationsanbindungen zu diesem können Geschäftsprozesse beim Auftraggeber beeinträchtigt werden.

Eine gegebenenfalls notwendige Rückholung ausgelagerter Prozesse kann stark erschwert sein, beispielsweise weil die ausgelagerten Verfahren nicht hinreichend dokumentiert sind oder weil der bisherige Dienstleister die Rückholung nicht unterstützt.

Beispiele:

- Ein Unternehmen hat seine Server in einem Rechenzentrum eines externen Dienstleisters installiert. Nach einem Brand in diesem Rechenzentrum war die Finanzabteilung des Unternehmens nicht mehr handlungsfähig. Es entstanden erhebliche finanzielle Verluste für das Unternehmen.
- Die Just-in-Time-Produktion eines Unternehmens war von der Zulieferung von Betriebsmitteln externer Dienstleister abhängig. Nachdem ein LKW durch einen Defekt beim Dienstleister ausfiel, verzögerte sich die Lieferung dringend benötigter Teile drastisch. Eine Reihe von Kunden konnte dadurch nicht fristgerecht beliefert werden.
- Ein Bankinstitut wickelte alle Geldtransporte mit einem Werttransportunternehmen ab. Das Werttransportunternehmen meldete überraschend Konkurs an. Die Vereinbarung und Tourenplanung mit einem neuen Werttransporter dauerte mehrere Tage. Als Folge kam es zu erheblichen Problemen und Zeitverzögerungen bei der Geldversorgung und -entsorgung der Bankfilialen.

Elementare Gefährdungen

G 0.12 Elektromagnetische Störstrahlung

Informationstechnik setzt sich heute zu einem großen Teil aus elektronischen Komponenten zusammen. Zwar wird zunehmend auch optische Übertragungstechnik eingesetzt, dennoch enthalten beispielsweise Computer, Netzkoppelelemente und Speichersysteme in der Regel sehr viele elektronische Bauteile. Durch elektromagnetische Störstrahlung, die auf solche Bauteile einwirkt, können elektronische Geräte in ihrer Funktion beeinträchtigt oder sogar beschädigt werden. Als Folge kann es unter anderem zu Ausfällen, Störungen, falschen Verarbeitungsergebnissen oder Kommunikationsfehlern kommen.

Auch drahtlose Kommunikation kann durch elektromagnetische Störstrahlung beeinträchtigt werden. Hierzu reicht unter Umständen eine ausreichend starke Störung der verwendeten Frequenzbänder.

Weiterhin können Informationen, die auf bestimmten Arten von Datenträgern gespeichert sind, durch elektromagnetische Störstrahlung gelöscht oder verfälscht werden. Dies betrifft insbesondere magnetisierbare Datenträger (Festplatten, Magnetbänder etc.) und Halbleiter-Speicher. Auch eine Beschädigung solcher Datenträger durch elektromagnetische Störstrahlung ist möglich.

Es gibt viele unterschiedliche Quellen elektromagnetischer Felder oder Strahlung, zum Beispiel Funknetze wie WLAN, Bluetooth, GSM, UMTS etc., Dauermagnete und kosmische Strahlung. Außerdem strahlt jedes elektrische Gerät mehr oder weniger starke elektromagnetische Wellen ab, die sich unter anderem durch die Luft und entlang metallischer Leiter (z. B. Kabel, Klimakanäle, Heizungsrohre etc.) ausbreiten können.

In Deutschland enthält das Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln (EMVG) Regelungen zu diesem Thema.

Elementare Gefährdungen

G 0.13 Abfangen kompromittierender Strahlung

Elektrische Geräte strahlen elektromagnetische Wellen ab. Bei Geräten, die Informationen verarbeiten (z. B. Computer, Bildschirme, Netzkoppelelemente, Drucker), kann diese Strahlung auch die gerade verarbeiteten Informationen mit sich führen. Derartige informationstragende Abstrahlung wird bloßstellende oder kompromittierende Abstrahlung genannt. Ein Angreifer, der sich beispielsweise in einem Nachbarhaus oder in einem in der Nähe abgestellten Fahrzeug befindet, kann versuchen, diese Abstrahlung zu empfangen und daraus die verarbeiteten Informationen zu rekonstruieren. Die Vertraulichkeit der Informationen ist damit in Frage gestellt. Eine mögliche Zielsetzung eines solchen Angriffes ist Industriespionage.

Die Grenzwerte des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmitteln (EMVG) reichen im Allgemeinen nicht aus, um das Abfangen der bloßstellenden Abstrahlung zu verhindern. Falls dieses Risiko nicht akzeptiert werden kann, müssen deshalb in aller Regel zusätzliche Schutzmaßnahmen getroffen werden.

Bloßstellende Abstrahlung ist nicht auf elektromagnetische Wellen beschränkt. Auch aus Schallwellen, zum Beispiel bei Druckern oder Tastaturen, können unter Umständen nützliche Informationen gewonnen werden.

Zu beachten ist außerdem, dass bloßstellende Abstrahlung in bestimmten Fällen auch durch äußere Manipulation von Geräten verursacht oder verstärkt werden kann. Wird zum Beispiel ein Gerät mit elektromagnetischen Wellen bestrahlt, kann es passieren, dass die reflektierten Wellen vertrauliche Informationen mit sich führen.

Elementare Gefährdungen

G 0.14 Ausspähen von Informationen (Spionage)

Mit Spionage werden Angriffe bezeichnet, die das Ziel haben, Informationen über Unternehmen, Personen, Produkte oder andere Zielobjekte zu sammeln, auszuwerten und aufzubereiten. Die aufbereiteten Informationen können dann beispielsweise eingesetzt werden, um einem anderem Unternehmen bestimmte Wettbewerbsvorteile zu verschaffen, Personen zu erpressen oder ein Produkt nachbauen zu können.

Neben einer Vielzahl technisch komplexer Angriffe gibt es oft auch viel einfachere Methoden, um an wertvolle Informationen zu kommen, beispielsweise indem Informationen aus mehreren öffentlich zugänglichen Quellen zusammengeführt werden, die einzeln unverfänglich aussehen, aber in anderen Zusammenhängen kompromittierend sein können. Da vertrauliche Daten häufig nicht ausreichend geschützt werden, können diese oft auf optischem, akustischem oder elektronischem Weg ausgespäht werden.

Beispiele:

- Viele IT-Systeme sind durch Identifikations- und Authentisierungsmechanismen gegen eine unberechtigte Nutzung geschützt, z. B. in Form von Benutzerkennung- und Passwort-Prüfung. Wenn das Passwort allerdings unverschlüsselt über die Leitung geschickt wird, ist es einem Angreifer unter Umständen möglich, dieses auszulesen.
- Um Geld an einem Geldausgabeautomaten abheben zu können, muss die korrekte PIN für die verwendete ec- oder Kreditkarte eingegeben werden. Leider ist der Sichtschutz an diesen Geräten häufig unzureichend, so dass ein Angreifer einem Kunden bei der Eingabe der PIN ohne Mühe über die Schulter schauen kann. Wenn der Angreifer hinterher die Karte stiehlt, kann er damit das Konto plündern.
- Um Zugriffsrechte auf einem PC zu erhalten oder diesen anderweitig zu manipulieren, kann ein Angreifer dem Benutzer ein Trojanisches Pferd schicken, das er als vorgeblich nützliches Programm einer E-Mail beigefügt hat. Neben unmittelbaren Schäden können über Trojanische Pferde vielfältige Informationen nicht nur über den einzelnen Rechner, sondern auch über das lokale Netz ausgespäht werden. Insbesondere verfolgen viele Trojanische Pferde das Ziel, Passwörter oder andere Zugangsdaten auszuspähen.
- In vielen Büros sind die Arbeitsplätze akustisch nicht gut gegeneinander abgeschirmt. Dadurch können Kollegen, aber auch Besucher eventuell Gespräche mithören und dabei Kenntnis von Informationen erlangen, die nicht für sie bestimmt oder sogar vertraulich sind.

Elementare Gefährdungen

G 0.15 Abhören

Mit Abhören werden gezielte Angriffe auf Kommunikationsverbindungen, Gespräche, Geräuschquellen aller Art oder IT-Systeme zur Informationssammlung bezeichnet. Dies beginnt beim unbemerkten, heimlichen Belauschen eines Gesprächs und reicht bis zu hoch technisierten komplexen Angriffen, um über Funk oder Leitungen gesendete Signale abzufangen, z. B. mit Hilfe von Antennen oder Sensoren.

Nicht nur wegen des geringen Entdeckungsrisikos ist das Abhören von Leitungen oder Funkverbindungen eine nicht zu vernachlässigende Gefährdung der Informationssicherheit. Grundsätzlich gibt es keine abhörsicheren Kabel. Lediglich der erforderliche Aufwand zum Abhören unterscheidet die Kabel. Ob eine Leitung tatsächlich abgehört wird, ist nur mit hohem messtechnischen Aufwand feststellbar.

Besonders kritisch ist die ungeschützte Übertragung von Authentisierungsdaten bei Klartextprotokollen wie HTTP, FTP oder Telnet, da diese durch die klare Strukturierung der Daten leicht automatisch zu analysieren sind.

Der Entschluss, irgendwo Informationen abzuhören, wird im Wesentlichen durch die Frage bestimmt, ob die Informationen den technischen bzw. den finanziellen Aufwand und das Risiko der Entdeckung wert sind. Die Beantwortung dieser Frage ist sehr von den individuellen Möglichkeiten und Interessen des Angreifers abhängig.

Beispiele:

- Bei Telefonaten kann für einen Angreifer nicht nur das Abhören von Gesprächen interessant sein. Auch die Informationen, die bei der Signalisierung übertragen werden, können von einem Angreifer missbraucht werden, z. B. falls durch eine fehlerhafte Einstellung im Endgerät das Passwort bei der Anmeldung im Klartext übertragen wird.
- Bei ungeschützter oder unzureichend geschützter Funkübertragung (z. B. wenn ein WLAN nur mit WEP abgesichert wird), kann ein Angreifer leicht die gesamte Kommunikation abhören.
- E-Mails können während ihres gesamten Weges durch das Netz gelesen werden, wenn sie nicht verschlüsselt sind. Unverschlüsselte E-Mails sollten daher nicht mit klassischen Briefen, sondern mit Postkarten verglichen werden.

Elementare Gefährdungen

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

Durch den Diebstahl von Datenträgern, IT-Systemen, Zubehör, Software oder Daten entstehen einerseits Kosten für die Wiederbeschaffung sowie für die Wiederherstellung eines arbeitsfähigen Zustandes, andererseits Verluste aufgrund mangelnder Verfügbarkeit. Wenn durch den Diebstahl vertrauliche Informationen offengelegt werden, kann dies weitere Schäden nach sich ziehen. Neben Servern und anderen teuren IT-Systemen werden auch mobile IT-Systeme, die unauffällig und leicht zu transportieren sind, häufig gestohlen. Es gibt aber auch Fälle, in denen gezielt Datenträger, wie Dokumente oder USB-Sticks, entwendet wurden, um an die darauf gespeicherten vertraulichen Informationen zu gelangen.

Beispiele:

- Im Frühjahr 2000 verschwand ein Notebook aus dem amerikanischen Außenministerium. In einer offiziellen Stellungnahme wurde nicht ausgeschlossen, dass das Gerät vertrauliche Informationen enthalten könnte. Ebenso wenig war bekannt, ob das Gerät kryptographisch oder durch andere Maßnahmen gegen unbefugten Zugriff gesichert war.
- In einem deutschen Bundesamt wurde mehrfach durch die gleichen ungesicherten Fenster eingebrochen. Neben anderen Wertsachen verschwanden auch mobile IT-Systeme. Ob Akten kopiert oder manipuliert wurden, konnte nicht zweifelsfrei ausgeschlossen werden.
- In Großbritannien gab es eine Reihe von Datenpannen, bei denen vertrauliche Unterlagen offengelegt wurden, weil Datenträger gestohlen wurden. In einem Fall wurden bei der britischen Luftwaffe mehrere Computer-Festplatten gestohlen, die sehr persönliche Informationen enthielten, die zur Sicherheitsüberprüfung von Mitarbeitern erfasst worden waren.
- Ein Mitarbeiter eines Call-Centers erstellte, kurz bevor er das Unternehmen verlassen musste, Kopien einer großen Menge von vertraulichen Kundendaten. Nach seinem Ausscheiden aus dem Unternehmen hat er diese Daten dann an Wettbewerber verkauft. Da anschließend Details über den Vorfall an die Presse gelangten, verlor das Call-Center viele wichtige Kunden.

Elementare Gefährdungen

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

Es gibt eine Vielzahl von Ursachen, die zu einem Verlust von Geräten, Datenträgern und Dokumenten führen können. Hierdurch ist unmittelbar die Verfügbarkeit betroffen, es können aber auch vertrauliche Informationen in fremde Hände gelangen, wenn die Datenträger nicht komplett verschlüsselt sind. Durch die Wiederbeschaffung von Geräten oder Datenträgern entstehen Kosten, aber auch, wenn diese wieder auftauchen, können Informationen offengelegt oder unerwünschte Programme aufgespielt worden sein.

Besonders mobile Endgeräte und mobile Datenträger können leicht verloren gehen. Auf kleinen Speicherkarten können heute riesige Datenmengen gespeichert werden. Es kommt aber auch immer wieder vor, dass Dokumente in Papierform versehentlich liegen gelassen werden, beispielsweise in Gaststätten oder Verkehrsmitteln.

Beispiele:

- Eine Mitarbeiterin nutzt in der Straßenbahn die Fahrt zum Arbeitsplatz, um einige Unterlagen zu sichten. Als sie hektisch an der Zielhaltestelle aussteigt, lässt sie die Papiere versehentlich auf ihrem Nachbarplatz liegen. Zwar sind die Unterlagen nicht vertraulich, in der Folge müssen jedoch mehrere Unterschriften hochrangiger Führungskräfte erneut eingeholt werden.
- Auf einer Großveranstaltung fällt einem Mitarbeiter beim Suchen in seiner Aktentasche versehentlich und unbemerkt eine Speicherkarte mit vertraulichen Kalkulationen auf den Boden. Der Finder sichtet den Inhalt auf seinem Laptop und verkauft die Informationen an die Konkurrenz.
- Ein Hersteller sendet CDs mit Software-Updates zur Fehlerbehebung per Post an seine Kunden. Einige dieser CDs gehen auf dem Versandweg verloren, ohne dass Absender oder Empfänger darüber informiert werden. Als Folge kommt es bei den betroffenen Kunden zu Fehlfunktionen der Software.

Elementare Gefährdungen

G 0.18 Fehlplanung oder fehlende Anpassung

Wenn organisatorische Abläufe, die direkt oder indirekt der Informationsverarbeitung dienen, nicht sachgerecht gestaltet sind, kann dies zu Sicherheitsproblemen führen. Obwohl jeder einzelne Prozessschritt korrekt durchgeführt wird, kommt es oft zu Schäden, weil Prozesse insgesamt fehlerhaft definiert sind.

Eine weitere mögliche Ursache für Sicherheitsprobleme sind Abhängigkeiten mit anderen Prozessen, die selbst keinen offensichtlichen Bezug zur Informationsverarbeitung haben. Solche Abhängigkeiten können bei der Planung leicht übersehen werden und dadurch Beeinträchtigungen während des Betriebes auslösen.

Sicherheitsprobleme können außerdem dadurch entstehen, dass Aufgaben, Rollen oder Verantwortung nicht eindeutig zugewiesen sind. Unter anderem kann es dadurch passieren, dass Abläufe verzögert, Sicherheitsmaßnahmen vernachlässigt oder Regelungen missachtet werden.

Gefahr besteht auch, wenn Geräte, Produkte, Verfahren oder andere Mittel zur Realisierung der Informationsverarbeitung nicht sachgerecht eingesetzt werden. Die Auswahl eines ungeeigneten Produktes oder Schwachstellen beispielsweise in der Anwendungsarchitektur oder im Netzdesign können zu Sicherheitsproblemen führen.

Beispiele:

- Wenn Wartungs- oder Reparaturprozesse nicht auf die fachlichen Anforderungen abgestimmt sind, kann es dadurch zu inakzeptablen Ausfallzeiten kommen.
- Es kann ein erhöhtes Risiko durch Angriffe auf die eigenen IT-Systeme entstehen, wenn sicherheitstechnische Anforderungen bei der Beschaffung von Informationstechnik nicht berücksichtigt werden.
- Wenn benötigtes Verbrauchsmaterial nicht zeitgerecht zur Verfügung gestellt wird, können die davon abhängigen IT-Verfahren ins Stocken geraten.
- Es können Schwachstellen entstehen, wenn bei der Planung eines IT-Verfahrens ungeeignete Übertragungsprotokolle ausgewählt werden.

Die Informationstechnik und das gesamte Umfeld einer Behörde bzw. eines Unternehmens ändern sich ständig. Sei es, dass Mitarbeiter ausscheiden oder hinzukommen, neue Hard- oder Software beschafft wird oder ein Zulieferbetrieb Konkurs anmeldet. Werden die dadurch notwendigen organisatorischen und technischen Anpassungen nicht oder nur ungenügend berücksichtigt, können sich Gefährdungen ergeben.

Beispiele:

- Durch bauliche Änderungen im Gebäude werden bestehende Fluchtwege verändert. Da die Mitarbeiter nicht ausreichend unterrichtet wurden, kann das Gebäude nicht in der erforderlichen Zeit geräumt werden.
- Bei der Übermittlung elektronischer Dokumente wird nicht darauf geachtet, ein für die Empfängerseite lesbares Datenformat zu

Elementare Gefährdungen

G 0.19 Offenlegung schützenswerter Informationen

Vertrauliche Daten und Informationen dürfen nur den zur Kenntnisnahme berechtigten Personen zugänglich sein. Neben der Integrität und der Verfügbarkeit gehört die Vertraulichkeit zu den Grundwerten der Informationssicherheit. Für vertrauliche Informationen (wie Passwörter, personenbezogene Daten, Firmen- oder Amtsgeheimnisse, Entwicklungsdaten) besteht die inhärente Gefahr, dass diese durch technisches Versagen, Unachtsamkeit oder auch durch vorsätzliche Handlungen offengelegt werden.

Dabei kann auf diese vertraulichen Informationen an unterschiedlichen Stellen zugegriffen werden, beispielsweise

- auf Speichermedien innerhalb von Rechnern (Festplatten),
- auf austauschbaren Speichermedien (USB-Sticks, CDs oder DVDs),
- in gedruckter Form auf Papier (Ausdrucke, Akten) und
- auf Übertragungswegen während der Datenübertragung.

Auch die Art und Weise, wie Informationen offengelegt werden, kann sehr unterschiedlich sein, zum Beispiel:

- unbefugtes Auslesen von Dateien,
- unbedachte Weitergabe, z. B. im Zuge von Reparaturaufträgen,
- unzureichende Löschung oder Vernichtung von Datenträgern,
- Diebstahl des Datenträgers und anschließendes Auswerten,
- Abhören von Übertragungsleitungen,
- Infektion von IT-Systemen mit Schadprogrammen,
- Mitlesen am Bildschirm oder Abhören von Gesprächen.

Werden schützenswerte Informationen offengelegt, kann dies schwerwiegende Folgen für eine Institution haben. Unter anderem kann der Verlust der Vertraulichkeit zu folgenden negativen Auswirkungen für eine Institution führen:

- Verstoß gegen Gesetze, zum Beispiel Datenschutz, Bankgeheimnis,
- Negative Innenwirkung, zum Beispiel Demoralisierung der Mitarbeiter,
- Negative Außenwirkung, zum Beispiel Beeinträchtigung der Beziehungen zu Geschäftspartnern, verlorenes Vertrauen von Kunden,
- Finanzielle Auswirkungen, zum Beispiel Schadensersatzansprüche, Bußgelder, Prozesskosten,
- Beeinträchtigung des informationellen Selbstbestimmungsrechtes.

Ein Verlust der Vertraulichkeit wird nicht immer sofort bemerkt. Oft stellt sich erst später heraus, z. B. durch Presseanfragen, dass Unbefugte sich Zugang zu vertraulichen Informationen verschafft haben.

Beispiel:

- Käufer von gebrauchten Rechnern, Festplatten, Mobiltelefonen oder ähnlichen Geräten finden darauf immer wieder höchst vertrauliche Informationen wie Patientendaten oder Kontonummern.

Elementare Gefährdungen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

Wenn Informationen, Software oder Geräte verwendet werden, die aus unzuverlässigen Quellen stammen oder deren Herkunft und Korrektheit nicht ausreichend geprüft wurden, kann der Einsatz hohe Gefahren mit sich bringen. Dies kann unter anderem dazu führen, dass geschäftsrelevante Informationen auf einer falschen Datenbasis beruhen, dass Berechnungen falsche Ergebnisse liefern oder dass falsche Entscheidungen getroffen werden. Ebenso können aber auch Integrität und Verfügbarkeit von IT-Systemen beeinträchtigt werden.

Beispiele:

- Ein Empfänger kann durch E-Mails, deren Herkunft er nicht geprüft hat, dazu verleitet werden, bestimmte Aktionen durchzuführen, die sich für ihn oder andere nachteilig auswirken. Beispielsweise kann die E-Mail interessante Anhänge oder Links enthalten, die beim Anklicken dazu führen, dass Schadsoftware beim Empfänger installiert wird. Der Absender der E-Mail kann dabei gefälscht oder dem eines bekannten Kommunikationspartners nachgeahmt sein.
- Die Annahme, dass eine Angabe wahr ist, weil es "in der Zeitung steht" oder "im TV ausgestrahlt wurde", ist nicht immer gerechtfertigt. Dadurch können falsche Aussagen in geschäftskritische Berichte eingearbeitet werden.
- Die Zuverlässigkeit von Informationen, die über das Internet verbreitet werden, ist sehr unterschiedlich. Wenn Ausführungen ohne weitere Quellenprüfungen aus dem Internet übernommen werden, können daraus Fehlentscheidungen resultieren.
- Wenn Updates oder Patches aus nicht vertrauenswürdigen Quellen eingespielt werden, kann dies zu unerwünschten Nebenwirkungen führen. Wenn die Herkunft von Software nicht überprüft wird, besteht ein erhöhtes Risiko, dass IT-Systeme mit schädlichem Code infiziert werden.

Elementare Gefährdungen

G 0.21 Manipulation von Hard- oder Software

Als Manipulation wird jede Form von gezielten, aber heimlichen Eingriffen bezeichnet, um Zielobjekte aller Art unbemerkt zu verändern. Manipulationen an Hard- oder Software können unter anderem aus Rachegefühlen, um einen Schaden mutwillig zu erzeugen, zur Verschaffung persönlicher Vorteile oder zur Bereicherung vorgenommen werden. Im Fokus können dabei Geräte aller Art, Zubehör, Datenträger (z. B. DVDs, USB-Sticks), Applikationen, Datenbanken oder ähnliches stehen.

Manipulationen an Hard- und Software führen nicht immer zu einem unmittelbaren Schaden. Wenn jedoch die damit verarbeiteten Informationen beeinträchtigt werden, kann dies alle Arten von Sicherheitsauswirkungen nach sich ziehen (Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit). Die Manipulationen können dabei umso wirkungsvoller sein, je später sie entdeckt werden, je umfassender die Kenntnisse der Täter sind und je tiefgreifender die Auswirkungen auf einen Arbeitsvorgang sind. Die Auswirkungen reichen von der unerlaubten Einsichtnahme in schützenswerte Daten bis hin zur Zerstörung von Datenträgern oder IT-Systemen. Manipulationen können dadurch auch erhebliche Ausfallzeiten nach sich ziehen.

Beispiele:

- In einem Schweizer Finanzunternehmen hatte ein Mitarbeiter die Einsatzsoftware für bestimmte Finanzdienstleistungen manipuliert. Dadurch war es ihm möglich, sich illegal größere Geldbeträge zu verschaffen.
- Durch Manipulationen an Geldausgabeautomaten ist es Angreifern mehrfach gelungen, die auf Zahlungskarten gespeicherten Daten unerlaubt auszulesen. In Verbindung mit ausgespähten PINs wurden diese Daten dann später missbraucht, um Geld zulasten der Karteninhaber abzuheben.

Elementare Gefährdungen

G 0.22 Manipulation von Informationen

Informationen können auf vielfältige Weise manipuliert werden, z. B. durch fehlerhaftes oder vorsätzlich falsches Erfassen von Daten, inhaltliche Änderung von Datenbank-Feldern oder von Schriftverkehr. Grundsätzlich betrifft dies nicht nur digitale Informationen, sondern beispielsweise auch Dokumente in Papierform. Ein Täter kann allerdings nur die Informationen manipulieren, auf die er Zugriff hat. Je mehr Zugriffsrechte eine Person auf Dateien und Verzeichnisse von IT-Systemen besitzt bzw. je mehr Zugriffsmöglichkeiten auf Informationen sie hat, desto schwerwiegendere Manipulationen kann sie vornehmen. Falls die Manipulationen nicht frühzeitig erkannt werden, kann der reibungslose Ablauf von Geschäftsprozessen und Fachaufgaben dadurch empfindlich gestört werden.

Archivierte Dokumente stellen meist schützenswerte Informationen dar. Die Manipulation solcher Dokumente ist besonders schwerwiegend, da sie unter Umständen erst nach Jahren bemerkt wird und eine Überprüfung dann oft nicht mehr möglich ist.

Beispiel:

- Eine Mitarbeiterin hat sich über die Beförderung ihrer Zimmergenossin in der Buchhaltung dermaßen geärgert, dass sie sich während einer kurzen Abwesenheit der Kollegin unerlaubt Zugang zu deren Rechner verschafft hat. Hier hat sie durch einige Zahlenänderungen in der Monatsbilanz enormen negativen Einfluss auf das veröffentlichte Jahresergebnis des Unternehmens genommen.

Elementare Gefährdungen

G 0.23 Unbefugtes Eindringen in IT-Systeme

Grundsätzlich beinhaltet jede Schnittstelle an einem IT-System nicht nur die Möglichkeit, darüber bestimmte Dienste des IT-Systems berechtigt zu nutzen, sondern auch das Risiko, dass darüber unbefugt auf das IT-System zugegriffen wird.

Beispiele:

- Wenn eine Benutzerkennung und das zugehörige Passwort ausgespäht werden, ist eine unberechtigte Nutzung der damit geschützten Anwendungen oder IT-Systeme denkbar.
- Über unzureichend gesicherte Fernwartungszugänge könnten Hacker unerlaubt auf IT-Systeme zugreifen.
- Bei unzureichend gesicherten Schnittstellen von aktiven Netzkomponenten ist es denkbar, dass Angreifer einen unberechtigten Zugang zur Netzkomponente erlangen. Wenn es ihnen außerdem gelingt, die lokalen Sicherheitsmechanismen zu überwinden, also z.B. an administrative Berechtigungen gelangt sind, könnten sie alle Administrationstätigkeiten ausüben.
- Viele IT-Systeme haben Schnittstellen für den Einsatz austauschbarer Datenspeicher, wie z. B. Zusatzspeicherkarten oder USB-Speichermedien. Bei einem unbeaufsichtigten IT-System mit der entsprechenden Hard- und Software besteht die Gefahr, dass hierüber große Datenmengen unbefugt ausgelesen oder Schadprogramme eingeschleust werden können.

Elementare Gefährdungen

G 0.24 Zerstörung von Geräten oder Datenträgern

Durch Fahrlässigkeit, unsachgemäße Verwendung aber auch durch ungeschulten Umgang kann es zu Zerstörungen an Geräten und Datenträgern kommen, die den Betrieb des IT-Systems empfindlich stören können.

Es besteht außerdem die Gefahr, dass durch die Zerstörung wichtige Informationen verloren gehen, die nicht oder nur mit großem Aufwand rekonstruiert werden können.

Beispiele:

- In einem Unternehmen nutzte ein Innentäter seine Kenntnis darüber, dass ein wichtiger Server empfindlich auf zu hohe Betriebstemperaturen reagiert, und blockierte die Lüftungsschlitze für den Netzteillüfter mit einem hinter dem Server versteckt aufgestellten Gegenstand. Zwei Tage später erlitt die Festplatte im Server einen temperaturbedingten Defekt, und der Server fiel für mehrere Tage aus.
- Ein Mitarbeiter hatte sich über das wiederholte Abstürzen des Systems so stark geärgert, dass er seine Wut an seinem Arbeitsplatzrechner ausließ. Hierbei wurde die Festplatte durch Fußtritte gegen den Rechner so stark beschädigt, dass sie unbrauchbar wurde. Die hier gespeicherten Daten konnten nur teilweise wieder durch ein Backup vom Vortag rekonstruiert werden.
- Durch umgestoßene Kaffeetassen oder beim Blumengießen eindringende Feuchtigkeit können in einem IT-System Kurzschlüsse hervorrufen.

Elementare Gefährdungen

G 0.25 Ausfall von Geräten oder Systemen

Werden auf einem IT-System zeitkritische Anwendungen betrieben, sind die Folgeschäden nach einem Systemausfall entsprechend hoch, wenn es keine Ausweichmöglichkeiten gibt.

Beispiele:

- Es wird eine Firmware in ein IT-System eingespielt, die nicht für diesen Systemtyp vorgesehen ist. Das IT-System startet daraufhin nicht mehr fehlerfrei und muss vom Hersteller wieder betriebsbereit gemacht werden.
- Bei einem Internet Service Provider (ISP) führte ein Stromversorgungsfehler in einem Speichersystem dazu, dass dieses abgeschaltet wurde. Obwohl der eigentliche Fehler schnell behoben werden konnte, ließen sich die betroffenen IT-Systeme anschließend nicht wieder hochfahren, da Inkonsistenzen im Dateisystem auftraten. Als Folge waren mehrere vom ISP betriebene Webserver tagelang nicht erreichbar.

Elementare Gefährdungen

G 0.26 Fehlfunktion von Geräten oder Systemen

Geräte und Systeme, die der Informationsverarbeitung dienen, haben heute häufig viele Funktionen und sind deshalb entsprechend komplex aufgebaut. Grundsätzlich betrifft dies sowohl Hardware- als auch Software-Komponenten. Durch die Komplexität gibt es in solchen Komponenten viele unterschiedliche Fehlerquellen. Als Folge kommt es immer wieder dazu, dass Geräte und Systeme nicht wie vorgesehen funktionieren und dadurch Sicherheitsprobleme entstehen.

Ursachen für Fehlfunktionen gibt es viele, zum Beispiel Materialermüdung, Fertigungstoleranzen, konzeptionelle Schwächen, Überschreitung von Grenzwerten, nicht vorgesehene Einsatzbedingungen oder fehlende Wartung. Da es keine perfekten Geräte und Systeme gibt, muss eine gewisse Restwahrscheinlichkeit für Fehlfunktionen ohnehin immer akzeptiert werden.

Durch Fehlfunktionen von Geräten oder Systemen können alle Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) beeinträchtigt werden. Hinzu kommt, dass Fehlfunktionen unter Umständen auch über einen längeren Zeitraum unbemerkt bleiben können. Dadurch kann es beispielsweise passieren, dass Berechnungsergebnisse verfälscht und nicht rechtzeitig korrigiert werden.

Beispiele:

- Aufgrund eines verstopften Lüftungsgitters kommt es zur Überhitzung eines Speichersystems, das daraufhin nicht komplett ausfällt, sondern nur sporadische Fehlfunktionen aufweist. Erst einige Wochen später wird bemerkt, dass die gespeicherten Informationen unvollständig sind.
- Eine wissenschaftliche Standard-Anwendung wird genutzt, um eine statistische Analyse für einen vorab erhobenen Datenbestand durchzuführen, der in einer Datenbank gespeichert ist. Laut Dokumentation ist die Anwendung jedoch für das eingesetzte Datenbank-Produkt nicht freigegeben. Die Analyse scheint zwar zu funktionieren, durch Stichproben stellt sich allerdings heraus, dass die berechneten Ergebnisse falsch sind. Als Ursache wurden Kompatibilitätsprobleme zwischen der Anwendung und der Datenbank identifiziert.

Elementare Gefährdungen

G 0.27 Ressourcenmangel

Wenn die vorhandenen Ressourcen in einem Bereich unzureichend sind, kann es zu Engpässen in der Versorgung mit diesen Ressourcen bis hin zu Überlastungen und Ausfällen kommen. Je nach Art der betroffenen Ressourcen können durch ein kleines Ereignis, dessen Eintritt zudem vorhersehbar war, im Endeffekt eine Vielzahl von Geschäftsprozessen beeinträchtigt werden. Ressourcenmangel kann im IT-Betrieb und bei Kommunikationsverbindungen auftreten, aber auch in anderen Bereichen einer Institution. Werden für bestimmte Aufgaben nur unzureichende personelle, zeitliche und finanzielle Ressourcen zur Verfügung gestellt, kann das vielfältige negative Auswirkungen haben. Es kann beispielsweise passieren, dass die in Projekten notwendigen Rollen nicht mit geeigneten Personen besetzt werden. Wenn Betriebsmittel wie Hard- oder Software nicht mehr ausreichen, um den Anforderungen gerecht zu werden, können Fachaufgaben unter Umständen nicht erfolgreich bearbeitet werden.

Häufig können personelle, zeitliche, finanzielle, technische und sonstige Mängel im Regelbetrieb für einen begrenzten Zeitraum noch ausgeglichen werden. Unter hohem Zeitdruck werden sie jedoch, beispielsweise in Notfall-Situationen, umso deutlicher.

Ressourcen können auch absichtlich überlastet werden, wenn jemand einen intensiven Bedarf an einem Betriebsmittel vorsätzlich generiert und dadurch eine intensive und dauerhafte Störung des Betriebsmittels provoziert, siehe auch G 0.40 Verhinderung von Diensten (Denial of Service).

Beispiele:

- Überlastete Elektroleitungen erhitzen sich, dies kann bei ungünstiger Verlegung zu einem Schwelbrand führen.
- Werden neue Anwendungen mit einem höheren als zum Planungszeitpunkt berücksichtigten Bandbreitenbedarf auf dem Netz betrieben, kann dies zu einem Verlust der Verfügbarkeit des gesamten Netzes führen, wenn die Netzinfrastruktur nicht ausreichend skaliert werden kann.
- Wenn die Administratoren wegen Überlastung die Protokoll-Dateien der von ihnen betreuten IT nur sporadisch kontrollieren, werden eventuell Angriffe nicht zeitnah erkannt.
- Webserver können durch eine hohe Menge zeitgleich eintreffender Anfragen so überlastet werden, dass ein geregelter Zugriff auf Daten fast unmöglich wird.
- Wenn sich ein Unternehmen in einem Insolvenzverfahren befindet, kann es passieren, dass kein Geld für dringend benötigte Ersatzteile vorhanden ist oder dass wichtige Dienstleister nicht bezahlt werden können.

Elementare Gefährdungen

G 0.28 Software-Schwachstellen oder -Fehler

Für jede Software gilt: je komplexer sie ist, desto häufiger treten Fehler auf. Auch bei intensiven Tests werden meist nicht alle Fehler vor der Auslieferung an die Kunden entdeckt. Werden Software-Fehler nicht rechtzeitig erkannt, können die bei der Anwendung entstehenden Abstürze oder Fehler zu weitreichenden Folgen führen. Beispiele hierfür sind falsche Berechnungsergebnisse, Fehlentscheidungen der Leitungsebene und Verzögerungen beim Ablauf der Geschäftsprozesse.

Durch Software-Schwachstellen oder -Fehler kann es zu schwerwiegenden Sicherheitslücken in einer Anwendung, einem IT-System oder allen damit vernetzten IT-Systemen kommen. Solche Sicherheitslücken können unter Umständen von Angreifern ausgenutzt werden, um Schadsoftware einzuschleusen, unerlaubt Daten auszulesen oder Manipulationen vorzunehmen.

Beispiele:

- Die meisten Warnmeldungen der Computer Emergency Response Teams (CERTs) in den letzten Jahren bezogen sich auf sicherheitsrelevante Programmierfehler. Dies sind Fehler, die bei der Erstellung von Software entstehen und dazu führen, dass diese Software von Angreifern missbraucht werden kann. Ein großer Teil dieser Fehler wurde durch Speicherüberläufe (Buffer Overflow) hervorgerufen.
- Internet-Browser sind heute eine wichtige Software-Komponente auf Clients. Browser werden häufig nicht nur zum Zugriff auf das Internet, sondern auch für interne Web-Anwendungen in Unternehmen und Behörden genutzt. Software-Schwachstellen oder -Fehler in Browsern können deshalb die Informationssicherheit insgesamt besonders stark beeinträchtigen.

Elementare Gefährdungen

G 0.29 Verstoß gegen Gesetze oder Regelungen

Wenn Informationen, Geschäftsprozesse und IT-Systeme einer Institution unzureichend abgesichert sind (beispielsweise durch ein unzureichendes Sicherheitsmanagement), kann dies zu Verstößen gegen Rechtsvorschriften mit Bezug zur Informationsverarbeitung oder gegen bestehende Verträge mit Geschäftspartnern führen. Welche Gesetze jeweils zu beachten sind, hängt von der Art der Institution bzw. ihrer Geschäftsprozesse und Dienstleistungen ab. Je nachdem, wo sich die Standorte einer Institution befinden, können auch verschiedene nationale Vorschriften zu beachten sein. Folgende Beispiele verdeutlichen dies:

- Der Umgang mit personenbezogenen Daten ist in Deutschland über eine Vielzahl von Vorschriften geregelt. Dazu gehören das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze, aber auch eine Vielzahl bereichsspezifischer Regelungen.
- Die Geschäftsführung eines Unternehmens ist dazu verpflichtet, bei allen Geschäftsprozessen eine angemessene Sorgfalt anzuwenden. Hierzu gehört auch die Beachtung anerkannter Sicherheitsmaßnahmen. In Deutschland gelten verschiedene Rechtsvorschriften wie KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich), GmbHG (Gesetz betreffend die Gesellschaften mit beschränkter Haftung) oder AktG (Aktiengesetz), aus denen sich zu Risikomanagement und Informationssicherheit entsprechende Handlungs- und Haftungsverpflichtungen der Geschäftsführung bzw. des Vorstands eines Unternehmens ableiten lassen.
- Die ordnungsmäßige Verarbeitung von buchungsrelevanten Daten ist in verschiedenen Gesetzen und Vorschriften geregelt. In Deutschland sind dies unter anderem das Handelsgesetzbuch (z. B. HGB §§ 238 ff.) und die Abgabenordnung (AO). Die ordnungsmäßige Verarbeitung von Informationen umfasst natürlich deren sichere Verarbeitung. Beides muss in vielen Ländern regelmäßig nachgewiesen werden, beispielsweise durch Wirtschaftsprüfer im Rahmen der Prüfung des Jahresabschlusses. Falls hierbei gravierende Sicherheitsmängel festgestellt werden, kann kein positiver Prüfungsbericht erstellt werden.
- In vielen Branchen (z.B. der Automobil-Industrie) ist es üblich, dass Hersteller ihre Zulieferer zur Einhaltung bestimmter Qualitäts- und Sicherheitsstandards verpflichten. In diesem Zusammenhang werden zunehmend auch Anforderungen an die Informationssicherheit gestellt. Verstößt ein Vertragspartner gegen vertraglich geregelte Sicherheitsanforderungen, kann dies Vertragsstrafen, aber auch Vertragsauflösungen bis hin zum Verlust von Geschäftsbeziehungen nach sich ziehen.

Nur wenige Sicherheitsanforderungen ergeben sich unmittelbar aus Gesetzen. Die Gesetzgebung orientiert sich jedoch im Allgemeinen am Stand der Technik als allgemeine Bewertungsgrundlage für den Grad der erreichbaren Sicherheit. Stehen bei einer Institution die vorhandenen Sicherheitsmaßnahmen in keinem gesunden Verhältnis zu den zu schützenden Werten und dem Stand der Technik, kann dies gravierende Folgen haben.

Elementare Gefährdungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

Ohne geeignete Mechanismen zur Zutritts-, Zugriffs- und Zugangskontrolle kann eine unberechtigte Nutzung von Geräten und Systemen praktisch nicht verhindert oder erkannt werden. Bei IT-Systemen ist der grundlegende Mechanismus die Identifikation und Authentisierung von Benutzern. Aber selbst bei IT-Systemen mit einer starken Identifikations- und Authentisierungsfunktion ist eine unberechtigte Nutzung denkbar, wenn die entsprechenden Sicherheitsmerkmale (Passwörter, Chipkarten, Token etc.) in falsche Hände gelangen. Auch bei der Vergabe und Pflege von Berechtigungen können viele Fehler gemacht werden, beispielsweise wenn Berechtigungen zu weitreichend oder an unautorisierte Personen vergeben oder nicht zeitnah aktualisiert werden.

Unbefugte können durch die unberechtigte Nutzung von Geräten und Systemen an vertrauliche Informationen gelangen, Manipulationen vornehmen oder Störungen verursachen.

Ein besonders wichtiger Spezialfall der unberechtigten Nutzung ist die unberechtigte Administration. Wenn Unbefugte die Konfiguration oder die Betriebsparameter von Hardware- oder Software-Komponenten ändern, können daraus schwere Schäden resultieren.

Beispiel:

- Bei der Kontrolle von Protokollierungsdaten stieß ein Netzadministrator auf zunächst unerklärliche Ereignisse, die an verschiedenen Tagen, aber häufig am frühen Morgen und am Nachmittag aufgetreten sind. Bei näherer Untersuchung stellte sich heraus, dass ein WLAN-Router unsicher konfiguriert war. Wartende Personen an der Bushaltestelle vor dem Firmengebäude haben diesen Zugang genutzt, um während der Wartezeit mit ihren mobilen Endgeräten im Internet zu surfen.

Elementare Gefährdungen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

Eine fehlerhafte oder nicht ordnungsgemäße Nutzung von Geräten, Systemen und Anwendungen kann deren Sicherheit beeinträchtigen, vor allem, wenn vorhandene Sicherheitsmaßnahmen missachtet oder umgangen werden. Dies führt häufig zu Störungen oder Ausfällen. Je nachdem, welche Arten von Geräten oder Systemen falsch genutzt werden, können aber auch Vertraulichkeit und Integrität von Informationen verletzt werden.

Ein besonders wichtiger Spezialfall der fehlerhaften Nutzung ist die fehlerhafte Administration. Fehler bei der Installation, Konfiguration, Wartung und Pflege von Hardware- oder Software-Komponenten können schwere Schäden nach sich ziehen.

Beispielsweise können zu großzügig vergebene Rechte, leicht zu erratende Passwörter, nicht ausreichend geschützte Datenträger mit Sicherungskopien oder bei vorübergehender Abwesenheit nicht gesperrte Terminals zu Sicherheitsvorfällen führen.

Gleichermaßen können durch die fehlerhafte Bedienung von IT-Systemen oder Anwendungen auch Daten versehentlich gelöscht oder verändert werden. Dadurch könnten aber auch vertrauliche Informationen an die Öffentlichkeit gelangen, beispielsweise wenn Zugriffsrechte falsch gesetzt werden.

Wenn Strom- oder Netzkabel ungeschützt verlegt werden, können sie unbeabsichtigt beschädigt werden, wodurch Verbindungen ausfallen können. Geräteanschlussleitungen können herausgerissen werden, wenn Mitarbeiter oder Besucher darüber stolpern.

Elementare Gefährdungen

G 0.32 Missbrauch von Berechtigungen

Abhängig von ihren Rollen und Aufgaben erhalten Personen entsprechende Zutritts-, Zugangs- und Zugriffsberechtigungen. Auf diese Weise soll einerseits der Zugang zu Informationen gesteuert und kontrolliert werden, und andererseits soll es den Personen ermöglicht werden, bestimmte Aufgaben zu erledigen. Beispielsweise benötigen Personen oder Gruppen bestimmte Berechtigungen, um Anwendungen ausführen zu können oder Informationen bearbeiten zu können.

Eine missbräuchliche Nutzung von Berechtigungen liegt vor, wenn vorsätzlich recht- oder unrechtmäßig erworbene Möglichkeiten außerhalb des vorgesehenen Rahmens genutzt werden. Ziel dabei ist häufig, sich persönliche Vorteile zu verschaffen oder einer Institution oder bestimmten Personen zu schaden.

In nicht wenigen Fällen verfügen Personen aus historischen, systemtechnischen oder anderen Gründen über höhere oder umfangreichere Zutritts-, Zugangs- oder Zugriffsrechte, als sie für ihre Tätigkeit benötigen. Diese Rechte können unter Umständen für Angriffe missbraucht werden.

Beispiele:

- Je feingranularer die Zugriffsrechte auf Informationen gestaltet werden, desto größer ist oft auch der Pflegeaufwand, um diese Berechtigungen auf dem aktuellen Stand zu halten. Es besteht deshalb die Gefahr, dass bei der Vergabe der Zugriffsrechte zu wenig zwischen den unterschiedlichen Rollen differenziert wird und dadurch der Missbrauch der Berechtigungen erleichtert wird.
- Bei verschiedenen Anwendungen werden Zugriffsberechtigungen oder Passwörter in Systembereichen gespeichert, auf die auch andere Benutzer zugreifen können. Dadurch könnten Angreifer die Berechtigungen ändern oder Passwörter auslesen.
- Personen mit zu großzügig vergebenen Berechtigungen könnten versucht sein, auf fremde Dateien zuzugreifen, beispielsweise eine fremde E-Mail einzusehen, weil bestimmte Informationen dringend benötigt werden.

Elementare Gefährdungen

G 0.33 Personalausfall

Der Ausfall von Personal kann erhebliche Auswirkungen auf eine Institution und deren Geschäftsprozesse haben. Personal kann beispielsweise durch Krankheit, Unfall, Tod oder Streik unvorhergesehen ausfallen. Des weiteren ist auch der vorhersagbare Personalausfall bei Urlaub, Fortbildung oder einer regulären Beendigung des Arbeitsverhältnisses zu berücksichtigen, insbesondere wenn die Restarbeitszeit z. B. durch einen Urlaubsanspruch verkürzt wird. Ein Personalausfall kann auch durch einen internen Wechsel des Arbeitsplatzes verursacht werden.

Beispiele:

- Aufgrund längerer Krankheit blieb der Netzadministrator einer Firma vom Dienst fern. In der betroffenen Firma lief das Netz zunächst fehlerfrei weiter. Nach zwei Wochen jedoch war nach einem Systemabsturz niemand in der Lage, den Fehler zu beheben, da es nur diesen in den Netzbetrieb eingearbeiteten Administrator gab. Dies führte zu einem Ausfall des Netzes über mehrere Tage.
- Während des Urlaubs eines Administrators musste in einer Institution auf die Backup-Medien im Datensicherungstresor zurückgegriffen werden. Der Zugangscode zum Tresor wurde erst kurz zuvor geändert und war nur diesem Administrator bekannt. Erst nach mehreren Tagen konnte die Datenrestaurierung durchgeführt werden, da der Administrator nicht eher im Urlaub erreichbar war.
- Im Falle eine Pandemie fällt nach und nach längerfristig immer mehr Personal aus, sei es durch die Krankheit selbst, durch die notwendige Pflege von Angehörigen oder durch die Betreuung von Kindern. Auch aus Angst vor Ansteckung in öffentlichen Verkehrsmitteln oder in der Institution bleiben einige Mitarbeiter vom Dienst fern. Als Folge können nur noch die notwendigsten Arbeiten erledigt werden. Die erforderliche Wartung der Systeme, sei es der zentrale Server oder die Klimaanlage im Rechenzentrum, ist nicht mehr zu leisten. Nach und nach fallen dadurch immer mehr Systeme aus.

Elementare Gefährdungen

G 0.34 Anschlag

Durch einen Anschlag kann eine Institution, bestimmte Bereiche der Institution oder einzelne Personen bedroht werden. Die technischen Möglichkeiten, einen Anschlag zu verüben, sind vielfältig: geworfene Ziegelsteine, Explosion durch Sprengstoff, Schusswaffengebrauch, Brandstiftung. Ob und in welchem Umfang eine Institution der Gefahr eines Anschlages ausgesetzt ist, hängt neben der Lage und dem Umfeld des Gebäudes stark von ihren Aufgaben und vom politisch-sozialen Klima ab. Unternehmen und Behörden, die in politisch kontrovers diskutierten Bereichen agieren, sind stärker bedroht als andere. Institutionen in der Nähe üblicher Demonstrationsaufmarschgebiete sind stärker gefährdet als solche in abgelegenen Orten. Für die Einschätzung der Gefährdung oder bei Verdacht auf Bedrohungen durch politisch motivierte Anschläge können in Deutschland die Landeskriminalämter oder das Bundeskriminalamt beratend hinzugezogen werden.

Beispiele:

- In den 1980er-Jahren wurde ein Sprengstoffanschlag auf das Rechenzentrum einer großen Bundesbehörde in Köln verübt. Durch die große Durchschlagskraft des Sprengkörpers wurden nicht nur Fenster und Wände, sondern auch viele IT-Systeme im Rechenzentrum zerstört.
- Bei dem Anschlag auf das World-Trade-Center in New York am 11. September 2001 wurden nicht nur viele Menschen getötet, sondern es wurden auch zahlreiche IT-Einrichtungen zerstört. Als Folge hatten mehrere Unternehmen erhebliche Schwierigkeiten, ihre Geschäftstätigkeiten fortzusetzen.

Elementare Gefährdungen

G 0.35 Nötigung, Erpressung oder Korruption

Nötigung, Erpressung oder Korruption können dazu führen, dass die Sicherheit von Informationen oder Geschäftsprozessen beeinträchtigt wird. Durch Androhung von Gewalt oder anderen Nachteilen kann ein Angreifer beispielsweise versuchen, das Opfer zur Missachtung von Sicherheitsrichtlinien oder zur Umgehung von Sicherheitsmaßnahmen zu bringen (Nötigung).

Anstatt zu drohen, können Angreifer auch gezielt Geld oder andere Vorteile anbieten, um Mitarbeiter oder andere Personen zum Instrument für Sicherheitsverletzungen zu machen (Korruption). Beispielsweise besteht die Gefahr, dass ein bestechlicher Mitarbeiter vertrauliche Dokumente an Unbefugte weiterleitet.

Durch Nötigung oder Korruption können grundsätzlich alle Grundwerte der Informationssicherheit beeinträchtigt werden. Angriffe können unter anderem darauf abzielen, vertrauliche Informationen an Unbefugte zu leiten, geschäftskritische Informationen zu manipulieren oder den reibungslosen Ablauf von Geschäftsprozessen zu stören.

Besondere Gefahr besteht, wenn sich solche Angriffe gegen hochrangige Führungskräfte oder Personen in besonderen Vertrauensstellungen richten.

Elementare Gefährdungen

G 0.36 Identitätsdiebstahl

Beim Identitätsdiebstahl täuscht ein Angreifer eine falsche Identität vor, er benutzt also Informationen über eine andere Person, um in deren Namen aufzutreten. Hierfür werden Daten wie beispielsweise Geburtsdatum, Anschrift, Kreditkarten- oder Kontonummern benutzt, um sich beispielsweise auf fremde Kosten bei einem Internet-Dienstleister anzumelden oder sich auf andere Weise zu bereichern. Identitätsdiebstahl führt häufig auch direkt oder indirekt zur Rufschädigung, aber verursacht auch einen hohen Zeitaufwand, um die Ursachen aufzuklären und negative Folgen für die Betroffenen abzuwenden. Einige Formen des Identitätsbetrugs werden auch als Maskerade bezeichnet.

Identitätsdiebstahl tritt besonders dort häufig auf, wo die Identitätsprüfung zu nachlässig gehandhabt wird, vor allem, wenn hierauf teure Dienstleistungen basieren.

Eine Person, die über die Identität seines Kommunikationspartners getäuscht wurde, kann leicht dazu gebracht werden, schutzbedürftige Informationen zu offenbaren.

Beispiele:

- Bei verschiedenen E-Mail-Providern und Auktionsplattformen im Internet reichte es zur Anmeldung anfangs, sich einen Phantasienamen auszudenken und diesen mit einer passenden Adresse aus dem Telefonbuch zu unterlegen. Zunächst konnten sich Angreifer auch unter erkennbar ausgedachten Namen anmelden, beispielsweise von Comicfiguren. Als dann schärfere Plausibilitätstests eingeführt wurden, sind hierfür auch Namen, Adressen und Kontonummern von echten Personen verwendet worden. Die Betroffenen haben hiervon erst erfahren, als die ersten Zahlungsaufforderungen bei ihnen eintrafen.
- Die Absender-Adressen von E-Mails lassen sich leicht fälschen. Es passiert immer wieder, dass Anwendern auf diese Weise vorgetäuscht wird, dass eine E-Mail von einem vertrauenswürdigen Kommunikationspartner stammt. Ähnliche Angriffe sind durch die Manipulation der Rufnummernanzeige bei Sprachverbindungen oder durch die Manipulation der Absenderkennung bei Faxverbindungen möglich.
- Ein Angreifer kann durch eine Maskerade versuchen, sich in eine bereits bestehende Verbindung einzuhängen, ohne sich selber authentisieren zu müssen, da dieser Schritt bereits von den originären Kommunikationsteilnehmern durchlaufen wurde.

Elementare Gefährdungen

G 0.37 Abstreiten von Handlungen

Personen können aus verschiedenen Gründen abstreiten, bestimmte Handlungen begangen zu haben, beispielsweise weil diese Handlungen gegen Anweisungen, Sicherheitsvorgaben oder sogar Gesetze verstoßen. Sie könnten aber auch leugnen, eine Benachrichtigung erhalten zu haben, zum Beispiel weil sie einen Termin vergessen haben. Im Bereich der Informationssicherheit wird daher häufig die Verbindlichkeit hervorgehoben, eine Eigenschaft, über die sichergestellt werden soll, dass erfolgte Handlungen nicht unberechtigt abgestritten werden können. Im englischen Sprachraum wird dafür der Begriff Non-Repudiation (Nichtabstreitbarkeit) verwendet.

Bei Kommunikation wird zusätzlich unterschieden, ob ein Kommunikationsteilnehmer den Nachrichtenempfang ableugnet (Repudiation of Receipt) oder den Versand (Repudiation of Origin). Den Nachrichtenempfang abzuleugnen kann unter anderem bei finanziellen Transaktionen von Bedeutung sein, z. B. wenn jemand bestreitet, eine Rechnung fristgemäß erhalten zu haben. Ebenso kann es passieren, dass ein Kommunikationsteilnehmer den Nachrichtenversand ableugnet, z.B. also eine getätigte Bestellung abstreitet. Nachrichtenversand oder -empfang kann beim Postversand ebenso abgeleugnet werden wie bei Fax- oder E-Mail-Nutzung.

Beispiel:

- Ein dringend benötigtes Ersatzteil wird elektronisch bestellt. Nach einer Woche wird das Fehlen reklamiert, inzwischen sind durch den Produktionsausfall hohe Kosten entstanden. Der Lieferant leugnet, je eine Bestellung erhalten zu haben.

Elementare Gefährdungen

G 0.38 Missbrauch personenbezogener Daten

Personenbezogene Daten sind fast immer besonders schützenswerte Informationen. Typische Beispiele sind Angaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Wenn der Schutz personenbezogener Daten nicht ausreichend gewährleistet ist, besteht die Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt wird.

Ein Missbrauch personenbezogener Daten kann beispielsweise vorliegen, wenn eine Institution zu viele personenbezogene Daten sammelt, sie ohne Rechtsgrundlage oder Einwilligung erhoben hat, sie zu einem anderen als dem bei der Erhebung zulässigen Zweck nutzt, personenbezogene Daten zu spät löscht oder unberechtigt weitergibt.

Beispiele:

- Personenbezogene Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben oder erstmals gespeichert worden sind. Es ist daher unzulässig, Protokolldateien, in denen die An- und Abmeldung von Benutzern an IT-Systemen ausschließlich für die Zugriffskontrolle festgehalten werden, zur Anwesenheits- und Verhaltenskontrolle zu nutzen.
- Personen, die Zugriff auf personenbezogene Daten haben, könnten diese unbefugt weitergeben. Beispielsweise könnte ein Mitarbeiter am Empfang eines Hotels die Anmeldedaten von Gästen an Werbefirmen verkaufen.

Elementare Gefährdungen

G 0.39 Schadprogramme

Ein Schadprogramm ist eine Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Zu den typischen Arten von Schadprogrammen gehören unter anderem Viren, Würmer und Trojanische Pferde. Schadprogramme werden meist heimlich, ohne Wissen und Einwilligung des Benutzers aktiv.

Schadprogramme bieten heutzutage einem Angreifer umfangreiche Kommunikations- und Steuerungsmöglichkeiten und besitzen eine Vielzahl von Funktionen. Unter anderem können Schadprogramme gezielt Passwörter ausforschen, Systeme fernsteuern, Schutzsoftware deaktivieren und Daten ausspionieren.

Als Schaden ist hier insbesondere der Verlust oder die Verfälschung von Informationen oder Anwendungen von größter Tragweite. Aber auch der Imageverlust und der finanzielle Schaden, der durch Schadprogramme entstehen kann, sind von großer Bedeutung.

Beispiele:

- In der Vergangenheit verbreitete sich das Schadprogramm W32/Bugbear auf zwei Wegen: Es suchte in lokalen Netzen nach Computern mit Freigaben, auf die schreibender Zugriff möglich war, und kopierte sich darauf. Zudem schickte es sich selbst als HTML-E-Mail an Empfänger im E-Mail-Adressbuch von befallenen Computern. Durch einen Fehler in der HTML-Routine bestimmter E-Mail-Programme wurde das Schadprogramm dort beim Öffnen der Nachricht ohne weiteres Zutun des Empfängers ausgeführt.
- Das Schadprogramm W32/Klez verbreitete sich in verschiedenen Varianten. Befallene Computer schickten den Virus an alle Empfänger im E-Mail-Adressbuch des Computers. Hatte dieser Virus einen Computer befallen, verhinderte er durch fortlaufende Manipulationen am Betriebssystem die Installation von Viren-Schutzprogrammen verbreiteter Hersteller und erschwerte so die Desinfektion der befallenen Computer erheblich.

Elementare Gefährdungen

G 0.40 Verhinderung von Diensten (Denial of Service)

Es gibt eine Vielzahl verschiedener Angriffsformen, die darauf abzielen, die vorgesehene Nutzung bestimmter Dienstleistungen, Funktionen oder Geräte zu verhindern. Der Oberbegriff für solche Angriffe ist "Verhinderung von Diensten" (englisch: "Denial of Service"). Häufig wird auch die Bezeichnung "DoS-Angriff" verwendet.

Solche Angriffe können unter anderem von verärgerten Mitarbeitern oder Kunden, aber auch von Mitbewerbern, Erpressern oder politisch motivierten Tätern ausgehen. Das Ziel der Angriffe können geschäftsrelevante Werte aller Art sein. Typische Ausprägungen von DoS-Angriffen sind

- Störungen von Geschäftsprozessen, z. B. durch Überflutung der Auftragsannahme mit fehlerhaften Bestellungen,
- Beeinträchtigungen der Infrastruktur, z. B. durch Blockieren der Türen der Institution,
- Herbeiführen von IT-Ausfällen, indem z. B. Dienste eines Servers im Netz gezielt überlastet werden.

Diese Art von Angriffen steht häufig im Zusammenhang mit verteilten Ressourcen, indem ein Angreifer diese Ressourcen so stark in Anspruch nimmt, dass sie den eigentlichen Nutzern nicht mehr zur Verfügung stehen. Bei IT-basierten Angriffen können z. B. die folgenden Ressourcen künstlich verknappt werden: Prozesse, CPU-Zeit, Arbeitsspeicher, Plattenplatz, Übertragungskapazität.

Beispiel:

- Im Frühjahr 2007 fanden über einen längeren Zeitraum starke DoS-Angriffe auf zahlreiche Internet-Angebote in Estland statt. Dadurch kam es in Estland zu erheblichen Beeinträchtigungen bei der Nutzung von Informationsangeboten und Dienstleistungen im Internet.

Elementare Gefährdungen

G 0.41 Sabotage

Sabotage bezeichnet die mutwillige Manipulation oder Beschädigung von Sachen oder Prozessen mit dem Ziel, dem Opfer dadurch Schaden zuzufügen. Besonders attraktive Ziele können Rechenzentren oder Kommunikationsanbindungen von Behörden bzw. Unternehmen sein, da hier mit relativ geringen Mitteln eine große Wirkung erzielt werden kann.

Die komplexe Infrastruktur eines Rechenzentrums kann durch gezielte Beeinflussung wichtiger Komponenten, gegebenenfalls durch Täter von außen, vor allem aber durch Innentäter, punktuell manipuliert werden, um Betriebsstörungen hervorzurufen. Besonders bedroht sind hierbei nicht ausreichend geschützte gebäudetechnische oder kommunikationstechnische Infrastruktur sowie zentrale Versorgungspunkte, die organisatorisch oder technisch gegebenenfalls auch nicht überwacht werden und für Externe leicht und unbeobachtet zugänglich sind.

Beispiele:

- In einem großen Rechenzentrum führte die Manipulation an der USV zu einem vorübergehenden Totalausfall. Der Täter hatte wiederholt die USV von Hand auf Bypass geschaltet und dann die Hauptstromversorgung des Gebäudes manipuliert. Insgesamt fanden in drei Jahren vier Ausfälle statt. Teilweise kam es sogar zu Hardware-Schäden. Die Betriebsunterbrechungen dauerten zwischen 40 und 130 Minuten.
- Innerhalb eines Rechenzentrums waren auch sanitäre Einrichtungen untergebracht. Durch Verstopfen der Abflüsse und gleichzeitiges Öffnen der Wasserzufuhr drang Wasser in zentrale Technikkomponenten ein. Die auf diese Weise verursachten Schäden führten zu Betriebsunterbrechungen des Produktivsystems.
- Für elektronische Archive stellt Sabotage ein besonderes Risiko dar, da hier meist auf kleinem Raum viele schützenswerte Dokumente verwahrt werden. Dadurch kann unter Umständen durch gezielte, wenig aufwendige Manipulationen ein großer Schaden verursacht werden.

Elementare Gefährdungen

G 0.42 Social Engineering

Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch soziale Handlungen zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Dadurch können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln. Ein typischer Fall von Angriffen mit Hilfe von Social Engineering ist das Manipulieren von Mitarbeitern per Telefonanruf, bei dem sich der Angreifer z. B. ausgibt als:

- Vorzimmerkraft, deren Vorgesetzter schnell noch etwas erledigen will, aber sein Passwort vergessen hat und es jetzt dringend braucht,
- Administrator, der wegen eines Systemfehlers anruft, da er zur Fehlerbehebung noch das Passwort des Benutzers benötigt.

Wenn kritische Rückfragen kommen, ist der Neugierige angeblich "nur eine Aushilfe" oder eine "wichtige" Persönlichkeit.

Eine weitere Strategie beim systematischen Social Engineering ist der Aufbau einer längeren Beziehung zum Opfer. Durch viele unwichtige Telefonate im Vorfeld kann der Angreifer Wissen sammeln und Vertrauen aufbauen, das er später ausnutzen kann.

Solche Angriffe können auch mehrstufig sein, indem in weiteren Schritten auf Wissen und Techniken aufgebaut wird, die in vorhergehenden Stufen erworben wurden.

Viele Anwender wissen, dass sie Passwörter an niemanden weitergeben dürfen. Social Engineers wissen dies und müssen daher über andere Wege an das gewünschte Ziel gelangen. Beispiele hierfür sind:

- Ein Angreifer kann das Opfer bitten, ihm unbekannte Befehle oder Applikationen auszuführen, z. B. weil dies bei einem IT-Problem helfen soll. Dies kann eine versteckte Anweisung für eine Änderung von Zugriffsrechten sein. So kann der Angreifer an sensible Informationen gelangen.
- Viele Benutzer verwenden zwar starke Passwörter, aber dafür werden diese für mehrere Konten genutzt. Wenn ein Angreifer einen nützlichen Netzdienst (wie ein E-Mail-Adressensystem) betreibt, an dem die Anwender sich authentisieren müssen, kann er an die gewünschten Passwörter und Logins gelangen. Viele Benutzer werden die Anmeldedaten, die sie für diesen Dienst benutzen, auch bei anderen Diensten verwenden.

Wenn sich Angreifer unerlaubt Passwörter oder andere Authentisierungsmerkmale verschaffen, beispielsweise mit Hilfe von Social Engineering, wird dies häufig auch als "Phishing" (Kunstwort aus "Password" und "Fishing") bezeichnet.

Beim Social Engineering tritt der Angreifer nicht immer sichtbar auf. Oft erfährt das Opfer niemals, dass es ausgenutzt wurde. Ist dies erfolgreich, muss der Angreifer nicht mit einer Strafverfolgung rechnen und besitzt außerdem eine Quelle, um später an weitere Informationen zu gelangen.

Elementare Gefährdungen

G 0.43 Einspielen von Nachrichten

Angreifer senden bei dieser Angriffsform speziell vorbereitete Nachrichten an Systeme oder Personen mit dem Ziel, für sich selbst einen Vorteil oder einen Schaden für das Opfer zu erreichen. Um die Nachrichten geeignet zu konstruieren, nutzen die Angreifer beispielsweise Schnittstellenbeschreibungen, Protokollspezifikationen oder Aufzeichnungen über das Kommunikationsverhalten in der Vergangenheit.

Es gibt zwei in der Praxis wichtige Spezialfälle des Einspielens von Nachrichten:

- Bei einer "Replay-Attacke" (Wiedereinspielen von Nachrichten) zeichnen Angreifer gültige Nachrichten auf und spielen diese Information zu einem späteren Zeitpunkt (nahezu) unverändert wieder ein. Es kann auch ausreichen, nur Teile einer Nachricht, wie beispielsweise ein Passwort, zu benutzen, um unbefugt in ein IT-System einzudringen.
- Bei einer "Man-in-the-Middle-Attacke" nimmt der Angreifer unbemerkt eine Vermittlungsposition in der Kommunikation zwischen verschiedenen Teilnehmern ein. In der Regel täuscht er hierzu dem Absender einer Nachricht vor, der eigentliche Empfänger zu sein, und er täuscht dem Empfänger vor, der eigentliche Absender zu sein. Wenn dies gelingt, kann der Angreifer dadurch Nachrichten, die nicht für ihn bestimmt sind, entgegennehmen und vor der Weiterleitung an den eigentlichen Empfänger auswerten und gezielt manipulieren.

Eine Verschlüsselung der Kommunikation bietet keinen Schutz vor Man-in-the-Middle-Attacken, wenn keine sichere Authentisierung der Kommunikationspartner stattfindet.

Beispiele:

- Ein Angreifer zeichnet die Authentisierungsdaten (z. B. Benutzerkennung und Passwort) während des Anmeldevorgangs eines Benutzers auf und verwendet diese Informationen, um sich Zugang zu einem System zu verschaffen. Bei rein statischen Authentisierungsprotokollen kann damit auch ein verschlüsselt übertragenes Passwort benutzt werden, um unbefugt auf ein fremdes System zuzugreifen.
- Um finanziellen Schaden beim Arbeitgeber (Unternehmen oder Behörde) zu verursachen, gibt ein Mitarbeiter eine genehmigte Bestellung mehrmals auf.

Elementare Gefährdungen

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

Wenn Unbefugte in ein Gebäude oder einzelne Räumlichkeiten eindringen, kann dies verschiedene andere Gefahren nach sich ziehen. Dazu gehören beispielsweise Diebstahl oder Manipulation von Informationen oder IT-Systemen. Bei qualifizierten Angriffen ist die Zeitdauer entscheidend, in der die Täter ungestört ihr Ziel verfolgen können.

Häufig wollen die Täter wertvolle IT-Komponenten oder andere Waren, die leicht veräußert werden können, stehlen. Ziel eines Einbruchs kann es jedoch unter anderem auch sein, an vertrauliche Informationen zu gelangen, Manipulationen vorzunehmen oder Geschäftsprozesse zu stören.

Durch das unbefugte Eindringen in Räumlichkeiten können somit mehrere Arten von Schäden entstehen:

- Schon durch das unbefugte Eindringen können Sachschäden entstehen. Fenster und/oder Türen werden gewaltsam geöffnet und dabei beschädigt, sie müssen repariert oder ersetzt werden.
- Entwendete, beschädigte oder zerstörte Geräte oder Komponenten müssen repariert oder ersetzt werden.
- Es können Schäden durch die Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder Anwendungen entstehen.

Beispiele:

- Vandalismus
- Bei einem Einbruch in ein Unternehmen an einem Wochenende wurde nur Bagatellschaden durch Aufhebeln eines Fensters angerichtet, lediglich eine Kaffeekasse und kleinere Einrichtungsgegenstände wurden entwendet. Bei einer Routinekontrolle wurde jedoch später festgestellt, dass ein zentraler Server genau zum Zeitpunkt des Einbruchs geschickt manipuliert wurde.

Elementare Gefährdungen

G 0.45 Datenverlust

Ein Datenverlust ist ein Ereignis, das dazu führt, dass ein Datenbestand nicht mehr wie erforderlich genutzt werden kann (Verlust der Verfügbarkeit). Eine häufige Form des Datenverlustes ist, dass Daten unbeabsichtigt oder unerlaubt gelöscht werden, zum Beispiel durch Fehlbedienung, Fehlfunktionen, Stromausfälle, Verschmutzung oder Schadsoftware.

Ein Datenverlust kann jedoch auch durch Beschädigung, Verlust oder Diebstahl von Geräten oder Datenträgern entstehen. Dieses Risiko ist bei mobilen Endgeräten und mobilen Datenträgern häufig besonders hoch.

Weiterhin ist zu beachten, dass viele mobile IT-Systeme nicht immer online sind. Die auf diesen Systemen gespeicherten Daten befinden sich daher nicht immer auf dem aktuellsten Stand. Wenn Datenbestände zwischen mobilen IT-Systemen und stationären IT-Systemen synchronisiert werden, kann es durch Unachtsamkeit oder Fehlfunktion zu Datenverlusten kommen.

Beispiele:

- Der PDA fällt aus der Hemdtasche und zerschellt auf den Fliesen, ein Mobiltelefon wird statt der Zeitung vom Hund apportiert, leider mit Folgen. Solche und ähnliche Ereignisse sind die Ursachen von vielen Totalverlusten der Daten mobiler Endgeräte.
- Es gibt Schadprogramme, die gezielt Daten auf infizierten IT-Systemen löschen. Bei einigen Schädlingen wird die Löschfunktion nicht sofort bei der Infektion ausgeführt, sondern erst, wenn ein definiertes Ereignis eintritt, zum Beispiel wenn die Systemuhr ein bestimmtes Datum erreicht.
- Viele Internet-Dienste können genutzt werden, um online Informationen zu speichern. Wenn das Passwort vergessen wird und nicht hinterlegt ist, kann es passieren, dass auf die gespeicherten Informationen nicht mehr zugegriffen werden kann, sofern der Dienstleister kein geeignetes Verfahren zum Zurücksetzen des Passwortes anbietet.
- Festplatten und andere Massenspeichermedien haben nur eine begrenzte Lebensdauer. Wenn keine geeigneten Redundanzmaßnahmen getroffen sind, kann es durch technische Defekte zu Datenverlusten kommen.

Elementare Gefährdungen

G 0.46 Integritätsverlust schützenswerter Informationen

Die Integrität von Informationen kann durch verschiedene Ursachen beeinträchtigt werden, z. B. durch Manipulationen, Fehlverhalten von Personen, Fehlbedienung von Anwendungen, Fehlfunktionen von Software oder Übermittlungsfehler.

- Durch die Alterung von Datenträgern kann es zu Informationsverlusten kommen.
- ÜbertragungsfehlerBei der Datenübertragung kann es zu Übertragungsfehlern kommen.
- SchadprogrammeDurch Schadprogramme können ganze Datenbestände verändert oder zerstört werden.
- FehleingabenDurch Fehleingaben kann es zu so nicht gewünschten Transaktionen kommen, die häufig lange Zeit nicht bemerkt werden.Angreifer können versuchen, Daten für ihre Zwecke zu manipulieren, z. B. um Zugriff auf weitere IT-Systeme oder Datenbestände zu erlangen.Durch Manipulation der Index-Datenbank können elektronische Archive veranlasst werden, gefälschte Dokumente zu archivieren oder wiederzugeben.
- Angreifer können versuchen, Daten für ihre Zwecke zu manipulieren, z. B. um Zugriff auf weitere IT-Systeme oder Datenbestände zu erlangen.Durch Manipulation der Index-Datenbank können elektronische Archive veranlasst werden, gefälschte Dokumente zu archivieren oder wiederzugeben.
- Durch Manipulation der Index-Datenbank können elektronische Archive veranlasst werden, gefälschte Dokumente zu archivieren oder wiederzugeben.

Wenn Informationen nicht mehr integer sind, kann es zu einer Vielzahl von Problemen kommen:

- Informationen können im einfachsten Fall nicht mehr gelesen, also weiterverarbeitet werden.Daten können versehentlich oder vorsätzlich so verfälscht werden, dass dadurch falsche Informationen weitergegeben werden. Hierdurch können beispielsweise Überweisungen in falscher Höhe oder an den falschen Empfänger ausgelöst werden, die Absenderangaben von E-Mails könnten manipuliert werden oder vieles mehr.Wenn verschlüsselte oder komprimierte Datensätze ihre Integrität verlieren (hier reicht die Änderung eines Bits), können sie unter Umständen nicht mehr entschlüsselt bzw. entpackt werden.Dasselbe gilt auch für kryptographische Schlüssel, auch hier reicht die Änderung eines Bits, damit die Schlüssel unbrauchbar werden. Dies führt dann ebenfalls dazu, dass Daten nicht mehr entschlüsselt oder auf ihre Authentizität überprüft werden können.Dokumente, die in elektronischen Archiven gespeichert sind, verlieren an Beweiskraft, wenn ihre Integrität nicht nachgewiesen werden kann.
- Daten können versehentlich oder vorsätzlich so verfälscht werden, dass dadurch falsche Informationen weitergegeben werden. Hierdurch können beispielsweise Überweisungen in falscher Höhe oder an den falschen Empfänger ausgelöst werden, die Absenderangaben von E-Mails könnten manipuliert werden oder vieles mehr.Wenn verschlüsselte oder komprimierte Datensätze ihre Integrität verlieren (hier reicht die Änderung eines Bits), können sie unter Umständen nicht mehr entschlüsselt bzw. entpackt werden.Dasselbe gilt auch für kryp-

tographische Schlüssel, auch hier reicht die Änderung eines Bits, damit die Schlüssel unbrauchbar werden. Dies führt dann ebenfalls dazu, dass Daten nicht mehr entschlüsselt oder auf ihre Authentizität überprüft werden können.Dokumente, die in elektronischen Archiven gespeichert sind, verlieren an Beweiskraft, wenn ihre Integrität nicht nachgewiesen werden kann.

- Wenn verschlüsselte oder komprimierte Datensätze ihre Integrität verlieren (hier reicht die Änderung eines Bits), können sie unter Umständen nicht mehr entschlüsselt bzw. entpackt werden.Dasselbe gilt auch für kryptographische Schlüssel, auch hier reicht die Änderung eines Bits, damit die Schlüssel unbrauchbar werden. Dies führt dann ebenfalls dazu, dass Daten nicht mehr entschlüsselt oder auf ihre Authentizität überprüft werden können.Dokumente, die in elektronischen Archiven gespeichert sind, verlieren an Beweiskraft, wenn ihre Integrität nicht nachgewiesen werden kann.
- Dasselbe gilt auch für kryptographische Schlüssel, auch hier reicht die Änderung eines Bits, damit die Schlüssel unbrauchbar werden. Dies führt dann ebenfalls dazu, dass Daten nicht mehr entschlüsselt oder auf ihre Authentizität überprüft werden können.Dokumente, die in elektronischen Archiven gespeichert sind, verlieren an Beweiskraft, wenn ihre Integrität nicht nachgewiesen werden kann.

Elementare Gefährdungen

G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe

IT-gestützte Angriffe können Auswirkungen haben, die

- von den Tätern nicht beabsichtigt sind oder
- nicht die unmittelbar angegriffenen Zielobjekte betreffen oder
- unbeteiligte Dritte schädigen.

Ursächlich hierfür sind die hohe Komplexität und Vernetzung moderner Informationstechnik sowie die Tatsache, dass die Abhängigkeiten der angegriffenen Zielobjekte und der zugehörigen Prozesse in der Regel nicht offenkundig sind.

Dadurch kann es unter anderem dazu kommen, dass der tatsächliche Schutzbedarf von Zielobjekten falsch eingeschätzt wird oder dass die Verantwortlichen für die Zielobjekte kein Eigeninteresse an der Behebung von Mängeln dieser Zielobjekte haben.

Beispiele:

- Auf IT-Systemen installierte Bots, mit denen die Täter verteilte Denial-of-Service-Angriffe (DDoS-Angriffe) durchführen können, stellen für die infizierten IT-Systeme selbst oft keine direkte Gefahr dar, weil sich die DDoS-Angriffe in der Regel gegen IT-Systeme Dritter richten.
- Schwachstellen von IoT-Geräten in WLANs können von Tätern als Einfallstor genutzt werden, um andere wichtigere Geräte im gleichen WLAN anzugreifen. Deshalb müssen solche IoT-Geräte auch dann geschützt werden, wenn sie selbst nur einen geringen Schutzbedarf haben.
- Ransomware-Angriffe auf IT-Systeme können unter Umständen Kettenreaktionen auslösen und damit auch Kritische Infrastrukturen treffen. Dies wiederum könnte zu Versorgungsengpässen der Bevölkerung führen, auch wenn die Täter dies möglicherweise gar nicht beabsichtigt haben.

ISMS: Sicherheitsmanagement

ISMS.1 Sicherheitsmanagement 109

ISMS: Sicherheitsmanagement

ISMS.1 Sicherheitsmanagement

1 Beschreibung

1.1 Einleitung

Mit (Informations-)Sicherheitsmanagement oder auch kurz IS-Management wird die Planungs-, Lenkungs- und Kontrollaufgabe bezeichnet, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen. Ein funktionierendes Sicherheitsmanagement muss in die existierenden Managementstrukturen einer jeden Institution eingebettet werden. Daher ist es praktisch nicht möglich, eine für jede Institution unmittelbar anwendbare Organisationsstruktur für das Sicherheitsmanagement anzugeben. Vielmehr werden häufig Anpassungen an spezifische Gegebenheiten erforderlich sein.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, aufzeigen, wie ein funktionierendes Informationssicherheitsmanagement eingerichtet und im laufenden Betrieb weiterentwickelt werden kann. Er beschreibt dazu sinnvolle Schritte eines systematischen Sicherheitsprozesses und gibt Anleitungen zur Erstellung eines umfassenden Sicherheitskonzeptes.

1.3 Abgrenzung

Der Baustein baut auf dem BSI-Standard 100-1 Managementsysteme für Informationssicherheit und BSI-Standard 100-2 Vorgehensweise nach IT-Grundschutz auf und fasst die wichtigsten Aspekte zum Sicherheitsmanagement hieraus zusammen.

2 Gefährdungslage

Bedrohungen und Schwachstellen im Umfeld des Sicherheitsmanagements können vielfältiger Natur sein. Häufig sind sie Symptom einer mangelhaften Gesamtorganisation des Sicherheitsprozesses. Stellvertretend für diese Vielzahl der Bedrohungen und Schwachstellen werden in diesem Baustein die folgenden typischen Gefährdungen betrachtet:

2.1 Fehlende persönliche Verantwortung im Sicherheitsprozess

Sind in einer Institution die Rollen im Sicherheitsprozess nicht eindeutig festgelegt, so ist es wahrscheinlich, dass viele Mitarbeiter ihre Verantwortung für die Informationssicherheit durch Verweis auf übergeordnete Hierarchie-Ebenen ablehnen. Als Folge werden Sicherheitsmaßnahmen nicht umgesetzt, da diese zunächst fast immer einen Mehraufwand im gewohnten Arbeitsablauf darstellen.

2.2 Mangelnde Unterstützung durch die Leitungsebene

Informationssicherheitsbeauftragte entstammen in der Regel nicht der Ebene der Behörden- bzw. Unternehmensleitung. Werden die Sicherheitsverantwortlichen nicht uneingeschränkt durch die Leitungsebene unterstützt, kann es schwierig werden, die notwendigen Maßnahmen auch von Personen, die in der Linienstruktur über ihnen stehen, wirksam einzufordern. In diesem Fall ist der Sicherheitsprozess nicht vollständig durchführbar.

2.3 Unzureichende strategische und konzeptionelle Vorgaben

In vielen Institutionen wird zwar ein Sicherheitskonzept erstellt, dessen Inhalt ist dann aber häufig nur wenigen Insidern bekannt. Dies führt dazu, dass die Vorgaben an Stellen, an denen organisatorischer Aufwand zu betreiben wäre, bewusst oder unbewusst nicht eingehalten werden. Sofern das Sicherheitskonzept strategische Zielsetzungen enthält, werden diese vielfach als bloße Sammlung von Absichtserklärungen betrachtet und keine ausreichenden Ressourcen für deren Umsetzung zur Verfügung gestellt. Vielfach wird fälschlicherweise davon ausgegangen, dass in einer automatisierten Umgebung Sicherheit automatisch produziert werde. Schadensfälle in der eigenen oder in ähnlich strukturierten Institutionen sind bisweilen Auslöser für mehr oder minder heftigen Aktionismus, bei dem häufig bestenfalls Teilaspekte verbessert werden.

2.4 Unzureichende oder fehlgeleitete Investitionen

Wenn die Leitungsebene einer Institution nicht ausreichend über den Sicherheitszustand der Geschäftsprozesse, IT-Systeme und Anwendungen und über vorhandene Mängel unterrichtet ist, werden nicht genügend Ressourcen für den Sicherheitsprozess bereitgestellt oder diese nicht sachgerecht eingesetzt. In letzterem Fall kann dies dazu führen, dass einem übertrieben hohen Sicherheitsniveau in einem Teilbereich schwerwiegende Mängel in einem anderen gegenüberstehen. Häufig ist auch zu beobachten, dass teure technische Sicherheitslösungen falsch eingesetzt werden und somit unwirksam sind oder sogar selbst zur Gefahrenquelle werden.

2.5 Unzureichende Durchsetzbarkeit von Sicherheitsmaßnahmen

Zur Erreichung eines durchgehenden und angemessenen Sicherheitsniveaus ist es erforderlich, dass unterschiedliche Zuständigkeitsbereiche innerhalb einer Institution miteinander kooperieren. Fehlende strategische Leitaussagen und unklare Zielsetzungen führen mitunter zu unterschiedlicher Interpretation der Bedeutung der Informationssicherheit. Dies kann zur Konsequenz haben, dass die notwendige Kooperation wegen vermeintlich fehlender Notwendigkeit oder ungenügender Priorisierung der Aufgabe "Informationssicherheit" letztlich unterbleibt und somit die Durchsetzbarkeit der Sicherheitsmaßnahmen nicht gegeben ist.

2.6 Fehlende Aktualisierung im Sicherheitsprozess

Neue Geschäftsprozesse, Anwendungen und IT-Systeme sowie neue Bedrohungen beeinflussen permanent den Status der Informationssicherheit innerhalb einer Institution. Fehlt ein effektives Revisionskonzept, das auch das Bewusstsein für die neuen Bedrohungen stärkt, verringert sich das Sicherheitsniveau und aus der realen Sicherheit wird schleichend eine gefährliche Scheinsicherheit.

2.7 Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen

Wenn Informationen, Geschäftsprozesse und IT-Systeme einer Institution unzureichend abgesichert sind (beispielsweise durch ein unzureichendes Sicherheitsmanagement), kann dies zu Verstößen gegen Rechtsvorschriften mit Bezug zur Informationsverarbeitung oder gegen bestehende Verträge mit Geschäftspartnern führen. Welche Gesetze jeweils zu beachten sind, hängt von der Art der Institution beziehungsweise ihrer Geschäftsprozesse und Dienstleistungen ab. Je nachdem, wo sich die Standorte einer Institution befinden, können auch verschiedene nationale und internationale Vorschriften zu beachten sein. Verfügt eine Institution über unzureichende Kenntnisse hinsichtlich internationaler Gesetzesvorgaben (zum Beispiel Datenschutz, Informationspflicht, Insolvenzrecht, Haftung oder Informationszugriff für Dritte), erhöht dies das Risiko entsprechender Verstöße. Es drohen rechtliche Konsequenzen.

In vielen Branchen ist es üblich, dass Anwender ihre Zulieferer und Dienstleister zur Einhaltung bestimmter Qualitäts- und Sicherheitsstandards verpflichten. In diesem Zusammenhang werden zunehmend auch Anforderungen an die Informationssicherheit gestellt. Verstößt ein Vertragspartner gegen vertraglich geregelte Sicherheitsanforderungen, kann dies Vertragsstrafen, aber auch Vertragsauflösungen bis hin zum Verlust von Geschäftsbeziehungen nach sich ziehen.

2.8 Störung der Geschäftsabläufe aufgrund von Sicherheitsvorfällen

Sicherheitsvorfälle können durch ein singuläres Ereignis oder eine Verkettung unglücklicher Umstände ausgelöst werden und dazu führen, dass Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen und IT-Systemen beeinträchtigt werden. Dies wirkt sich dann schnell negativ auf wesentliche Fachaufgaben und Geschäftsprozesse der betroffenen Institution aus. Auch wenn nicht alle Sicherheitsvorfälle in der Öffentlichkeit bekannt werden, können sie trotzdem zu negativen Auswirkungen in den Beziehungen zu Geschäftspartnern und Kunden führen. Dabei ist es nicht einmal so, dass die beträchtlichsten und weitreichendsten Sicherheitsvorfälle durch die größten Sicherheitsschwachstellen ausgelöst wurden. In vielen Fällen hat die Verkettung kleiner Ursachen zu riesigen Schäden geführt.

2.9 Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes Sicherheitsmanagement

Ein unzureichendes Sicherheitsmanagement kann dazu führen, dass falsche Prioritäten gesetzt werden und nicht an denjenigen Stellen investiert wird, die den größten Mehrwert für die Institution bringen. Dies kann zu folgenden Fehlern führen:

- Es wird in teure Sicherheitslösungen investiert, ohne dass eine Basis an notwendigen organisatorischen Regelungen vorhanden ist. Nicht geklärte Zuständigkeiten und Verantwortlichkeiten können trotz teurer Investitionen zu schweren Sicherheitsvorfällen führen.
- Es wird in den Bereichen einer Institution in Informationssicherheit investiert, die für Informationssicherheit besonders sensibilisiert sind. Andere Bereiche, die vielleicht für die Erfüllung der Fachaufgaben und der Erreichung der Geschäftsziele wichtiger sind, werden aufgrund von knappen Mitteln oder Desinteresse der Verantwortlichen vernachlässigt.
- Es wird nur in einzelne Teilbereiche investiert. Im Gesamtsystem verbleiben jedoch erhebliche Sicherheitslücken.
- Durch die einseitige Erhöhung des Schutzes einzelner Grundwerte kann sich der Gesamtschutz verringern.
- Ein inhomogener und unkoordinierter Einsatz von Sicherheitsprodukten kann zu hohem finanziellen und personellen Ressourceneinsatz führen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen für den Bereich Sicherheitsmanagement aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte (ISB) für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der ISB ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Informationssicherheitsbeauftragter (ISB)
Weitere Verantwortliche	Institutionsleitung, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene [Institutionsleitung]

Die Leitungsebene MUSS die Gesamtverantwortung für Informationssicherheit in der Institution übernehmen, so dass dies für alle Beteiligten deutlich erkennbar ist. Die Leitungsebene der Institution MUSS den Sicherheitsprozess initiieren, steuern und kontrollieren. Die Leitungsebene MUSS Informationssicherheit vorleben.

Die Behörden- bzw. Unternehmensleitung MUSS die Zuständigkeiten für Informationssicherheit festlegen und die zuständigen Mitarbeiter mit den erforderlichen Kompetenzen und Ressourcen ausstatten. Die Leitungsebene MUSS sich regelmäßig über den Status der Informationssicherheit informieren lassen, insbesondere MUSS sie sich über mögliche Risiken und Konsequenzen aufgrund fehlender Sicherheitsmaßnahmen informieren lassen.

ISMS.1.A2 Festlegung der Sicherheitsziele und -strategie [Institutionsleitung]

Der Sicherheitsprozess MUSS durch die Leitungsebene initiiert und etabliert werden. Dafür MÜSSEN angemessene Sicherheitsziele sowie eine Strategie für Informationssicherheit festgelegt und dokumentiert werden. Es MÜSSEN konzeptionelle Vorgaben erarbeitet und organisatorische Rahmenbedingungen geschaffen werden, um den ordnungsgemäßen und sicheren Umgang mit Informationen innerhalb aller Geschäftsprozesse des Unternehmens oder der Behörde zu ermöglichen.

Die Sicherheitsstrategie und -ziele MÜSSEN von der Institutionsleitung getragen und verantwortet werden. Sicherheitsziele und -strategie MÜSSEN regelmäßig daraufhin überprüft werden, ob sie noch aktuell und angemessen sind sowie wirksam umgesetzt werden können.

ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit [Institutionsleitung]

Die Leitungsebene MUSS eine übergeordnete Leitlinie zur Informationssicherheit verabschieden, die den Stellenwert der Informationssicherheit, die Sicherheitsziele, die wichtigsten Aspekte der Sicherheitsstrategie sowie die Organisationsstruktur für Informationssicherheit beschreibt. Für die Sicherheitsleitlinie MUSS ein klarer Geltungsbereich festgelegt sein. In der Leitlinie zur Informationssicherheit MÜSSEN die Sicherheitsziele und der Bezug der Sicherheitsziele zu den Geschäftszielen und Aufgaben der Institution erläutert werden.

Die Leitlinie zur Informationssicherheit MUSS allen Mitarbeitern und sonstigen Mitgliedern der Institution bekannt gegeben werden. Sie SOLLTE regelmäßig aktualisiert werden.

ISMS.1.A4 Benennung eines Informationssicherheitsbeauftragten [Institutionsleitung]

Die Leitungsebene MUSS einen Informationssicherheitsbeauftragten benennen, der die Informationssicherheit in der Institution fördert und den Sicherheitsprozess steuert und koordiniert. Der Informationssicherheitsbeauftragte MUSS mit angemessenen Ressourcen ausgestattet werden. Er MUSS die Möglichkeit haben, bei Bedarf direkt an die Leitungsebene zu berichten. Der Informationssicherheitsbeauftragte MUSS ausreichend qualifiziert sein und ausreichend Gelegenheit haben, sich fortzubilden.

Der Informationssicherheitsbeauftragte MUSS bei allen größeren Projekten sowie bei der Einführung neuer Anwendungen und IT-Systeme frühzeitig beteiligt werden.

ISMS.1.A5 Vertragsgestaltung bei Bestellung eines externen Informationssicherheitsbeauftragten [Institutionsleitung]

Wenn die Rolle des Informationssicherheitsbeauftragten nicht durch einen internen Mitarbeiter besetzt werden kann, MUSS ein externer Informationssicherheitsbeauftragten bestellt werden. Der hierzu geschlossene Dienstleistungsvertrag MUSS alle Aufgaben des Informationssicherheitsbeauftragten sowie die damit verbundenen Rechte und Pflichten umfassen. Der Vertrag MUSS eine geeignete Vertraulichkeitsvereinbarung umfassen. Der externe Informationssicherheitsbeauftragte MUSS über die notwendigen Qualifikationen verfügen. Der Vertrag MUSS eine kontrollierte Beendigung des Vertragsverhältnisses einschließlich Übergabe der Aufgaben an den Auftraggeber gewährleisten.

ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit [Institutionsleitung]

Es MUSS eine geeignete, übergreifende Organisationsstruktur für Informationssicherheit vorhanden sein. Dafür MÜSSEN Rollen definiert sein, die die verschiedenen Aufgaben für die Erreichung der Sicherheitsziele wahrnehmen. Außerdem MÜSSEN Personen benannt sein, die qualifiziert sind und denen ausreichend Ressourcen zur Verfügung stehen, um diese Rollen auszufüllen. Die Aufgaben, Verantwortungen und Kompetenzen im Sicherheitsmanagement MÜSSEN nachvollziehbar definiert und zugewiesen sein. Für alle wichtigen Funktionen der IS-Organisation MUSS es wirksame Vertretungsregelungen geben.

Kommunikationswege MÜSSEN geplant, beschrieben, eingerichtet und bekannt gemacht werden. Es MUSS für alle Aufgaben und Rollen festgelegt sein, wer wen informiert und wer bei welchen Aktionen in welchen Umfang informiert werden muss.

Es MUSS regelmäßig geprüft werden, ob die Organisationsstruktur für Informationssicherheit noch angemessen ist oder an neue Rahmenbedingungen angepasst werden muss.

ISMS.1.A7 Festlegung von Sicherheitsmaßnahmen

Im Rahmen des Sicherheitsprozesses MÜSSEN für die gesamte Informationsverarbeitung ausführliche und angemessene Sicherheitsmaßnahmen festgelegt werden. Alle Sicherheitsmaßnahmen SOLLTEN systematisch in Sicherheitskonzepten dokumentiert und regelmäßig aktualisiert werden.

ISMS.1.A8 Integration der Mitarbeiter in den Sicherheitsprozess [Vorgesetzte]

Alle Mitarbeiter MÜSSEN in den Sicherheitsprozess integriert sein, das heißt, sie müssen über Hintergründe und Gefährdungen informiert sein und Sicherheitsmaßnahmen kennen und umsetzen, die ihren Arbeitsplatz betreffen. Sie MÜSSEN in die Lage versetzt werden, Sicherheit aktiv mitzugestalten, also in ihre Geschäftsprozesse mit einzubringen. Daher SOLLTEN die Mitarbeiter frühzeitig bei der Planung von Sicherheitsmaßnahmen oder der Gestaltung organisatorischer Regelungen beteiligt werden.

Bei der Einführung von Sicherheitsrichtlinien und Sicherheitswerkzeugen MÜSSEN die Mitarbeiter ausreichend informiert sein, wie diese anzuwenden sind.

ISMS.1.A9 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse [Institutionsleitung]

Informationssicherheit MUSS in alle Geschäftsprozesse integriert werden. Es MUSS dabei gewährleistet sein, dass nicht nur bei neuen Prozessen und Projekten, sondern auch bei laufenden Aktivitäten alle erforderlichen Sicherheitsaspekte berücksichtigt werden. Informationssicherheit SOLLTE außerdem mit anderen Bereichen in der Institution, die sich mit Sicherheit und Risikomanagement beschäftigen, abgestimmt werden.

Der Informationssicherheitsbeauftragte MUSS an sicherheitsrelevanten Entscheidungen ausreichend beteiligt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Sicherheitsmanagement. Sie SOLLTEN grundsätzlich umgesetzt werden.

ISMS.1.A10 Erstellung eines Sicherheitskonzepts

Für den festgelegten Geltungsbereich (Informationsverbund) SOLLTE ein angemessenes Sicherheitskonzept als das zentrale Dokument im Sicherheitsprozess erstellt werden. Das Sicherheitskonzept kann auch aus mehreren Teilkonzepten bestehen, die sukzessive erstellt werden, um zunächst in ausgewählten Bereichen das erforderliche Sicherheitsniveau herzustellen.

Im Sicherheitskonzept MÜSSEN aus den Sicherheitszielen der Institution, dem identifizierten Schutzbedarf und der Risikobewertung konkrete Sicherheitsmaßnahmen passend zum betrachteten Informationsverbund abgeleitet werden. Sicherheitsprozess und Sicherheitskonzept MÜSSEN die individuell geltenden Vorschriften und Regelungen berücksichtigen.

Die im Sicherheitskonzept vorgesehenen Maßnahmen MÜSSEN zeitnah in die Praxis umgesetzt werden. Dies MUSS geplant und die Umsetzung kontrolliert werden. Es SOLLTE regelmäßig überprüft werden, ob die ausgewählten Maßnahmen geeignet, angemessen, umsetzbar und effizient sind, um die Sicherheitsziele und -anforderungen zu erreichen.

Jeder Mitarbeiter SOLLTE zumindest über die ihn unmittelbar betreffenden Teile des Sicherheitskonzeptes informiert sein.

ISMS.1.A11 Aufrechterhaltung der Informationssicherheit

Der Sicherheitsprozess, die Sicherheitskonzepte, die Leitlinie zur Informationssicherheit und die Organisationsstruktur für Informationssicherheit SOLLTEN regelmäßig auf Wirksamkeit und Angemessenheit überprüft und aktualisiert werden. Hierzu SOLLTEN regelmäßig Vollständigkeits- bzw. Aktualisierungsprüfungen des Sicherheitskonzeptes durchgeführt werden. Ebenso SOLLTEN regelmäßig Sicherheitsrevisionen durchgeführt werden. Dazu SOLLTE geregelt sein, welche Bereiche und Sicherheitsmaßnahmen wann und von wem zu überprüfen sind. Überprüfungen des Sicherheitsniveaus SOLLTEN regelmäßig (mindestens jährlich) sowie anlassbezogen durchgeführt werden.

Die Prüfungen SOLLTEN von qualifizierten und unabhängigen Personen durchgeführt werden. Die ermittelten Ergebnisse der Überprüfungen SOLLTEN nachvollziehbar dokumentiert sein. Darauf aufbauend SOLLTEN Mängel abgestellt und Korrekturmaßnahmen ergriffen werden.

ISMS.1.A12 Management-Berichte zur Informationssicherheit [Institutionsleitung]

Die Leitungsebene SOLLTE regelmäßig über den Stand der Informationssicherheit informiert werden, vor allem über die aktuelle Gefährdungslage und Wirksamkeit und Effizienz des Sicherheitsprozesses, um das weitere Vorgehen im Sicherheitsprozess steuern zu können. Die Management-Berichte SOLLTEN die wesentlichen relevanten Informationen über den Sicherheitsprozess enthalten, insbesondere über Probleme, Erfolge und Verbesserungsmöglichkeiten. Sie SOLLTEN klar priorisierte und mit realistischen Abschätzungen des zu erwartenden Umsetzungsaufwands versehene Maßnahmenvorschläge enthalten.

Die Management-Entscheidungen über erforderliche Aktionen, Umgang mit Restrisiken und mit Veränderungen von sicherheitsrelevanten Prozessen SOLLTEN dokumentiert sein. Die Management-Berichte und Management-Entscheidungen SOLLTEN revisionssicher archiviert werden.

ISMS.1.A13 Dokumentation des Sicherheitsprozesses

Der Ablauf des Sicherheitsprozesses, wichtige Entscheidungen und die Arbeitsergebnisse der einzelnen Phasen wie Sicherheitskonzept, Richtlinien oder Untersuchungsergebnisse von Sicherheitsvorfällen SOLLTEN ausreichend dokumentiert werden.

Es SOLLTE eine geregelte Vorgehensweise für die Erstellung und Archivierung von Dokumentationen im Rahmen des Sicherheitsprozesses geben. Es SOLLTEN Regelungen existieren, um die Aktualität und Vertraulichkeit der Dokumentationen zu wahren. Von den vorhandenen Dokumenten SOLLTE die jeweils aktuelle Version kurzfristig zugänglich sein. Außerdem SOLLTEN alle Vorgängerversionen zentral archiviert werden.

ISMS.1.A14 Sensibilisierung zur Informationssicherheit

Alle Mitarbeiter der Institution und sonstige relevante Personen (wie extern Beschäftigte oder Projektmitarbeiter) SOLLTEN systematisch und zielgruppengerecht zu Sicherheitsrisiken sensibilisiert und zu Fragen der Informationssicherheit geschult werden (siehe ORP.3 Sensibilisierung und Schulung zur Informationssicherheit).

ISMS.1.A15 Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit

Informationssicherheit erfordert ausreichende finanzielle und personelle Ressourcen sowie eine geeignete Ausstattung. Der Bedarf SOLLTE vom ISB der Leitungsebene kommuniziert werden, diese SOLLTE die erforderlichen Ressourcen bereitstellen.

Die Sicherheitsstrategie SOLLTE wirtschaftliche Aspekte berücksichtigen. Bei der Festlegung von Sicherheitsmaßnahmen SOLLTEN die für die Umsetzung erforderlichen Ressourcen beziffert werden. Die für Informationssicherheit eingeplanten Ressourcen SOLLTEN termingerecht bereitgestellt werden. Der Informationssicherheitsbeauftragte bzw. das Informationssicherheitsmanagement-Team MÜSSEN genügend Zeit für ihre Sicherheitsaufgaben haben. Bei Arbeitsspitzen oder besonderen Aufgaben SOLLTEN zusätzliche interne Mitarbeiter eingesetzt oder auf externe Experten zurückgegriffen werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

ISMS.1.A16 Erstellung von zielgruppengerechten Sicherheitsrichtlinien (CIA)

Alle Mitarbeiter SOLLTEN die ihren Arbeitsbereich betreffenden Sicherheitsaspekte kennen und beachten. Um Sicherheitsthemen zielgruppengerecht zu vermitteln, SOLLTE es neben den allgemeinen auch zielgruppenorientierte Sicherheitsrichtlinien geben, die bedarfsgerecht die relevanten Sicherheitsthemen abbilden.

ISMS.1.A17 Abschließen von Versicherungen (A)

Es SOLLTE geprüft werden, ob für Restrisiken Versicherungen abgeschlossen werden sollen, um eventuelle Schäden abzudecken. Es SOLLTE regelmäßig überprüft werden, ob die bestehenden Versicherungen der aktuellen Lage entsprechen.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [27002] ISO/IEC 27002:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013

- [BSI1] Managementsysteme für Informationssicherheit, BSI Standard 100-1
  BSI Standard 200-1, Bundesamt für Sicherheit in der Informationstechnik, Version 1, 2017, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/IT-Grundschutz-Modernisierung/GS_Standards/gs_standards_node.html

- [BSI2] IT-Grundschutz-Vorgehensweise, BSI-Standard 200-2
  BSI Standard 200-2, Bundesamt für Sicherheit in der Informationstechnik, Version 1, 2017
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/IT-Grundschutz-Modernisierung/GS_Standards/gs_standards_node.html

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Sicherheitsmanagement" von Bedeutung.

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen

Elementare Gefährdungen / Anforderungen	G 0.18	G 0.27	G 0.29
ISMS.1.A1	x	x	
ISMS.1.A2	x		
ISMS.1.A3	x		
ISMS.1.A4	x	x	
ISMS.1.A5	x		
ISMS.1.A6	x		
ISMS.1.A7	x		
ISMS.1.A8	x		x
ISMS.1.A9	x		
ISMS.1.A10	x		
ISMS.1.A11	x		x
ISMS.1.A12			x
ISMS.1.A13	x		
ISMS.1.A14			x
ISMS.1.A15	x		x
ISMS.1.A16	x	x	
ISMS.1.A17	x		

Bundesamt
für Sicherheit in der
Informationstechnik

ORP: Organisation und Personal

ORP.5	Compliance Management (Anforderungsmanagement)	**148**
ORP.2	Personal	**126**
ORP.4	Identitäts- und Berechtigungsmanagement	**140**
ORP.1	Organisation	**119**
ORP.3	Sensibilisierung und Schulung	**133**

IT-Grundschutz

ORP: Organisation und Personal

ORP.1 Organisation

1 Beschreibung

1.1 Einleitung

Jedes Unternehmen und jede Behörde muss eine Organisation haben, die das Zusammenspiel der verschiedenen Rollen und Einheiten mit den Geschäftsprozessen und Ressourcen in der Institution steuert. Die meisten Institutionen haben eine Organisationseinheit, die für Regelung und Steuerung des allgemeinen Betriebs sowie für Planung, Organisation und Durchführung aller Verwaltungsdienstleistungen verantwortlich ist. Diverse Aufgaben der Informationssicherheit müssen von dieser Einheit umgesetzt oder mitgetragen werden.

1.2 Zielsetzung

Mit diesem Bausteins werden Anforderungen an eine Organisation beschrieben, die dazu dienen, dass Informationssicherheit geeignet, gesteuert und betrieben werden kann.

1.3 Abgrenzung

In diesem Baustein werden allgemeine und übergreifende Anforderungen im Bereich Organisation zur Schaffung der Informationssicherheit aufgeführt. Dazu sind Informationsflüsse, Prozesse, Rollenverteilung, die Aufbau- und Ablauforganisation zu regeln. Der Baustein Organisation bildet damit den Rahmen für die Umsetzung der Informationssicherheit durch andere Bausteine. Spezielle Anforderungen organisatorischer Art, die in unmittelbarem Zusammenhang mit Anforderungen anderer Bausteine stehen (z. B. Server-Administration), werden in den entsprechenden Bausteinen aufgeführt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Organisation von besonderer Bedeutung:

2.1 Fehlende oder unzureichende Regelungen

Die Bedeutung übergreifender organisatorischer Regelungen und Vorgaben für das Ziel Informationssicherheit, z. B. zu den Zuständigkeiten oder der Verteilung von Kontrollaufgaben, nimmt mit der Komplexität der Geschäftsprozesse und dem Umfang der Informationsverarbeitung, aber auch mit dem Schutzbedarf der zu verarbeitenden Informationen zu.

Fehlende Regelungen können zu massiven Sicherheitslücken führen, beispielsweise weil Mitarbeiter nicht wissen, wie sie bei Vorfällen reagieren sollen. Probleme können auch dadurch entstehen, dass Regelungen veraltet, unpraktikabel, oder unverständlich formuliert sind.

2.2 Nicht beachtete Regelungen

Regelungen lediglich festzulegen, führt noch nicht dazu, dass sie beachtet werden. Allen Mitarbeitern müssen die geltenden Regelungen auch bekannt sein. Ein Schaden, der entsteht, weil bestehende Regelungen nicht bekannt sind, darf sich nicht mit den Aussagen entschuldigen lassen: "Ich habe nicht gewusst, dass ich dafür zuständig bin." oder "Ich habe nicht gewusst, wie ich zu verfahren hatte."

Beispiele für Folgeschäden durch nicht eingehaltene Regelungen sind:

- Vertrauliche Informationen werden in Hörweite fremder Personen diskutiert, beispielsweise in Pausengesprächen von Besprechungen oder über Mobiltelefonate in öffentlichen Umgebungen.
- Dokumente werden auf einem Webserver veröffentlicht, ohne dass geprüft wurde, ob diese tatsächlich zur Veröffentlichung vorgesehen und freigegeben sind.
- Aufgrund von fehlerhaft administrierten Zugriffsrechten kann ein Mitarbeiter Daten zu ändern, ohne die Brisanz dieser Integritätsverletzung einschätzen zu können.

2.3 Fehlende, ungeeignete, inkompatible Betriebsmittel

Eine nicht ausreichende Bereitstellung von Betriebsmitteln kann einen Betrieb erheblich beeinträchtigen. Störungen können sich ergeben, wenn benötigte Betriebsmittel nicht in ausreichender Menge vorhanden sind oder nicht termingerecht bereit gestellt werden. Ebenso kann es vorkommen, dass ungeeignete oder sogar inkompatible Betriebsmittel beschafft werden, die infolgedessen nicht eingesetzt werden können.

Beispiel: Der Speicherplatz der Festplatten bei PCs und Servern und auch der mobilen Datenträger steigt ständig. Leider wird häufig vergessen, IT-Komponenten und Datenträger zu beschaffen, die für eine regelmäßige Datensicherung ausreichend Kapazität bieten.

Ebenso muss die Funktionsfähigkeit der eingesetzten Betriebsmittel gewährleistet sein. Werden Wartungsarbeiten nicht oder nur unzureichend durchgeführt, können daraus hohe Schäden entstehen. Beispiele:

- Die Batterien einer unterbrechungsfreien Stromversorgung (USV) verfügen infolge fehlender Wartung über eine unzureichende Kapazität (zu geringer Säuregehalt). Die USV kann einen Stromausfall nicht mehr ausreichend lange überbrücken.
- Die Feuerlöscher verfügen aufgrund fehlender Wartung nicht mehr über einen ausreichenden Druck, so dass ihre brandbekämpfende Wirkung nicht mehr gewährleistet ist.

2.4 Unbefugter Zutritt zu schutzbedürftigen Räumen

Alle Räume, inklusive dienstlich genutzter Räume im häuslichen Umfeld oder unterwegs, in denen schutzbedürftige Informationen aufbewahrt bzw. weiterverarbeitet werden, müssen vor dem unbefugtem Zutritt von Dritten geschützt werden. Unbefugte Personen können in solchen Räumen durch vorsätzliche Handlungen (Manipulationen oder Vandalismus), aber auch durch unbeabsichtigtes Fehlverhalten (aufgrund mangelnder Fachkenntnisse) Schäden verursachen. Selbst wenn keine unmittelbaren Schäden erkennbar sind, kann der Betriebsablauf schon dadurch gestört werden, falls untersucht werden muss, wie ein solcher Vorfall möglich war oder ob Schäden aufgetreten sind oder Manipulationen vorgenommen wurden.

Eindringlinge könnten beispielsweise Passwörter zurückgesetzt, direkt auf die Server zugegriffen oder aktive Netzkomponenten manipuliert haben. Außerdem könnten sie sensible Informationen auf Papier oder Datenträgern entwendet oder verändert haben.

2.5 Unerlaubte Ausübung von Rechten

Rechte wie Zutritts-, Zugangs- und Zugriffsberechtigungen werden als organisatorische Maßnahmen eingesetzt, um Informationen, Geschäftsprozesse und IT-Systeme vor unbefugtem Zugriff zu schützen. Werden solche Rechte an die falsche Person vergeben oder wird ein Recht unautorisiert ausgeübt, können sich eine Vielzahl von Gefahren daraus ergeben. Beispielsweise könnten Unbefugte Zugang zu Personaldaten erhalten.

2.6 Gefährdung durch Betriebsfremde

Bei Betriebsfremden kann grundsätzlich nicht vorausgesetzt werden, dass sie mit ihnen zugänglichen Informationen und der Informationstechnik entsprechend den Vorgaben der besuchten Institution umgehen, vor allem, da sie diese in den seltensten Fällen kennen.

Besucher, Reinigungs- und Fremdpersonal können interne Informationen, Geschäftsprozesse und-Systeme auf verschiedene Art und Weise gefährden, angefangen von der unsachgemäßen Behandlung der technischen Einrichtungen, über den Versuch des "Spielens" an IT-Systemen bis zum Diebstahl von Unterlagen oder IT-Komponenten.

Beispiele:

- Besucher können, wenn sie unbegleitet sind, Zugriff auf Unterlagen, Datenträger oder Geräte haben, diese beschädigen oder unbefugt Kenntnis von schützenswerten Informationen erlangen.
- Durch Reinigungspersonal kann versehentlich eine Steckverbindung gelöst werden, Wasser kann in Geräte gelangen, Unterlagen können verlegt oder sogar mit dem Abfall entfernt werden.

2.7 Manipulation von Informationen und Geräten

Außentäter, aber auch Innentäter, können Mängel in der Organisation nutzen und versuchen, Geräte, Zubehör, Schriftstücke und andere Datenträger zu manipulieren. Manipulationen können dabei vom falschen Erfassen von Daten, der Änderungen von Zugriffsrechten bis hin zur Manipulation von Betriebssystemen, Datenträgern oder IT-Systemen reichen. Die Angriffe sind umso wirkungsvoller, je später sie entdeckt werden, je umfassender die Kenntnisse des Täters sind und je tief greifender die Folgen für einen Arbeitsvorgang sind.

Beispiel: In einem Schweizer Finanzunternehmen wurde durch einen Mitarbeiter die Einsatzsoftware für bestimmte Finanzdienstleistungen manipuliert. Damit war es ihm möglich, sich illegal größere Geldbeträge zu verschaffen.

2.8 Zerstörung, Vandalismus, Sabotage

Personen können aus unterschiedlichen Beweggründen (Rache, Böswilligkeit, Frust) heraus versuchen, Geschäftsprozesse zu stören, Geräte oder Informationen zu manipulieren oder zu zerstören.

Sowohl Außentäter (z. B. enttäuschte Einbrecher, außer Kontrolle geratene Demonstranten) als auch Innentäter (z. B. frustrierte oder psychisch labile Mitarbeiter) können durch Vandalismus fremdes Eigentum zerstören oder beschädigen. Während Vandalismus meist Ausdruck spontaner, blinder Zerstörungswut ist, bezeichnet Sabotage die mutwillige Manipulation oder Beschädigung von Sachen mit dem Ziel, dem Opfer Schaden zuzufügen. Besonders attraktive Ziele von Sabotage können Rechenzentren oder Kommunikationsanbindungen von Behörden bzw. Unternehmen sein, da hier mit relativ geringen Mitteln eine große Wirkung erzielt werden kann.

2.9 Diebstahl und Verlust von Informationen und Geräten

Der Diebstahl oder Verlust von Datenträgern, IT-Systemen oder Daten kann neben den unmittelbaren materiellen Verlusten zu diversen Folgeschäden führen, wenn keine angemessenen organisatorischen Vorkehrungen getroffen worden sind.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz im Bereich der Organisation aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte (ISB) für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt.

Bausteinverantwortlicher	Leiter Organisation
Weitere Verantwortliche	Haustechnik, ICS-Informationssicherheitsbeauftragter, IT-Betrieb, Informationssicherheitsbeauftragter (ISB), Institutionsleitung, Leiter Haustechnik, Leiter IT, Leiter Produktion und Fertigung, Mitarbeiter

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

ORP.1.A1 Festlegung von Verantwortlichkeiten und Regelungen [Institutionsleitung]

Für alle sicherheitsrelevanten Aufgaben MÜSSEN sowohl Verantwortlichkeiten als auch Befugnisse festgelegt sein. Es MÜSSEN verbindliche Regelungen zur Informationssicherheit für die verschiedenen betrieblichen Aspekte übergreifend festgelegt werden. Es MUSS auch klar geregelt sein, welche Informationen mit wem ausgetauscht werden dürfen und wie diese dabei zu schützen sind.Die Regelungen MÜSSEN regelmäßig überarbeitet werden. Sie MÜSSEN allen Mitarbeitern bekannt gegeben werden.

ORP.1.A2 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten [Leiter IT, Informationssicherheitsbeauftragter (ISB), Institutionsleitung]

Für alle Informationen, Geschäftsprozesse, Anwendungen und IT-Komponenten MUSS festgelegt werden, wer für diese und deren Sicherheit verantwortlich ist. Alle Mitarbeiter MÜSSEN darüber informiert sein, insbesondere wofür sie in welcher Weise verantwortlich sind.

ORP.1.A3 Beaufsichtigung oder Begleitung von Fremdpersonen [Mitarbeiter]

Die Mitarbeiter MÜSSEN dazu angehalten werden, betriebsfremde Personen nicht unbeaufsichtigt zu lassen.

ORP.1.A4 Funktionstrennung zwischen operativen und kontrollierenden Aufgaben

Innerhalb einer Institution SOLLTEN alle relevanten Aufgaben und Funktionen definiert und klar voneinander abgegrenzt sein. Die Aufgaben und die hierfür erforderlichen Rollen und Funktionen MÜSSEN so strukturiert sein, dass operative und kontrollierende Funktionen auf verschiedene Personen verteilt werden. Für unvereinbare Funktionen MUSS eine Funktionstrennung festgelegt und dokumentiert sein. Auch Vertreter MÜSSEN der Funktionstrennung unterliegen.

ORP.1.A5 Vergabe von Berechtigungen [Leiter IT]

Es MUSS festgelegt werden, welche Zutritts-, Zugangs- und Zugriffsrechte an welche Personen im Rahmen ihrer Aufgaben und Funktionen vergeben werden. Es DÜRFEN immer nur so viele Rechte vergeben werden, wie für die Aufgabenwahrnehmung notwendig ist. Es MUSS ein geregeltes Verfahren für die Vergabe, die Verwaltung und den Entzug von Berechtigungen geben (siehe auch ORP.4 Identitäts- und Berechtigungsmanagement). Die Dokumentation der Berechtigungen MUSS aktuell und vollständig sein.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Organisation. Sie SOLLTEN grundsätzlich umgesetzt werden.

ORP.1.A6 Der aufgeräumte Arbeitsplatz [Mitarbeiter]

Alle Mitarbeiter SOLLTEN darauf hingewiesen werden, dass an unbeaufsichtigten Arbeitsplätzen weder sensible Informationen noch IT-Systeme frei zugänglich sein dürfen. Arbeitsplätze SOLLTEN stichprobenartig kontrolliert werden, ob schutzbedürftige Informationen offen zugreifbar sind.

ORP.1.A7 Geräteverwaltung [Leiter IT, Leiter Produktion und Fertigung, Leiter Haustechnik]

Es SOLLTE eine Übersicht vorhanden sein über alle Geräten, die in der Institution genutzt werden und die Einfluss auf die Informationssicherheit haben können. Dazu gehören neben IT-Systemen und ICS-Komponenten auch solche aus dem Bereich Internet of Things. Es SOLLTE geeignete Prüf- und Genehmigungsverfahren vor Einsatz der Geräte geben.

ORP.1.A8 Betriebsmittelverwaltung [Leiter IT]

Die Betriebsmittel, die zur Aufgabenerfüllung und zur Einhaltung der Sicherheitsanforderungen erforderlich sind, SOLLTEN in ausreichender Menge vorhanden sein. Es SOLLTE geeignete Prüfverfahren vor Einsatz der Betriebsmittel geben. Für die Bestandsführung SOLLTEN die Betriebsmittel in Bestandsverzeichnissen aufgelistet werden. Um den Missbrauch von Daten zu verhindern, SOLLTE die zuverlässige Löschung oder Vernichtung von Betriebsmitteln geregelt sein.

ORP.1.A9 Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln [Mitarbeiter, Informationssicherheitsbeauftragter (ISB)]

Betriebs- und Sachmittel SOLLTEN so entsorgt werden, dass keine Rückschlüsse auf ihre Verwendung oder Inhalte gezogen werden können. Die Entsorgung von schutzbedürftigen Materialien SOLLTE geregelt sein. Alle Mitarbeiter SOLLTEN diese Regelungen kennen. Zur Entsorgung von schutzbedürftigem Material SOLLTEN geeignete Entsorgungseinrichtungen wie z. B. Aktenvernichter vorhanden sein. Zur Entsorgung gesammeltes schutzbedürftiges Material SOLLTE vor unberechtigtem Zugriff geschützt sein.

ORP.1.A10 Reaktion auf Verletzungen der Sicherheitsvorgaben [Informationssicherheitsbeauftragter (ISB)]

Es SOLLTE geregelt sein, welche Reaktionen bei Verdacht auf Verletzungen der Sicherheitsvorgaben erfolgen. Nur so ist eine zielgerichtete und zeitnahe Reaktion möglich.

ORP.1.A11 Rechtzeitige Beteiligung der Personalvertretung [Leiter IT]

Die Personalvertretung (Arbeitnehmer-, Mitarbeitervertretung) SOLLTE bei sie betreffenden Verfahren und Projekten rechtzeitig informiert werden.

ORP.1.A12 Regelungen für Wartungs- und Reparaturarbeiten [IT-Betrieb, Haustechnik, ICS-Informationssicherheitsbeauftragter]

Technische Geräte SOLLTEN regelmäßig gewartet werden. Es SOLLTE geregelt sein, welche Sicherheitsaspekte bei Wartungs- und Reparaturarbeiten zu beachten sind und wer für die Wartung oder Reparatur von Geräten verantwortlich ist. Mitarbeiter SOLLTEN wissen, dass Wartungspersonal bei Arbeiten im Haus beaufsichtigt werden muss. Durchgeführte Wartungsarbeiten SOLLTEN dokumentiert werden.

ORP.1.A13 Sicherheit bei Umzügen [Leiter IT, Leiter Haustechnik, Informationssicherheitsbeauftragter (ISB)]

Vor einem geplanten Umzug SOLLTEN rechtzeitig Sicherheitsrichtlinien für diesen Zweck erarbeitet bzw. aktualisiert werden. Alle Mitarbeiter SOLLTEN über die vor, während und nach dem Umzug zu beachtenden Sicherheitsmaßnahmen informiert werden. Während des Umzugs SOLLTE ein Mindestmaß an Zutritts- und Zugangskontrolle vorhanden sein. Es SOLLTE nach dem Umzug überprüft werden, dass das zu transportierende Umzugsgut vollständig und unbeschädigt bzw. unverändert angekommen ist.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

ORP.1.A14 Kontrollgänge [Haustechnik, Informationssicherheitsbeauftragter (ISB)] (CIA)

Es SOLLTEN Kontrollgänge durchgeführt werden, um zu überprüfen, inwieweit Sicherheitsvorgaben umgesetzt werden. Einfach zu behebende Nachlässigkeiten SOLLTEN sofort behoben werden (z. B. Fenster schließen). Darüber hinaus SOLLTEN Ursachen hinterfragt und beseitigt werden.

4 Weiterführende Informationen

4.1 Literatur

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Organisation" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.38 Missbrauch personenbezogener Daten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.14	G 0.16	G 0.17	G 0.18	G 0.19	G 0.22	G 0.25	G 0.26	G 0.27	G 0.29	G 0.38	G 0.45	G 0.46
ORP.1.A1	x			x	x	x				x	x		x
ORP.1.A2	x	x		x	x	x	x	x	x	x	x		x
ORP.1.A3	x	x			x	x							
ORP.1.A4					x	x				x	x		
ORP.1.A5	x	x			x	x					x		x
ORP.1.A6	x	x			x	x					x		x
ORP.1.A7	x	x		x	x	x	x	x					
ORP.1.A8	x	x		x	x				x				
ORP.1.A9	x				x						x		
ORP.1.A10	x	x	x		x	x	x	x		x	x	x	x
ORP.1.A11				x						x			
ORP.1.A12	x			x	x	x	x	x	x		x		x
ORP.1.A13	x	x		x	x	x	x	x			x		x
ORP.1.A14	x	x			x	x							

ORP: Organisation und Personal

ORP.2 Personal

1 Beschreibung

1.1 Einleitung

Das Personal eines Unternehmens bzw. einer Behörde bildet die Grundlage für dessen bzw. deren Erfolg oder Misserfolg. Gleichzeitig sind die Mitarbeiterinnen und Mitarbeiter ein wesentlicher Bestandteil der Informationssicherheit. Wie die Erfahrung zeigt, sind selbst die aufwendigsten Sicherheitsvorkehrungen ohne das richtige Verhalten der Mitarbeiter wirkungslos. Ein Bewusstsein dafür, was Informationssicherheit für die Institution und deren Geschäftsprozesse bedeutet und der richtige Umgang der Mitarbeiter mit den zu schützenden Informationen der Institution sind daher wesentlich.

1.2 Zielsetzung

Ziel dieses Bausteins ist es aufzuzeigen, welche personellen Sicherheitsmaßnahmen durch die Personalabteilung oder die Vorgesetzten einer Institution zu ergreifen sind, damit die Mitarbeiterinnen und Mitarbeiter sicher mit den Informationen der Institution umgehen und sich so verhalten, wie es den Sicherheitszielen der Institution und den Sicherheitsanforderungen der zu schützenden Informationen entspricht. Beginnend mit der Einstellung von Mitarbeitern bis hin zu deren Weggang ist eine Vielzahl von Maßnahmen erforderlich. Darüber hinaus dürfen natürlich auch weitere Personengruppen, die mit den Informationen der Institution in Berührung kommen, nicht vergessen werden, wie Mitarbeiter von Dienstleistern und Kunden. Auch für den Umgang mit Externen, wie z. B. Besuchern, Reinigungspersonal oder Wartungstechnikern, müssen angemessene Sicherheitsmaßnahmen vorhanden sein.

1.3 Abgrenzung

Dieser Baustein beschäftigt sich mit den Anforderungen, die durch die Personalabteilung oder die Vorgesetzten einer Institution zu beachten und zu erfüllen sind. Personelle Anforderungen, die an eine bestimmte Funktion gebunden sind, wie z. B. die Ernennung des Systemadministrators eines LAN, werden in den Bausteinen angeführt, die sich mit dem jeweiligen Themengebiet beschäftigen.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Personal von besonderer Bedeutung:

2.1 Personalausfall

Der Ausfall von Personal kann dazu führen, dass bestimmte Aufgaben nicht mehr oder nicht zeitnah wahrgenommen werden können.

2.2 Missbrauch von Berechtigungen

Jeder, der Informationen bearbeiten soll, benötigt dafür angemessene Berechtigungen. Nutzer können diese missbrauchen, indem sie diese ausnutzen, um Informationen zu manipulieren, weiterzugeben oder auf andere Weise der Institution zu schaden.

2.3 Fehlende oder unzureichende Regelungen

Wenn Regelungen zur Informationssicherheit fehlen, unzureichend, nicht umsetzbar oder unverständlich sind, kann das dazu führen, dass notwendige Sicherheitsmaßnahmen nicht umgesetzt werden (siehe auch G 0.29 Verstoß gegen Gesetze oder Regelungen).

2.4 Unzureichende Kenntnis über Regelungen

Die Festlegung von Regelungen allein sichert noch nicht deren Beachtung und keinen störungsfreien Betrieb. Allen Mitarbeitern müssen die geltenden Regelungen auch bekannt sein, vor allem den Funktionsträgern. Ein Schaden, der entsteht, weil bestehende Regelungen nicht bekannt sind, darf sich nicht mit den Aussagen entschuldigen lassen: "Ich habe nicht gewusst, dass ich dafür zuständig bin." oder "Ich habe nicht gewusst, wie ich zu verfahren hatte."

2.5 Fehlverhalten

Fehlverhalten von Personen aller Art kann dazu führen, dass Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen, Geschäftsprozessen oder IT-Systemen gestört werden. Je nach Schutzbedarf der Informationen oder der Systeme und je nach Berechtigungen der Verursacher können die Schäden gering oder kritisch sein.

2.6 Social Engineering

Beim Social Engineering werden menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt, um unberechtigten Zugang zu Informationen oder IT-Systemen durch "Aushorchen" zu erlangen. Dadurch können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln.

2.7 Sorglosigkeit im Umgang mit Informationen

Häufig ist zu beobachten, dass in Institutionen zwar eine Vielzahl von organisatorischen und technischen Sicherheitsverfahren vorhanden sind, diese jedoch durch den sorglosen Umgang mit den Vorgaben und der Technik wieder ausgehebelt werden. Ein typisches Beispiel hierfür sind die fast schon sprichwörtlichen Zettel am Monitor, auf denen Zugangspasswörter notiert sind.

2.8 Unberechtigte Verwendung eigener IT-Systeme

Die unberechtigte Verwendung eigener IT-Systeme durch Mitarbeiter kann grundsätzlich nur schwer verhindert werden. Der Verwendung des eigenen Laptops, USB-Sticks oder Smartphones innerhalb der IT-Landschaft einer Institution kann zu diversen Sicherheitsrisiken, wie zum Beispiel dem unbeabsichtigten Einbringen von Schadprogrammen, führen.

2.9 Missbrauch sozialer Netzwerke

Soziale Netzwerke sind als Plattformen sehr erfolgreich. Allerdings gibt es neben den diversen Vorteilen auch Sicherheitsrisiken, die Benutzer nicht aus den Augen verlieren sollten. So können die in sozialen Netzwerken veröffentlichten Daten zum geschickten Passwortraten verwendet werden. Darüber hinaus eignen sich soziale Netze besonders für Social Engineering Angriffe, da hier zum einen viele Hintergrundinformationen gesammelt werden können und zum anderen das unter "Bekannten" angenommene Vertrauen ausgenutzt werden kann.

2.10 Manipulation oder Zerstörung von Geräten, Informationen oder Software

Außen-, aber auch Innentäter können aus unterschiedlichen Beweggründen heraus versuchen, Geräte, Informationen oder Software zu manipulieren oder zerstören. Die Auswirkungen reichen von der unerlaubten Einsichtnahme in schützenswerte Daten bis zur Zerstörung von IT-Systemen, die erhebliche Ausfallzeiten nach sich ziehen können.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Personal aufgeführt. Grundsätzlich ist die Personalabteilung für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	Personalabteilung
Weitere Verantwortliche	IT-Betrieb, Informationssicherheitsbeauftragter (ISB), Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

ORP.2.A1 Geregelte Einarbeitung neuer Mitarbeiter [Vorgesetzte]

Die Personalabteilung sowie die Vorgesetzten MÜSSEN dafür sorgen, dass neue Mitarbeiter zu Beginn ihrer Beschäftigung in ihre neuen Aufgaben eingearbeitet und über bestehende Regelungen, Gepflogenheiten und Verfahrensweisen informiert werden. Hierbei SOLLTE eine Checkliste unterstützend wirken.

Zur geregelten Einarbeitung neuer Mitarbeiter MÜSSEN diese auf bestehende Regelungen und Handlungsanweisungen zur Informationssicherheit hingewiesen werden. Alle Mitarbeiter MÜSSEN über Regelungen zur Informationssicherheit, deren Veränderungen und ihre spezifischen Auswirkungen auf einen Geschäftsprozess oder auf das jeweilige Arbeitsumfeld unterrichtet werden.

Alle Mitarbeiter MÜSSEN explizit darauf verpflichtet werden, einschlägige Gesetze, Vorschriften und interne Regelungen einzuhalten. Außerdem MÜSSEN alle Mitarbeiter darauf hingewiesen werden, dass alle während der Arbeit erhaltenen Informationen ausschließlich zum internen Gebrauch bestimmt sind, solange sie nicht anders gekennzeichnet sind.

ORP.2.A2 Geregelte Verfahrensweise beim Weggang von Mitarbeitern [Vorgesetzte, IT-Betrieb]

Vor dem Weggang eines Mitarbeiters MUSS eine rechtzeitige Einweisung des Nachfolgers, idealerweise durch den ausscheidenden Mitarbeiter, durchgeführt werden. Ist eine direkte Übergabe nicht möglich MUSS vom ausscheidenden Mitarbeiter eine ausführliche Dokumentation angefertigt werden. Außerdem MÜSSEN von ausscheidenden Mitarbeitern alle im Rahmen ihrer Tätigkeit erhaltenen Unterlagen, Schlüssel und Geräte sowie Ausweise und Zutrittsberechtigungen eingezogen werden.

Die IT-Administration MUSS außerdem dafür Sorge tragen, dass ehemaligen Mitarbeitern sämtliche Zugriffsberechtigungen auf IT-Systeme entzogen bzw. diese bei Aufgabenwechseln angepasst werden.

Vor der Verabschiedung MUSS noch einmal explizit auf Verschwiegenheitsverpflichtungen hingewiesen werden.

Weiterhin MÜSSEN Notfall- und andere Ablaufpläne aktualisiert werden. Alle betroffenen Stellen innerhalb der Institution, wie zum Beispiel das Sicherheitspersonal, MÜSSEN ebenfalls über das Ausscheiden des Mitarbeiters informiert werden. Um alle Aktivitäten, die mit dem Weggang von Mitarbeitern einhergehen, geregelt abarbeiten zu können, SOLLTE ähnlich der Einstellung auch hier die Erstellung und die Abarbeitung einer Checkliste hilfreich sein.

ORP.2.A3 Vertretungsregelungen [Vorgesetzte]

Die Vorgesetzten MÜSSEN für die Einführung und Aufrechterhaltung von Vertretungsregelungen Sorge tragen.Dabei MUSS sichergestellt werden, dass für alle wesentlichen Geschäftsprozesse und Aufgaben entsprechende und praktikable Vertretungsregelungen vorhanden sind. Bei diesen Regelungen MUSS der Aufgabenumfang der Vertretung im Vorfeld klar definiert werden. Hierbei reicht das einfache Benennen eines Vertreters nicht aus, sondern es MUSS sichergestellt werden, dass dieser über das für die Vertretung benötigte Wissen verfügt. Ist dies nicht der Fall, MUSS überprüft werden, wie der Vertreter zu schulen ist oder ob es ausreicht, den aktuellen Verfahrens- oder Projektstand ausreichend zu dokumentieren. Ist es im Ausnahmefall nicht möglich, für einzelne Mitarbeiter einen kompetenten Vertreter zu benennen oder zu schulen, MUSS frühzeitig überlegt werden, ob und wenn ja, welche externen Kräfte für den Vertretungsfall eingesetzt werden können.

ORP.2.A4 Regelungen für den Einsatz von Fremdpersonal

Bei der Beschäftigung von externem Personal MUSS dieses grundsätzlich wie alle eigenen Mitarbeiter auf die Einhaltung der geltenden Gesetze, Vorschriften und internen Regelungen verpflichtet werden. Kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal kann wie Besucher behandelt und MUSS in sicherheitsrelevanten Bereichen beaufsichtigt werden. Bei längerfristig beschäftigtem Fremdpersonal wiederum MUSS dieses ähnlich der eigenen Mitarbeiter in seine Aufgaben eingewiesen werden. Für solche Mitarbeiter MUSS außerdem eine Vertretungsregelung eingeführt werden. Bei ihrem Weggang MUSS analog zu eigenem Personal eine geregelte Über- und Rückgabe der Arbeitsergebnisse und eventuell ausgehändigter Zugangsberechtigungen erfolgen.

ORP.2.A5 Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal

Bevor Externe Zugang und Zugriff zu vertraulichen Informationen erhalten, MÜSSEN mit ihnen Vertraulichkeitsvereinbarungen abgeschlossen werden. Durch die verwendeten Vertraulichkeitsvereinbarungen MÜSSEN alle wichtigen Aspekte zum Schutz von organisationsinternen Informationen berücksichtigt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Personal. Sie SOLLTEN grundsätzlich umgesetzt werden.

ORP.2.A6 Überprüfung von Kandidaten bei der Auswahl von Personal

Bei der Auswahl von neuen Mitarbeitern SOLLTEN die erforderlichen Qualifikationen und Fähigkeiten genau formuliert sein. Anschließend SOLLTE anhand der Unterlagen und im Bewerbungsgespräch geprüft werden, ob diese bei den Bewerbern tatsächlich vorhanden sind. Besonders SOLLTE darauf geachtet werden, dass keine Interessenkonflikte auftreten. Um nach einem Stellenwechsel Interessenkonflikte zu vermeiden, SOLLTEN Konkurrenzverbote und Karenzzeiten vereinbart werden.

ORP.2.A7 Überprüfung der Vertrauenswürdigkeit von Mitarbeitern

Neue Mitarbeiter SOLLTEN vor ihrer Einstellung auf ihre Vertrauenswürdigkeit hin überprüft werden. Deshalb SOLLTEN alle Beteiligten bei der Personalauswahl mit der gebotenen Sorgfalt bemüht sein, Angaben der Bewerber/-innen, die relevant sind für die Einschätzung ihrer Vertrauenswürdigkeit, auf ihre Glaubhaftigkeit hin zu überprüfen, soweit dies möglich ist. Insbesondere SOLLTE der vorgelegte Lebenslauf auf Vollständigkeit, Plausibilität und Korrektheit kritisch geprüft werden. Dabei SOLLTEN kritisch erscheinende Daten durch dezidierte Nachfrage und dem Verlangen weiterer Nachweise geprüft werden.

ORP.2.A8 Aufgaben und Zuständigkeiten von Mitarbeitern [Informationssicherheitsbeauftragter (ISB)]

Die Aufgaben und Zuständigkeiten von Mitarbeitern SOLLTEN in geeigneter Weise dokumentiert sein, beispielsweise durch Arbeitsverträge oder Vereinbarungen. Der IT-Sicherheitsbeauftragte SOLLTE dafür sorgen, dass alle Mitarbeiter ihre Aufgaben und Zuständigkeiten im Sicherheitsprozess kennen. Insbesondere SOLLTE vereinbart sein, dass jeder Mitarbeiter auch außerhalb der Arbeitszeit und außerhalb des Betriebsgeländes eine Verantwortlichkeit für Informationssicherheit hat.

ORP.2.A9 Schulung von Mitarbeitern

Die Mitarbeiter SOLLTEN entsprechend ihrer Tätigkeit regelmäßig geschult werden, damit sie in Bezug auf die ihnen übertragenen Tätigkeiten immer auf einem entsprechend aktuellen Stand sind. In allen Bereichen SOLLTE sichergestellt werden, dass kein Mitarbeiter basierend auf einem veralteten Wissensstand seiner Arbeit nachgeht. Weiterhin SOLLTE den Mitarbeitern während ihrer Beschäftigung die Möglichkeit gegeben werden, sich im Rahmen ihres Tätigkeitsfeldes weiterzubilden.

Alle Mitarbeiter SOLLTEN in die Geräte, Anwendungen und Aktivitäten eingewiesen sein, die zur sicheren Verarbeitung von Informationen dienen. Darüber hinaus SOLLTEN alle Mitarbeiter regelmäßig im Bereich der Informationssicherheit geschult und über alltägliche Risiken und mögliche Gegenmaßnahmen unterrichtet werden. Die Mitarbeiter SOLLTEN darüber hinaus angehalten werden, Regelungen zur Informationssicherheit eigenverantwortlich umzusetzen. Bei größerem Schulungsbedarf SOLLTEN einzelne Mitarbeiter gesondert geschult und innerhalb des Tätigkeitsbereichs als Multiplikatoren für die restlichen Mitarbeiter eingesetzt werden.

ORP.2.A10 Vermeidung von Störungen des Betriebsklimas

Es SOLLTE, auch aus Sicht der Informationssicherheit, Maßnahmen ergriffen werden um für ein positives Betriebsklima zu sorgen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

ORP.2.A11 Analyse der Sicherheitskultur (CIA)

Die für die Institution ausgewählten Sicherheitsmaßnahmen SOLLTEN sich immer an der Institution und ihren Mitarbeitern orientieren. Dabei SOLLTEN, unter Beibehaltung der rechtlichen Rahmenbedingungen, analysiert werdenwie genau sich die Mitarbeiter aus Sicherheitssicht verhalten. Darauf aufbauend SOLLTE untersucht werden, wo die personelle und organisatorische Sicherheit noch verbessert werden kann.

ORP.2.A12 Benennung separater Ansprechpartner (CIA)

Zur Zufriedenheit der Mitarbeiter SOLLTE ein Verantwortlicher als vertrauenswürdiger Ansprechpartner benannt werden. Im Fall von größeren organisatorischen oder technischen Veränderungen SOLLTE die Benennung eines solchen Ansprechpartners geprüft werden.

ORP.2.A13 Sicherheitsüberprüfung (CIA)

Im Hochsicherheitsbereich SOLLTE eine zusätzliche Sicherheitsüberprüfung zur grundlegenden Überprüfung der Vertrauenswürdigkeit von Mitarbeitern durchgeführt werden.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [ISF] The Standard of Good Practice
  Information Security Forum (ISF), 06.2016

- [NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations
  Special Publication 800-53, Revision 4, NIST, 04.2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Personal" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.32 Missbrauch von Berechtigungen

G 0.33 Personalausfall

G 0.34 Anschlag

G 0.35 Nötigung, Erpressung oder Korruption

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.38 Missbrauch personenbezogener Daten

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.14	G 0.16	G 0.17	G 0.19	G 0.22	G 0.27	G 0.29	G 0.32	G 0.33	G 0.34	G 0.35	G 0.36	G 0.37	G 0.38	G 0.41	G 0.42	G 0.44	G 0.45	G 0.46
ORP.2.A1	x						x							x		x		x	x
ORP.2.A2		x															x	x	x
ORP.2.A3			x				x							x					
ORP.2.A4			x														x	x	x
ORP.2.A5	x	x	x	x	x	x	x	x	x				x	x			x	x	x
ORP.2.A6	x											x				x			
ORP.2.A7		x					x									x		x	x
ORP.2.A8								x									x		
ORP.2.A9				x		x									x	x			
ORP.2.A10					x	x									x				
ORP.2.A11							x			x	x					x		x	x
ORP.2.A12							x												
ORP.2.A13			x						x							x		x	x

ORP: Organisation und Personal

ORP.3 Sensibilisierung und Schulung

1 Beschreibung

1.1 Einleitung

Um Informationssicherheit innerhalb einer Institution erfolgreich und effizient zu verwirklichen, sind die Mitarbeiter ein notwendiger und bedeutender Erfolgsfaktor. Daher müssen sich alle Mitarbeiter über ihre Rollen im Informationssicherheitsmanagement bewusst sein. Sie müssen die Sicherheitsziele der Institution kennen sowie die Sicherheitsmaßnahmen verstehen und bereit sein, sie wirkungsvoll zu unterstützen. Hierfür müssen in der Institution ein Sicherheitsbewusstsein (Awareness) sowie eine Sicherheitskultur aufgebaut und gestaltet werden.

Mitarbeiter müssen für relevante Gefährdungen sensibilisiert werden und wissen, wie sich diese auf ihre Institution auswirken können. Je besser die Mitarbeiter die Gefährdungslage kennen, desto eher werden entsprechende Sicherheitsmaßnahmen akzeptiert. Mitarbeiter müssen über die erforderlichen Kenntnisse verfügen, um Maßnahmen richtig verstehen und anwenden zu können. Insbesondere muss ihnen bekannt sein, was von ihnen im Hinblick auf Informationssicherheit erwartet wird und wie sie in sicherheitskritischen Situationen reagieren sollen.

1.2 Zielsetzung

In diesem Baustein wird beschrieben, wie ein effektives Sensibilisierungs- und Schulungsprogramm zur Informationssicherheit aufgebaut und aufrechterhalten werden kann. Ziel der Sensibilisierung und Schulung für Informationssicherheit ist es, die Wahrnehmung der Mitarbeiter für sicherheitskritische Situationen und ihre Auswirkungen zu schärfen sowie ihnen die notwendigen Kenntnisse und Kompetenzen für sicherheitsbewusstes Verhalten zu vermitteln.

1.3 Abgrenzung

Dieser Baustein betrachtet Anforderungen an die Sensibilisierung und Schulung zur Informationssicherheit, die sowohl das Umfeld innerhalb der Institution als auch die Telearbeit und das mobile Arbeiten betreffen. Die relevanten Themen der Informationssicherheit müssen entsprechend den Institutionsvorgaben regelmäßig geschult und sensibilisiert werden.

Der Baustein *ORP.3 Sensibilisierung und Schulung* beschreibt die prozessualen, technischen, methodischen und organisatorischen Anforderungen an die Sensibilisierung und Schulung von Informationssicherheit. Andere Schulungsthemen werden durch die Abteilung Personal oder die Abteilung Weiterbildungsmanagement der Institution geplant, gestaltet und durchgeführt.

Um Redundanzen zu vermeiden und die Effizienz der Aus- und Weiterbildung in der Institution zu stärken, sollte sich der Informationssicherheitsbeauftragte regelmäßig nicht nur mit der Personalabteilung, sondern auch mit anderen Sicherheit-nahen Bereichen (Datenschutz, Gesundheits- und Arbeitsschutz, Brandschutz, etc.) austauschen.

In vielen der anderen IT-Grundschutz-Bausteine werden konkrete Schulungsinhalte zu den betrachteten Themen beschrieben. Dieser Baustein beschäftigt sich damit, wie in den Bereichen Sensibilisierung und Schulung der Informationssicherheit ein planvolles, zyklisches und organisatorisches Vorgehen effizient gestaltet werden kann.

2 Gefährdungslage

Folgende spezifischen Bedrohungen und Schwachstellen sind für den Bereich Sensibilisierung und Schulung von besonderer Bedeutung.

2.1 Unzureichende Kenntnis über Regelungen

Regelungen zur Informationssicherheit lediglich festzulegen, sichert noch nicht, dass sie beachtet werden. Allen Mitarbeitern müssen die geltenden Regelungen auch bekannt sein, insbesondere den Funktionsträgern. Bei vielen Sicherheitsvorfällen ist die Nichtbeachtung von Regelungen zwar nicht der alleinige Auslöser des Vorfalls, aber ein Grund für dessen Wirksamkeit. Sicherheitslücken aufgrund unzureichender Kenntnisse über Regelungen können die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen, mit denen gearbeitet wird, gefährden. Die Aufgabenerfüllung und die Abwicklung von Geschäftsprozessen können dadurch in jeder Hinsicht (z. B. zeitlich, qualitativ, bezüglich der Verbindlichkeit) eingeschränkt werden.

2.2 Unzureichende Sensibilisierung für Informationssicherheit

Die Erfahrung zeigt, dass es nicht genügt, lediglich die Umsetzung von bestimmten Sicherheitsmaßnahmen anzuordnen. Ohne ein Verständnis dafür, welche Gründe es für die Maßnahmen gibt und welchem Zweck sie dienen, führen die Maßnahmen häufig ins Leere oder werden ignoriert. Werden Mitarbeiter unzureichend zu Informationssicherheitsthemen sensibilisiert, entstehen somit in den technischen und organisatorischen Geschäftsprozessen betriebliche und umsetzungsbedingte Risiken. Die Sicherheitskultur, die Sicherheitsziele und die Sicherheitsstrategie der Institution können gefährdet sein, wenn Mitarbeiter keinen konkreten Bezug zu ihrer realen Arbeitswelt herstellen können, sofern ihnen nicht der Sinn und Zweck von Sicherheitsmaßnahmen vermittelt wird. Dies führt zu fehlender Akzeptanz von Sicherheitsmaßnahmen und Mängeln bei der Einhaltung.

2.3 Wenig erfolgreiche Aktivitäten zur Sensibilisierung und Schulung

Nicht immer sind die zur Sensibilisierung und Schulung durchgeführten Aktivitäten so erfolgreich wie gewünscht. Ursachen dafür können sein:

- fehlende Management-Unterstützung
- unklare Ziele
- schlechte Planung
- mangelnde Erfolgskontrolle
- fehlende Kontinuität
- zu geringe finanzielle oder personelle Ressourcen

Werden keine geeigneten Maßnahmen ergriffen, um den Erfolg der durchgeführten Aktivitäten sicherzustellen, kann das Ziel der jeweiligen Schulungsaktivität häufig nicht erreicht werden. Wenn die Institution unzureichende Aktivitäten zur Sensibilisierung und Schulung der Mitarbeiter durchführt, können sind Aspekte der Informationssicherheit gefährdet sein, was direkt zu Einschränkungen der Aufgabenerfüllung führt.

2.4 Unzureichende Schulung der Mitarbeiter zu Sicherheitsfunktionalitäten

Häufig wenden Mitarbeiter neu eingeführte Sicherheitsprogramme und -funktionalitäten deswegen nicht an, weil sie nicht wissen, wie sie bedient werden und eine selbstständige Einarbeitung als im täglichen Arbeitsablauf zu zeitaufwendig gesehen wird. Darüber hinaus können fehlende Schulungen nach Einführung einer neuen Software zu unbeabsichtigten Fehlbedienungen oder falscher Konfigurationen führen. Daher reicht die Beschaffung und Installation einer (Sicherheits-)Software nicht aus. Sofern Mit-

arbeiter zu Software- oder Sicherheitsfunktionen nicht ausreichend geschult werden, können sie nicht geeignet mit den IT-Systemen und Anwendungen der Institution arbeiten. Dies kann zu Fehlern in der Bedienung führen und Arbeitsabläufe unnötig verzögern. Gerade bei kritischen IT-Systemen und Anwendungen kann eine Fehlbedienung existenzbedrohende Auswirkungen hervorrufen.

2.5 Nicht erkannte Sicherheitsvorfälle

Im täglichen Betrieb von IT- und ICS-Komponenten können viele Störungen und Fehler auftreten. Dabei besteht die Gefahr, dass Sicherheitsvorfälle durch das Personal nicht als solche identifiziert werden und auch Cyber-Angriffe bzw. Angriffsversuche unerkannt bleiben. Sicherheitsvorfälle und technische Fehler sind mitunter nicht einfach zu unterscheiden. Werden Benutzer und Administratoren nicht gezielt darin geschult und sensibilisiert, Sicherheitsvorfälle zu erkennen und auf diese angemessen zu reagieren, können Sicherheitslücken unentdeckt bleiben und ausgenutzt werden. Falls Sicherheitsvorfälle nicht rechtzeitig oder gar nicht erkannt werden, können entsprechende und vollumfängliche Gegenmaßnahmen nicht rechtzeitig ergriffen werden. Kleine Sicherheitslücken der Institution können sich verschärfen und zu kritischen Gefährdungen für die Integrität, Vertraulichkeit und Verfügbarkeit heranwachsen. Dies kann Geschäftsprozesse behindern, finanzielle Schäden hervorrufen oder regulatorische und gesetzliche Sanktionen nach sich ziehen.

2.6 Nichtbeachtung von Sicherheitsmaßnahmen

Aus den verschiedensten Gründen, wie Nachlässigkeit oder Hektik, kann es dazu kommen, dass also vertrauliche Dokumente an Arbeitsplätzen offen herumliegen, Fluchttüren von beiden Seiten geöffnet werden können oder E-Mails nicht verschlüsselt werden. Dadurch können Schäden entstehen, die sonst verhindert oder zumindest vermindert worden wären.

2.7 Sorglosigkeit im Umgang mit Informationen

Häufig ist zu beobachten, dass in Institutionen zwar eine Vielzahl von organisatorischen und technischen Sicherheitsverfahren vorhanden sind, diese jedoch durch den sorglosen Umgang mit den Vorgaben und der Technik wieder ausgehebelt werden. Ein typisches Beispiel hierfür sind die fast schon sprichwörtlichen Zettel am Monitor, auf denen Zugangspasswörter notiert sind. Ebenso schützt eine Festplattenverschlüsselung beim Laptop nicht davor, dass die vertraulichen Informationen vom Sitznachbarn im Zug einfach mitgelesen werden können. Die besten technischen Sicherheitslösungen helfen nicht, wenn Ausdrucke mit vertraulichen Informationen am Drucker liegenbleiben oder in frei zugänglichen Altpapiercontainern landen.

Wenn die Mitarbeiter sorglos mit Informationen umgehen, werden festgelegte Prozesse der Informationssicherheit unwirksam. Unbefugte könnten z. B. Nachlässigkeiten im Umgang mit Informationen ausnutzen, um gezielt Wirtschaftsspionage zu betreiben.

2.8 Mangelhafte Akzeptanz von Informationssicherheit

Verschiedene Umstände können dazu führen, dass in einer Institution oder auch in Teilen einer Institution Anforderungen und Vorgaben zur Informationssicherheit nicht akzeptiert werden und damit keine Einsicht in die Notwendigkeit besteht, Sicherheitsmaßnahmen umzusetzen. Dies kann beispielsweise durch die Kultur der Institution (Motto: "Das war bei uns schon immer so!") oder fehlende Vorbildfunktion durch das Management bedingt sein. Aber auch unangemessene oder übertriebene Sicherheitsanforderungen können dazu führen, dass Mitarbeiter Sicherheitsmaßnahmen ablehnen. Ebenso könnte auch ein anderes soziales Umfeld oder ein anderer kultureller Hintergrund ("andere Länder, andere Sitten") dazu führen, dass Sicherheitsmaßnahmen nicht umgesetzt werden. Probleme könnten auch dadurch entstehen, dass bestimmte Benutzerrechte oder auch die Ausstattung mit bestimmter Hard- oder Software als Statussymbol gesehen werden. Einschränkungen in diesen Bereichen können auf großen Widerstand stoßen.

2.9 Social Engineering

Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch "Aushorchen" von Mitarbeitern zu erlangen. Beim Social Engineering baut ein Angreifer meistens einen direkten Kontakt zu einem Opfer auf, z. B. per Telefon, E-Mail oder auch über Soziale Netzwerke. Angriffe über Social Engineering sind häufig mehrstufig. Indem der Angreifer Insider-Wissen vorspiegelt und gleichzeitig an die Hilfsbereitschaft appelliert, kann er sein Wissen in weiteren Schritten ausbauen. Wenn Mitarbeiter für diese Art von Angriffen nicht ausreichend sensibilisiert sind, besteht die Gefahr, dass sie durch geschickte Kommunikation so manipuliert werden, dass sie unzulässig handeln. Dies kann dazu führen, dass sie interne Informationen weitergeben, sich Schadsoftware einfangen oder sogar Geld an angebliche Geschäftspartner überweisen.

Beim "Cheftrick" – der englische Fachbegriff lautet CEO Fraud – wird Sachbearbeitern, die Geld im Namen des Unternehmens transferieren dürfen, ein fiktiver Auftrag des Chefs vorgegaukelt. Sie sollen für ein angeblich dringendes und geheimhaltungsbedürftiges Geschäft Transaktionen durchführen, die für das weitere Bestehen des Unternehmens äußerst wichtig sind. Mit dieser Masche gelang es Trickbetrügern im Laufe des Jahres 2016 in tausenden von Unternehmen, Schäden im sechs- bis achtstelligen Bereich anzurichten. Die Schäden weltweit gehen in die Milliarden.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich *Sensibilisierung und Schulung* aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	Informationssicherheitsbeauftragter (ISB)
Weitere Verantwortliche	IT-Betrieb, Institutionsleitung, Personalabteilung, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

ORP.3.A1 Sensibilisierung des Managements für Informationssicherheit [Vorgesetzte, Institutionsleitung]

Die Institutionsleitung MUSS die Sicherheitskampagnen und Schulungsmaßnahmen für die Mitarbeiter nachdrücklich und aktiv unterstützen. Daher MUSS vor dem Beginn eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit die Unterstützung des Managements eingeholt werden. Das Management MUSS ausreichend für Sicherheitsfragen sensibilisiert werden.

Alle Vorgesetzten MÜSSEN die Informationssicherheit unterstützen, indem sie mit gutem Beispiel vorangehen. Führungskräfte MÜSSEN die Sicherheitsvorgaben umsetzen und ihre Mitarbeiter auf deren Einhaltung hinweisen.

ORP.3.A2 Ansprechpartner zu Sicherheitsfragen

In jeder Institution MUSS es Ansprechpartner für Sicherheitsfragen geben, die sowohl scheinbar einfache wie auch komplexe oder technische Fragen beantworten können. Die Ansprechpartner MÜSSEN allen Mitarbeitern der Institution bekannt sein. Diesbezügliche Informationen MÜSSEN in der Institution für alle leicht zugänglich sein und verfügbar sein.

ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT [Vorgesetzte, Personalabteilung, IT-Betrieb]

Alle Mitarbeiter und externen Benutzer MÜSSEN in den sicheren Umgang mit IT-, ICS- und IoT-Komponenten eingewiesen und sensibilisiert werden, soweit dies für ihre Arbeitszusammenhänge relevant ist. Dafür MÜSSEN verbindliche, verständliche, aktuelle und verfügbare Richtlinien zur Nutzung der jeweiligen Komponenten zur Verfügung stehen. Werden IT-, ICS- oder IoT-Systeme oder Dienste in einer Weise benutzt, die den Interessen der Institution widersprechen, MUSS dies kommuniziert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Sensibilisierung und Schulung. Sie SOLLTEN grundsätzlich umgesetzt werden.

ORP.3.A4 Konzeption eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit

Um die Mitarbeiter zu sensibilisieren, SOLLTE ein zielgruppenorientiertes Sensibilisierungs- und Schulungsprogramm erstellt werden. Es SOLLTE regelmäßig überprüft und aktualisiert werden.

ORP.3.A5 Analyse der Zielgruppen für Sensibilisierungs- und Schulungsprogramme

Sensibilisierungs- und Schulungsprogramme SOLLTEN sich an den jeweiligen Zielgruppen orientieren. Dazu SOLLTE eine Zielgruppenanalyse durchgeführt werden, sodass Maßnahmen auf spezielle Anforderungen und unterschiedliche Hintergründe fokussiert werden können.

ORP.3.A6 Planung und Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit

Alle Mitarbeiter SOLLTEN entsprechend ihren Aufgaben und Verantwortlichkeiten zu Informationssicherheitsthemen geschult werden. Es SOLLTE daher Sensibilisierungs- und Schulungsmaßnahmen geben, die den Mitarbeitern alle Informationen und Fähigkeiten vermitteln, die erforderlich sind, um in der Institution geltende Sicherheitsregelungen und -maßnahmen umsetzen zu können. Aus diesem Grund SOLLTEN die Sensibilisierungs- und Schulungsinhalte entsprechend den Zielgruppen, Aufgaben und Verantwortlichkeiten der Mitarbeiter strukturiert und geplant werden. Die geplanten Sensibilisierungs- und Schulungsmaßnahmen SOLLTEN gemäß dieser Planung in adäquater Form umgesetzt werden. Sensibilisierungs- und Schulungsprogramme SOLLTEN regelmäßig auf Aktualität überprüft und bei geändertem Bedarf angepasst bzw. weiterentwickelt werden.

ORP.3.A7 Schulung zur Vorgehensweise nach IT-Grundschutz

Sicherheitsverantwortliche SOLLTEN mit der IT-Grundschutz-Methodik vertraut sein. Wurde ein Schulungsbedarf verifiziert, SOLLTE eine entsprechende IT-Grundschutz-Schulung geplant und deren Inhalt vorher festgelegt werden. Innerhalb der Schulung SOLLTE die Vorgehensweise anhand praxisnaher Beispiele geübt werden.

ORP.3.A8 Messung und Auswertung des Lernerfolgs [Personalabteilung]

Die Lernerfolge im Bereich Informationssicherheit SOLLTEN zielgruppenbezogen gemessen und ausgewertet werden, um festzustellen, inwieweit die in den Sensibilisierungs- und Schulungsprogrammen beschriebenen Ziele erreicht sind. Die Messungen SOLLTEN sowohl quantitative als auch qualitative Aspekte der Sensibilisierungs- und Schulungsprogramme berücksichtigen. Die Ergebnisse SOLLTEN bei der Verbesserung des Sensibilisierungs- und Schulungsangebots geeignet einfließen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

ORP.3.A9 Spezielle Schulung von exponierten Personen und Institutionen (CIA)

Besonders exponierte Personen wie Funktionsträger sowie die Mitarbeiter in besonders exponierten Institutionen oder Organisationsbereichen SOLLTEN vertiefende Schulungen in Hinblick auf mögliche Gefährdungen sowie geeignete Verhaltensweisen und Vorsichtsmaßnahmen erhalten.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [ISF] The Standard of Good Practice
  Information Security Forum (ISF), 06.2016

- [NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations
  Special Publication 800-53, Revision 4, NIST, 04.2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Sensibilisierung und Schulung" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.19 Offenlegung schützenswerter Informationen

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.38 Missbrauch personenbezogener Daten

G 0.42 Social Engineering

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.14	G 0.15	G 0.19	G 0.24	G 0.29	G 0.30	G 0.31	G 0.32	G 0.36	G 0.37	G 0.38	G 0.42	G 0.45	G 0.46
ORP.3.A1	x	x	x	x	x	x	x	x	x	x	x	x	x	x
ORP.3.A2	x	x	x	x	x	x	x	x	x	x	x	x	x	x
ORP.3.A3	x	x	x	x	x	x	x	x	x	x	x	x	x	x
ORP.3.A4					x									
ORP.3.A5					x									
ORP.3.A6					x									
ORP.3.A7	x	x	x	x	x	x	x	x	x	x	x	x	x	
ORP.3.A8					x									
ORP.3.A9	x	x	x	x	x	x	x	x	x	x	x	x	x	x

ORP: Organisation und Personal

ORP.4 Identitäts- und Berechtigungsmanagement

1 Beschreibung

1.1 Einleitung

Benutzer oder auch IT-Komponenten, die auf die Ressourcen einer Institution zugreifen, müssen zweifelsfrei identifiziert und authentisiert werden. Die Verwaltung der dafür notwendigen Informationen wird als Identitätsmanagement bezeichnet.

Beim Berechtigungsmanagement geht es darum, ob und wie Benutzer oder IT-Komponenten auf Informationen oder Dienste zugreifen und diese benutzen dürfen, ihnen also basierend auf dem Benutzerprofil Zutritt, Zugang oder Zugriff zu gewähren oder zu verweigern ist. Berechtigungsmanagement bezeichnet die Prozesse, die für Zuweisung, Entzug und Kontrolle der Rechte erforderlich sind.

Die Übergänge zwischen beiden Begriffen sind fließend, daher wird in diesem Baustein der Begriff Identitäts- und Berechtigungsmanagement (englisch Identity and Access Management, IAM) benutzt.

1.2 Zielsetzung

Ziel des Bausteins ist es, dass Benutzer oder auch IT-Komponenten ausschließlich auf die IT-Ressourcen und Informationen zugreifen können, die sie für ihre Arbeit benötigen und für die sie autorisiert sind, und unautorisierten Benutzern oder IT-Komponenten den Zugriff zu verwehren. Dazu werden Anforderungen formuliert, mit denen Institutionen ein sicheres Identitäts- und Berechtigungsmanagement aufbauen sollten.

1.3 Abgrenzung

In diesem Baustein werden grundsätzliche Anforderungen für den Aufbau eines Identitäts- und Berechtigungsmanagement beschrieben.

Anforderungen, die Komponenten eines Identitäts- und Berechtigungsmanagement betreffen wie Betriebssysteme oder Verzeichnisdienste, sind in den entsprechenden Bausteinen zu finden (z.B. SYS.1.3 Unix-Server, SYS.1.2.2 Windows Server 2012, APP.2.1 Allgemeiner Verzeichnisdienst, APP.2.2 Active Directory).

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Identitäts- und Berechtigungsmanagement von besonderer Bedeutung:

2.1 Fehlende oder unzureichende Prozesse beim Identitäts- und Berechtigungsmanagement

Wenn beim Identitäts- und Berechtigungsmanagement Prozesse unzureichend definiert sind oder nicht befolgt werden, erhält der zuständige Administrator möglicherweise keine Informationen über personelle Veränderungen. Das kann dazu führen, dass beispielsweise ein Benutzerkonto eines ausgeschiedenen Mitarbeiters nicht gelöscht wird. Er kann somit weiterhin auf schützenswerte Informationen oder auch Cloud-Anwendungen zugreifen.

Auch ist es möglich, dass Mitarbeiter, die in eine neue Abteilung versetzt wurden, ihre alten Berechtigungen behalten und dadurch mit der Zeit umfangreiche Gesamt-Berechtigungen ansammeln.

2.2 Fehlende zentrale Deaktivierungsmöglichkeit von Benutzerzugängen

In Institutionen haben Mitarbeiter oft Benutzerzugänge zu diversen IT-Systemen wie Produktiv-, Test-, Qualitätssicherungs- oder Projekt-Systeme. Diese befinden sich meist in unterschiedlichen Verantwortungsbereichen und werden von unterschiedlichen Administratoren verwaltet. Das führt dazu, dass nicht auf allen IT-Systemen eine gleiche und eindeutige Benutzerkennung verwendet wird und es meist auch keine zentrale Übersicht über die Benutzerzugänge auf den einzelnen IT-Systemen gibt. In einem solchen Szenario ist es nicht möglich, bei einem Angriff oder einem Passwortdiebstahl umgehend alle Benutzerzugänge eines Mitarbeiters zu deaktivieren. Auch können bei dem Ausscheiden eines Mitarbeiters aus der Institution nicht umgehend alle Zugänge gesperrt werden.

2.3 Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten

Wenn die Vergabe von Zutritts-, Zugangs- und Zugriffsrechten schlecht geregelt ist, führt das schnell zu gravierenden Sicherheitslücken, z. B. durch Wildwuchs in der Rechtevergabe. Bei der Einführung von Identitätsmanagement-Systemen oder Revisionen stellt sich häufig heraus, dass verschiedene Personen in unterschiedlichsten Organisationseinheiten für die Vergabe von Berechtigungen zuständig sind. Dies führt schnell dazu, dass Benutzer Berechtigungen auf Zuruf erhalten oder umgekehrt nur über unnötig komplizierte Wege an diese kommen. Dadurch können einerseits fehlende Berechtigungen die tägliche Arbeit behindern, andererseits können so Berechtigungen ohne Erfordernis vergeben werden und so ein Sicherheitsrisiko darstellen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Identitäts- und Berechtigungsmanagement aufgeführt. Grundsätzlich ist der ISB für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	Informationssicherheitsbeauftragter (ISB)
Weitere Verantwortliche	Administrator, Benutzer, Leiter IT

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

ORP.4.A1 Regelung für die Einrichtung von Benutzern und Benutzergruppen [Administrator, Leiter IT]

Es MUSS geregelt werden, wie Benutzer und Benutzergruppen einzurichten sind. Alle Benutzer und Benutzergruppen DÜRFEN NUR über separate administrative Rollen eingerichtet werden.

ORP.4.A2 Regelung für Einrichtung, Änderung und Entzug von Berechtigungen [Administrator, Leiter IT]

Benutzerkennungen und Berechtigungen DÜRFEN NUR aufgrund des tatsächlichen Bedarfs vergeben werden. Bei personellen Veränderungen MÜSSEN die nicht mehr benötigten Benutzerkennungen und Berechtigungen entfernt werden. Beantragen Mitarbeiter Berechtigungen, die über den Standard hinausgehen, DÜRFEN diese NUR nach zusätzlicher Begründung vergeben werden. Alle Berechtigungen MÜSSEN über separate administrative Rollen eingerichtet werden.

ORP.4.A3 Dokumentation der zugelassenen Benutzer und Rechteprofile [Administrator, Leiter IT]

Es MUSS eine Dokumentation der zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile erfolgen. Die Dokumentation der zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile MUSS regelmäßig auf Aktualität überprüft werden. Die Dokumentation MUSS vor unberechtigtem Zugriff geschützt werden. Sofern sie in elektronischer Form erfolgt, SOLLTE sie in das Datensicherungsverfahren einbezogen werden.

ORP.4.A4 Aufgabenverteilung und Funktionstrennung [Leiter IT]

Es MÜSSEN die für den IT-Einsatz relevanten Aufgaben und Funktionen definiert werden. Auch MUSS festgelegt werden, welche Aufgaben und Funktionen nicht miteinander vereinbar sind. Diese Trennungen MÜSSEN umgesetzt werden. Sie SOLLTEN dokumentiert werden.

ORP.4.A5 Vergabe von Zutrittsberechtigungen [Leiter IT]

Es MUSS festgelegt werden, welche Zutrittsberechtigungen an welche Personen im Rahmen ihrer Funktion vergeben werden. Werden Zutrittsmittel wie Chipkarten verwendet, so MUSS die Ausgabe bzw. der Entzug dokumentiert werden. Die Zutrittsberechtigten SOLLTEN auf den korrekten Umgang mit den Zutrittsmitteln geschult werden. Bei längeren Abwesenheiten SOLLTEN berechtigte Personen vorübergehend gesperrt werden.

ORP.4.A6 Vergabe von Zugangsberechtigungen [Leiter IT]

Es MUSS festgelegt werden, welche Zugangsberechtigungen an welche Personen im Rahmen ihrer Funktion vergeben bzw. entzogen werden. Werden Zugangsmittel wie Chipkarten verwendet, so MUSS die Ausgabe bzw. der Entzug dokumentiert werden. Die Zugangsberechtigten SOLLTEN auf den korrekten Umgang mit den Zugangsmitteln geschult werden. Bei längeren Abwesenheiten SOLLTEN berechtigte Personen vorübergehend gesperrt werden.

ORP.4.A7 Vergabe von Zugriffsrechten [Leiter IT]

Es MUSS festgelegt werden, welche Zugriffsrechte an welche Personen im Rahmen ihrer Funktion vergeben bzw. entzogen werden. Werden Zugangsmittel wie Chipkarten verwendet, so MUSS die Ausgabe bzw. der Entzug dokumentiert werden. Die Zugriffsrechte SOLLTEN auf den korrekten Umgang mit den Zugangsmitteln geschult werden. Bei längeren Abwesenheiten SOLLTEN berechtigte Personen vorübergehend gesperrt werden.

ORP.4.A8 Regelung des Passwortgebrauchs [Benutzer, Leiter IT]

Die Institution MUSS den Passwortgebrauch verbindlich regeln. Dabei MUSS festgelegt werden, dass nur Passwörter mit ausreichender Länge und Komplexität verwendet werden. Die Passwörter SOLLTEN in angemessenen Zeitabständen geändert werden. Die Passwörter MÜSSEN sofort gewechselt, sobald sie unautorisierten Personen bekannt geworden sind oder der Verdacht darauf besteht. Passwörter MÜSSEN geheim gehalten werden. Standardpasswörter MÜSSEN durch ausreichend starke Passwörter ersetzt und vordefinierte Logins geändert werden. Es SOLLTE überprüft werden, dass die mögliche Passwortlänge auch im vollen Umfang von dem IT-System geprüft wird. Bei erfolglosen Anmeldeversuchen SOLLTE das System keinen Hinweis darauf geben, ob Passwort oder Benutzerkennung falsch sind.

ORP.4.A9 Identifikation und Authentisierung [Leiter IT]

Der Zugang zu allen IT-Systemen und Diensten MUSS durch eine angemessene Identifikation und Authentisierung der zugreifenden Benutzer, Dienste oder IT-Systeme abgesichert sein. Vorkonfigurierte Zugangsmittel MÜSSEN vor dem produktiven Einsatz geändert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Identitäts- und Berechtigungsmanagement. Sie SOLLTEN grundsätzlich umgesetzt werden.

ORP.4.A10 Schutz von Benutzerkonten mit weitreichenden Berechtigungen [Leiter IT]

Benutzerkonten mit weitreichenden Berechtigungen SOLLTEN mit mindestens zwei Authentisierungsmerkmalen geschützt werden.

ORP.4.A11 Zurücksetzen von Passwörtern [Leiter IT]

Für das Zurücksetzen von Passwörtern SOLLTE ein angemessenes sicheres Verfahren definiert und umgesetzt werden. Die Support-Mitarbeiter, die Passwörter zurücksetzen können, SOLLTEN entsprechend geschult werden. Bei höherem Schutzbedarf des Passwortes SOLLTE eine Strategie definiert werden, falls der Support-Mitarbeiter aufgrund fehlender sicherer Möglichkeiten der Übermittlung des Passwortes die Verantwortung nicht übernehmen kann.

ORP.4.A12 Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen [Leiter IT]

Es SOLLTE ein Authentisierungskonzept erstellt werden. Darin SOLLTE für jedes IT-System und jede Anwendung definiert werden, welche Funktions- und Sicherheitsanforderungen an die Authentisierung gestellt werden. Authentisierungsinformationen SOLLTEN kryptografisch sicher geschützt übertragen und gespeichert werden.

ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen [Leiter IT]

Es SOLLTEN dem Schutzbedarf angemessene Identifikations- und Authentisierungsmechanismen verwendet werden. Authentisierungsdaten SOLLTEN durch das IT-System bzw. IT-Anwendungen bei der Verarbeitung jederzeit gegen Ausspähung, Veränderung und Zerstörung geschützt werden.

ORP.4.A14 Kontrolle der Wirksamkeit der Benutzertrennung am IT-System [Administrator]

In angemessenen Zeitabständen SOLLTE überprüft werden, ob die Benutzer von IT-Systemen sich regelmäßig nach Aufgabenerfüllung abmelden und nicht mehrere Benutzer unter der gleichen Kennung arbeiten.

ORP.4.A15 Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement [Leiter IT]

Für das Identitäts- und Berechtigungsmanagement SOLLTEN folgenden Prozesse definiert und umgesetzt werden:

- Richtlinien verwalten,
- Identitätsprofile verwalten,
- Benutzerkennungen verwalten
- Berechtigungsprofile verwalten,
- Rollen verwalten.

ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle [Administrator]

Es SOLLTE eine Richtlinie für die Zugriffs- und Zugangskontrolle von IT-Systemen, IT-Komponenten und Netzen erstellt werden. Es SOLLTEN Standard-Rechteprofile benutzt werden, die den Funktionen und Aufgaben der Mitarbeiter entsprechen. Für jedes IT-System und jede IT-Anwendung SOLLTE eine schriftliche Zugriffsregelung existieren. Außerdem SOLLTEN alle eingerichteten Benutzer und vergebenen Rechte dokumentiert sein. Es SOLLTE geregelt sein, dass Benutzer nur auf IT-Systeme und Dienste zugreifen können, wenn sie vorher angemessen identifiziert und authentisiert wurden.

ORP.4.A17 Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen [Leiter IT]

Beim Einsatz eines Identitäts- und Berechtigungsmanagement-System SOLLTE es für die Institution und deren jeweilige Geschäftsprozesse, Organisationsstrukturen und Abläufe sowie deren Schutzbedarf passen. Das Identitäts- und Berechtigungsmanagement-System SOLLTE die in der Institution vorhandenen Vorgaben zum Umgang mit Identitäten und Berechtigungen abbilden können. Das ausgewählte Identitäts- und Berechtigungsmanagement-System SOLLTE den Grundsatz der Funktionstrennung realisieren können. Das Identitäts- und Berechtigungsmanagement-System SOLLTE angemessen vor Angriffen geschützt werden.

ORP.4.A18 Einsatz eines zentralen Authentifizierungsdienstes [Leiter IT]

Um ein zentrales Identitäts- und Berechtigungsmanagement aufzubauen, SOLLTE ein zentraler netzbasierter Authentisierungsdienst eingesetzt werden. Der Einsatz eines zentralen netzbasierten Authentisierungsdienstes SOLLTE sorgfältig geplant werden. Dazu SOLLTEN die Sicherheitsanforderungen dokumentiert werden, die für die Auswahl eines solchen Dienstes relevant sind.

ORP.4.A19 Einweisung aller Mitarbeiter in den Umgang mit Authentisierungsverfahren und -mechanismen [Benutzer, Leiter IT]

Alle Mitarbeiter SOLLTEN in den korrekten Umgang mit den Authentisierungsverfahren eingewiesen werden. Es SOLLTE verständliche Richtlinien für den Umgang mit Authentisierungsverfahren geben. Die Mitarbeiter SOLLTEN über relevante Regelungen informiert werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

ORP.4.A20 Notfallvorsorge für das Identitäts- und Berechtigungsmanagement-System [Leiter IT] (CIA)

Es SOLLTE geprüft werden, inwieweit ein ausgefallenes Identitäts- und Berechtigungsmanagement-System sicherheitskritisch für die Geschäftsprozesse ist. Für Notfälle SOLLTE ein Berechtigungskonzept vorhanden sein und es SOLLTEN Notfallberechtigungen existieren.

ORP.4.A21 Mehr-Faktor-Authentisierung [Leiter IT] (C)

Bei höherem Schutzbedarf SOLLTE eine sichere Zwei- oder Mehr-Faktor-Authentisierung, z. B. mit kryptographischen Zertifikaten, Chipkarten oder Token, zur Authentisierung verwendet werden.

4 Weiterführende Informationen

4.1 Literatur

- [29146] ISO/IEC 29146:2016
  Information technology - Security techniques - A framework for access management, 06.2016
- [ISFTS14] The Standard of Good Practice - Area TS1.4 Identiy and Access Management
  ISF, insbesondere Area TS1.4 Identiy and Access Management, Juni 2016
- [NIST80053A] NIST Special Publication 800-53A
  Assessing Security and Privacy Controls in Federal Information Systems, insebsondere Bereiche AC und IA, 12.2014

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Identitäts- und Berechtigungsmanagement" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen Anforderungen	G 0.14	G 0.15	G 0.16	G 0.18	G 0.22	G 0.23	G 0.25	G 0.29	G 0.30	G 0.31	G 0.32	G 0.36	G 0.37	G 0.44	G 0.46
ORP.4.A1				x											
ORP.4.A2				x											
ORP.4.A3				x											
ORP.4.A4					x			x			x		x		
ORP.4.A5			x	x				x						x	
ORP.4.A6				x		x		x							
ORP.4.A7				x		x		x							
ORP.4.A8				x		x		x							
ORP.4.A9	x	x		x	x	x			x		x	x	x		x
ORP.4.A10	x										x	x			
ORP.4.A11				x		x						x			
ORP.4.A12	x										x	x			
ORP.4.A13	x										x	x			
ORP.4.A14				x				x					x		
ORP.4.A15				x											
ORP.4.A16				x											
ORP.4.A17				x					x	x					
ORP.4.A18	x	x		x								x			
ORP.4.A19										x					
ORP.4.A20							x								
ORP.4.A21						x			x		x	x			

ORP: Organisation und Personal

ORP.5 Compliance Management (Anforderungsmanagement)

1 Beschreibung

1.1 Einleitung

In jeder Institution gibt es aus den verschiedensten Richtungen gesetzliche, vertragliche, strukturelle und interne Richtlinien und Vorgaben, die beachtet werden müssen. Viele davon haben direkte oder indirekte Auswirkungen auf das Informationssicherheitsmanagement.

Die Anforderungen sind je nach Branche, Land und anderen Rahmenbedingungen unterschiedlich. Weiterhin unterliegt beispielsweise eine Behörde anderen externen Regelungen als eine Aktiengesellschaft. Die Leitungsebene der Institution muss die Einhaltung der Anforderungen (neudeutsch: Compliance) sicherstellen und ein Compliance Management System betreiben.

Je nach Größe einer Institution kann diese verschiedene Managementprozesse haben, die sich mit unterschiedlichen Aspekten des Risikomanagements beschäftigen, z. B. Sicherheitsmanagement, Datenschutzmanagement, Compliance Management, Controlling. Diese sollten vertrauensvoll zusammenarbeiten, um Synergieeffekte zu nutzen und Konflikte frühzeitig auszuräumen.

1.2 Zielsetzung

Ziel des Bausteins Compliance Management ist es, aufzuzeigen, wie jederzeit ein Überblick über die verschiedenen Anforderungen an die einzelnen Bereiche einer Institution geschaffen werden kann. Dazu wird beschrieben, wie aus gesetzlichen, vertraglichen, strukturellen und internen Richtlinien und Vorgaben Sicherheitsanforderungen abgeleitet werden können.

1.3 Abgrenzung

In diesem Baustein werden ausgewählte Anforderungen betrachtet, die sich aus gesetzlichen oder vertraglichen Vorgaben ergeben und die Auswirkungen auf die Gestaltung der Informationssicherheit in der Institution haben. Es wird nicht auf bereichsspezifische Gesetze eingegangen.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Compliance Management von besonderer Bedeutung:

2.1 Verstoß gegen rechtliche Vorgaben

Die unzureichende Umsetzung von Informationssicherheit kann dazu führen, dass gegen gesetzliche Regelungen oder vertragliche Vereinbarungen verstoßen wird. Institution müssen außerdem eine Vielzahl branchenspezifischer, nationaler und internationaler rechtlicher Rahmenbedingungen beachten. Da dies sehr komplex werden kann, kann es passieren, dass unabsichtlich gegen rechtliche Vorgaben verstoßen wird oder dies sogar vorsätzlich in Kauf genommen wird. Beispiel:

- Viele Cloud-Dienstleister bieten ihre Services in einem internationalen Umfeld an. Damit unterliegen die Anbieter oft anderen nationalen Gesetzgebungen. Häufig sehen Cloud-Anwender nur auf niedrige Kosten und schätzen die zu beachtenden rechtlichen Rahmenbedingungen wie Datenschutz, Informationspflichten, Insolvenzrecht, Haftung, Informationszugriff für Dritte falsch ein.

2.2 Unzulässige Weitergabe von Informationen

Durch das Fehlverhalten von Personen kann es dazu kommen, dass schützenswerte Informationen unzulässig weitergegeben werden. Beispiele hierfür sind:

- Vertrauliche Informationen werden in Hörweite fremder Personen diskutiert, beispielsweise in Pausengesprächen von Besprechungen oder über Mobiltelefonate in öffentlichen Umgebungen.
- Der Vorgesetzte einer Fachabteilung verdächtigt einen Mitarbeiter, mit der Konkurrenz zusammenzuarbeiten. Um ihm dies nachzuweisen, bittet er den Leiter des IT-Betriebs, ihm "auf dem kleinen Dienstweg" Einblick in die E-Mails dieses Mitarbeiters zu geben. Der Leiter IT-Betrieb weist den Mail-Administrator an, hierfür einen Zugriff einzurichten, ohne die hierfür notwendigen Zustimmungen einzuholen.

2.3 Unzureichende Identifikationsprüfung von Kommunikationspartnern

In persönlichen Gesprächen, am Telefon oder auch in E-Mails sind viele Personen bereit, weit mehr Informationen preiszugeben, als sie das in schriftlicher Form oder in größerer Runde tun würden. Hierbei wird häufig vom Kommunikationspartner stillschweigend erwartet, dass die Gesprächs- oder E-Mail-Inhalte vertraulich behandelt werden. Darüber hinaus besteht die Neigung, die Identität des Kommunikationspartners nicht zu hinterfragen, da dies als unhöflich empfunden wird. Ebenso werden häufig Berechtigungen nicht ausreichend geprüft, sondern aus der (behaupteten) Rolle implizit abgeleitet. Typische Beispiele hierfür sind:

- Ein Mitarbeiter erhält eine E-Mail von einem angeblichen Bekannten seiner Vorgesetzten, mit der angeblich die schnelle Überweisung eines ausstehenden Betrages vereinbart wurde.
- Ein Mann im Blaumann mit Montagekoffer erhält Zugang zum Rechenzentrum, nachdem er etwas von "Wasserrohren" murmelt.

2.4 Unbeabsichtigte Weitergabe interner Informationen

Bei der Weitergabe von Informationen kommt es immer wieder vor, dass neben den gewünschten Informationen versehentlich auch andere Informationen übermittelt werden. Dadurch können vertrauliche geeignete Informationen in die falschen Hände geraten. Beispiele hierfür sind

- alte Dateien oder Restinformationen auf weitergegebenen Datenträgern, Übermittlung anderer als der vorgesehenen Daten oder Versand an falsche Empfänger.
- 2015 konnte ein französischer Fernsehsender stundenlang kein Programm ausstrahlen, nachdem Hacker sich Zugriff auf interne IT-Systeme verschafft hatten. In einer Pressekonferenz, nachdem der Sender wieder arbeiten konnte, wurde im Hintergrund eine Notizwand in alle Welt übertragen, an der Passwörter für alle möglichen internen und externen Kennungen hingen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich *Compliance Management* aufgeführt. Grundsätzlich ist der Änderungsmanager (Compliance Manager) für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	Anforderungsmanager (Compliance Manager)
Weitere Verantwortliche	Benutzer, IT-Betrieb, Informationssicherheitsbeauftragter (ISB), Institutionsleitung, Leiter Organisation, Personalabteilung, Verantwortliche der einzelnen Anwendungen, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

ORP.5.A1 Identifikation der rechtlichen Rahmenbedingungen [Leiter Organisation, Institutionsleitung]

In der Institution MUSS ein Prozess aufgebaut sein, um alle relevanten gesetzlichen, vertraglichen und sonstigen Vorgaben zu identifizieren. Alle rechtlichen Rahmenbedingungen mit Auswirkungen auf das Sicherheitsmanagement MÜSSEN identifiziert und dokumentiert werden.

Die für die einzelnen Bereiche der Institution relevanten gesetzlichen und vertraglichen Vorgaben SOLLTEN in einer strukturierten Übersicht herausgearbeitet werden. Die Dokumentation MUSS auf dem aktuellen Stand gehalten werden. Die als sicherheitsrelevant identifizierten Anforderungen MÜSSEN bei der Planung und Konzeption von Geschäftsprozessen, Anwendungen und IT-Systemen oder bei der Beschaffung neuer Komponenten einfließen.

ORP.5.A2 Beachtung rechtlicher Rahmenbedingungen [Vorgesetzte, Leiter Organisation, Institutionsleitung]

Führungskräfte, welche die rechtliche Verantwortung für die Institution vor Ort tragen, MÜSSEN für die Einhaltung der rechtlichen Vorgaben sorgen. Die Verantwortlichkeiten und Zuständigkeiten für die Einhaltung rechtlicher Vorgaben MÜSSEN festgelegt sein.

Es MÜSSEN geeignete Maßnahmen identifiziert und umgesetzt werden, um Verstöße gegen relevante Anforderungen zu vermeiden. Wenn Verstöße gegen relevante Anforderungen erkannt werden, MÜSSEN sachgerechte Korrekturmaßnahmen ergriffen werden, um die Abweichungen zu beheben.

ORP.5.A3 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen [Vorgesetzte, Personalabteilung]

Alle Mitarbeiter MÜSSEN in einschlägige Gesetze (z. B. zum Datenschutz), Vorschriften und interne Regelungen eingewiesen und verpflichtet werden, diese einzuhalten. Den Mitarbeitern MUSS bekannt sein, welcher rechtliche Rahmen ihre Tätigkeit bestimmt.

Gemeinsam mit den Basisanforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Compliance Management. Sie SOLLTEN grundsätzlich umgesetzt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Compliance Management (Anforderungsmanagement). Sie SOLLTEN grundsätzlich umgesetzt werden.

ORP.5.A4 Konzeption und Organisation des Compliance Managements [Institutionsleitung]

Es SOLLTEN geeignete Prozesse und Organisationsstrukturen aufgebaut werden, um den Überblick über die verschiedenen rechtlichen Anforderungen an die einzelnen Bereiche der Institution zu gewährleisten. Dafür SOLLTEN Verantwortliche benannt und deren Aufgaben in Bezug auf das Compliance Management festgelegt werden.

Compliance Manager und ISB SOLLTEN regelmäßig zusammenarbeiten. Sie SOLLTEN gemeinsam Sicherheitsanforderungen ins Compliance Management integrieren, sicherheitsrelevante Anforderungen in Sicherheitsmaßnahmen überführen und deren Umsetzung kontrollieren.

ORP.5.A5 Ausnahmegenehmigungen [Vorgesetzte, Informationssicherheitsbeauftragter (ISB)]

In Einzelfällen kann es erforderlich sein, von getroffenen Regelungen abzuweichen. Begründete Ausnahmen SOLLTEN aber in jedem Fall durch eine autorisierte Stelle nach einer Risikoabschätzung genehmigt werden. Es SOLLTE ein Genehmigungsverfahren für Ausnahmegenehmigungen geben. Es SOLLTE eine Übersicht über alle erteilten Ausnahmegenehmigungen geben. Ein entsprechendes Verfahren für die Dokumentation und ein Überprüfungsprozess SOLLTE etabliert werden. Alle Ausnahmegenehmigungen SOLLTEN befristet sein.

ORP.5.A6 Einweisung des Personals in den sicheren Umgang mit IT [Vorgesetzte, Personalabteilung]

Alle Mitarbeiter und alle externen IT-Benutzer SOLLTEN in den sicheren Umgang mit der IT der Institution eingewiesen werden. Dazu SOLLTE ihnen eine verbindliche, verständliche, aktuelle und verfügbare Richtlinie zur IT-Nutzung an die Hand gegeben werden. Diese Richtlinie SOLLTE beschreiben, welche Rechte und Pflichten sie bei der IT-Nutzung haben und welche Sicherheitsmaßnahmen zu ergreifen sind. Veränderungen SOLLTEN den Mitarbeitern rechtzeitig bekannt gegeben werden.

ORP.5.A7 Aufrechterhaltung der Informationssicherheit [Informationssicherheitsbeauftragter (ISB)]

Um das bestehende Sicherheitsniveau aufrechtzuerhalten und fortlaufend zu verbessern, SOLLTEN alle Sicherheitsmaßnahmen des Sicherheitskonzeptes regelmäßig auf Einhaltung und Verbesserungsbedarf überprüft werden. Die Prüfungen SOLLTEN durch unabhängige, fachlich qualifizierte, interne oder externe Personen durchgeführt werden. Die Ergebnisse der Überprüfungen SOLLTEN nachvollziehbar dokumentiert und der Leitung bekannt gegeben werden. Gefundene Mängel SOLLTEN zeitnah behoben werden.

ORP.5.A8 Regelmäßige Überprüfungen des Compliance Managements

Es SOLLTE ein Verfahren etabliert sein, wie das Compliance Management und die sich aus diesem ergebenden Anforderungen und Maßnahmen regelmäßig auf Effizienz und Effektivität überprüft werden (siehe auch DER.1.3 Audits und Revisionen). Es SOLLTE regelmäßig geprüft werden, ob die Organisationsstruktur und die Prozesse des Compliance Managements noch angemessen sind.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

ORP.5.A9 Schutz gegen nachträgliche Veränderungen von Informationen [Informationssicherheitsbeauftragter (ISB), Benutzer] (I)

Damit Dateien nicht unbemerkt verändert werden können, SOLLTEN ausreichende Sicherheitsmaßnahmen ergriffen werden. Je nach Datenformat und Schutzbedarf SOLLTEN dafür geeignete Methoden ausgewählt werden. Dazu gehören beispielsweise digitale Signaturen und andere kryptographische Verfahren, Copyright-Vermerke oder die Verwendung von Dateiformaten, die nachträgliche Änderungen bzw. auszugsweise Weiterverarbeitung erschweren. Die Mitarbeiter SOLLTEN informiert werden, welche Sicherheitsmechanismen hierfür eingesetzt werden sollen und wie diese zu benutzen sind.

ORP.5.A10 Klassifizierung von Informationen (CIA)

Es gibt in vielen Bereichen einer Institution Informationen, die einen höheren Schutzbedarf haben oder besonderen Restriktionen unterliegen, z. B. personenbezogene, finanzrelevante, vertrauliche oder Copyright-geschützte Daten. Für diese gelten je nach ihrer Kategorisierung unterschiedliche Beschränkungen im Umgang mit ihnen. Daher SOLLTEN möglichst alle Informationen entsprechend ihrem Schutzbedarf klassifiziert und, falls möglich, gekennzeichnet werden. Die Mitarbeiter SOLLTEN regelmäßig auf den sorgfältigen Umgang mit Informationen hingewiesen sowie über die Restriktionen beim Umgang mit klassifizierten Daten informiert werden.

ORP.5.A11 Erhebung der rechtlichen Rahmenbedingungen für kryptographische Verfahren und Produkte [IT-Betrieb, Verantwortliche der einzelnen Anwendungen] (CI)

Beim Einsatz kryptographischer Produkte sind diverse gesetzliche Rahmenbedingungen zu beachten. Die rechtlichen Rahmenbedingungen für den Einsatz kryptographischer Verfahren und Produkte SOLLTEN für alle Länder ermittelt und dokumentiert werden, in denen diese genutzt werden sollen.

4 Weiterführende Informationen

4.1 Literatur

- [19600] ISO 19600:2014
  ISO, Compliance management systems, 2014

- [27002K18] ISO/IEC 27002:2013 Kapitel 18 Compliance
  ISO, Information technology-security technique- Code of practice for information on security controls, insbesondere Kapitel 18 "Compliance", 2013

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Compliance Management (Anforderungsmanagement)" von Bedeutung.

G 0.29 Verstoß gegen Gesetze oder Regelungen

Elementare Gefährdungen Anforderungen	G 0.29
ORP.5.A1	x
ORP.5.A2	x
ORP.5.A3	x
ORP.5.A4	x
ORP.5.A5	x
ORP.5.A6	x
ORP.5.A7	x
ORP.5.A8	x
ORP.5.A9	x
ORP.5.A10	x
ORP.5.A11	x

Bundesamt
für Sicherheit in der
Informationstechnik

CON: Konzeption und Vorgehensweise

CON.3	Datensicherungskonzept	**169**
CON.6	Löschen und Vernichten	**189**
CON.1	Kryptokonzept	**155**
CON.2	Datenschutz	**164**
CON.5	Entwicklung und Einsatz von Fachanwendungen	**182**
CON.7	Informationssicherheit auf Auslandsreisen	**195**
CON.4	Auswahl und Einsatz von Standardsoftware	**175**

CON: Konzeption und Vorgehensweise

CON.1 Kryptokonzept

1 Beschreibung

1.1 Einleitung

Mit der in diesem Baustein beschriebene Vorgehensweise wird ein Überblick über kryptografische Verfahren und Produkte gegeben, die in einer Institution eingesetzt werden können. Es wird beschrieben, wie in einer heterogenen Umgebung sowohl die lokal gespeicherten Daten als auch die zu übertragenden Daten wirkungsvoll durch kryptografische Verfahren und Techniken geschützt werden können. Darüber hinaus werden geeignete organisatorische und prozessuale Anforderungen beschrieben, mit denen die Vertraulichkeit, Integrität und Authentizität gewährleistet werden können.

Ergänzend zu den Verfahren und Techniken, mit denen lokal gespeicherte Daten und übertragene Informationen geschützt werden können, werden im vorliegendem Baustein auch Kryptomodule beschrieben. Mit einem Kryptomodul ist ein Produkt gemeint, das die im Kryptokonzept dargelegte Sicherheitsfunktionalität bietet. Ein solches Produkt kann dabei aus Hardware, Software, Firmware oder aus einer Kombination hieraus bestehen. Hinzukommen noch Bauteile wie Speicher, Prozessoren, Busse und Stromversorgung, die notwendig sind, um die Kryptoprozesse umzusetzen. Ein Kryptomodul kann in unterschiedlichsten Rechner- oder Telekommunikationssystemen verwendet werden, um sensible Daten bzw. Informationen zu schützen. Dies ist im vorliegenden Baustein erst bei erhöhtem Schutzbedarf relevant.

1.2 Zielsetzung

Der Baustein beschreibt, wie Informationen in Institutionen kryptografisch abgesichert werden und wie hierfür ein entsprechendes Kryptokonzept erstellt werden sollte.

1.3 Abgrenzung

In diesem Baustein werden allgemeine Anforderungen, organisatorische Rahmenbedingungen und prozessuale Abläufe für kryptografische Produkte und Verfahren betrachtet. Die mit dem Betrieb von Kryptomodulen zusammenhängenden Kern-IT-Aufgaben werden nicht in diesem Baustein behandelt. Dafür müssen die Anforderungen der Bausteine der Schicht OPS.1.1 *Kern-IT-Betrieb* erfüllt werden.

Wie einzelne Anwendungen (z. B. E-Mails) oder IT-Systeme (z. B. Laptops) kryptografisch abgesichert werden können, ist nicht Gegenstand des vorliegenden Bausteins, sondern wird in den entsprechenden Bausteinen behandelt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Kryptokonzept von besonderer Bedeutung:

2.1 Unzureichendes Schlüsselmanagement bei Verschlüsselung

Durch ein unzureichendes Schlüsselmanagement könnten Angreifer auf verschlüsselte Daten zugreifen. So kann es beispielsweise sein, dass sich aufgrund fehlender Regelungen verschlüsselte Informationen mitsamt den zugehörigen Schlüsseln auf demselben Datenträger befinden. Dadurch kann bei symmetrischen Verfahren jeder, der auf den Datenträger oder den Kommunikationskanal zugreifen kann, die Informationen entschlüsseln, sofern das eingesetzte Verschlüsselungsverfahren bekannt ist.

2.2 Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptografischen Verfahren

Wenn Institutionen kryptografische Verfahren und Produkte einsetzen, müssen sie dabei diverse gesetzliche Rahmenbedingungen beachten. In einigen Ländern dürfen beispielsweise kryptografische Verfahren nicht ohne staatliche Genehmigung eingesetzt werden. Das kann dazu führen, dass Empfänger im Ausland verschlüsselte Datensätze nicht lesen können, da sie die benötigten kryptografischen Produkte nicht einsetzen dürfen oder sich vielleicht sogar strafbar machen.

Außerdem ist in sehr vielen Ländern auch der Export von Produkten mit starker Kryptografie erheblich eingeschränkt. Das kann dazu verleiten, schützenswerte Daten unverschlüsselt zu lassen oder mit unsicheren Verfahren zu schützen. Dadurch sind einerseits Angreifern Tür und Tor geöffnet und andererseits kann so auch gegen nationales Recht verstoßen werden. So können beispielsweise Datenschutzgesetze vorschreiben, dass adäquate kryptografische Verfahren eingesetzt werden müssen, um personenbezogene Daten zu schützen.

2.3 Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten

Setzt beispielsweise eine Institution ein Kryptomodul ein, das entweder zu kompliziert zu bedienen ist oder sich nicht intuitiv bedienen lässt, könnten die Benutzer aus Bequemlichkeit oder aus pragmatischen Gründen darauf verzichten, dieses zu benutzen und stattdessen die Informationen im Klartext übertragen. Dadurch können die übertragenen Informationen von Angreifern abgehört werden.

Auch kann eine Fehlbedienung eines Kryptomoduls dazu führen, dass vertrauliche Informationen von Angreifern abgegriffen werden, etwa wenn diese im Klartext übertragen werden, weil versehentlich der Klartext-Modus aktiviert wurden.

2.4 Software-Schwachstellen oder -Fehler in Kryptomodulen

Software-Schwachstellen oder -Fehler in Kryptomodulen schwächen die Sicherheit der eingesetzten kryptografischen Verfahren und können dazu führen, dass die damit geschützten Informationen mitgelesen werden. Dadurch ist es möglich, dass Angreifer die Kryptomodule manipulieren (z. B. über Schadsoftware) und so sensible Daten abfließen oder auch ganze Produktionsprozesse stillstehen, weil sich Daten nicht mehr entschlüsselt lassen.

2.5 Ausfall eines Kryptomoduls

Kryptomodule können durch technische Defekte, Stromausfälle oder absichtliche Zerstörung ausfallen. Dadurch könnten bereits verschlüsselte Daten sich nicht mehr entschlüsseln lassen, solange das erforderliche Kryptomodul nicht mehr verfügbar ist. Dadurch können ganze Prozessketten stillstehen, z. B. wenn weitere IT-Anwendungen auf die Daten angewiesen sind.

2.6 Unsichere kryptografische Algorithmen oder Produkte

Unsichere oder veraltete kryptografische Algorithmen lassen sich von einem potenziellen Angreifer mit vertretbaren Ressourcen brechen. Bei Verschlüsselungsalgorithmen bedeutet dies, dass es gelingt, aus dem verschlüsselten Text den ursprünglichen Klartext zu ermitteln, ohne dass zusätzliche Informationen, wie z. B. der verwendete kryptografische Schlüssel, bekannt sind. Werden unsichere kryptographische Algorithmen eingesetzt, können Angreifer den kryptographischen Schutz unterlaufen und somit auf schützenswerte Informationen der Institution zugreifen.

Selbst wenn in einer Institution ausschließlich sichere (z. B. zertifizierte) Produkte eingesetzt werden, kann eine Kommunikation dennoch unsicher werden, beispielsweise wenn der Kommunikationspartner kryptografische Verfahren benutzt, die nicht dem Stand der Technik entsprechen.

2.7 Fehler in verschlüsselten Daten oder kryptografischen Schlüsseln

Werden Informationen verschlüsselt und die Chiffrate dann verändert, lassen sich die verschlüsselten Informationen eventuell nicht mehr korrekt entschlüsseln. Je nach Betriebsart der Verschlüsselungsroutinen kann dies bedeuten, dass nur wenige Bytes falsch entschlüsselt oder auch sämtliche Daten falsch entschlüsselt werden. Ist keine Datensicherung vorhanden, sind solche Daten verloren.

Noch kritischer kann sich ein Fehler in den verwendeten kryptografischen Schlüsseln auswirken. Schon die Änderung eines einzigen Bits eines kryptografischen Schlüssels führt dazu, dass sämtliche damit verschlüsselten Daten nicht mehr entschlüsselt werden können.

2.8 Unautorisierte Nutzung eines Kryptomoduls

Gelingt es einem Angreifer, ein Kryptomodul unautorisiert zu benutzen, kann er kritische Sicherheitsparameter manipulieren. Hierdurch bieten die kryptografischen Verfahren keine ausreichende Sicherheit mehr. Weiterhin kann ein Angreifer das Kryptomodul so manipulieren, dass es zwar auf den ersten Blick korrekt arbeitet, sich jedoch tatsächlich in einem unsicheren Zustand befindet. Dadurch bleibt er längere Zeit unentdeckt und kann auf zahlreiche sensible Informationen zugreifen.

2.9 Kompromittierung kryptografischer Schlüssel

Die Sicherheit kryptografischer Verfahren hängt entscheidend davon ab, wie vertraulich die verwendeten kryptografischen Schlüssel bleiben. Daher wird ein potenzieller Angreifer in der Regel versuchen, die verwendeten Schlüssel zu ermitteln. Das könnte ihm zum Beispiel gelingen, indem er flüchtige Speicher ausliest oder ungeschützte Schlüssel findet, die zum Beispiel in einer Datensicherung hinterlegt sind. Kennt er den verwendeten Schlüssel und das eingesetzte Kryptoverfahren, kann er relativ leicht die Daten entschlüsseln.

Bei einer Festplattenverschlüsselung (etwa Trusted Disk) kann ein Angreifer z. B. einen Keylogger zwischen Tastatur und Rechner schalten, um an das Passwort zu gelangen, das dazu benötigt wird, um die Festplatte zu entschlüsseln.

2.10 Gefälschte Zertifikate

Zertifikate dienen dazu, einen öffentlichen kryptografischen Schlüssel an eine Person zu binden. Diese Bindung des Schlüssels an den Namen der Person wird wiederum kryptografisch mittels einer digitalen Signatur häufig von einer vertrauenswürdigen dritten Stelle abgesichert.

Diese Zertifikate werden von Dritten dann benutzt, um digitale Signaturen der im Zertifikat ausgewiesenen Person zu prüfen bzw. um dieser Person Daten mit dem im Zertifikat aufgezeichneten Schlüssel verschlüsselt zuzusenden.

Ist ein solches Zertifikat gefälscht, werden digitale Signaturen fälschlicherweise als korrekt geprüft und der Person im Zertifikat zugeordnet oder es werden Daten mit einem möglicherweise unsicheren Schlüssel verschlüsselt und versandt.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für Kryptokonzepte aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte (ISB) dafür zuständig, die Anforderungen zu erfüllen. Außerdem ist er dafür verantwortlich, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Informationssicherheitsbeauftragter (ISB)
Weitere Verantwortliche	Fachverantwortliche, IT-Betrieb, Leiter IT, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

CON.1.A1 Auswahl geeigneter kryptografischer Verfahren [Fachverantwortliche]

Es MÜSSEN geeignete kryptografische Verfahren ausgewählt werden. Dabei MUSS sichergestellt sein, dass etablierte Algorithmen verwendet werden, die von der Fachwelt intensiv untersucht wurden und von denen keine Sicherheitslücken bekannt sind. Ebenso MÜSSEN aktuell empfohlene Schlüssellängen eingesetzt werden.

CON.1.A2 Datensicherung bei Einsatz kryptografischer Verfahren [IT-Betrieb]

In Datensicherungen MÜSSEN kryptografische Schlüssel derart gespeichert bzw. aufbewahrt werden, dass Unbefugte nicht darauf zugreifen können. Langlebige kryptografische Schlüssel MÜSSEN außerhalb der eingesetzten IT-Systeme aufbewahrt werden. Bei einer Langzeitspeicherung verschlüsselter Daten SOLLTE regelmäßig geprüft werden, ob die verwendeten kryptografischen Algorithmen und die Schlüssellängen noch dem Stand der Technik entsprechen. Es MUSS sichergestellt sein, dass auf verschlüsselt gespeicherte Daten auch nach längeren Zeiträumen noch zugegriffen werden kann. Verwendete Kryptoprodukte SOLLTEN archiviert werden. Die Konfigurationsdaten von Kryptoprodukten SOLLTEN gesichert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Kryptokonzept. Sie SOLLTEN grundsätzlich umgesetzt werden.

CON.1.A3 Verschlüsselung der Kommunikationsverbindungen

Es SOLLTE geprüft werden, ob mit vertretbarem Aufwand eine Verschlüsselung der Kommunikationsverbindungen möglich und praktikabel ist. Ist dies der Fall, SOLLTEN Kommunikationsverbindungen geeignet verschlüsselt werden.

CON.1.A4 Geeignetes Schlüsselmanagement [IT-Betrieb, Fachverantwortliche]

Kryptografische Schlüssel SOLLTEN immer mit geeigneten Schlüsselgeneratoren und in einer sicheren Umgebung erzeugt werden. Ein Schlüssel SOLLTE möglichst nur einem Einsatzzweck dienen. Insbesondere SOLLTEN für die Verschlüsselung und Signaturbildung unterschiedliche Schlüssel benutzt werden.

Wenn Schlüssel verwendet werden, SOLLTE die authentische Herkunft und die Integrität der Schlüsseldaten überprüft werden.

Alle kryptografischen Schlüssel SOLLTEN hinreichend häufig gewechselt werden. Es SOLLTE eine festgelegte Vorgehensweise für den Fall geben, dass ein Schlüssel offen gelegt wurde. Alle erzeugten kryptografischen Schlüssel SOLLTEN sicher aufbewahrt und verwaltet werden.

CON.1.A5 Sicheres Löschen und Vernichten von kryptografischen Schlüsseln [IT-Betrieb]

Nicht mehr benötigte Schlüssel und Zertifikate SOLLTEN sicher gelöscht bzw. vernichtet werden. Auf Produkte mit unkontrollierbarer Schlüsselablage SOLLTE generell verzichtet werden.

CON.1.A6 Bedarfserhebung für kryptografische Verfahren und Produkte [IT-Betrieb, Fachverantwortliche]

Es SOLLTE festgelegt werden, für welche Aufgaben kryptografische Verfahren eingesetzt werden sollen. Danach SOLLTEN die Anwendungen, IT-Systeme und Kommunikationsverbindungen identifiziert werden, die notwendig sind, um die Aufgaben zu erfüllen. Diese SOLLTEN kryptografisch abgesichert werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

CON.1.A7 Erstellung einer Sicherheitsrichtlinie für den Einsatz kryptografischer Verfahren und Produkte (CIA)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTE eine spezifische Richtlinie für den Einsatz von Kryptoprodukten erstellt werden. In der Sicherheitsrichtlinie SOLLTE geregelt werden, wer für den sicheren Betrieb der kryptografischen Produkte verantwortlich ist. Für die benutzen Kryptoprodukte SOLLTEN es Vertretungsregelungen geben.

Auch SOLLTEN notwendige Schulungs- und Sensibilisierungsmaßnahmen für Benutzer sowie Verhaltensregeln und Meldewege bei Problemen oder Sicherheitsvorfällen festgelegt werden. Weiter SOLLTE die Richtlinie definieren, wie sichergestellt wird, dass Kryptomodule sicher konfiguriert, korrekt eingesetzt und regelmäßig gewartet werden.

Die Richtlinie SOLLTE allen relevanten Mitarbeitern bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von ihr abgewichen, SOLLTE dies mit dem ISB abgestimmt und dokumentiert werden. Es SOLLTE regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

CON.1.A8 Erhebung der Einflussfaktoren für kryptografische Verfahren und Produkte (CIA)

Bevor eine Entscheidung getroffen werden kann, welche kryptografischen Verfahren und Produkte bei erhöhtem Schutzbedarf eingesetzt werden, SOLLTEN unter anderem folgende Einflussfaktoren ermittelt werden:

- Sicherheitsaspekte (siehe CON.1.A6 *Bedarfserhebung für kryptografische Verfahren und Produkte*),
- technische Aspekte,
- personelle und organisatorische Aspekte,
- wirtschaftliche Aspekte,
- Lebensdauer von kryptografischen Verfahren und der eingesetzten Schlüssellängen
- Zulassung von kryptografischen Produkten und
- gesetzliche Rahmenbedingungen.

CON.1.A9 Auswahl eines geeigneten kryptografischen Produkts [IT-Betrieb, Fachverantwortliche] (CI)

Bevor ein kryptografisches Produkt ausgewählt wird, SOLLTE die Institution festlegen, welche Anforderungen das Produkt erfüllen muss. Dabei SOLLTEN Aspekte, wie Funktionsumfang, Interoperabilität, Wirtschaftlichkeit sowie Fehlbedienungs- und Fehlfunktionssicherheit betrachtet werden. Es SOLLTE geprüft werden, ob zertifizierte Produkte vorrangig eingesetzt werden sollen. Auch die zukünftigen Einsatzorte SOLLTEN bei der Auswahl beachtet werden, da es z. B. Export- und Importbeschränkungen für kryptografische Produkte gibt.

CON.1.A10 Entwicklung eines Kryptokonzepts (CI)

Es SOLLTE ein Kryptokonzept entwickelt werden, das in das Sicherheitskonzept der Institution integriert wird. Im Konzept SOLLTEN alle technischen und organisatorischen Vorgaben für die eingesetzten kryptografischen Produkte beschrieben werden. Auch SOLLTEN alle relevanten Anwendungen, IT-Systeme und Kommunikationsverbindungen aufgeführt sein. Das erstellte Kryptokonzept SOLLTE regelmäßig aktualisiert werden.

CON.1.A11 Sichere Konfiguration der Kryptomodule [IT-Betrieb] (CI)

Kryptomodule SOLLTEN sicher installiert und konfiguriert werden. Es SOLLTEN alle voreingestellten Schlüssel geändert werden. Anschließend SOLLTE getestet werden, ob die Kryptomodule korrekt funktionieren und vom Benutzer auch bedient werden können.

Weiterhin SOLLTEN die Anforderungen an die Einsatzumgebung festgelegt werden. Wenn ein IT-System geändert wird, SOLLTE getestet werden, ob die eingesetzten kryptografischen Verfahren noch greifen. Die Konfiguration der Kryptomodule SOLLTE dokumentiert und regelmäßig überprüft werden.

CON.1.A12 Sichere Rollenteilung beim Einsatz von Kryptomodulen [IT-Betrieb] (CI)

Bei der Konfiguration eines Kryptomoduls SOLLTEN Benutzerrollen festgelegt werden. Es SOLLTE mit Zugriffskontroll- und Authentisierungsmechanismen verifiziert werden, ob ein Mitarbeiter den gewünschten Dienst auch tatsächlich benutzen darf. Das Kryptomodul SOLLTE so konfiguriert sein, dass bei jedem Rollenwechsel oder bei Inaktivität nach einer bestimmten Zeitdauer die Authentisierungsinformationen erneut eingegeben werden müssen.

CON.1.A13 Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen (CI)

Das Zusammenwirken von Betriebssystem und Kryptomodulen SOLLTE gewährleisten, dass

- die installierten Kryptomodule nicht unbemerkt abgeschaltet oder umgangen werden können,
- die angewendeten oder gespeicherten Schlüssel nicht kompromittiert werden können,
- die zu schützenden Daten nur mit Wissen und unter Kontrolle des Benutzers auch unverschlüsselt auf Datenträgern abgespeichert werden bzw. das informationsverarbeitende System verlassen können und
- Manipulationsversuche am Kryptomodul erkannt werden.

CON.1.A14 Schulung von Benutzern und Administratoren [Vorgesetzte, Leiter IT, Fachverantwortliche] (CIA)

Es SOLLTEN Schulungen durchgeführt werden, in denen Benutzern und Administratoren der Umgang mit den von ihnen zu bedienenden Kryptomodulen vermittelt wird. Den Benutzern SOLLTEN genau erläutert werden, was die spezifischen Sicherheitseinstellungen von Kryptomodulen bedeuten und warum sie wichtig sind. Außerdem SOLLTEN sie auf die Gefahren hingewiesen werden, wenn diese Sicherheitseinstellungen aus Bequemlichkeit umgangen oder deaktiviert werden. Die Schulungsinhalte SOLLTEN immer entsprechend der jeweiligen Einsatzszenarien angepasst werden.

Administratoren SOLLTEN zudem lernen, wie sie mit Hilfsmitteln zur Untersuchung kryptografischer Einstellungen umgehen müssen. Auch SOLLTEN sie einen Überblick über kryptografische Grundbegriffe erhalten.

CON.1.A15 Reaktion auf praktische Schwächung eines Kryptoverfahrens (CI)

Es SOLLTE ein Prozess etabliert werden, der im Falle eines geschwächten kryptografischen Verfahrens herangezogen werden kann, um die Informationssicherheit der Institution zu gewährleisten. Dabei SOLLTE sichergestellt werden, dass das geschwächte kryptografische Verfahren abgesichert werden kann oder durch eine geeignete Alternative abgelöst wird.

CON.1.A16 Physische Absicherung von Kryptomodulen [Leiter IT] (CI)

Es SOLLTE verhindert werden, dass unautorisiert physisch auf Modulinhalte des Kryptomoduls zugegriffen wird. Hard- und Softwareprodukte, die als Kryptomodule eingesetzt werden, SOLLTEN einen Selbsttest durchführen können.

CON.1.A17 Abstrahlsicherheit [Leiter IT] (C)

Es SOLLTE untersucht werden, ob zusätzliche Maßnahmen hinsichtlich der Abstrahlsicherheit notwendig sind. Dies SOLLTE insbesondere gemacht werden, wenn staatliche Verschlusssachen (VS) der Geheimhaltungsgrade VS-VERTRAULICH und höher verarbeitet werden.

CON.1.A18 Kryptografische Ersatzmodule [Leiter IT] (CIA)

Es SOLLTEN Ersatzkryptomodule vorrätig gehalten werden.

4 Weiterführende Informationen

4.1 Literatur

- [27001A10] ISO/IEC 27001:2013 - Annex A.10 Cryptography
  Information technology - Security techniques - Information security management systems - Requirements, insbesondere Annex A, A.10 Cryptography, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [BSILEK] Leitfaden Erstellung von Kryptokonzepten
  Bundesamt für Sicherheit in der Informationstechnik (BSI), 07.2008
  https://www.bsi.bund.de/DE/
  Themen/Sicherheitsberatung/Arbeitshilfen/Kryptokonzept/Kryptokonzept_node.html

- [BSIMKK] Musterkryptokonzept
  BSI, 05.2010
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/
  Sicherheitsberatung/Krypto/2010-04-28_Musterkryptokonzept_V12_pdf.pdf

- [ISFTS2] The Standard of Good Practice - Area TS2 Cryptography
  Information Security Forum (ISF), insbesondere Area TS2 Cryptography, 06.2016

- [NIST800175B] NIST Special Publication 800-175B
  Guidelines for Using Cryptographic Standards in the Federal Goverment, 03.2013
  https://csrc.nist.gov/publications/drafts/800-175/sp800-175b_draft.pdf

- [TR02102] Kryptographische Verfahren- Empfehlungen und Schlüssellängen
  BSI, (zuletzt abgerufen am 27.09.2017)
  https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Kryptokonzept" von Bedeutung.

G 0.13 Abfangen kompromittierender Strahlung

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.37 Abstreiten von Handlungen

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.43 Einspielen von Nachrichten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.13	G 0.14	G 0.15	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.29	G 0.30	G 0.31	G 0.32	G 0.37	G 0.40	G 0.43	G 0.45	G 0.46
CON.1.A1		x	x	x				x						x				x		x		
CON.1.A2		x	x												x						x	x
CON.1.A3		x	x																			x
CON.1.A4		x	x	x	x			x							x							x
CON.1.A5		x	x		x	x		x							x							
CON.1.A6				x																		
CON.1.A7				x	x							x				x						
CON.1.A8				x										x								
CON.1.A9		x	x	x				x	x				x	x	x			x				x
CON.1.A10				x																		
CON.1.A11		x	x	x	x	x	x	x														
CON.1.A12								x						x	x	x	x					x
CON.1.A13					x	x	x	x														
CON.1.A14					x											x						
CON.1.A15				x										x								
CON.1.A16							x	x			x				x							
CON.1.A17	x	x	x																			
CON.1.A18										x	x	x							x			

CON: Konzeption und Vorgehensweise

CON.2 Datenschutz

1 Beschreibung

1.1 Einleitung

Aufgabe des Datenschutzes ist es, Personen davor zu schützen, dass diese durch den Umgang mit personenbezogenen Daten auf der Seite von Institutionen an der Ausübung von Grundrechten beeinträchtigt werden. Die Verfassung der Bundesrepublik Deutschland gewährleistet das Recht der Bürgerinnen und Bürger, grundsätzlich selbst über die Verwendung ihrer personenbezogenen Daten zu bestimmen. Die Datenschutzgesetze des Bundes und der Bundesländer nehmen darauf Bezug , wenn sie den Schutz des Rechts auf informationelle Selbstbestimmung hervorheben. Die EU-Grundrechte-Charta formuliert in Artikel 8 unmittelbar das Recht auf den Schutz personenbezogener Daten (Absatz 1), hebt die Notwendigkeit einer Rechtsgrundlage zur Datenverarbeitung hervor (Absatz 2) und schreibt die Überwachung der Einhaltung von Datenschutzvorschriften durch eine unabhängige Stelle vor (Absatz 3). Die Datenschutz-Grundverordnung [DSGVO] führt diese Anforderungen der Grundrechte-Charta näher aus. Von herausragender Bedeutung ist dabei der Artikel 5 DSGVO, der die Grundsätze versammelt, die teilweise als *Schutzziele* ausgewiesen sind. Das Standard-Datenschutz-Modell (SDM) bietet eine Methode, um diese geforderte Umsetzung von Datenschutzvorschriften, auf der Grundlage von sieben Schutzzielen bzw. Gewährleistungszielen, systematisch überwachen zu können.

1.2 Zielsetzung

Ziel des Bausteins ist es, die Verbindung der Anforderungen des Standard-Datenschutzmodells zum IT-Grundschutz darzustellen.

1.3 Abgrenzung

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat mit dem Standard-Datenschutzmodell ein Konzept entwickelt, dass die in den deutschen und europäischen Rechtsvorschriften genannten technischen und organisatorischen Maßnahmen auf der Basis von Gewährleistungszielen systematisiert. Damit dient das Modell einerseits den für die Verarbeitung verantwortlichen Stellen, erforderliche Maßnahmen systematisch zu planen und umzusetzen und fördert somit die datenschutzgerechte Ausgestaltung und Organisation von informationstechnischen Verfahren und Applikationen. Andererseits bietet das Modell den Datenschutzbehörden eine Möglichkeit, mit einer einheitlichen Systematik zu einem transparenten, nachvollziehbaren, belastbaren Gesamturteil über ein Verfahren und dessen Komponenten zu gelangen. Das SDM ist als Methode geeignet, die Wirksamkeit der technischen und organisatorischen Maßnahmen einer Verarbeitung auf der Grundlage und nach den Kriterien der DSGVO regelmäßig zu überprüfen, zu bewerten und zu evaluieren.

Das SDM nimmt bei der Auswahl geeigneter technischer und organisatorischer Maßnahmen die Perspektive des Betroffenen und dessen Grundrechtsausübung ein und unterscheidet sich daher grundlegend von der Sicht des IT-Grundschutzes. IT-Grundschutz hat vorrangig die Informations-

sicherheit im Blickfeld und soll die Daten verarbeitende Institution schützen. Für die Auswahl von Maßnahmen nach dem SDM ist hingegen die Beeinträchtigung maßgeblich, die ein Betroffener durch die Datenverarbeitung der Institution hinnehmen muss.

Vor diesem Hintergrund ist zwischen der Auswahl von Maßnahmen zur Gewährleistung der Informationssicherheit für Institutionen durch verantwortliche Stellen und der von Maßnahmen zur Gewährleistung der Betroffenenrechte zu unterscheiden. Die IT-Grundschutz-Methodik dient vorrangig der Informationssicherheit, das Standard-Datenschutzmodell dient der Umsetzung von Betroffenenrechten.

Das Standard-Datenschutz-Modell hat daher die folgenden Ansprüche:

- Es überführt datenschutzrechtliche Anforderungen in einen Katalog von Gewährleistungszielen.
- Es gliedert die betrachteten Verfahren in die Komponenten Daten, IT-Systeme und Prozesse.
- Es berücksichtigt die Einordnung von Daten in die drei Schutzbedarfsabstufungen normal, hoch und sehr hoch und ergänzt diese um entsprechende Betrachtungen auf der Ebene auch von Prozessen und IT-Systemen.
- Es bietet einen hieraus systematisch abgeleiteten Katalog mit standardisierten Schutzmaßnahmen.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Datenschutz von besonderer Bedeutung:

2.1 Missachtung von Datenschutz-Gesetzen oder Nutzung eines unvollständigen Risikomodells

Nach der EU-Datenschutz-Grundverordnung ist die Verarbeitung personenbezogener Daten grundsätzlich verboten und bedarf einer Rechtsgrundlage. Die Erhebung, Nutzung und Übermittlung personenbezogener Daten ist nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder wenn ein Betroffener eingewilligt hat (vergleiche. Artikel 6 [DSGVO]).

Aus der Sicht des Datenschutzes ist die Institution, die personenbezogene Daten erhebt, nutzt, übermittelt oder empfängt (zusammengefasst: „verarbeitet“) grundsätzlich ein Risiko für Personen. An diesem Risiko ändert sich nichts, wenn die Datenverarbeitung einer Institution rechtskonform ausgestaltet ist.

Ein demgegenüber noch einmal erhöhtes Risiko besteht für Personen dann, wenn eine Institution eine Datenverarbeitung nicht hinreichend zweckbestimmt oder Zweck überdehnend oder gänzlich zweckungebunden oder intransparent oder ohne integritätssichernde Maßnahmen und ohne hinreichende Optionen für Eingriffsmöglichkeiten durch Betroffene durchführt.

Ein in der Praxis besonders häufiges Risiko für Betroffene stellen Zugriffe durch möglicherweise befugte Dritte dar. Dabei kann es sich typischerweise um ausländische Konzernmütter, Sicherheitsbehörden, Banken und Versicherungen, öffentliche Leistungsverwaltungen, IT-Hersteller und IT-Dienstleister (beispielsweise durch übernommene Patienten- und Klienten-Verzeichnisse) oder Forschungsinstitutionen handeln. Oftmals wird in diesen Kontexten die Ordnungsmäßigkeit eines Zugriffs nicht geprüft, beispielsweise weil eine langjährig eingefahrene Praxis fortgesetzt wird oder weil nachrangige Mitarbeiter das für sie persönliche Risiko scheuen, das in einem Thematisieren des Vorliegens einer hinreichenden Rechtsgrundlage liegen kann. Ferner werden aus (teilweise) negativen Prüfergebnissen durch eine Rechtsabteilung oder einen Datenschutzbeauftragten dann oftmals seitens der Verantwortlichen keine Konsequenzen gezogen.

Ein weiteres Risiko sowohl für Personen als auch für verantwortliche Institutionen besteht dadurch, wenn für rechtmäßig erfolgende Zugriffe durch Dritte keine Standard-Prozesse für einen (zumeist nur bedingten) Zugriff auf IT-Dienste oder die Übermittlung von Datenbeständen vorgesehen sind oder wenn keine Nachweise über die Ordnungsmäßigkeit der Durchführung, in Form von Protokollen und Dokumentationen, erbracht werden können.

Eine große Gefahr für Personen ist ferner eine mangelhafte Datensicherheit. Erwägungsgrund 75 der DS-GVO beschreibt die mit der Verarbeitung personenbezogener Daten einhergehenden Risiken und damit die Gefährdungslage durch unbefugten Zugriff wie folgt:

„Die Risiken für die Rechte und Freiheiten natürlicher Personen - mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere - können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.“

2.2 Festlegung eines zu niedrigen Schutzbedarfs

Eine weitere Gefahr für Personen ist die Festsetzung eines unzutreffenden Schutzbedarfs. Ein falsch angesetzter Schutzbedarf würde dazu führen, dass wesentliche Anforderungen an eine datenschutzrechtliche Gestaltung der Funktionen eines Verfahrens und des Betriebs spezifischer Datenschutz-Schutzmaßnahmen nicht beachtet werden. Der Schutzbedarf, der typischerweise durch die Institution selber festgelegt wird, die verantwortlich personenbezogene Daten verarbeitet, kann aus Sicht von Personen aus verschiedenen Gründen falsch oder zu niedrig angesetzt sein:

- Die Institution hat den gegenüber der Informationssicherheit erweiterten Schutzzielekatalog des Datenschutzes nicht berücksichtigt.
- Die Institution hat bei der Schutzbedarfsermittlung nicht zwischen den Risiken für die Umsetzung der Grundrechte der Betroffenen und den Risiken für die Institution unterschieden.
- Die Institution hat zwar die beiden Schutzinteressen unterschieden, aber die Funktionen des Verfahrens und der Schutzmaßnahmen zu Gunsten der Institution bzw. zu Ungunsten betroffener Personen gestaltet.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Datenschutz aufgeführt. Grundsätzlich ist der Datenschutzbeauftragte zuständig dafür, die Einhaltung der Anforderungen der DSGVO zu überwachen (zu Details und Einschränkungen siehe Art. 39 DSGVO). Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	Datenschutzbeauftragter
Weitere Verantwortliche	-

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

CON.2.A1 Umsetzung Standard-Datenschutzmodell

Das Standard-Datenschutzmodell ist das Werkzeug, um personenbezogene Verfahren nicht nur sicher, sondern auch datenschutzgerecht einzurichten und zu betreiben. Es MUSS deshalb geprüft werden, ob das SDM angewendet wird. Eine etwaige Nichtberücksichtigung des vollständigen Schutzziele-Katalogs und eine Nichtanwendung der SDM-Methodik sowie der Referenzmaßnahmen MÜSSEN begründet werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Datenschutz. Sie SOLLTEN grundsätzlich umgesetzt werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

4 Weiterführende Informationen

4.1 Literatur

- [DSGVO] EU-Datenschutz-Grundverordnung
  „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)“, 04.2016
  http://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32016R0679

- [SDM] Standard-Datenschutzmodell (SDM)
  DSB-Konferenz: SDM-Handbuch (V1.0, Deutsch / Englisch), 2016
  https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Datenschutz" von Bedeutung.

G 0.18 Fehlplanung oder fehlende Anpassung

Elementare Gefährdungen Anforderungen	G 0.18
CON.2.A1	x

CON: Konzeption und Vorgehensweise

CON.3 Datensicherungskonzept

1 Beschreibung

1.1 Einleitung

Unternehmen und Behörden speichern immer mehr Daten und sind gleichzeitig immer stärker auf sie angewiesen. Gehen Daten dann verloren, z. B. durch defekte Hardware oder Malware, können gravierende Schäden entstehen. Durch regelmäßige Datensicherungen lassen sich solche Auswirkungen jedoch minimieren: Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen.

1.2 Zielsetzung

Dieser Baustein zeigt auf, wie Institutionen ein Datensicherungskonzept erstellen können und welche Anforderungen dabei zu beachten sind.

1.3 Abgrenzung

Der Baustein beschreibt die grundsätzlichen Anforderungen, die zu einem angemessenen Datensicherungskonzept beitragen. Nicht behandelt werden Anforderungen an die Aufbewahrung und Erhaltung von elektronischen Dokumenten für die Langzeitspeicherung. Diese finden sich im Baustein OPS.1.2.2 *Archivierung*. Dieser Baustein beinhaltet keine system- oder anwendungsspezifischen Anforderungen zur Protokollierung, diese sind in den jeweiligen Bausteinen des IT-Grundschutz-Kompendiums zu finden, wie beispielsweise SYS.1.1. Allgemeiner Server, APP.3.2 Webserver oder NET.3.2 Firewall.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Datensicherung von besonderer Bedeutung:

2.1 Fehlende Datensicherung

Institutionen sind stärker denn je auf ihre IT-Systeme und die darin gespeicherten Daten angewiesen. Wenn Daten verloren gehen, z. B. durch Malware, technische Fehlfunktionen, einen Brand oder wenn Mitarbeiter Daten absichtlich oder unabsichtlich löschen und es keine Datensicherung gibt, ist das mitunter ein existenzbedrohender Schaden für die Institution, z. B. wenn alle Kundendaten verloren sind.

2.2 Fehlende Wiederherstellungstests

Eine Institution sichert regelmäßig ihre wichtigen Daten, darunter vor allem ihre Kundendaten. Wenn jedoch nicht regelmäßig getestet wird, ob sich die Daten wieder einspielen lassen, können die gesicherten Daten im Falle einer notwendigen Wiederherstellung nicht nutzbar sind. Im Fall der Kundendaten könnte dies für die Institution erhebliche Schäden bedeuten bis hin zur Einstellung des Vertriebs.

2.3 Ungeeignete Aufbewahrung der Backup-Datenträger

Auf Backup-Datenträgern befinden sich zahlreiche schützenswerte Informationen der Institution. Sind die Datenträger an einem unsicheren Ort aufbewahrt, kann ein Angreifer (z. B. ein Innentäter), eventuell darauf zugreifen und schützenswerte Informationen stehlen oder manipulieren. Ebenso können Backup-Datenträger durch ungünstige Lagerung oder klimatische Raumbedingungen unbrauchbar werden und dann, wenn sie benötigt werden, nicht mehr verfügbar sein.

2.4 Fehlende oder unzureichende Dokumentation

Werden Datensicherungsmaßnahmen nicht oder nur mangelhaft dokumentiert, kann die Wiederherstellung länger dauern als geplant. Dadurch können sich wichtige Prozesse verzögern, z. B. in der Produktion. Auch ist es möglich, dass sich eine Datensicherung gar nicht mehr einspielen lässt und die Daten damit verloren sind.

2.5 Missachtung gesetzlicher Vorschriften

Wenn bei der Datensicherung gesetzliche Vorgaben, z. B. Datenschutzgesetze, nicht beachtet werden, können gegen die Institution Bußgelder verhängt oder Schadenersatzansprüche geltend gemacht werden.

2.6 Unsichere Cloud-Anbieter

Lagern Institutionen ihre Datensicherung zu einem Cloud-Anbieter aus, könnte auch ein Angreifer auf die Backup-Daten zugreifen oder das Backup kann nicht schnell genug wieder eingespielt werden. In der Folge sind schützenswerte Daten abgeflossen oder Datensicherungen im Notfall nicht in der benötigen Zeit verfügbar.

2.7 Ungenügende Speicherkapazitäten

Die Menge an verarbeiteten und folglich auch gespeicherten Daten nimmt stetig zu. Verfügen die Backup-Medien nicht über genügend Speicher, werden aktuellere Daten eventuell nicht mehr gesichert oder die eingesetzte Backup-Software überschreibt automatisch alte und eventuell noch benötigte Datensicherungen. Werden die Verantwortlichen hierüber nicht informiert, da z. B. das Monitoring unzureichend ist, gehen Daten eventuell ganz verloren oder es sind im Notfall nur die falschen Versionen verfügbar.

2.8 Unzureichendes Datensicherungskonzept

Wird für Datensicherungsmaßnahmen kein angemessenes Datensicherungskonzepts erstellt und befolgt, können gesicherte Daten in Bedarfsfall nicht wiederhergestellt werden. Bei den gesicherten Daten handelt es sich meist um schützenswerte Informationen, so dass das Backup verschlüsselt wird. Ist bei einem Datenverlust auch der Schlüssel zum Entschlüsseln des Backups betroffen, weil nicht bedacht wurde, diesen getrennt vorzuhalten, kann eine Wiederherstellung nicht möglich sein.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Datensicherung aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt.

Bausteinverantwortlicher	Informationssicherheitsbeauftragter (ISB)
Weitere Verantwortliche	Fachverantwortliche, IT-Betrieb, Leiter IT

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

CON.3.A1 Erhebung der Einflussfaktoren der Datensicherung [IT-Betrieb, Fachverantwortliche]

Für jedes IT-System und eventuell für einzelne besonders wichtige IT-Anwendungen MÜSSEN die relevanten Einflussfaktoren ermittelt werden, wie z. B. Änderungsvolumen, Änderungszeitpunkte, Verfügbarkeitsanforderungen, Integritätsbedarf. Dazu SOLLTEN die Administratoren und die Verantwortlichen der einzelnen IT-Anwendungen befragt werden. Die Ergebnisse MÜSSEN nachvollziehbar und geeignet festgehalten werden. Neue Anforderungen MÜSSEN zeitnah in einem aktualisierten Datensicherungskonzept berücksichtigt werden.

CON.3.A2 Festlegung der Verfahrensweise für die Datensicherung [IT-Betrieb, Fachverantwortliche]

Für jedes IT-System und für jede Datenart MUSS ein Verfahren festgelegt werden, wie die Daten zu sichern sind. Dazu MÜSSEN Art, Häufigkeit und Zeitpunkte der Datensicherungen bestimmt werden. Weiterhin MÜSSEN die Verantwortlichkeiten für die Datensicherungen festgelegt werden. Auch MUSS definiert sein, welche Speichermedien benutzt und wie die Transport- und Aufbewahrungsmodalitäten auszusehen haben.

CON.3.A3 Ermittlung von rechtlichen Einflussfaktoren auf die Datensicherung

Die rechtlichen Anforderungen an die Datensicherung MÜSSEN ermittelt und in das Minimal- bzw. in das Datensicherungskonzept einfließen.

CON.3.A4 Erstellung eines Minimaldatensicherungskonzeptes

Es MUSS ein Minimaldatensicherungskonzept erstellt werden, dass festgelegt, welche Anforderungen für die Datensicherung mindestens einzuhalten sind. Dazu zählen kurze Beschreibungen, wie die Datensicherung erstellt und wiederhergestellt werden kann, welche Parameter gewählt wurden und welche Hard- und Software eingesetzt wird.

CON.3.A5 Regelmäßige Datensicherung [IT-Betrieb]

Es MÜSSEN regelmäßige Datensicherungen durchgeführt werden. Dabei MÜSSEN mindestens die Daten regelmäßig gesichert werden, die nicht aus anderen Informationen ableitbar sind. Die erstellten Datensicherungen MÜSSEN geeignet vor dem Zugriff Dritter geschützt werden. Es MUSS regelmäßig getestet werden, ob die Datensicherung auch wie gewünscht funktioniert, vor allem, ob gesicherte Daten problemlos zurückgespielt werden können

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Datensicherungskonzept. Sie SOLLTEN grundsätzlich umgesetzt werden.

CON.3.A6 Entwicklung eines Datensicherungskonzepts [Leiter IT, Fachverantwortliche]

Es SOLLTE ein Datensicherungskonzept erstellt werden. Dieses SOLLTE mit allen Verantwortlichen abgestimmt werden. Darin SOLLTEN sämtliche zu berücksichtigende IT-Systeme aufgeführt werden. Die Mitarbeiter SOLLTEN über den sie betreffenden Teil des Datensicherungskonzepts unterrichtet werden. Es SOLLTE regelmäßig kontrolliert werden, ob das Datensicherungskonzept korrekt umgesetzt wird.

CON.3.A7 Beschaffung eines geeigneten Datensicherungssystems [Leiter IT, IT-Betrieb]

Bevor ein Datensicherungssystem beschafft wird, SOLLTE eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Die angeschafften Datensicherungssysteme SOLLTEN die Anforderungen des Sicherheits- und des Datensicherungskonzepts erfüllen.

CON.3.A8 Funktionstests und Überprüfung der Wiederherstellbarkeit [IT-Betrieb]

Es SOLLTE regelmäßig getestet werden, ob die Datensicherung auch wie gewünscht funktioniert und vor allem, ob gesicherte Daten problemlos und in angemessener Zeit zurückgespielt werden können.

CON.3.A9 Voraussetzungen für die Online-Datensicherung [Leiter IT, IT-Betrieb]

Wenn für die Datensicherung ein Online-Speicher genutzt werden soll, SOLLTEN mindestens folgende Punkte geregelt werden:

- Gestaltung des Vertrages,
- Ort der Datenspeicherung,
- Vereinbarungen zur Dienstgüte (SLA),
- geeignete Authentisierungsmethoden,
- Verschlüsselung der Daten und
- Verschlüsselung auf dem Transportweg.

CON.3.A10 Verpflichtung der Mitarbeiter zur Datensicherung

Alle Mitarbeiter SOLLTEN über die Regelungen zur Datensicherung informiert sein. Auch SOLLTEN sie darüber informiert werden, welche Aufgaben sie bei der Erstellung von Datensicherungen haben und zu ihrer Durchführung verpflichtet werden.

CON.3.A11 Sicherungskopie der eingesetzten Software [IT-Betrieb]

Von eingesetzten Softwareprogrammen SOLLTEN Sicherungskopien angefertigt werden, sofern das rechtlich erlaubt und technisch möglich ist. Dabei SOLLTEN alle notwendigen Pakete und Informationen vorhanden sein, um die Software im Notfall wieder installieren zu können. Auch SOLLTEN die originalen Installationsquellen sowie die Lizenznummern an einem geeigneten Ort sicher aufbewahrt werden.

CON.3.A12 Geeignete Aufbewahrung der Backup-Datenträger [IT-Betrieb]

Die Backup-Datenträger SOLLTEN vor unbefugtem Zugriff geschützt werden. Sie SOLLTEN räumlich von den Quell-Systemen getrennt werden. Der Aufbewahrungsort SOLLTE so klimatisiert sein, dass die Datenträger längerfristig aufbewahrt werden können.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

CON.3.A13 Einsatz kryptografischer Verfahren bei der Datensicherung [IT-Betrieb]

Um die Vertraulichkeit und Integrität der gesicherten Daten zu gewährleisten, SOLLTEN alle Daten verschlüsselt werden. Es SOLLTE sichergestellt werden, dass sich die verschlüsselten Daten auch nach längerer Zeit wieder einspielen lassen. Verwendete kryptografische Schlüssel SOLLTEN mit einer getrennten Datensicherung geschützt werden.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [BKBU] Leitfaden Backup / Recovery / Disaster Recovery
  Bitkom, 2016
  https://www.bitkom.org/noindex/Publikationen/2017/Leitfaden/170125-LF-Backup-Recovery.pdf

- [ISF] The Standard of Good Practice
  Information Security Forum (ISF), 06.2016

- [NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations
  Special Publication 800-53, Revision 4, NIST, 04.2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Datensicherungskonzept" von Bedeutung.

G 0.02 Ungünstige klimatische Bedingungen

G 0.04 Verschmutzung, Staub, Korrosion

G 0.14 Ausspähen von Informationen (Spionage)

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.02	G 0.04	G 0.14	G 0.18	G 0.19	G 0.22	G 0.25	G 0.26	G 0.28	G 0.29	G 0.31	G 0.45	G 0.46
CON.3.A1			x		x		x			x		x	x
CON.3.A2				x									
CON.3.A3			x		x		x			x		x	x
CON.3.A4				x									
CON.3.A5				x		x							
CON.3.A6				x									
CON.3.A7										x			
CON.3.A8							x	x	x				
CON.3.A9				x			x	x			x	x	
CON.3.A10				x								x	x
CON.3.A11										x		x	
CON.3.A12	x	x				x	x					x	
CON.3.A13				x		x						x	

CON: Konzeption und Vorgehensweise

CON.4 Auswahl und Einsatz von Standardsoftware

1 Beschreibung

1.1 Einleitung

Unter Standardsoftware wird Software verstanden, die auf dem Markt angeboten und meistens über den Fachhandel bezogen wird, zum Beispiel über Kataloge oder Onlineportale. Sie zeichnet sich dadurch aus, dass Institutionen sie selbst installieren und mit wenig Aufwand anpassen können.

In diesem Baustein wird dargestellt, wie Institutionen unter Sicherheitsgesichtspunkten mit Standardsoftware umgehen sollten. So müssen Institution einen Anforderungskatalog für Standardsoftware erstellen, ein geeignetes Produkt auswählen, es sicher installieren, die Lizenzen geeignet verwalten und das Produkt auch wieder sicher deinstallieren können.

1.2 Zielsetzung

Der Baustein zeigt systematisch auf, welche Schutzmaßnahmen zu ergreifen sind, damit Standardsoftware auf sichere Art geplant, beschafft, betrieben und ausgesondert werden kann. Übergeordnetes Ziel ist dabei, die mit der Standardsoftware verarbeiteten Informationen zu schützen.

1.3 Abgrenzung

Dieser Baustein befasst sich ausschließlich mit standardisierten Programmen, die so konzipiert sind, dass sie vom Anwender selbstständig ohne Unterstützung durch den Hersteller oder externe Dienstleister eingesetzt und angepasst werden können.

Der vorliegende Baustein geht nicht auf Software-Tests und -Freigaben ein. Anforderungen dazu sind in OPS.1.1.6 *Software-Tests und -Freigaben* aufgeführt. Auch die Softwareentwicklung wird nicht thematisiert. Dazu sollten die Anforderungen des Bausteins CON.4 *Softwareentwicklung* gesondert berücksichtigt werden.

Angaben zur Aussonderung werden vertiefend im Baustein *OPS.1.2.7 Verkauf/Aussonderung von IT* betrachtet. Weiterführende Anforderungen an Cloud-Anwendungen sind in den Bausteinen OPS.2.2 *Cloud-Nutzung* und APP.5.3 *Cloud-Anwendungen aus Client-Sicht* geregelt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich *Standardsoftware* von besonderer Bedeutung:

2.1 Fehlende Anpassung der Standardsoftware an den Bedarf der Institution

Wenn eingekaufte Standardsoftware nicht an die Anforderungen der Institution angepasst wird, kann der interne Betrieb erheblich gestört werden. Formate könnten z. B. nicht mit bereits eingesetzten Programmen kompatibel sein oder neue Produkt könnten einen zu geringen Funktionsumfang haben. Das kann zu Leistungsverlusten, Störungen oder Fehlern innerhalb der Geschäftsprozesse führen.

2.2 Offenlegung schützenswerter Informationen durch fehlerhafte Konfiguration

Ist eine Standardsoftware fehlerhaft konfiguriert, z. B. wenn nicht benötigte Funktionen noch aktiviert sind, können unbeabsichtigt schützenswerte Informationen offengelegt werden. Das kann zu finanziellen Einbußen oder Reputationsschäden führen. Zusätzlich könnte die Institution auch gegen geltendes Recht verstoßen, z. B. wenn personenbezogene Daten offengelegt werden.

2.3 Bezug von Standardsoftware und Updates aus unzuverlässiger Quelle

Werden Standardsoftware oder zugehörige Updates aus unzuverlässigen Quellen bezogen, kann die Integrität und Funktionalität der Software nicht sichergestellt werden. Dies gilt auch für Erweiterungen (*Plug-ins* oder *Add-ons*). Die Installation kompromittierter Software kann dazu führen, dass Schadcode in der Institution verteilt wird und dass die Software nicht wie vorgesehen funktioniert. Darüber hinaus kann die Integrität und Verfügbarkeit von IT-Systemen beeinträchtigt werden.

2.4 Manipulation von Daten durch Benutzer

Die in Standardsoftware verwendeten Daten können auf vielfältige Weise durch Benutzer manipuliert werden, z. B. wenn sie Daten fehlerhaft oder vorsätzlich falsch erfassen, inhaltlich verändern oder einfach löschen. Dadurch sind alle Fachprozesse beeinträchtigt, in deren Rahmen die entsprechende Anwendung eingesetzt wird. Werden die manipulierten Daten nicht erkannt, führt das zur Verarbeitung verfälschter Informationen. Darüber hinaus können Sicherheitslücken entstehen, die Angreifer ausnutzen können.

2.5 Software-Schwachstellen in Standardsoftware

Trotz intensiver Tests werden meist nicht alle Schwachstellen und Fehler in Standardsoftware entdeckt, bevor sie an die Kunden ausgeliefert wird. Werden diese nicht rechtzeitig erkannt, können daraus resultierende Abstürze oder Fehler zu weitreichenden Folgen führen. Darüber hinaus können Vertraulichkeit und Integrität der gespeicherten Daten und die Verfügbarkeit betroffener IT-Systeme beeinträchtigt werden. Durch Software-Schwachstellen bzw. -Fehler kann es außerdem zu schwerwiegenden Sicherheitslücken in Standardsoftware kommen. Diese können unter Umständen von Angreifern ausgenutzt werden, um Schadcode einzuschleusen.

2.6 Einsatz nicht-lizenzierter Standardsoftware

Wird Standardsoftware ohne gültige Software-Lizenz eingesetzt, weil beispielsweise das Lizenzvolumen unbemerkt überschritten wurde, kann das Vertragsstrafen zur Folge haben. Umgekehrt werden möglicherweise zu hohe Lizenzkosten entrichtet, wenn Standardsoftware an Arbeitsplätzen installiert ist, an denen sie nicht benötigt wird.

2.7 Unerlaubtes Ausüben von Rechten in Standardsoftware

Zutritts-, Zugangs- und Zugriffsrecht werden als organisatorische Maßnahmen eingesetzt, um Informationen, Geschäftsprozesse und IT-Systeme vor unbefugtem Zugriff zu schützen. Können unautorisierte Personen Standardsoftware oder bestimmte Funktionen benutzen, kann das die Vertraulichkeit und Integrität der Informationen gefährden, indem diese verändert, gelöscht oder unsachgemäß erstellt werden. Solche Sicherheitslücken entstehen beispielsweise durch fehlerhafte Rechtevergaben. Betroffene Geschäftsprozesse können korrumpiert werden, unbeabsichtigt fehlerhafte Informationen verarbeiten oder schützenswerte Informationen offenlegen.

2.8 Datenverlust durch fehlerhafte Nutzung von Standardsoftware

Durch falsch benutze Standardsoftware können Mitarbeiter Daten versehentlich löschen oder so verändern, dass diese unbrauchbar gemacht werden. Dadurch können ganze Geschäftsprozesse blockiert werden. Auch eine fehlerhafte Benutzung von Funktionen zur Verschlüsselung kann dazu führen, dass die Daten zwar noch vorhanden sind, aber nicht mehr entschlüsselt werden können. In diesem Fall können die Daten nicht mehr oder nur noch mit erhöhtem Aufwand wieder hergestellt werden, was zu einer zusätzlichen finanziellen Belastung der Institution führen kann.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz von *Standardsoftware* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Beschaffungsstelle, Fachabteilung

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

CON.4.A1 Sicherstellen der Integrität von Standardsoftware

Bei der Installation von Standardsoftware MUSS sichergestellt werden, dass es sich dabei um ein originales unverändertes Softwareprogramm handelt. Dazu MUSS es entweder von Originaldatenträgern oder von geprüften identischen Kopien des originalen Installationsprogramms installiert werden. Der Zugriff auf die Installationsroutinen MUSS auf berechtigte Mitarbeiter eingeschränkt werden. Die Originaldatenträger oder das Installationsprogramm MÜSSEN auf Schadsoftware überprüft werden. Von den Installationsdateien SOLLTEN Sicherungskopien angelegt und geprüft werden.

CON.4.A2 Entwicklung der Installationsanweisung für Standardsoftware

Für die ausgewählte Standardsoftware MUSS eine Installationsanweisung erstellt werden. Auch MÜSSEN geeignete Parameter für die Konfiguration sowie organisatorische Rahmenbedingungen für die Installation der Software vorgegeben werden.

CON.4.A3 Sichere Installation und Konfiguration von Standardsoftware

Freigegebene Standardsoftware MUSS so installiert und konfiguriert werden, dass dabei die entsprechenden Installationsanweisungen (siehe CON.4.A2 *Entwicklung der Installationsanweisungen für Standardsoftware*) eingehalten werden. Wird von diesen Anweisungen abgewichen, MUSS das durch den Vorgesetzten genehmigt werden. Alle Installationen MÜSSEN vom IT-Betrieb durchgeführt werden. Dabei MUSS sichergestellt sein, dass lediglich die benötigten Programmfunktionen installiert werden.

Die Software MUSS so konfiguriert werden, dass sie die Sicherheitsrichtlinien der Institution erfüllt. Nicht benötigte Dienste und Funktionen MÜSSEN deinstalliert werden. Falls dies nicht möglich ist, MÜSSEN sie abgeschaltet werden. Bevor und nachdem Standardsoftware installiert wurde, SOLLTEN von allen beteiligten IT-Systemen Datensicherungen durchgeführt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Auswahl und Einsatz von Standardsoftware. Sie SOLLTEN grundsätzlich umgesetzt werden.

CON.4.A4 Festlegung der Verantwortlichkeiten im Bereich Standardsoftware [Fachabteilung]

Für die Einführung einer Standardsoftware SOLLTEN Verantwortliche benannt werden. Dabei SOLLTE mindestens festgelegt werden, wer einen Anforderungskatalog erstellt, das Produkt auswählt, es testet und freigibt und wer letztlich für die Installation verantwortlich ist. Zusätzlich SOLLTE ein Einführungs- und Freigabeprozess definiert werden. Für den Betrieb von Standardsoftware SOLLTEN technische und fachliche Produktverantwortliche benannt werden.

CON.4.A5 Erstellung eines Anforderungskatalogs für Standardsoftware [Fachabteilung]

Vor der Beschaffung einer Standardsoftware SOLLTE ein Anforderungskatalog erstellt werden, der neben funktionalen auch Sicherheitsanforderungen umfasst. Dazu SOLLTEN auch die Programmanforderungen der Fach- und IT-Abteilungen erhoben werden. Der fertige Anforderungskatalog SOLLTE mit allen betroffenen Fachabteilungen abgestimmt werden.

CON.4.A6 Auswahl einer geeigneten Standardsoftware [Fachabteilung, Beschaffungsstelle]

Anhand des Anforderungskatalogs (siehe CON4.1.A5 *Erstellung eines Anforderungskatalogs für Standardsoftware*) SOLLTEN die am Markt erhältlichen Produkte gesichtet und mithilfe einer Bewertungsskala miteinander verglichen werden. Danach SOLLTE untersucht werden, ob die Produkte aus der engeren Wahl die Anforderungen der Institution auch wirklich erfüllen. Gibt es mehrere Produktalternativen, SOLLTEN auch zusätzliche Aufwände berücksichtigt werden, z. B. für Schulungen oder für die Migration. Letztlich SOLLTE die Beschaffungsstelle gemeinsam mit dem Leiter der anfordernden Fachabteilung und des IT-Betriebs anhand der Bewertungen und Testergebnisse ein geeignetes Softwareprodukt auswählen.

CON.4.A7 Überprüfung der Lieferung von Standardsoftware [Fachabteilung]

Es SOLLTE überprüft werden, ob neue Softwareprodukte vollständig und korrekt geliefert wurden. Dabei SOLLTE mindestens kontrolliert werden, ob die Lieferung bestellt wurde, für wen sie bestimmt ist und ob alle notwendigen Komponenten vorhanden sind. Auch reine Download-Software inklusive zugehöriger Lizenzdateien oder -schlüsseln SOLLTE entsprechend geprüft werden. Die Ergebnisse der Überprüfung SOLLTEN dokumentiert werden. Danach SOLLTEN alle gelieferten Produkte und Lizenzinformationen mit eindeutigen Identifizierungsmerkmalen versehen und in ein Bestandsverzeichnis übernommen werden.

CON.4.A8 Lizenzverwaltung und Versionskontrolle von Standardsoftware

Lizenzpflichtige Standardsoftware-Produkte, die auf IT-Systemen der Institution eingesetzt werden, SOLLTEN lizenziert sein. Um das sicherzustellen, SOLLTEN die installierten Programmversionen und die Lizenzen regelmäßig kontrolliert werden. Dafür SOLLTEN entsprechende Listen, Datenbanken oder spezielle Lizenzverwaltungsprogramme verwendet werden. Die Bestandslisten für die Lizenzen SOLLTEN immer auf dem aktuellen Stand sein. Darüber hinaus SOLLTEN die verschiedenen Konfigurationen der installierten Standardsoftware dokumentiert werden.

CON.4.A9 Deinstallation von Standardsoftware

Bei der Deinstallation von Standardsoftware SOLLTEN alle Dateien entfernt werden, die für den Betrieb der Software auf dem IT-System angelegt worden sind. Auch SOLLTEN alle Einträge in Systemdateien, die für das Produkt vorgenommen wurden, gelöscht werden. Um Standardsoftware wieder vollständig deinstallieren zu können, SOLLTEN die während der Installation durchgeführten Systemänderungen entweder manuell oder mit entsprechenden Programmen dokumentiert werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

CON.4.A10 Implementierung zusätzlicher Sicherheitsfunktionen (CIA)

Es SOLLTE geprüft werden, ob sich die Sicherheitsfunktionen der betriebenen Standardsoftware für einen erhöhten Schutzbedarf eignen. Ist das nicht der Fall, SOLLTEN geeignete Funktionen implementiert werden, um den Betrieb abzusichern.

Grundsätzlich SOLLTE ein erhöhter Schutzbedarf jedoch bereits bedacht werden, wenn die Anforderungen definiert werden und das Produkt ausgewählt wird.

CON.4.A11 Nutzung zertifizierter Standardsoftware (CIA)

Bei der Beschaffung von Standardsoftware SOLLTE festgelegt werden, ob eine Zusicherung des Herstellers, Vertreibers oder Anbieters über implementierte Sicherheitsfunktionen als ausreichend vertrauenswürdig anerkannt werden kann. Ist dies nicht der Fall, SOLLTE eine Zertifizierung der Anwendung nach Common Criteria als Entscheidungskriterium in Betracht gezogen werden. Stehen mehrere Produkte zur Auswahl, SOLLTEN Sicherheitszertifikate insbesondere dann berücksichtigt werden, wenn der evaluierte Funktionsumfang die Mindestfunktionalität (weitestgehend) umfasst und die Mechanismenstärke dem Schutzbedarf entspricht. Gibt es auf dem Markt kein geeignetes und zertifiziertes Produkt, SOLLTE die Einsatzumgebung der Standardsoftware entsprechend einem hohen Schutzbedarf abgesichert sein.

CON.4.A12 Einsatz von Verschlüsselung, Checksummen oder digitalen Signaturen (CI)

Wenn Daten mit erhöhtem Schutzbedarf übertragen oder gespeichert werden, SOLLTEN sie vorher verschlüsselt werden. Gibt es in einer Standardsoftware eine integrierte Verschlüsselungsfunktion, SOLLTE geprüft werden, ob diese ausreichend sicher ist. Das SOLLTE besonders bei älteren Produktversionen überprüft werden. Benutzer SOLLTEN im Umgang mit den Verschlüsselungsfunktionen geschult und sensibilisiert werden.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [CC] Common Criteria for Information Technology Security Evaluation (CC)
  erschienen in der Normenreihe ISO 15408: Information technology- Security techniques- Evaluation criteria for IT security, Version 3.1, (zuletzt abgerufen am 28.09.2017)
  www.commoncriteriaportal.org

- [ISF] The Standard of Good Practice
  Information Security Forum (ISF), 06.2016

- [NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations
  Special Publication 800-53, Revision 4, NIST, 04.2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

- [TR02102] Kryptographische Verfahren- Empfehlungen und Schlüssellängen
  BSI, (zuletzt abgerufen am 27.09.2017)
  https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Auswahl und Einsatz von Standardsoftware" von Bedeutung.

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.22 Manipulation von Informationen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.18	G 0.19	G 0.20	G 0.22	G 0.28	G 0.29	G 0.30	G 0.31	G 0.45	G 0.46
CON.4.A1							x			x
CON.4.A2								x		
CON.4.A3	x	x						x		
CON.4.A4							x			
CON.4.A5						x			x	x
CON.4.A6	x									
CON.4.A7			x		x					
CON.4.A8						x				
CON.4.A9		x						x		
CON.4.A10				x					x	x
CON.4.A11	x									
CON.4.A12		x		x			x		x	x

CON: Konzeption und Vorgehensweise

CON.5 Entwicklung und Einsatz von Fachanwendungen

1 Beschreibung

1.1 Einleitung

Als Fachanwendungen werden komplexe Anwendungen bezeichnet, die für individuelle und spezifische fachliche Aufgaben konzipiert sind sowie in der Regel nicht als Standardlösungen gekauft und eingesetzt werden. Stattdessen werden Basislösungen für den individuellen Einsatzzweck von Institutionen angepasst, oder die Anwendungen werden vollständig durch Dritte oder der Institution selbst entwickelt. Zu diesen Fachanwendungen gehören beispielsweise Personalverwaltungssoftware, Verfahren zur Verwaltung von Sozialdaten oder Meldedaten. Eine sorgfältige Planung von Sicherheitsmaßnahmen vor Auswahl und Inbetriebnahme einer Anwendung ist wesentlich für das erreichte Sicherheitsniveau, da Fehler in der Planung wie z. B. fehlende Sicherheitsfunktionen im laufenden Betrieb nicht oder nur mit hohen Zusatzaufwänden ausgeglichen werden können.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, aufzuzeigen, welche grundlegenden Sicherheitsanforderungen bei Planung, Beschaffung, Inbetriebnahme, regulärem Betrieb und Außerbetriebnahme einer Fachanwendung zu berücksichtigen sind.

1.3 Abgrenzung

Der Fokus dieses Bausteins liegt auf organisatorischen und konzeptionellen Aspekten der Informationssicherheit von Fachanwendungen. Auswahl, Konfiguration und sicherer Betrieb von Sicherheitsfunktionen in Anwendungen sind in diesem Baustein nur allgemein und grundlegend beschrieben. Eine konkrete Beschreibung für breit genutzte Standardanwendungen findet sich in den weiteren Bausteinen der Schicht APP *Anwendungen* sowie im Baustein CON.4 *Auswahl und Einsatz von Standardsoftware*.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Fachanwendungen von besonderer Bedeutung:

2.1 Verlust der Vertraulichkeit oder Integrität in Fachanwendungen

Mit Fachanwendungen werden in der Regel vertrauliche Informationen verarbeitet, wie beispielsweise alle Arten von personenbezogenen Daten oder Geschäftsgeheimnisse. Werden diese Daten offengelegt oder ungewollt geändert, können hieraus Vertrags- oder Rechtsverstöße (einschließlich Datenschutzrechtsverstöße) resultieren. Insbesondere bei einem Verlust der Integrität können Rechtsverstöße durch Prozess- oder Verfahrensfehler entstehen. Wenn die Informationen nicht

mehr verfügbar sind, können so Geschäfts- oder Fachaufgaben nicht mehr erfüllt werden. Der Verlust der Vertraulichkeit, Integrität und Verfügbarkeit kann so erhebliche Folgen haben, wie z. B. strafrechtlichen und finanziellen Konsequenzen, oder in Einzelfällen sogar Personenschäden.

2.2 Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten

Wenn die Vergabe von Zutritts- und Zugriffsrechten schlecht geregelt ist, führt das schnell zu gravierenden Sicherheitslücken, z. B. durch Wildwuchs in der Rechtevergabe. Dies führt schnell dazu, dass Benutzer Berechtigungen auf Zuruf erhalten oder umgekehrt nur über unnötig komplizierte Wege an diese kommen. Dadurch können einerseits fehlende Berechtigungen die tägliche Arbeit behindern, andererseits können so Berechtigungen ohne Erfordernis vergeben werden und so ein Sicherheitsrisiko darstellen.

2.3 Unzugängliche vertragliche Regelungen mit einem externen Dienstleister

Aufgrund von unzulänglichen vertraglichen Regelungen mit einem externen Dienstleister, insbesondere bei der Erstellung, Unterstützung der Einführung und Wartung der Anwendung, können vielfältige und auch schwerwiegende Sicherheitsprobleme auftreten. Wenn Aufgaben, Leistungsparameter oder Aufwände ungenügend oder missverständlich beschrieben wurden, kann die Folge sein, dass aus Unkenntnis, aufgrund fehlender Qualifizierung oder wegen fehlender Ressourcen Sicherheitsmaßnahmen nicht umgesetzt werden. Dies kann eine Vielzahl negativer Auswirkungen nach sich ziehen, wie die Nichterfüllung regulatorischer Anforderungen und Pflichten, die fehlende Einhaltung von Auskunftspflichten und Gesetzen bis hin zur fehlenden Übernahme von Verantwortung aufgrund des Verlusts von Kontroll- und Steuerungsmöglichkeiten.

2.4 Software-Konzeptionsfehler

Bei der Planung von Anwendungen, Programmen und Protokollen können sicherheitsrelevante Konzeptionsfehler entstehen. Diese ergeben sich häufig daraus, dass für einen bestimmten Zweck vorgesehene Anwendungsmodule und Protokolle in anderen Einsatzszenarien wiederverwendet werden. Wenn hier andere Sicherheitsvorgaben relevant sind, also beispielsweise für abgeschottete betriebliche Umgebungen vorgesehene Anwendungsmodule und Protokolle ans Internet angebunden werden, kann dies zu massiven Sicherheitslücken führen.

2.5 Software-Schwachstellen

Bei Software-Schwachstellen handelt es sich um Fehler, die ein Sicherheitsrisiko für die mit der Anwendung verarbeiteten Daten darstellen. Diese Sicherheitsrisiken ergeben sich daraus, dass vorgesehene Sicherheitsmechanismen unwirksam sind oder es durch technischen Fortschritt werden, oder wenn dadurch Sicherheitsmechanismen gezielt umgangen werden können. Darüber hinaus können Softwarefehler auch zu mangelhafter Verarbeitungsleistung (Performance-Mängel) oder dem Ausfall der Anwendung führen. Mögliche Folgen eines Ausfalls sind Arbeitsausfall, Umsatzverluste oder Verstöße gegen vertragliche Vereinbarungen oder rechtliche Vorgaben.

2.6 Undokumentierte Funktionen

Viele Anwendungen enthalten häufig für Entwicklungs- oder Supportzwecke durch den Hersteller eingebaute undokumentierte Funktionen. Diese sind meistens den Benutzern nicht bekannt. Undokumentierte Funktionen sind dann problematisch, wenn sie das Umgehen wesentlicher Sicherheitsmechanismen, wie z. B. solcher zum Zugriffsschutz, erlauben. Dies kann die Vertraulichkeit und Integrität der verarbeiteten Daten erheblich beeinträchtigen.

2.7 Fehlende oder unzureichende Sicherheitsmaßnamen in Anwendungen

Sicherheitsmechanismen oder Sicherheitsfunktionen sollen in der Anwendung sicherstellen, dass bei der Verarbeitung von Informationen Vertraulichkeit, Integrität und Verfügbarkeit im benötigten Maße gewährleistet werden können. Häufig steht bei der Entwicklung einer Anwendung aber die fachliche Funktionalität oder der Zeit- und Kostenrahmen im Vordergrund, so dass wichtige Sicherheitsmechanismen zu schwach ausgeprägt sind, sodass sie einfach umgangen werden können, oder sogar ganz fehlen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen an Planung, Auswahl, Beschaffung, Inbetriebnahme, Betrieb und Aussonderung von Fachanwendungen aufgeführt. Grundsätzlich ist der die Anwendung einsetzende Fachbereich für die Erfüllung dieser Anforderungen zuständig. In der Praxis können diese Anforderungen nur erfüllt werden, wenn die IT-Betriebsverantwortlichen (z. B. IT-Leiter) und der Informationssicherheitsbeauftragten (ISB) hinzugezogen bzw. beteiligt werden.

Bausteinverantwortlicher	Fachverantwortliche
Weitere Verantwortliche	Datenschutzbeauftragter, IT-Betrieb, Leiter IT

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

CON.5.A1 Festlegung benötigter Sicherheitsfunktionen der Fachanwendung [IT-Betrieb]

Für die Fachanwendung MÜSSEN die notwendigen Sicherheitsfunkionen bei der fachlichen Auswahl und der Integration in die IT-betrieblichen Infrastrukturen und Betriebsprozesse berücksichtigt werden. Die Auswahl und Umsetzung geeigneter Sicherheitsfunktionen in der Fachanwendung MUSS auf Grundlage der Daten, die in der Anwendung verarbeitet werden, und gegebenenfalls einer ergänzenden Risikoanalyse, erfolgen. Die Sicherheitsfunkionen MÜSSEN geeignet dokumentiert werden.

CON.5.A2 Test und Freigabe von Fachanwendungen [Leiter IT, Datenschutzbeauftragter]

Für einen geordneten Betriebsübergang einer Anwendung sowie bei wesentlichen Änderungen MUSS ein geeignetes Vorgehen bei Test und Freigabe entwickelt werden. Dabei MÜSSEN berücksichtigt werden:

- die fachliche Ebene (Vertreten durch die Fachverantwortlichen),
- die Ebene des IT-Betriebes (Vertreten durch den IT-Leiter),
- die Ebene der Informationssicherheit (Vertreten durch den Informationssicherheitsbeauftragten),
- die Ebene des Datenschutzes (Vertreten durch den Datenschutzbeauftragten) sowie
- je nach Art und Komplexität einer Anwendung weitere Funktionsträger wie z.B. die Personalvertretung.

CON.5.A3 Sichere Installation einer Fachanwendung [IT-Betrieb]

Es MUSS eine Installationsanweisung erstellt werden, die alle benötigten Anwendungsmodule (Bibliotheken), die Installationsreihenfolge und die Konfiguration der Anwendungsmodule beinhaltet. Die Installationsanweisung SOLLTE die notwendigen Aspekte bezüglich der Installationsumgebung berücksichtigen. Die Fachanwendung MUSS gemäß der Installationsanweisung installiert werden.

Bei Änderungen in der Anwendung und funktionalen Updates MUSS die Installationsanweisung aktualisiert werden.

CON.5.A4 Heranführen von Nutzerinnen und Nutzern an die Anwendung

Benutzer und Administratoren MÜSSEN an die korrekte Nutzung und Administration der Anwendung einschließlich der Sicherheitsfunktionen herangeführt werden. Hierzu SOLLTEN Richtlinien und Arbeitsanweisungen zur Nutzung und Administration der Anwendung, Schulungen und Einweisungen, Handbücher und Online-Hilfen sowie eine Benutzerunterstützung durch Schlüsselanwender angeboten werden.

CON.5.A5 Sicherer Betrieb einer Fachanwendung [IT-Betrieb]

Berechtigungen zur Nutzung und Administration einer Fachanwendung MÜSSEN korrekt vergeben und regelmäßig auf Korrektheit hin überprüft werden. Nicht mehr benötigte Berechtigungen MÜSSEN wieder entzogen werden.

Es MUSS sichergestellt werden, dass Protokolldaten regelmäßig ausgewertet und gesetzlich vorgegebene Speicherfristen für Protokolldaten eingehalten werden.

Sicherheitskritische Patches und Updates MÜSSEN durch den Hersteller der Anwendung auf Grundlage geeigneter vertraglicher Vereinbarungen bereitgestellt und zeitnah eingespielt werden. Dabei MUSS sichergestellt werden, dass Patches und Updates zuvor geeignet getestet und freigegeben wurden.

Es MÜSSEN regelmäßig Datensicherungen und Rücksicherungsübungen durchgeführt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Entwicklung und Einsatz von Fachanwendungen. Sie SOLLTEN grundsätzlich umgesetzt werden.

CON.5.A6 Umfassende Dokumentation der Anforderungen an die Anwendung

Die e relevanten Anforderungen an die Anwendung SOLLTEN dokumentiert werden. Diese Dokumentation SOLLTE bei Änderungen an der Anwendung sowie funktionalen Updates fortgeschrieben werden.

CON.5.A7 Erstellung eines Mandantenkonzeptes [Leiter IT]

Es SOLLTE mit einem Mandantenkonzept sichergestellt werden, dass Anwendungen und Daten verschiedener Kunden sauber getrennt betrieben werden. Dieses SOLLTE durch den Betreiber der mandantenfähigen Anwendung erstellt und den nutzenden Institutionen zur Verfügung gestellt werden. Die benötigten Mechanismen zur Mandantentrennung beim Dienstleister SOLLTEN ausreichend umgesetzt sein.

CON.5.A8 Geeignete Steuerung der Anwendungsentwicklung [Leiter IT]

Bei einer Entwicklung einer individuellen Anwendung SOLLTE ein geeignetes Steuerungs- und Projektmanagementmodell verwendet werden. Dabei SOLLTEN insbesondere die benötigten Qualifikationen beim Personal, die Abdeckung aller relevanten Phasen während des Lebenszyklus der Software, ein geeignetes Entwicklungsmodell, Risikomanagement und Qualitätsziele berücksichtigt werden.

CON.5.A9 Außerbetriebnahme von Anwendungen [Leiter IT]

Die Außerbetriebnahme von Anwendungen SOLLTE geplant werden. Es SOLLTE für alle Daten geklärt sein, welche Daten migriert, archiviert oder gelöscht werden. Nicht mehr benötigte Daten SOLLTEN sicher gelöscht werden. Die Außerbetriebnahme von Anwendungen sowie der zugehörigen IT-Systeme und Datenträger SOLLTE nachvollziehbar dokumentiert werden.

CON.5.A10 Notfallvorsorge für Anwendungen [Leiter IT]

Die Fachanwendungen SOLLTEN in die Planung zur Notfallvorsorge aufgenommen werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

CON.5.A11 Geeignete und rechtskonforme Beschaffung

Bei der Beschaffung einer Fachanwendung SOLLTEN die bestehenden rechtlichen und organisatorischen Vorgaben umgesetzt werden. Werden bei der Beschaffung, Entwicklung oder dem Betrieb einer Anwendung Dienstleister einbezogen, SOLLTEN in den Verträgen die relevanten Sicherheitsaspekte berücksichtigt werden.

In der Institution SOLLTEN definierte Prozesse und festgelegte Ansprechpartner existieren, die die Berücksichtigung der jeweiligen Rahmenbedingungen sicherstellen. Es SOLLTE geklärt werden, welche Rolle Zertifizierungen bei der Vergabeentscheidung spielen.

CON.5.A12 Treuhänderische Hinterlegung

Für geschäftskritische Anwendungen SOLLTE geprüft werden, ob es notwendig ist, diese gegen Ausfall des Herstellers der Anwendung abzusichern. Dabei SOLLTE die treuhänderische Hinterlegung von nicht zum Lieferumfang der Anwendung gehörenden Materialien bei einer Escrow-Agentur erwogen werden, wie z. B. dokumentiertem Code, Konstruktionspläne, Schlüssel, Passwörter. In diesem Falle SOLLTEN die Pflichten der Escrow-Agentur bei der Lagerung und Herausgabe (wann darf das Hinterlegungsgut an wen herausgegeben werden?) vertraglich geregelt werden.

CON.5.A13 Entwicklung eines Redundanzkonzeptes für Anwendungen [Leiter IT]

Besteht hinsichtlich der Verfügbarkeit einer Anwendung ein hoher oder sehr hoher Schutzbedarf, so SOLLTE ein Redundanzkonzept erstellt werden. Dieses SOLLTE folgende Aspekte beinhalten:

- Planung eines eingeschränkten IT-Betriebs sowie der Wiederherstellung im Notfall (Notfallvorsorgekonzeption)
- Redundanz auf Anwendungsebene mittels Loadbalancing oder Anwendungsclustern / Cloud-Services
- Möglichkeiten zum Schwenken der Anwendungen auf andere Systeme

Ergänzend SOLLTE sichergestellt werden, dass das Redundanzkonzept auch die für den Anwendungsbetrieb benötigten Gebäude und Räume, Systeme und Kommunikationsverbindungen einbezieht. Das Redundanzkonzept SOLLTE mit dem Notfallkonzept abgestimmt sein. Die Maßnahmen aus dem Redundanzkonzept SOLLTEN regelmäßig getestet und geübt werden.

4 Weiterführende Informationen

4.1 Literatur

- [12207] ISO/IEC 12207
  Systems and software engineering - Software life cycle processes, ISO, 02.2008
  https://www.iso.org/standard/43447.html

- [15408] Common Criteria for Information Technology Security Evaluation (ISO 15408)
  Insbesondere Teil 2 "Security functional requirements", Common Criteria, 09.2012
  https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf

- [27001A14] ISO/IEC 27001: 2013 - Annex A.14 System Acquisition
  Information technology - Security technigues - Information security management systems - Requirements, insbesonder Annex A, A.14 Sytem Acquisition, development and maintenance, ISO, 04.2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [ISFBA] The Standard of Good Practice - Area BA - Business Application Management
  insbesonder Area BA - Business Application Management, Information Security Forum (ISF), 06.2016

- [NIST80053F145] NIST Special Publication 800-53 - REVISION 4 - APPENDIX PAGE F-145 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, insbesondere APPENDIX F-PS PAGE F-145, FAMILY: SYSTEM AND SERVICES ACQUISITION, FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION and FAMILY: SYSTEM AND INFORMATION INTEGRITY, NIST, 2015
  http://nvlpubs.nist.gov/GGTSPU-fw1.bsi.bund.de-8690-598708-um44WKCwoM5r2JP4-LOD/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Entwicklung und Einsatz von Fachanwendungen" von Bedeutung.

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.38 Missbrauch personenbezogener Daten

G 0.39 Schadprogramme

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.18	G 0.19	G 0.22	G 0.23	G 0.26	G 0.28	G 0.29	G 0.30	G 0.31	G 0.38	G 0.39	G 0.45	G 0.46
CON.5.A1	x	x		x						x	x	x	x
CON.5.A2	x		x	x	x	x						x	
CON.5.A3				x									
CON.5.A4		x						x	x			x	x
CON.5.A5		x		x				x	x	x	x	x	x
CON.5.A6													
CON.5.A7	x	x					x						
CON.5.A8	x			x	x	x							x
CON.5.A9		x								x		x	
CON.5.A10												x	
CON.5.A11				x	x		x	x	x		x		
CON.5.A12			x									x	
CON.5.A13												x	

CON: Konzeption und Vorgehensweise

CON.6 Löschen und Vernichten

1 Beschreibung

1.1 Einleitung

Damit Informationen nicht in falsche Hände geraten, ist eine geregelte Vorgehensweise erforderlich, um Daten und Datenträger vollständig und zuverlässig zu löschen oder zu vernichten. Schutzbedürftige Informationen, die auf analogen und digitalen Datenträgern gespeichert sind, müssen hierbei betrachtet werden.

Wenn nicht oder nur unzureichend gelöschte Datenträger weitergegeben, verkauft oder ausgesondert werden, können dadurch unbeabsichtigt schützenswerte Informationen weitergegeben werden und erhebliche Schäden entstehen. Daher muss jede Institution eine Vorgehensweise zum sicheren Löschen und Vernichten haben.

1.2 Zielsetzung

In diesem Baustein wird beschrieben, wie Informationen in Institutionen sicher gelöscht und vernichtet und wie ein entsprechendes Konzept hierfür erstellt werden sollte.

1.3 Abgrenzung

Der Baustein beinhaltet nur die allgemeinen prozessualen, technischen und organisatorischen Anforderungen an das Löschen und Vernichten. Einzelne Bausteine der Schichten CON (Konzepte und Vorgehensweisen), Sicherheitsmanagement (ISMS), ORP (Organisation und Personal), OPS (Betrieb), DER (Detektion und Reaktion), IND (Industrielle IT), APP (Anwendungen), SYS (IT-Systeme), NET (Netze und Kommunikation) und INF (Infrastruktur) können ergänzende und spezifischere Anforderungen an das Löschen und Vernichten definieren. Vor allem die Bausteine OPS.1.1.6 *Datensicherung*, OPS 1.2.2 *Archivierung,* OPS.1.2.3 *Informations- und Datenträgeraustausch und* OPS.1.2.7 *Verkauf/Aussonderung von IT* sind zusätzlich zu berücksichtigen, da diese Themen direkt mit dem Löschen und Vernichten verbunden sind.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Löschen und Vernichten von besonderer Bedeutung:

2.1 Fehlende oder unzureichend dokumentierte Regelungen beim Löschen und Vernichten

Wenn es keine dokumentierten Prozesse und Verfahrensweisen für das Löschen und Vernichten von Informationen und Datenträgern gibt oder werden diese nicht korrekt angewendet, können vertrauliche Informationen nicht wirklich sicher vernichtet werden und so in falsche Hände geraten. Diese Gefahr ist bei auszusondernden Datenträgern und IT-Systemen besonders hoch, da durch

unzureichende Regelungen eventuell Informationen auf ihnen verbleiben. Diese Daten könnten durch unbefugte Dritte ausgelesen oder entwendet werden. Wenn darunter existenzielle Informationen sind, wäre so die gesamte Institution gefährdet.

2.2 Vertraulichkeitsverlust durch Restinformationen auf Datenträgern

Bei elektronischer Datenübermittlung oder Datenträgerweitergabe passiert es immer wieder, dass auch Informationen weitergegeben werden, die die Institution nicht verlassen sollten.

Bei den meisten Dateisystemen werden Dateien, die der Benutzer löscht, nicht wirklich vernichtet. Es werden lediglich die Verweise auf die Datei aus den Verwaltungsinformationen des Dateisystems gelöscht und die zu der Datei gehörenden Blöcke als frei markiert. Der tatsächliche Inhalt der Blöcke auf dem Datenträger bleibt jedoch erhalten und kann mit entsprechenden Werkzeugen rekonstruiert werden. Dadurch können sich Angreifer Zugriff auf die Datei verschaffen, z. B. wenn solche Datenträger an Dritte weitergegeben oder ungeeignet entsorgt werden. So könnten vertrauliche Informationen nach außen gelangen.

2.3 Unstrukturierte Datenhaltung

Durch unzureichende Vorgaben, sowie fehlende Schulung der Mitarbeiter, können Informationen unübersichtlich auf benutzten Datenträgern gespeichert werden. Das kann dazu führen, dass Informationen nicht vollständig gelöscht werden können, da kein Zuständiger mehr weiß, was in welchen Dateien gespeichert ist. Auch können Angreifer eventuell unbemerkt auf Informationen zugreifen, wenn viele Kopien einer Datei existieren und diese in verschiedenen Verzeichnissen mit unterschiedlichen Schutzfunktionen vorliegen. Kopien werden oft nicht nur in verschiedenen Verzeichnissen eines Datenträgers abgelegt. Viel kritischer ist es, wenn mehrere Kopien auf unterschiedlichen Datenträgern abgelegt werden und nicht mehr ersichtlich ist, wo was wann abgelegt wurde. Gesteigert wird dieses Problem, wenn die Datenträger dezentral beschafft und nicht kontrolliert werden. Eine unstrukturierte Datenhaltung gefährdet sowohl die Verfügbarkeit (das Arbeiten mit den Daten) als auch die Integrität und Vertraulichkeit.

2.4 Vertraulichkeitsverlust durch Auslagerungs- und temporäre Dateien

In Auslagerungsdateien oder Auslagerungspartitionen befinden sich mitunter vertrauliche Daten, z. B. Passwörter oder kryptografische Schlüssel. Die Auslagerungsdateien und damit auch die darin befindlichen Informationen sind jedoch nicht geschützt, da sie z. B. ausgelesen werden können, wenn die Festplatte ausgebaut und in einem anderen IT-System eingebaut wird.

Auch fallen im laufenden Betrieb vieler Anwendungen Dateien an, die nicht für den produktiven Betrieb benötigt werden (z. B. Browser-Historie). Auch diese Dateien können sicherheitsrelevante Informationen enthalten. Werden Auslagerungs- oder temporäre Dateien nicht sicher gelöscht, können schützenswerte Informationen, Passwörter und Schlüssel von Unbefugten missbraucht werden, um sich einen Zugang zu weiteren IT-Systemen und Daten zu verschaffen, Wettbewerbsvorteile auf dem Markt zu erlangen oder gezielt Benutzerverhalten auszuspionieren.

2.5 Ungeeignete Entsorgung der Datenträger und Dokumente

Wenn Datenträger oder Dokumente nicht geeignet entsorgt werden, können hieraus eventuell Informationen extrahiert werden, die Dritten nicht in die Hände fallen sollten. So können Angreifer z. B. Datenträger aus unzureichend gesicherten Entsorgungseinrichtungen stehlen. Auch wenn beauftragte Entsorgungsdienstleister ungenügend kontrolliert werden, kann die Vertraulichkeit nicht ausreichend sichergestellt werden.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Löschen und Vernichten aufgeführt. Grundsätzlich ist der ISB für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür

verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Informationssicherheitsbeauftragter (ISB)
Weitere Verantwortliche	Beschaffungsstelle, Datenschutzbeauftragter, Fachverantwortliche, IT-Betrieb, Leiter Haustechnik, Leiter IT, Leiter Organisation, Mitarbeiter

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

CON.6.A1 Regelung der Vorgehensweise für die Löschung und Vernichtung von Informationen [Leiter IT, Leiter Organisation]

Die Institution MUSS das Löschen und Vernichten von Informationen regeln. Dabei MUSS je nach Organisationseinheit geregelt werden, welche Informationen und Betriebsmittel unter welchen Voraussetzungen gelöscht und entsorgt werden dürfen. Ebenso MUSS festgelegt werden, in welchen räumlichen Bereichen Entsorgungs- und Vernichtungseinrichtungen aufgebaut werden sollen.

Außerdem MUSS schon in der Planungsphase festgelegt sein, wer für das Löschen und Vernichten von Informationen und Betriebsmitteln zuständig ist und welche Schnittstellen es zwischen den Organisationseinheiten gibt. Ebenso MUSS der Informationsfluss intern und zwischen den Zuständigen der Institution mit möglichen Outsourcing-Dienstleistern geregelt werden.

CON.6.A2 Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln und Informationen [Mitarbeiter, Leiter IT, Leiter Haustechnik]

Alle schutzbedürftigen Informationen und Betriebsmittel MÜSSEN sicher entsorgt werden. Zu diesem Zweck MÜSSEN abgesicherte und geeignete Entsorgungseinrichtungen auf dem Gelände der Institution verfügbar sein. Dabei MUSS auch berücksichtigt werden, dass Informationen und Betriebsmittel eventuell erst gesammelt und dann später entsorgt werden. Eine solche zentrale Sammelstelle MUSS vor unbefugten Zugriffen abgesichert werden.

Wenn externe Dienstleister beauftragt werden, MUSS der Entsorgungsvorgang ausreichend sicher und nachvollziehbar sein. Die mit der Entsorgung beauftragten Unternehmen SOLLTEN regelmäßig daraufhin überprüft werden, ob der Entsorgungsvorgang noch dem Sollzustand entspricht.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Löschen und Vernichten. Sie SOLLTEN grundsätzlich umgesetzt werden.

CON.6.A3 Löschen der Datenträger vor und nach dem Austausch [Fachverantwortliche]

Bevor bereits benutzte Datenträger weitergegeben oder noch einmal eingesetzt werden, SOLLTEN alle darauf befindlichen Daten sicher gelöscht werden. Dazu SOLLTEN den Mitarbeitern geeignete Verfahren (siehe CON.6.A4 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern*) zur Verfügung stehen.

CON.6.A4 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern [Leiter IT, Leiter Organisation]

Für das Löschen und Vernichten SOLLTEN geeignete Verfahren ausgewählt werden. So SOLLTE es für verschiedene Datenträgerarten immer geeignete Geräte und Werkzeuge geben, mit denen der verantwortliche Mitarbeiter die gespeicherten Informationen löschen oder vernichten kann. Es SOLLTE regelmäßig kontrolliert werden, ob die gewählten Verfahren noch dem Stand der Technik entsprechen und für die Institution noch ausreichend sicher sind. Die ausgewählten Verfahrensweisen SOLLTEN allen Mitarbeitern bekannt sein.

CON.6.A5 Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern [Mitarbeiter, Leiter IT, IT-Betrieb, Fachverantwortliche]

Es SOLLTE geregelt und dokumentiert werden, wie IT-Systeme und Datenträger außer Betrieb zu nehmen sind. Dabei SOLLTE sichergestellt sein, dass vor der Aussonderung alle auf einem IT-System oder Datenträger gespeicherten Informationen sicher gelöscht sind. Bei der Aussonderung SOLLTEN neben "klassischen" IT-Systemen auch alle IT-Systeme berücksichtigt werden, die dauerhafte Speicherelemente enthalten.

CON.6.A6 Einweisung aller Mitarbeiter in die Methoden zur Löschung oder Vernichtung von Informationen [Leiter IT]

Alle Mitarbeiter SOLLTEN in die Methoden und Verfahrensweisen zum Löschen und Vernichten von Informationen eingewiesen werden. Dabei SOLLTE nach den Anforderungen des Bausteins *ORP.3 Sensibilisierung und Schulung* vorgegangen werden.

CON.6.A7 Beseitigung von Restinformationen [IT-Betrieb, Mitarbeiter]

Wenn Datenträger und Dateien weitergegeben werden, SOLLTE sichergestellt sein, dass sie keine sogenannten Restinformationen enthalten. Dazu SOLLTE ein Prozess in der Institution etabliert und dokumentiert werden. Damit die Mitarbeiter ihn auch ausreichend umsetzen, SOLLTEN sie über die Gefahren von Rest- und Zusatzinformationen in Dateien informiert werden. Es SOLLTE stichprobenartig überprüft werden, ob die in Dateien enthaltenen Restinformationen auch wirklich gelöscht werden.

CON.6.A8 Richtlinie für die Löschung und Vernichtung von Informationen [Mitarbeiter, Leiter IT, Datenschutzbeauftragter]

Die Regelungen der Institution zum Löschen und Vernichten SOLLTEN in einer Richtlinie dokumentiert werden. Die Richtlinie SOLLTE allen relevanten Verantwortlichen und Mitarbeitern der Institution bekannt sein und die Grundlage für deren Arbeit und Handeln bilden. Inhaltlich SOLLTE die Richtlinie alle eingesetzten Datenträger, Anwendungen, IT-Systeme und sonstigen Betriebsmittel und Informationen enthalten, die vom Löschen und Vernichten betroffen sind. Es SOLLTE regelmäßig und stichprobenartig überprüft werden, ob die Mitarbeiter sich an die Richtlinie halten. Die Richtlinie SOLLTE regelmäßig aktualisiert werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

CON.6.A9 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern bei erhöhtem Schutzbedarf [Leiter IT, Leiter Organisation] (CIA)

Für das Löschen und Vernichten SOLLTEN Verfahren ausgewählt werden, die dem erhöhten Schutzbedarf der Informationen und Betriebsmittel gerecht werden.

CON.6.A10 Beschaffung geeigneter Geräte zur Löschung oder Vernichtung von Daten [Leiter Organisation, Leiter IT, Beschaffungsstelle] (CIA)

Bevor Geräte zur Löschung oder Vernichtung von Daten beschafft werden, SOLLTE eine Anforderungsdokumentation erstellt werden, anhand derer die auf dem Markt verfügbaren Werkzeuge miteinander verglichen werden können.

CON.6.A11 Vernichtung von Datenträgern durch externe Dienstleister [Leiter Organisation, Datenschutzbeauftragter] (CIA)

Auf dem Gelände der Institution SOLLTEN alle zu vernichtenden Datenträger bis zur Abholung durch den externen Dienstleister sicher vor unbefugten Zugriffen aufbewahrt werden. Der Abtransport SOLLTE ebenfalls dem Schutzbedarf entsprechend abgesichert sein. Die Institution SOLLTE den Entsorgungsprozess regelmäßig durch eingewiesene Personen kontrollieren lassen.

Zudem SOLLTEN die in OPS.2.1 *Outsourcing-Nutzung* beschriebenen generellen Anforderungen an Dienstleister und deren Mitarbeiter umgesetzt werden.

4 Weiterführende Informationen

4.1 Literatur

- [27001A8.3] ISO/IEC 27001:2013 - Annex A.8.3 Media handling
  ISO, Information technology- Security techniques- Information security management system-Requirements, insbesondere Annex A, A.8.3 Media handling, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [DIN663991] DIN 66399-1:2012-10 Büro- und Datentechnik Teil 1
  Teil 1: Grundlagen und Begriffe, 2012

- [DIN663992] DIN 66399-2:2012-10 Büro- und Datentechnik Teil 2
  Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern, 2012

- [DIN663993] DIN SPEC 66399-3:2013-02 - Büro- und Datenträgertechnik Teil 3
  Teil 3: Prozess der Datenträgervernichtung, 2013

- [SP80088] NIST Special Publication 800-88 Revision 1
  NIST, Guidelines for Media Sanitization, 12.2014
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Löschen und Vernichten" von Bedeutung.

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

Elementare Gefährdungen / Anforderungen	G 0.18	G 0.19	G 0.31	G 0.44
CON.6.A1	x	x		
CON.6.A2		x		x
CON.6.A3		x	x	
CON.6.A4		x		
CON.6.A5		x		
CON.6.A6		x	x	
CON.6.A7		x	x	
CON.6.A8	x	x	x	
CON.6.A9		x		
CON.6.A10		x	x	
CON.6.A11		x		x

CON: Konzeption und Vorgehensweise

CON.7 Informationssicherheit auf Auslandsreisen

1 Beschreibung

1.1 Einleitung

Die Bedeutung berufsbedingt notwendiger Reisetätigkeiten hat in den letzten Jahren durch die Globalisierung und die dadurch zunehmende internationale Vernetzung von Behörden und Unternehmen stetig zugenommen. Um auch außerhalb des regulären Arbeitsumfeldes arbeiten zu können, ist es unabdingbar geworden, neben Unterlagen in Papierform auch Informationstechnik mitzuführen, sei es z. B. Notebook, Smartphone, Tablet, Wechselfestplatte oder USB-Stick. Bei Geschäftsreisen, vor allem bei Auslandsreisen, sind eine Vielzahl an Bedrohungen und Risiken für die Informationssicherheit zu beachten, die im normalen Geschäftsbetrieb nicht existieren.

Jede Reise ist grundsätzlich verschieden, da sich aufgrund der Abhängigkeit von Parametern, wie dem Reisezweck (z. B. geschäftliche Besprechung, Tagung, Kongress, Seminar), der Reisedauer und dem Reiseziel, jeweils eine neue Bedrohungslage, auch in Bezug auf den Schutz geschäftskritischer Informationen, ergibt.

Der Schutz betrieblicher Informationen ist aufgrund der ständig wechselnden Zieldestinationen, bestimmter Umstände bzw. regulatorischer und gesetzlicher Anforderungen nicht immer einfach zu realisieren. So können z. B. die gesetzlichen und regulatorischen Anforderungen die Einreisekontrolle und somit den Schutz der Vertraulichkeit von Daten beeinflussen. Dies zeigt, dass sich abhängig von Art und Dauer der Reise sowie dem Reiseziel individuelle Anforderungen an die Informationssicherheit ergeben. Politische, gesellschaftliche, religiöse, geografische, klimatische, gesetzliche und regulatorische Besonderheiten einzelner Reiseziele spielen hier eine maßgebliche Rolle.

1.2 Zielsetzung

Zielsetzung dieses Bausteins ist der Schutz aller Informationen, die auf Auslandsreisen sowohl in elektronischer als auch physischer Form mitgeführt werden, in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit. Vertrauliche Informationen, die jeder reisende Mitarbeiter im Kopf mitführt, sind ebenfalls Gegenstand dieses Bausteines. Daher ist die Erstellung angemessener Regelungen und Maßnahmen für den Umgang mit schützenswerten Informationen und Daten auf Auslandsreisen unter Einbindung relevanter anderer Rahmenbedingungen, wie z. B. IT, Datenschutz, Recht, unerlässlich.

Aufgrund dessen werden in diesem Baustein szenariospezifische Gefährdungen und Anforderungen herausgestellt, die in direktem Zusammenhang mit dem sicheren Einsatz von Informationstechnologie, den Informationen und den diese verarbeitenden Geräten auf Auslandsreisen stehen.

Dieser Baustein dient den Verantwortlichen einer Institution als Orientierungshilfe für die Etablierung angemessener Sicherheitsmaßnahmen im Rahmen der Informationssicherheit auf Auslandsreisen. Dabei werden die wesentlichen Grundsätze aufgezeigt, die in diesem Zusammenhang zu be-

rücksichtigen sind. Viele der genannten Gefährdungen haben auch Gültigkeit bei Inlandsreisen oder grundsätzlich bei der Verarbeitung von Informationen in fremden bzw. nicht unter eigener Kontrolle stehenden Umgebungen.

1.3 Abgrenzung

Der Baustein umfasst grundsätzlich die Anforderungen, die zu einem angemessenen Schutz von Informationen auf Auslandsreisen beitragen. Dabei hat der Schutz der Vertraulichkeit und Integrität von schützenswerten Informationen auf Reisen den gleichen Stellenwert wie am Sitz der Institution.

Gefährdungen und Anforderungen, die den lokalen Informationsverbund betreffen, werden hier nicht betrachtet.

Da im Baustein CON.6 *Informationssicherheit auf Auslandsreisen* speziell die prozessualen, technischen und organisatorischen Anforderungen betrachtet werden, die spezifisch für geschäftliche Arbeit auf Reisen sind, werden Anforderungen der Schichten Netze und Kommunikation (NET), IT-Systeme (SYS) und Anwendungen (APP) nicht betrachtet. Alle notwendigen Bausteine, vor allem SYS.2.1 *Allgemeine Clients, NET.3.3 VPN, SYS 3.2.2 Mobile Device Management,* müssen gesondert berücksichtigt werden.

Zudem sind die Anforderungen aus den themenüberschneidenden Bausteinen *INF.10 Mobiler Arbeitsplatz und INF.9 Telearbeitsplatz* zu beachten und umzusetzen.

Innerhalb dieses Bausteins kommt es außerdem zu Überschneidungen mit weiteren Bausteinen und Themenfeldern, die hier nicht betrachtet werden:

- Erfüllung der Datenschutzanforderungen
- Präventive Maßnahmen zum Schutz von Informationen (auch technische Anforderungen, die an tragbare IT-Systeme gestellt werden, z. B. Abstrahl-/Abhörschutz)
- Personelle Sicherheit

2 Gefährdungslage

Nachfolgend beschrieben sind die spezifischen Bedrohungen und Schwachstellen im Bereich Informationssicherheit, die auf Auslandsreisen von besonderer Bedeutung sind.

Die Bedrohungslage ist für einige Gefährdungen auf Grund dieses Szenarios besonders erhöht. Dies ergibt sich z. B. aus der Kommunikation über öffentliche Netze, die nicht im Zugriff der eigenen Institution sind. Dadurch werden wieder Gefahren relevant, gegen welche sich die Institution vielleicht schon abgesichert hat.

Hinzu kommt, dass die Eintrittswahrscheinlichkeit eines Risikos auf Auslandsreisen in Abhängigkeit des gewählten Ziellandes meist deutlich höher gegenüber Inlandsreisen ist.

2.1 Abhören und Ausspähen von Informationen/Wirtschaftsspionage

Mit Spionage werden Angriffe bezeichnet, die das Ziel haben, Informationen über Institutionen, Personen, Produkte oder andere Zielobjekte zu sammeln, auszuwerten und aufzubereiten. Insbesondere bei Reisen ins Ausland sind unbekannte Gefahrenquellen vorhanden, auf die vom Informationssicherheitsmanagement der eigenen Institution keinen Einfluss genommen werden kann. Grundsätzlich bestehen in fremden Räumen und fremden IT-Umgebungen viele Gefahren durch das gezielte Abhören von Raumgesprächen, Leitungen, Telefongesprächen oder Datenübertragungen. Dies kann vor allem im Ausland durch entsprechende rechtliche Möglichkeiten problematisch und für den Reisenden nur schwer einschätzbar sein.

Dies kann sowohl öffentliche Plätze und Räume betreffen wie auch Gegebenheiten in anderen Institutionen, aber auch in institutionseigenen Repräsentanzen im Ausland. Auch Geräte wie z. B. Mobiltelefone können dazu benutzt werden, unbemerkt Gespräche aufzuzeichnen oder abzuhören. Zudem sind viele IT-Systeme standardmäßig mit Mikrofon und Kameras ausgestattet, die angegriffen und dann ausgenutzt werden können.

Darüber hinaus kann es bei bestimmten Ländern Restriktionen bei der Ein- und Ausreise geben, die regulatorische Vorgaben des Herkunftslandes und Anforderungen der Institution außer Kraft setzen bzw. diesen widersprechen. Als Beispiel kann hier die Möglichkeit genannt werden, dass bei Reisen in andere Länder, wie z. B. die USA, Einsicht in auf Notebooks und anderen tragbaren IT-Systemen gespeicherte Daten verlangt werden kann. Hierbei können zum Teil vertrauliche und personenbezogene Daten nicht nur eingesehen, sondern auch kopiert und gespeichert werden. Da es sich bei diesen Informationen z. B. auch um Strategiepapiere oder streng vertrauliche Entwürfe eines Unternehmens oder einer Behörde handeln könnte, muss in diesem Zusammenhang immer mit einem potentiellen Missbrauch dieser gerechnet werden (Wirtschaftsspionage).

Weiterhin können im Rahmen der Kommunikation übertragene Signale auf der Strecke nicht physisch gegen unbefugtes Mithören und Aufzeichnen abgeschirmt werden. Deshalb könnten Einwahlpunkte/Hotspots o. ä. angegriffen oder abgehört und über diese Informationen erlangt werden. Hierzu gehören z. B. Standortinformationen oder MAC-Adressen, aber auch unverschlüsselt übertragene Datenpakete und Informationen wie Metadaten inklusive Empfänger- und Absenderdaten, Adressen oder Telefonnummern.

Auf Auslandsreisen besteht nicht nur die Gefahr, dass Informationen auf technisch komplexem Weg ausgespäht werden können. Oft können schützenswerte Daten auf optischem, akustischem oder elektronischem Weg einfacher ausgespäht werden, da im Ausland häufig nicht die gewohnten Ansprüche an Sicherheitsbestimmungen in Bezug auf die Informationssicherheit gestellt werden können. Dies betrifft z. B. das allgemeine Sicherheitslevel, welches in anderen Ländern vorherrscht, sowie die Gegebenheiten vor Ort, die ein Reisender zwangsläufig nutzen muss.

Hier können z. B. die unverschlüsselte Übertragung von Benutzer-ID und/oder Passwörtern genannt werden, aber auch Gefährdungen wie nicht gesperrte oder leicht einsehbare Bildschirme, worüber ein Angreifer Informationen erlangen kann.

2.2 Offenlegung und Missbrauch schützenswerter Informationen (elektronisch und physisch)

Beim Austausch von Informationen, sowohl beim Versand oder der Übergabe von Datenträgern als auch persönlich oder telefonisch, kommt es immer wieder vor, dass neben den eigentlich gewünschten Informationen auch ungewollt andere schutzbedürftige Informationen übermittelt werden. Dieser Umstand ist auch auf Auslandsreisen gegeben. Hier wird die Kommunikation bzw. der Informationsaustausch durch technisch unsichere Gegebenheiten zum Teil noch erschwert. Zudem kann es vorkommen, dass Geschäftsreisende vertrauliche Dokumente sowohl physischer als auch elektronischer Art in öffentlichen Räumen oder im Hotelzimmer aufgrund von Unachtsamkeit offen einsehbar liegen lassen.

Die Kommunikation mit unbekannten IT-Systemen und Netzen birgt immer ein Gefährdungspotenzial für das eigene Endgerät. So können z. B. auch vertrauliche Informationen, die nicht dazu bestimmt sind, weitergegeben zu werden, mit kopiert werden.

Auf der anderen Seite können fremde Datenträger auch Schadprogramme enthalten. Hier besteht die Gefahr, dass diese wichtige Daten stehlen, manipulieren, verschlüsseln oder vernichten könnten. Ebenso können aber auch Integrität und Verfügbarkeit von IT-Systemen beeinträchtigt werden. Dieser Aspekt wird durch die Tatsache begünstigt, dass ein Datenaustausch im Ausland häufig über unsichere Medien stattfindet. Dieser wichtige Aspekt ist den Mitarbeitern allerdings nicht immer bewusst.

2.3 Unbemerkter Zugriff auf mobile Endgeräte

Mobile Endgeräte wie Notebooks, Smartphones, Tablets oder PDAs sind größtenteils darauf ausgelegt, einen einfachen Datenaustausch mit anderen IT-Systemen zu ermöglichen. Dies kann über ein Verbindungskabel oder auch drahtlos, z. B. über WLAN, Bluetooth oder eine Mobilfunkverbindung, erfolgen. Wo auf Reisen im Ausland ein offener Zugang zu IT-Systemen möglich ist, können Angreifer daher von mobilen Endgeräten unter Umständen Informationen unauffällig abfragen, verändern oder mitnehmen. Eine nachträgliche Überprüfung oder gar ein Nachweis sind nicht immer möglich, da häufig die Zugriffe nicht entsprechend protokolliert werden

2.4 Vortäuschen einer falschen Identität

Im Rahmen von Kommunikation auf Reisen besteht eine erhöhte Gefahr, dass Angreifer sowohl persönlich als auch elektronisch versuchen, eine falsche Identität vorzutäuschen oder eine autorisierte Identität zu übernehmen (technisch z. B. durch Maskerade, Spoofing-Arten, Hijacking, Man-in-the-Middle-Angriffe oder ähnlichem). Hierbei kann der Benutzer über die Identität seines Kommunikationspartners so getäuscht werden, dass er schützenswerte Informationen preisgibt. Eine falsche digitale Identität erlangt er z. B. durch das Ausspähen von Benutzer-ID und Passwort, die Manipulation des Absenderfeldes einer Nachricht oder durch die Manipulation einer Adresse im Netz.

Ausländische Geschäftspartner kennt ein Mitarbeiter nicht immer persönlich. Daher kann es passieren, dass ein Mitarbeiter der ersten Person, die sich mit dem richtigen Namen bzw. Hintergrundwissen vorstellt, Glauben schenkt und dieser wertvolle Informationen weitergibt.

Da die Sicherheitsanforderungen an Vertraulichkeit und Integrität in institutionsfremden, vor allem ausländischen, Gebäuden und Räumen nie vollständig sichergestellt werden kann, besteht auch immer ein Restrisiko, dass sonst selbstverständlich erscheinende Dinge manipuliert sein könnten, wie die Rufnummernanzeige am Telefon oder die Absenderkennung eines Faxabsenders, durch die eine falsche Identität vorgetäuscht und Informationen erlangt werden können.

2.5 Fehlendes Sicherheitsbewusstsein und Sorglosigkeit im Umgang mit Informationen

Häufig ist zu beobachten, dass in Institutionen organisatorische Regelungen und technische Sicherheitsverfahren für tragbare IT-Systeme und mobile Datenträger vorhanden sind, diese jedoch durch den sorglosen Umgang mit den Vorgaben und der Technik wieder ausgehebelt werden. So ist z. B. immer wieder zu beobachten, dass mitgebrachte mobile Datenträger während der Pausen unbeaufsichtigt im Besprechungsraum oder auch im Zugabteil zurückgelassen werden.

Darüber hinaus werden zum Teil Geschenke in Form von Datenträgern, wie z. B. USB-Sticks, von Mitarbeitern angenommen und unüberlegt an das eigene Notebook angeschlossen. Hier besteht dann die Gefahr, dass das Notebook mit Schadsoftware infiziert wird und dadurch schützenswerte Daten gestohlen, manipuliert oder verschlüsselt und damit vorübergehend (siehe 2.7 Nötigung, Erpressung, Entführung und Korruption) unbrauchbar gemacht werden.

In öffentlichen Verkehrsmitteln oder auch während Geschäftsessen ist immer wieder zu beobachten, dass Menschen offene Gespräche über geschäftskritische Informationen führen. Diese können dann von Außenstehenden leicht mitgehört und möglicherweise zum schwerwiegenden Nachteil des Mitarbeiters oder seiner Institution verwendet werden.

2.6 Verstoß gegen lokale Gesetze oder Regelungen

Bei Reisen ins Ausland sind insbesondere abweichende Gesetze und Regularien bzw. zusätzliche Bestimmungen der Zieldestination zu berücksichtigen, da diese von der nationalen Rechtslage schwerwiegend abweichen können. Einschlägige Gesetze und Verordnungen (z. B. zu Datenschutz, Informationspflichten, Haftung, Informationszugriffe für Dritte) des Ziellandes sind Reisenden häufig unbekannt oder werden falsch eingeschätzt. Dadurch kann nicht nur im Aus-, sondern auch im Inland gegen eine Vielzahl von Gesetzen verstoßen werden, beispielsweise wenn im Ausland personenbezogene Daten inländischer Kunden bei einer Auslandsdienstreise ungeschützt über öffentliche Netze übertragen werden.

2.7 Nötigung, Erpressung, Entführung und Korruption

Die Sicherheit von Informationen, aber auch die der Reisenden selber könnte bei Auslandsreisen durch Nötigung, Erpressung und in diesem Zusammenhang auch Entführung beeinträchtigt werden. Im Ausland gelten oft andere Sicherheitsrisiken aufgrund politischer und gesellschaftlicher Umstände. Mitarbeiter könnten in eine Opferrolle gedrängt werden, in der ihnen Gewalt angedroht wird, um sie zur Her-

ausgabe von schützenswerten Daten zu zwingen. Dabei werden sie genötigt, Sicherheitsrichtlinien und -maßnahmen zu umgehen bzw. zu missachten. Im Fokus stehen hierbei oftmals hochrangige Führungskräfte oder Mitarbeiter, die eine besondere Vertrauensstellung genießen.

Angreifer verfolgen vor allem das Ziel, schützenswerte Informationen zu stehlen oder zu manipulieren, um den Ablauf der Geschäftsprozesse zu beeinträchtigen oder sich und andere zu bereichern. Hier spielen vor allem politische, ideologische und wirtschaftliche Ziele der Angreifer eine Rolle.

Neben der Androhung von Gewalt existiert auch die Möglichkeit, Reisenden gezielt Geld oder andere Vorteile anzubieten (Bestechung), um diese zur Herausgabe von vertraulichen Informationen an Unbefugte bzw. zu Sicherheitsverletzungen zu bewegen (Korruption). Generell wird durch Nötigung, Erpressung (in diesem Zusammenhang auch Entführung) und Korruption die Umsetzung der in der Informationssicherheit geltenden Regelungen gestört bzw. gänzlich ausgehebelt.

2.8 Informationen aus unzuverlässiger Quelle/Vortäuschen

Im Rahmen einer Auslandstätigkeit können dem Reisenden absichtlich falsche (irreführende) Informationen zugespielt werden, um diesen zu täuschen. In Folge dieser Täuschung könnten falsche Aussagen in geschäftskritische Berichte eingearbeitet werden. Dies kann unter anderem dazu führen, dass geschäftsrelevante Informationen auf einer falschen Datenbasis beruhen, Berechnungen falsche Ergebnisse liefern und darauf basierend falsche Entscheidungen getroffen werden.

2.9 Beeinträchtigung der IT durch wechselnde Einsatzumgebung

Informationstechnik wird bei Reisen in sehr unterschiedlichen Umgebungen eingesetzt und ist dadurch vielen Gefährdungen ausgesetzt. Dazu gehören z. B. schädigende Umwelteinflüsse, wie zu hohe oder zu niedrige Temperaturen, ebenso wie Staub oder Feuchtigkeit. Zu anderen Problemen, die durch die Mobilität der Geräte entstehen, gehören z. B. Transportschäden.

Zudem führen bei Auslandstätigkeit häufig nicht greifende IT-Betriebsprozesse wie Patch Management, Change Management und Berechtigungsmanagement zu Schwachstellen, die besonders in ungesicherten IT-Netzen im Ausland schnell ausgenutzt werden können.

2.10 Diebstahl oder Verlust von Geräten, Datenträgern und Dokumenten

Insbesondere auf Reisen im Ausland ist damit zu rechnen, dass mobile Endgeräte leicht verloren gehen oder gestohlen werden können. Je kleiner und begehrter diese Geräte sind, desto höher ist dieses Risiko. Neben dem rein materiellen Schaden durch den unmittelbaren Verlust des mobilen Gerätes kann durch die Offenlegung schützenswerter Daten (z. B. E-Mails, Notizen von Besprechungen, Adressen oder sonstige Dokumente) weiterer (finanzieller und/oder Reputations-)Schaden entstehen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Informationssicherheit auf Auslandsreisen aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt.

Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept regelmäßig überprüft werden.

Bausteinverantwortlicher	Informationssicherheitsbeauftragter (ISB)
Weitere Verantwortliche	Benutzer, Datenschutzbeauftragter, Fachverantwortliche, IT-Betrieb, Notfallbeauftragter, Personalabteilung

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

CON.7.A1 Sicherheitsrichtlinie zur Informationssicherheit auf Auslandsreisen

Alle für die Informationssicherheit relevanten Aspekte, die in Verbindung mit den Tätigkeiten im Ausland stehen, MÜSSEN betrachtet und geregelt werden. Anforderungen an die Sicherheitsmaßnahmen, die in diesem Zusammenhang ergriffen werden, MÜSSEN in einer Sicherheitsrichtlinie zur Informationssicherheit auf Auslandsreisen dokumentiert werden. Diese Regelungen und die Sicherheitsrichtlinie für Auslandsreisen, oder ein entsprechendes Merkblatt zur Informationssicherheit auf Auslandsreisen, in dem die zu beachtenden Sicherheitsmaßnahmen erläutert werden, MÜSSEN transnational agierenden Mitarbeitern ausgehändigt werden.

Erweiternd MUSS ein Sicherheitskonzept zum Umgang mit tragbaren IT-Systemen auf Auslandsreisen erstellt und regelmäßig überprüft werden, das alle Sicherheitsanforderungen und -maßnahmen angemessen detailliert beschreibt.

CON.7.A2 Sensibilisierung der Mitarbeiter zur Sicherheitsrichtlinie Informationssicherheit auf Auslandsreisen [IT-Betrieb, Datenschutzbeauftragter]

Benutzer MÜSSEN im verantwortungsvollen Umgang mit Informationstechnik bzw. tragbaren IT-Systemen auf Auslandsreisen geschult und sensibilisiert werden. Insbesondere MÜSSEN ihnen die Gefahren, die durch den unangemessenen Umgang mit Informationen, die unsachgemäße Vernichtung von Daten und Datenträgern, Schadsoftware und unsicheren Datenaustausch entstehen, vermittelt, aber auch die Grenzen der eingesetzten Sicherheitsmaßnahmen aufgezeigt werden. Sie MÜSSEN dazu befähigt und bestärkt werden, bei Ungereimtheiten fachliche Beratung einzuholen bzw. einem Verlust oder Diebstahl vorzubeugen. Außerdem SOLLTEN Mitarbeiter auf gesetzliche Anforderungen einzelner Reiseziele in Bezug auf die Reisesicherheit hingewiesen werden. Hier steht der Informationssicherheitsbeauftragte in der Verantwortung, sich über gesetzliche Anforderungen im Rahmen der Informationssicherheit (z. B. Datenschutz, IT-Sicherheitsgesetz) zu informieren und die Mitarbeiter zu sensibilisieren.

CON.7.A3 Identifikation länderspezifischer Regelungen, Reise- und Umgebungsbedingungen [Personalabteilung]

Vor Reiseantritt MÜSSEN durch das Informationssicherheitsmanagement bzw. die Personalabteilung die jeweils geltenden Regelungen der einzelnen Länder geprüft und an die entsprechenden Mitarbeiter kommuniziert werden.

Die Institution MUSS geeignete Regelungen und Maßnahmen erstellen, umsetzen und kommunizieren, die den angemessenen Schutz unternehmensinterner Daten in Abhängigkeit der individuellen Reise- und Umgebungsbedingung ermöglichen.

Außerdem MUSS sich ein Mitarbeiter vor Reiseantritt mit den klimatischen Bedingungen des Reiseziels auseinandersetzen und abklären, welche Schutzmaßnahmen er für sich (z. B. Impfungen) und die mitgeführte Informationstechnik benötigt.

CON.7.A4 Verwendung von Sichtschutz-Folien [Benutzer]

Benutzer MÜSSEN insbesondere im Ausland darauf achten, dass z. B. bei der Arbeit mit dem Notebook keine schützenswerten Informationen erspäht werden können. Dazu MUSS auf allen mobilen IT-Systemen ein angemessener Sichtschutz verwendet werden, der den gesamten Bildschirm des jeweiligen Gerätes, also Notebooks, Tablets oder Smartphones umfasst und ein Ausspähen von Informationen erschwert.

CON.7.A5 Verwendung der Bildschirm-/Code-Sperre [Benutzer]

Durch die Verwendung einer Bildschirm-/Code-Sperre wird verhindert, dass Dritte auf Daten auf mobilen Endgeräten, wie z. B. Notebooks oder Mobiltelefonen zugreifen können. Eine entsprechende Sperrmöglichkeit MUSS verwendet werden. Der Benutzer MUSS dazu einen angemessenen Code bzw. ein sicheres Gerätepasswort verwenden. Die Bildschirmsperre MUSS sich nach einer kurzen Zeit der Inaktivität automatisch aktivieren.

CON.7.A6 Zeitnahe Verlustmeldung [Benutzer, Notfallbeauftragter]

Mitarbeiter MÜSSEN ihrer Institution umgehend melden, wenn Informationen, IT-Systeme oder Datenträger verloren oder gestohlen wurden. Hierfür MUSS es klare Meldewege und Ansprechpartner innerhalb der Institution geben. Die Institution MUSS die möglichen Auswirkungen des Verlustes bewerten und geeignete Gegenmaßnahmen ergreifen.

CON.7.A7 Sicherer Remote-Zugriff [IT-Betrieb, Benutzer]

Um Mitarbeitern auf Auslandsreisen einen sicheren Fernzugriff auf das Netz der Institution zu ermöglichen, MUSS zuvor ein sicherer Remote-Zugang, z.B. via VPN, durch den IT-Betrieb eingerichtet worden sein. Der VPN-Zugang MUSS kryptographisch abgesichert sein. Außerdem MÜSSEN Benutzer über angemessen sichere Zugangsdaten verfügen, um sich gegenüber Endgerät und dem Netz erfolgreich zu authentisieren. Mitarbeiter MÜSSEN den sicheren Remote-Zugriff für jegliche darüber mögliche Kommunikation nutzen. Es MUSS sichergestellt werden, dass nur autorisierte Personen auf IT-Systeme zugreifen dürfen, die über einen Fernzugriff verfügen. Mobile IT-Systeme MÜSSEN im Rahmen der Möglichkeiten vor dem direkten Anschluss an das Internet durch eine restriktiv konfigurierte Personal Firewall geschützt werden.

CON.7.A8 Sichere Nutzung von öffentlichen WLANs [Benutzer]

Grundsätzlich MUSS geregelt werden, ob mobile IT-Systeme direkt auf das Internet zugreifen dürfen.

Der Zugriff auf das Netz der Institution über öffentlich zugängliche WLANs MUSS über ein Virtual Private Network (VPN) oder vergleichbare Sicherheitsmechanismen realisiert sein (siehe CON.6.A7 Sicherer Remote-Zugriff). Die sichere Nutzung von WLANs ist im Baustein NET.2.2 WLAN-Nutzung beschrieben, die Nutzung von WLAN-Hotspots MUSS ebenfalls abgesichert sein und ist im Baustein INF.10 Mobiler Arbeitsplatz beschrieben.

CON.7.A9 Sicherer Umgang mit mobilen Datenträgern [Benutzer]

Vor der Verwendung mobiler Datenträger MUSS überprüft werden, dass diese nicht mit Schadsoftware infiziert sind. Vor der Weitergabe mobiler Datenträger MUSS sichergestellt werden, dass keine schützenswerten Informationen darauf enthalten sind. Nach der Verwendung MUSS der Datenträger, insbesondere wenn dieser an andere weitergegeben wird, sicher gelöscht werden. Dazu MUSS der Datenträger mit einem in der Institution festgelegten, ausreichend sicheren Verfahren überschrieben werden.

CON.7.A10 Verschlüsselung tragbarer IT-Systeme und Datenträger [Benutzer, IT-Betrieb]

Damit schützenswerte Informationen nicht durch unberechtigte Dritte eingesehen werden können, MUSS vor Reiseantritt durch den Mitarbeiter sichergestellt werden, dass alle schützenswerten Informationen entsprechend den internen Richtlinien abgesichert sind. Mobile Datenträger und Clients SOLLTEN dabei vor Reiseantritt verschlüsselt werden. Die kryptographischen Schlüssel MÜSSEN getrennt vom verschlüsselten Gerät aufbewahrt werden. Bei der Verschlüsselung von Daten SOLLTEN die gesetzlichen Regelungen des Ziellandes beachtet werden, dies betrifft insbesondere landesspezifische Gesetze zur Herausgabe von Passwörtern und zur Entschlüsselung von Daten.

CON.7.A11 Einsatz von Diebstahl-Sicherungen [Benutzer]

Zum Schutz der mobilen IT-Systeme außerhalb der Institution SOLLTEN Diebstahl-Sicherungen eingesetzt werden, vor allem an den Orten, an denen ein erhöhter Publikumsverkehr herrscht oder die Fluktuation von Benutzern sehr hoch ist. Die Beschaffungs- und Einsatzkriterien für Diebstahl-Sicherungen SOLLTEN an die Prozesse der Institution angepasst und dokumentiert werden.

CON.7.A12 Sicheres Vernichten von schutzbedürftigen Materialien und Dokumenten [Benutzer]

Insbesondere im Ausland können Dokumente und andere schutzbedürftige Datenträger nicht immer sicher entsorgt werden. Die Institution MUSS den Mitarbeitern Möglichkeiten aufzeigen, geschäftskritische Dokumente angemessen zu vernichten. Die Mitarbeiter MÜSSEN diese einhalten und DÜRFEN interne Unterlagen der Institution NICHT öffentlich entsorgen. Ist dies vor Ort nicht möglich oder handelt es sich um Dokumente bzw. Datenträger mit besonders schützenswerten Informationen, so MÜSSEN diese bis zur Rückkehr behalten und anschließend angemessen vernichtet werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Informationssicherheit auf Auslandsreisen. Sie SOLLTEN grundsätzlich umgesetzt werden.

CON.7.A13 Mitnahme von Daten und Datenträgern [IT-Betrieb, Benutzer]

Vor Reiseantritt SOLLTE geprüft werden, welche Daten während der Reise nicht unbedingt auf den mitgenommenen IT-Systemen, wie dem Notebook, Tablet oder Smartphone, gebraucht werden. Ist es nicht notwendig, diese Daten auf den Geräten zu belassen, SOLLTEN diese physisch gelöscht werden (siehe CON.6.A9 Sicheres Löschen der Informationen auf Datenträgern). Ergibt sich allerdings die Notwendigkeit, schützenswerte Daten mit auf Reisen zu nehmen, SOLLTE dies nur in verschlüsselter Form erfolgen.

Darüber hinaus SOLLTE schriftlich geregelt sein, welche mobilen Datenträger auf Auslandsreisen mitgenommen werden dürfen und welche Sicherheitsmaßnahmen dabei zu berücksichtigen sind (z. B. Schutz vor Schadsoftware, Verschlüsselung geschäftskritischer Daten, Aufbewahrung mobiler Datenträger). Die Mitarbeiter SOLLTEN diese Regelungen vor Reiseantritt kennen und beachten (siehe u.a. CON.6.A12 Verschlüsselung tragbarer IT-Systeme und Datenträger).

Diese sicherheitstechnischen Anforderungen richten sich nach dem Schutzbedarf der zu bearbeitenden Daten im Ausland und der Daten, auf die zugegriffen werden soll.

CON.7.A14 Kryptographisch abgesicherte E-Mail-Kommunikation [Benutzer, IT-Betrieb]

Bei der E-Mail-basierten Kommunikation SOLLTE der Mitarbeiter diese entsprechend den internen Vorgaben der Institution kryptographisch absichern.

Bei Kommunikation über E-Mail-Dienste, z. B. Webmail, SOLLTE durch die Institution vorab geklärt werden, welche Sicherheitsmechanismen beim Provider umgesetzt werden und ob damit die internen Sicherheitsanforderungen erfüllt werden. Hierzu zählen z. B. der sichere Betrieb der Server, Aufbau einer verschlüsselten Verbindung und Dauer der Datenspeicherung. Die E-Mails SOLLTEN ebenfalls geeignet verschlüsselt bzw. digital signiert werden. Öffentliche IT-Systeme, etwa in Hotels oder Internetcafés, SOLLTEN nicht für den Zugriff auf E-Mails genutzt werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

CON.7.A15 Abstrahlsicherheit tragbarer IT-Systeme [IT-Betrieb] (C)

Es SOLLTE vor Beginn der Reise festgelegt werden, welchen Schutzbedarf die einzelnen Informationen haben, die auf dem mobilen Datenträger bzw. Client des Mitarbeiters im Ausland verarbeitet werden. Informationstragende oder auch bloßstellende Abstrahlung dieser Datenträger und Clients kann von anderen empfangen bzw. abgefangen werden, sodass Informationen rekonstruiert und die Vertraulichkeit dieser Daten in Frage gestellt werden können. Die Institution SOLLTE hier prüfen, ob ein solcher Schutzbedarf für vertrauliche Informationen vorliegt, und entsprechend abstrahlarme bzw. -sichere Datenträger und Clients einsetzen.

CON.7.A16 Integritätsschutz durch Check-Summen oder digitale Signaturen (I)

Check-Summen SOLLTEN im Rahmen der Datenübertragung oder auch Datensicherung verwendet werden, um die Integrität der Daten überprüfen zu können. Besser noch SOLLTEN digitale Signaturen verwendet werden, um die Vertraulichkeit und Integrität von schützenswerten Informationen zu bewahren.

CON.7.A17 Verwendung dedizierter Reise-Hardware [IT-Betrieb] (CIA)

Zur Verhinderung des unberechtigten Abflusses schützenswerter Informationen der Institution auf Auslandsreisen (z. B. bei der Einreise oder der Ausreise) SOLLTE dem Mitarbeiter vorkonfigurierte Reise-Hardware zur Verfügung gestellt werden. Diese Reise-Hardware SOLLTE auf Basis des Minimalprinzips nur die Funktionen und Informationen zur Verfügung stellen, die zur Durchführung der Geschäftstätigkeit unbedingt erforderlich sind.

CON.7.A18 Eingeschränkte Berechtigungen auf Auslandsreisen [IT-Betrieb, Fachverantwortliche] (CI)

Vor Reiseantritt SOLLTE der Fachverantwortliche für das Sicherheitsmanagements der Institution prüfen, welche Berechtigungen der Mitarbeiter wirklich braucht, um seinem Alltagsgeschäft im Ausland nachgehen zu können. Dabei SOLLTE geprüft werden, ob Zugriffsrechte für die Reisedauer des Benutzers entzogen werden können, um einen unbefugten Zugriff auf zu verhindern.

4 Weiterführende Informationen

4.1 Literatur

- [IWS] Initiative Wirtschaftsschutz
  https://www.wirtschaftsschutz.info, (zuletzt abgerufen am 28.09.2017)

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Informationssicherheit auf Auslandsreisen" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.35 Nötigung, Erpressung oder Korruption

G 0.36 Identitätsdiebstahl

G 0.39 Schadprogramme

G 0.42 Social Engineering

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen Anforderungen	G 0.14	G 0.15	G 0.16	G 0.17	G 0.18	G 0.19	G 0.20	G 0.29	G 0.30	G 0.31	G 0.35	G 0.36	G 0.39	G 0.42	G 0.45	G 0.46
CON.7.A1	x		x	x	x	x		x	x	x						
CON.7.A2	x				x			x		x				x		
CON.7.A3				x	x	x		x	x						x	x
CON.7.A4			x			x			x				x			
CON.7.A5			x			x		x	x				x			
CON.7.A6						x			x							
CON.7.A7	x	x							x							
CON.7.A8		x			x	x		x		x						
CON.7.A9			x			x										
CON.7.A10					x	x		x				x				x
CON.7.A11			x	x					x	x					x	
CON.7.A12			x		x	x		x		x						
CON.7.A13			x	x	x	x			x		x				x	x
CON.7.A14	x	x				x		x				x				x
CON.7.A15									x			x				
CON.7.A16										x					x	x
CON.7.A17	x				x				x		x				x	
CON.7.A18					x					x						

Bundesamt
für Sicherheit in der
Informationstechnik

OPS: Betrieb

OPS.2.4	Fernwartung	274
OPS.2.1	Outsourcing für Kunden	265
OPS.1.1.4	Schutz vor Schadprogrammen	222
OPS.1.1.3	Patch- und Änderungsmanagement	215
OPS.1.1.2	Ordnungsgemäße IT-Administration	207
OPS.1.1.5	Protokollierung	228
OPS.1.1.6	Software-Tests und -Freigaben	235
OPS.1.2.2	Archivierung	242
OPS.1.2.3	Informations- und Datenträgeraustausch	251
OPS.1.2.4	Telearbeit	259
OPS.3.1	Outsourcing für Dienstleister	284

OPS.1.1: Kern-IT-Betrieb / Kernaufgaben

OPS.1.1.2 Ordnungsgemäße IT-Administration

1 Beschreibung

1.1 Einleitung

Die fortlaufende Administration von IT-Systemen und -Komponenten ist für den IT-Betrieb grundlegend. Die Systemadministratoren richten dabei IT-Systeme und Anwendungen ein, beobachten den Betrieb und reagieren mit Maßnahmen, die die Funktion und die Leistungsfähigkeit der Systeme erhalten, oder sie passen die Systeme an die veränderten Bedürfnisse an. Dabei erfüllen sie auch eine Reihe von Aufgaben für die Sicherheit: Sie sorgen nicht nur dafür, dass die Systeme verfügbar bleiben, sondern setzen auch Sicherheitsmaßnahmen um und überprüfen, ob sie wirksam sind. Dazu verfügen sie über sehr weitreichende Berechtigungen, sodass es für die Sicherheit des Informationsverbunds auch sehr wichtig ist, die Systemadministration vor unbefugten Zugriffen selbst abzusichern.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, aufzuzeigen, wie mit einer ordnungsgemäßen IT-Administration die Sicherheitsanforderungen von IT-Anwendungen, -Systemen und Netzen erfüllt werden.

Mit der Umsetzung dieses Bausteins sorgt die Institution einerseits dafür, dass die für die Sicherheit des Informationsverbunds erforderlichen Tätigkeiten in der Systemadministration ordnungsgemäß und systematisch durchgeführt werden. Andererseits reagiert die Institution damit auch auf die besonderen Gefährdungen, die sich aus dem Umgang mit Administrationsprivilegien und aus dem Zugang zu schützenswerten Bereichen der Institution zwangsläufig ergeben.

1.3 Abgrenzung

Der Baustein beschreibt allgemeine Sicherheitsanforderungen an eine ordnungsgemäße IT-Administration. Er betrachtet dabei laufende administrative Tätigkeiten, die vom dafür vorgesehenen Personal an den Standorten der Institution durchgeführt werden. Er ist abzugrenzen gegen eine Fernadministration von IT-Systemen über externe Schnittstellen, sowie von der Fernwartung von Geräten und Komponenten durch die jeweiligen Hersteller oder Zulieferer, die im Baustein *OPS.2.4 Fernwartung* betrachtet wird.

Gegenstand des Bausteins sind übergreifende Anforderungen an den Administrationsprozess als solchen. Spezifische Anforderungen an das Management einzelner IT-Systeme und -Komponenten werden im Baustein *OPS.1.1.2 Netz- und Systemmanagement* behandelt. Dort finden sich entsprechend Anforderungen, wie Systeme installiert und in Betrieb genommen werden, wie Änderungen und Wartungsarbeiten durchgeführt oder Systeme ausgesondert werden.

Die weiteren Bausteine des Bereichs *OPS.1.1 Kern-IT-Betrieb* beschreiben Aspekte des IT-Betriebs, die zusätzlich zum vorliegenden Baustein relevant sind. Sie sollen daher in Ergänzung zu diesem Baustein zusätzlich betrachtet und modelliert werden.

Eine besondere Sicherheitsrelevanz hat in einer Institution die ordnungsgemäße Administration von Benutzern und Rechten. Deshalb wird dieses Thema ebenfalls in einem eigenen Baustein behandelt (siehe *ORP.4 Identitäts- und Berechtigungsmanagement).*

Die im vorliegenden Baustein beschriebenen Anforderungen sind auch dann anzuwenden, wenn administrative Aufgaben durch Dritte durchgeführt werden. Besondere Anforderungen für solche Fälle werden zusätzlich in den Bausteinen *OPS.2.1 Outsourcing für Kunden und OPS.3.1 Outsourcing für Dienstleister* beschrieben.

Weiterhin bezieht sich der Baustein Ordnungsgemäße IT-Administration auf den Regelbetrieb. In Ausnahmesituationen, insbesondere bei einem möglichen IT-Angriff und der Kompromittierung von Systemen, sind abweichende Anforderungen zu beachten, die in den entsprechenden Bausteinen aus dem Bereich *DER.2 Security Incident Management* beschrieben werden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich ordnungsgemäße IT-Administration von besonderer Bedeutung:

2.1 Versäumnisse durch ungeregelte Zuständigkeiten

Sofern die IT-Organisation die administrativen Zuständigkeiten, z. B. in den Bereichen Planung, Installation, Dokumentation, Patch-Management und Überwachung nicht klar geregelt hat oder die Regelungen den beteiligten Mitarbeitern nicht bekannt und verständlich sind, kann das zur Folge haben, dass sicherheitsrelevante Aufgaben aus diesen Bereichen nicht oder nicht systematisch durchgeführt werden. Typische Beispiele sind eine unklare Abgrenzung der Zuständigkeiten zwischen IT und Telekommunikationstechnik, zwischen Büro-IT und Fertigungsanlagen oder zwischen Anwendungs- und Plattformbetrieb.

2.2 Personalausfall von Kernkompetenzträgern

Auch Administratoren können ungeplant oder längerfristig ausfallen. Ohne eingearbeitete Vertreter ist nicht sichergestellt, dass die von ihnen betreuten Systeme und Anwendungen ordnungsgemäß und sicher weiterbetrieben werden können. Administratoren bauen zum Teil sehr umfangreiches Detailwissen zu den von ihnen betreuten Systemen und Anwendungen auf, das einerseits die eingesetzten Produkte und Lösungen, andererseits aber gerade auch Besonderheiten der Einsatzumgebung und der spezifischen Konfiguration umfasst. Mit diesem Wissen können sie Fehlersituationen schnell erkennen und Anforderungen einfacher umsetzen, was häufig dazu führt, dass gerade bei komplexen Systemen die Administration durch einzelne Personen erfolgt. Fällt diese Person aus, ist auch das Wissen für die Institution nicht mehr verfügbar.

2.3 Missbrauch von administrativen Berechtigungen

Administrative Berechtigungen erlauben es, umfassend auf Dokumente, Kommunikationsinhalte und Datenbanken zuzugreifen. Administratoren können diese weitreichenden Berechtigungen nicht nur dazu benutzen, die ihnen übertragenen Aufgaben zu erfüllen, sondern auch für eigene Zwecke oder im Sinne von Dritten. So könnten sie z. B. Personalunterlagen einsehen oder Kommunikationsvorgänge von Kollegen mitlesen. Weiterhin könnten auch Dritte durch Druck oder andere Anreize auf Administratoren einwirken, um mit ihrer Hilfe missbräuchlich auf Daten oder Systeme zuzugreifen.

2.4 Erleichterung von Angriffen

Die privilegierten Systemzugänge der Administratoren stehen häufig im Fokus von Angreifern. Werden administrative Aufgaben nicht ordnungsgemäß wahrgenommen, so können dadurch Angriffe auf den Informationsverbund erheblich erleichtert werden. So können durch Fahrlässigkeit Fehler in der

Konfiguration entstehen, vorgesehene Schutzmaßnahmen nicht oder nur unzulänglich umgesetzt oder auftretende Verdachtsmomente nicht verfolgt werden. Ursachen dafür sind z. B. ein fehlendes Sicherheitsbewusstsein, hoher Zeitdruck oder fehlende Prozesse und Verfahrensweisen. Daraus können sich Schwachstellen ergeben, die von Angreifern ausgenutzt werden könnten.

2.5 Störung des Betriebs

Administrative Tätigkeiten beeinflussen unmittelbar den Betrieb von IT-Systemen und Anwendungen. So können zum Beispiel laufende Benutzersitzungen abgebrochen werden, wenn IT-Systeme neu gestartet werden, oder berechtigte Zugriffe verhindert werden, wenn ein Firewall-Regelwerk angepasst wird. Werden solche Vorgänge ausgeführt, ohne zu berücksichtigen, wie sie sich auf die Benutzer auswirken und ohne sie mit den betroffenen Bereichen abzustimmen, kann der Betrieb erheblich gestört werden.

2.6 Fehlende Aufklärungsmöglichkeiten für Vorfälle

Mängel in der Dokumentation des IT-Betriebs oder fehlende Aufzeichnungen können dazu führen, dass IT-Sicherheitsvorfälle nicht aufgeklärt oder nachverfolgt werden können. Da bei Sicherheitsvorfällen häufig nicht einfach erkennbar ist, wie z. B. der Angriff abgelaufen ist, welches Ausmaß er hatte oder wie manipuliert wurde, muss das erst durch geeignete Untersuchungen ermittelt werden. Das setzt jedoch voraus, dass beispielsweise der Sollzustand von Systemen vor dem Sicherheitsvorfall dokumentiert und prüfbar ist, oder dass ordnungsgemäße von unbefugten Änderungen an Systemen anhand geeigneter Aufzeichnungen unterschieden werden können. Fehlen entsprechende Informationen, so können Vorfälle nur schwer oder überhaupt nicht mehr aufgeklärt werden. Auch eine gerichtsfeste Beweisführung gegenüber den Tätern ist in solchen Fällen nicht mehr möglich.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Ordnungsgemäße IT-Administration aufgeführt. Grundsätzlich ist der Leiter IT für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Leiter IT
Weitere Verantwortliche	IT-Betrieb, Informationssicherheitsbeauftragter (ISB), Leiter Personal

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

OPS.1.1.2.A1 Personalauswahl für administrative Tätigkeiten [Leiter Personal]

Wenn Mitarbeiter administrative Aufgaben innerhalb der IT-Umgebung übernehmen sollen, MÜSSEN sie unter Berücksichtigung der Sicherheitsanforderungen der von ihnen betreuten Systeme und Anwendungen folgende Kriterien erfüllen:

- Die Mitarbeiter MÜSSEN über die notwendige fachliche Qualifikation verfügen, um die ihnen übertragenen Aufgaben ordnungsgemäß bewältigen zu können. Es MÜSSEN weiterhin ausreichende Kenntnisse zu den jeweils betreuten IT-Systemen, Anwendungen und Plattformen vorhanden sein. Die Mitarbeiter MÜSSEN die in der Institution für die Dokumentation verwendete Sprache beherrschen und über ausreichende Englischkenntnisse zum Verständnis typischer IT-Dokumentationen verfügen.

- Die Mitarbeiter MÜSSEN die ihnen übertragenen Aufgaben zuverlässig und sorgfältig erledigen können.
- Es MUSS eine Rollentrennung von administrativen und kontrollierenden Rollen (z.B. Revision) vorgenommen werden.

Die Administratoren und deren Vertreter MÜSSEN ausreichend Zeit zur sorgfältigen Erfüllung ihrer Aufgaben haben. Alle Administratoren und deren Vertreter MÜSSEN ausreichend Möglichkeiten zur Fortbildung erhalten

Diese Anforderungen MÜSSEN auch dann erfüllt werden, wenn administrative Aufgaben an Dritte übertragen werden.

OPS.1.1.2.A2 Vertretungsregelungen und Notfallvorsorge

Für alle administrativen Aufgaben und Verantwortlichkeiten MÜSSEN Vertretungsregelungen getroffen werden.

Es MUSS sichergestellt sein, dass benannte Vertreter auf die zu betreuenden IT-Systeme zugreifen können. Um auch in Notfallsituationen administrativ auf Systeme und Anwendungen zugreifen zu können, SOLLTEN entsprechende Notfalluser mit Administrationsrechten eingerichtet werden.

OPS.1.1.2.A3 Geregelte Einstellung von IT-Administratoren [Leiter Personal]

Wenn Mitarbeiter administrative Aufgaben innerhalb der IT-Umgebung übernehmen, MÜSSEN sie in ihre Tätigkeit, insbesondere in die vorhandene IT-Architektur und die von ihnen zu betreuenden IT-Systeme und Anwendungen eingewiesen werden. Die in der Institution gültigen und für ihre Tätigkeit relevanten Sicherheitsbestimmungen MÜSSEN den IT-Administratoren bekannt gemacht werden. Auch MÜSSEN sie dazu verpflichtet werden, die relevanten Datenschutzgesetze und andere gesetzliche und betriebliche Regelungen einzuhalten.

Diese Anforderungen MÜSSEN auch dann erfüllt werden, wenn administrative Aufgaben an Dritte übertragen werden.

OPS.1.1.2.A4 Beendigung der Tätigkeit als IT-Administrator [Leiter Personal]

Wenn IT-Administratoren von ihren Aufgaben wieder entbunden werden, MÜSSEN alle ihnen zugewiesenen persönlichen Administrationskennungen gesperrt werden. Es MUSS geprüft werden, welche Passwörter die ausscheidenden Mitarbeiter darüber hinaus noch kennen, z. B. Superuser-Zugänge, Notfalluser, WLAN-Passwörter. Solche Passwörter MÜSSEN geändert werden. Den Mitarbeitern ausgehändigte Geräte, Speichermedien und Zugangsmittel (z. B. Token, Chipkarten) MÜSSEN vollständig zurückgegeben werden.

Weiterhin MUSS geprüft werden, ob die ausscheidenden Mitarbeiter gegenüber Dritten als Ansprechpartner benannt wurden. z. B. in Verträgen oder als Admin-C-Eintrag bei Internet-Domains. In diesem Fall MÜSSEN die betroffenen Parteien informiert und neue Ansprechpartner festgelegt werden. Die Benutzer der betroffenen IT-Systeme und Anwendungen MÜSSEN darüber informiert werden, dass der bisherige IT-Administrator ausgeschieden ist.

Diese Anforderungen MÜSSEN auch dann erfüllt werden, wenn administrative Aufgaben an Dritte übertragen wurden und die dort beschäftigten Mitarbeiter aus ihrer Tätigkeit ausscheiden.

OPS.1.1.2.A5 Administrationskennungen

Jeder Administrator und jeder Vertreter eines Administrators MUSS eine eigene, eindeutige Administratorkennung haben. Die vergebenen Administrationsrechte MÜSSEN sich aus den Erfordernissen der jeweils übernommenen IT-Administrationsaufgaben ableiten.

Administratoren DÜRFEN unter diesen Kennungen nur administrative Arbeiten durchführen. Sie DÜRFEN NICHT für Routinetätigkeiten benutzt werden, für die keine erweiterten Berechtigungen erforderlich sind, z. B. E-Mail-Kommunikation, Informationsrecherche im Internet. Für solche Aufgaben MÜSSEN den IT-Administratoren zusätzlich persönliche, nicht-privilegierte Konten eingerichtet werden.

OPS.1.1.2.A6 Schutz administrativer Kennungen

Administrationskennungen MÜSSEN durch geeignete Authentisierungsmechanismen angemessen geschützt sein. Werden dafür Passwörter benutzt, DÜRFEN gleichartige Passwörter NICHT für IT-Systeme in anderen Schutzzonen verwendet werden.

Für Administrationszugriffe MÜSSEN sichere Protokolle verwendet werden, wenn dies nicht über eine lokale Konsole erfolgt. Diese MÜSSEN sicherstellen, dass die Kommunikation nach dem Stand der Technik verschlüsselt ist.

Jeder Anmeldevorgang über eine Administrationskennung (Login) MUSS protokolliert werden, sodass nachvollziehbar ist, wann, auf welchem Weg und unter welcher Nutzerkennung auf das System zugegriffen wurde.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Ordnungsgemäße IT-Administration. Sie SOLLTEN grundsätzlich umgesetzt werden.

OPS.1.1.2.A7 Regelung der IT-Administrationstätigkeit [Leiter Personal]

Die Befugnisse, Aufgaben und Pflichten der IT-Administratoren SOLLTEN in einer Arbeitsanweisung oder Richtlinie verbindlich festgeschrieben werden. Die Aufgabenverteilung zwischen den einzelnen Administratoren SOLLTE so vorgenommen werden, dass einerseits Überschneidungen in den Zuständigkeiten vermieden werden und andererseits keine Administrationslücken entstehen. Die Regelungen SOLLTEN regelmäßig aktualisiert werden. Die Vorgaben SOLLTEN insbesondere eigenmächtige Änderungen der IT-Administratoren im Informationsverbund ausschließen, soweit diese über die ihnen explizit übertragenen Aufgaben hinausgehen und nicht notwendig sind, um einen Sicherheitsvorfall oder Störfall abzuwenden.

OPS.1.1.2.A8 Administration von Fachanwendungen [IT-Betrieb]

Die in diesem Baustein aufgeführten Basisanforderungen SOLLTEN auch für Mitarbeiter mit administrativen Aufgaben für einzelne Fachanwendungen durchgängig umgesetzt werden. Die Aufgabenteilung zwischen Anwendungs- und Systemadministration SOLLTE klar definiert und schriftlich festgehalten werden. Zwischen den Verantwortlichen für die System- und Fachanwendungsadministration SOLLTEN Schnittstellen definiert sein (z. B. Ansprechpartner, Kommunikationswege, regelmäßiger Austausch).

Wenn administrativ in den Anwendungsbetrieb eingegriffen wird (z. B. Versionswechsel, Wartungsfenster), SOLLTE das im Vorfeld mit dem Fachbereich abgestimmt sein und die Bedürfnisse des Fachbereichs berücksichtigen.

OPS.1.1.2.A9 Ausreichende Ressourcen für den IT-Betrieb

Es SOLLTEN ausreichende Personal- und Sachressourcen bereitgestellt werden, um die anfallenden administrativen Aufgaben ordnungsgemäß zu bewältigen. Dabei SOLLTE berücksichtigt werden, dass auch für unvorhersehbare Tätigkeiten entsprechende Kapazitäten vorhanden sein müssen, insbesondere um sicherheitsrelevante Ereignisse zu behandeln und aufzuklären.

Die Ressourcenplanung SOLLTE in regelmäßigen Zyklen, z. B. jährlich, geprüft und den aktuellen Erfordernissen angepasst werden.

OPS.1.1.2.A10 Fortbildung und Information [Leiter Personal]

Für die eingesetzten IT-Administratoren SOLLTEN geeignete Fort- und Weiterbildungsmaßnahmen ergriffen werden, damit sie immer auf dem aktuellen Stand der Technik sind. Dabei SOLLTEN auch technische Entwicklungen berücksichtigt werden, die noch nicht eingesetzt, aber für die Institution in abseh-

barer Zeit wichtig werden könnten. Die Fortbildungsmaßnahmen SOLLTEN durch einen Schulungsplan untersetzt werden und das gesamte Team berücksichtigen, sodass alle erforderlichen Qualifikationen im Team mehrfach vorhanden sind.

Administratoren SOLLTEN sich regelmäßig über die Sicherheit der von ihnen betreuten Systeme, Dienste und Protokolle informieren, vor allem über aktuelle Gefährdungen und Sicherheitsmaßnahmen.

OPS.1.1.2.A11 Dokumentation von IT-Administrationstätigkeiten [IT-Betrieb]

Systemänderungen SOLLTEN in geeigneter Form nachvollziehbar dokumentiert werden. Aus der Dokumentation SOLLTE hervorgehen,

- welche Änderungen erfolgt sind,
- wann die Änderungen erfolgt sind,
- wer die Änderungen durchgeführt hat,
- auf welcher Grundlage bzw. aus welchem Anlass die Änderungen erfolgt sind.

OPS.1.1.2.A12 Regelungen für Wartungs- und Reparaturarbeiten [IT-Betrieb]

IT-Systeme SOLLTEN regelmäßig gewartet werden. Es SOLLTE geregelt sein, welche Sicherheitsaspekte bei Wartungs- und Reparaturarbeiten zu beachten sind und wer für die Wartung oder Reparatur von Geräten verantwortlich ist. Mitarbeiter SOLLTEN wissen, dass Wartungspersonal bei Arbeiten im Haus beaufsichtigt werden muss. Durchgeführte Wartungsarbeiten SOLLTEN dokumentiert werden.

OPS.1.1.2.A13 Absicherung von Fernwartung [IT-Betrieb, Informationssicherheitsbeauftragter (ISB)]

Fernwartung SOLLTE nur durchgeführt werden, wenn angemessene Sicherheitsmaßnahmen ergriffen wurden. Es SOLLTE sichergestellt werden, dass Fernwartungszugriffe immer nur vom lokalen IT-System initiiert werden können. Die Durchführung der Fernwartung SOLLTE ausreichend protokolliert werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.1.1.2.A14 Sicherheitsüberprüfung von Administratoren (CIA)

Im Hochsicherheitsbereich SOLLTE eine zusätzliche Sicherheitsüberprüfung durchgeführt werden um die Vertrauenswürdigkeit von Mitarbeitern zu bestätigen.

OPS.1.1.2.A15 Aufteilung von Administrationstätigkeiten (CI)

Es SOLLTEN unterschiedliche Administrationsrollen für Teilaufgaben eingerichtet werden. Bei der Abgrenzung der Aufgaben SOLLTEN die Art der Daten und die vorhandene Systemarchitektur berücksichtigt werden.

OPS.1.1.2.A16 Zugangsbeschränkungen für administrative Zugänge (CIA)

Bei erhöhtem Schutzbedarf SOLLTE der Zugang zu administrativen Oberflächen oder Schnittstellen mit Filter- und Separierungsmaßnahmen technisch beschränkt werden, d. h. sie SOLLTEN für Personen außerhalb der zuständigen IT-Administrationsteams nicht erreichbar sein. Administrative Zugriffe auf IT-Systeme in anderen Schutzzonen SOLLTEN stets mittelbar über einen Sprungserver in der jeweiligen Sicherheitszone erfolgen. Zugriffe von anderen Systemen oder aus anderen Sicherheitszonen heraus SOLLTEN abgewiesen werden.

OPS.1.1.2.A17 IT-Administration im Vier-Augen-Prinzip (CI)

Bei besonders sicherheitskritischen Systemen SOLLTE der Zugang zu Kennungen mit administrativen Berechtigungen so realisiert werden, dass dafür zwei Mitarbeiter erforderlich sind. Dabei SOLLTE jeweils ein IT-Administrator die anstehenden administrativen Tätigkeiten ausführen, während er von einem weiteren IT-Administrator kontrolliert wird.

OPS.1.1.2.A18 Durchgängige Protokollierung administrativer Tätigkeiten (CI)

Administrative Tätigkeiten SOLLTEN möglichst protokolliert werden. Bei besonders sicherheitskritischen Systemen SOLLTEN alle administrativen Zugriffe durchgängig und vollständig protokolliert werden. Die ausführenden IT-Administratoren SOLLTEN dabei selbst keine Berechtigung haben, die aufgezeichneten Protokolldateien zu verändern oder zu löschen. Die Protokolldateien SOLLTEN für eine Zeitdauer aufbewahrt werden, die dem Schutzbedarf angemessen ist und die es ermöglicht, nachträgliche Eingriffe in das System aufzuklären.

OPS.1.1.2.A19 Berücksichtigung von Hochverfügbarkeitsanforderungen [Informationssicherheitsbeauftragter (ISB)] (A)

Die IT-Administratoren SOLLTEN analysieren, für welche der von ihnen betreuten Systeme und Netze Hochverfügbarkeitsanforderungen bestehen. Für diese Bereiche SOLLTEN sie sicherstellen, dass die eingesetzten Komponenten und Architekturen sowie die zugehörigen Betriebsprozesse geeignet sind, um diese Anforderungen zu erfüllen. Dies erfordert im Regelfall eine umfassende Hochverfügbarkeitsplanung.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [HVK] Hochverfügbarkeitskompendium
  BSI, (zuletzt abgerufen am 28.09.2017)
  https://www.bsi.bund.de/DE/
  Themen/Sicherheitsberatung/Hochverfuegbarkeit/HVKompendium/hvkompendium_node.html

- [ISF] The Standard of Good Practice
  Information Security Forum (ISF), 06.2016

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Ordnungsgemäße IT-Administration" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.33 Personalausfall

G 0.35 Nötigung, Erpressung oder Korruption

G 0.37 Abstreiten von Handlungen

G 0.42 Social Engineering

Elementare Gefährdungen / Anforderungen	G 0.14	G 0.16	G 0.21	G 0.22	G 0.27	G 0.29	G 0.30	G 0.31	G 0.32	G 0.33	G 0.35	G 0.37	G 0.42
OPS.1.1.2.A1	x	x	x	x				x	x		x		
OPS.1.1.2.A2										x			
OPS.1.1.2.A3	x	x	x	x		x	x		x		x		x
OPS.1.1.2.A4	x		x	x			x		x		x	x	
OPS.1.1.2.A5	x		x	x			x					x	
OPS.1.1.2.A6	x		x	x			x					x	
OPS.1.1.2.A7	x		x	x		x	x		x				
OPS.1.1.2.A8							x	x	x				
OPS.1.1.2.A9					x			x		x			
OPS.1.1.2.A10								x					
OPS.1.1.2.A11				x			x		x			x	
OPS.1.1.2.A12	x	x	x	x		x	x						x
OPS.1.1.2.A13	x		x	x			x		x			x	
OPS.1.1.2.A14	x	x	x	x			x		x				
OPS.1.1.2.A15			x	x					x		x		x
OPS.1.1.2.A16	x		x	x			x						
OPS.1.1.2.A17	x		x	x	x		x	x	x	x	x	x	x
OPS.1.1.2.A18	x		x	x			x		x			x	
OPS.1.1.2.A19					x					x			

OPS.1.1: Kern-IT-Betrieb / Kernaufgaben

OPS.1.1.3 Patch- und Änderungsmanagement

1 Beschreibung

1.1 Einleitung

Die immer schnellere IT-Entwicklung und die steigenden Anforderungen der Benutzer stellen viele Behörden und Unternehmen vor die Aufgabe, die Komponenten ihrer Informationstechnik korrekt und zeitnah zu aktualisieren. Auch zeigt sich in der Praxis, dass Sicherheitslücken oder Betriebsstörungen häufig auf fehlerhafte oder nicht erfolgte Patches und Änderungen zurückzuführen sind. Ein fehlendes oder vernachlässigtes Patch- und Änderungsmanagement führt also schnell zu Lücken in der Sicherheit der einzelnen Komponenten und damit zu möglichen Angriffspunkten.

Aufgabe des Patch- und Änderungsmanagements ist es allgemein, verändernde Eingriffe in Anwendungen, Infrastruktur, Dokumentationen, Prozessen und Verfahren steuer- und kontrollierbar zu gestalten.

1.2 Zielsetzung

In diesem Baustein wird aufgezeigt, wie ein funktionierendes Patch- und Änderungsmanagement in einer Institution aufgebaut und wie der entsprechende Prozess kontrolliert und optimiert werden kann.

1.3 Abgrenzung

Die Beschreibungen in diesem Baustein konzentrieren sich auf den IT-Betrieb, können aber auch sinngemäß in anderen Geschäftsprozessen umgesetzt werden. Mit Änderungsmanagement wird die Aufgabe bezeichnet, Änderungen zu planen und zu steuern. Da dieser Prozess sehr aufwändig ist, zielen die Standard-Anforderungen des Bausteins vor allem auf größere Informationsverbünde. Für kleinere Institutionen ist die Erfüllung der Standard-Anforderungen zu prüfen, der Aufwand sollte hier aber nicht über den Nutzen gestellt werden. Das Patchmanagement stellt einen Teilbereich bzw. speziellen Prozess innerhalb des Änderungsmanagements dar, der auf die Aktualisierung von Software zielt und in jedem Fall anzuwenden ist. In den einzelnen Bausteinen der Schichten SYS und APP finden sich zusätzliche Anforderungen bezüglich des Patchmanagements, wo dies erforderlich ist.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Patch- und Änderungsmanagement von besonderer Bedeutung:

2.1 Mangelhaft festgelegte Verantwortlichkeiten

Durch mangelhaft festgelegte, sich überschneidende oder ungeklärte Verantwortlichkeiten können beispielsweise Änderungsanforderungen langsamer kategorisiert und priorisiert werden und sich dadurch insgesamt die Verteilung von Patches und Änderungen verzögert. Auch wenn Patches und Änderungen vorschnell ohne Testlauf und Berücksichtigung aller (fachlichen) Aspekte freigegeben werden, kann sich das gravierend auf die Sicherheit auswirken.

Im Extremfall können mangelhaft festgelegte Verantwortlichkeiten die gesamte Institution komplett oder in großem Umfang beeinträchtigen. Störungen im Betrieb wirken sich auf die Verfügbarkeit aus. Werden sicherheitsrelevante Patches nicht oder verspätet verteilt, können die Vertraulichkeit und Integrität beeinträchtigt werden.

2.2 Mangelhafte Kommunikation beim Änderungsmanagement

Wenn das Patch- und Änderungsmanagement innerhalb der Institution wenig akzeptiert wird oder die beteiligten Personen mangelhaft kommunizieren, kann das dazu führen, dass Änderungsanforderungen verzögert bearbeitet werden, oder über eine Änderungsanforderung falsch entschieden wird.

Dadurch kann das Sicherheitsniveau insgesamt verringert und der IT-Betrieb kann ernsthaft gestört werden. In jedem Fall wird bei mangelhafter Kommunikation der Änderungsprozess ineffizient, da oft zu viel Zeit und Ressourcen investiert werden müssen. Dies wirkt sich negativ auf die Reaktionsfähigkeit der Institution aus und kann im Extremfall dazu führen, dass Sicherheitslücken entstehen oder wichtige Geschäftsziele nicht erreicht werden.

2.3 Mangelhafte Berücksichtigung von Geschäftsprozessen

Ungeeignete Änderungen können unter anderem den reibungslosen Ablauf der Geschäftsprozesse beeinträchtigen oder gar dazu führen, dass die beteiligten IT-Systeme komplett ausfallen. Auch ein noch so umfangreiches Testverfahren kann nicht vollkommen ausschließen, dass sich eine Änderung im späteren Produktivbetrieb als fehlerbehaftet erweist.

Wird im Änderungsprozess die Auswirkung, Kategorie oder Priorität einer eingereichten Änderungsanforderung hinsichtlich der Geschäftsprozesse falsch eingeschätzt, kann sich das angestrebte Sicherheitsniveau verringern. Zu solchen Fehleinschätzungen kommt es überwiegend, wenn sich die IT-Verantwortlichen und die zuständigen Fachabteilungen nicht ausreichend abstimmen.

2.4 Unzureichende Ressourcen beim Patch- und Änderungsmanagement

Für ein wirkungsvolles Patch- und Änderungsmanagement sind angemessene personelle, zeitliche und finanzielle Ressourcen erforderlich. Sind diese nicht verfügbar, können beispielsweise die notwendigen Rollen mit ungeeigneten Personen besetzt werden. Auch können so Schnittstellen für bestimmte Informationen, beispielsweise zwischen der IT und den entsprechenden Ansprechpartnern in den Fachbereichen, nicht geschaffen werden, oder die erforderlichen Kapazitäten für die Infrastruktur der Test- und Verteilungsumgebungen werden nicht bereitgestellt. Können die personellen, zeitlichen und finanziellen Mängel im Regelbetrieb häufig noch ausgeglichen werden, zeigen sie sich unter hohem Zeitdruck, beispielsweise wenn Notfallpatches eingespielt werden müssen, um so deutlicher.

2.5 Probleme bei der automatisierten Verteilung von Patches und Änderungen

Häufig werden Patches und Änderungen nicht manuell, sondern zentral softwareunterstützt verteilt. Wird eine solche Software benutzt, können fehlerhafte Patches und Änderungen im gesamten Informationsverbund ausgebracht werden, wodurch massenhafte Sicherheitsprobleme entstehen können. Besonders gravierend ist es, wenn auf vielen Systemen gleichzeitig Software installiert wird, die Sicherheitslücken enthält.

Treten nur vereinzelte Fehler auf, lassen sie sich oft per Hand beheben. Problematisch wird es aber, wenn IT-Systeme dauerhaft nicht im LAN erreichbar sind. Ein Beispiel sind Außendienstmitarbeiter, die ihre IT-Systeme nur selten und unregelmäßig an das LAN anschließen. Wenn das Werkzeug so konfiguriert wird, dass die Aktualisierungen nur innerhalb eines bestimmten Zeitraums verteilt werden und dann nicht alle IT-Systeme erreichbar sind, können diese Systeme nicht aktualisiert werden.

2.6 Mangelhafte Wiederherstellungsoptionen beim Patch- und Änderungsmanagement

Wenn Patches oder Änderungen verteilt werden, ohne dass eine Wiederherstellungsoption vorgesehen ist, oder wenn die Wiederherstellungsroutinen der eingesetzten Software nicht oder nicht angemessen wirksam sind, kann fehlerhaft aktualisierte Software nicht zeitnah korrigiert werden. Dadurch können wichtige IT-Systeme ausfallen und hohe Folgeschäden entstehen. Neben der Integrität von Daten ist hier vor allem die Verfügbarkeit gefährdet.

2.7 Mangelhafte Berücksichtigung von mobilen Endgeräten

Mobile Endgeräte sind eine besondere Herausforderung für das Änderungsmanagement, da sie wegen ihrer wechselnden Einsatzorte und ihrer Anbindung an Funknetze nicht immer in die automatisierte Verteilung von Patches und Änderungen eingebunden sind. Auch sind Bandbreite und stabile Datenübertragung bei mobilen Endgeräten nicht immer gewährleistet. Werden solche Geräte im Patch- und Änderungsmanagement nicht gesondert berücksichtigt, können Patches und Änderungen möglicherweise unvollständig verteilt werden, beanspruchen mehr Zeit als geplant und bedeuten auch immer ein Sicherheitsrisiko.

2.8 Unzureichendes Notfallvorsorgekonzept für das Patch- und Änderungsmanagement

Das Patch- und Änderungsmanagement trägt dazu bei, Informationssicherheit in einer Institution technisch umzusetzen. Die von diesem Prozess verwendeten IT-Systeme sind als kritisch für den IT-Betrieb anzusehen. Dazu gehören beispielsweise die zentralen Server, die Patches und Änderungen verteilen, die Datenbanken mit den aktuellen Konfigurationen der IT-Systeme sowie die Backupserver für die Wiederherstellungspunkte. Fällt zum Beispiel der Server aus, der die Änderungen verteilt, können eventuell neu erscheinende kritische Updates nicht mehr zeitnah eingespielt werden. Des Weiteren können fehlende Datensicherungen der aktuellen Konfigurationen der IT-Systeme dazu führen, dass in einem Notfall nicht mehr sichergestellt ist, dass wichtige IT-Komponenten möglichst schnell wieder in den ursprünglichen Zustand versetzt werden können.

2.9 Fehleinschätzung der Relevanz von Patches und Änderungen

Werden Änderungen falsch priorisiert, könnten beispielsweise zuerst unwichtige Patches installiert werden. Wichtige Patches hingegen werden dann zu spät installiert und Sicherheitslücken bleiben so länger bestehen. Das Patch- und Änderungsmanagement wird oft durch softwarebasierte Werkzeuge unterstützt. Auch diese Werkzeuge können Softwarefehler enthalten und dadurch unzureichende oder fehlerhafte Angaben über eine Änderung machen. Werden die Angaben, die ein solches Tool über eine Änderung macht, nicht überprüft und auf Plausibilität getestet, kann es zu Abweichungen zwischen tatsächlicher und angenommener Umsetzung von Änderungen kommen.

2.10 Manipulation von Daten und Werkzeugen beim Änderungsmanagement

Das Patch- und Änderungsmanagement agiert oft von zentraler Stelle aus. Aufgrund seiner exponierten Stellung ist es besonders gefährdet: Wenn es Angreifern gelingen sollte, die beteiligten Server zu übernehmen, könnten sie über diesen zentralen Punkt manipulierte Softwareversionen gleichzeitig auf eine Vielzahl von IT-Systemen verteilen. Oft entstehen weitere Angriffspunkte dadurch, dass diese Systeme von externen Partnern betrieben werden (Outsourcing). Es könnten auch Wartungszugänge eingerichtet sein, die es Angreifern ermöglichen, auf den zentralen Server zur Verteilung von Änderungen zuzugreifen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen an das Patch- und Änderungsmanagement aufgeführt. Grundsätzlich ist der *IT-Betrieb* für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Administrator, Fachverantwortliche, Leiter IT, Änderungsmanager

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

OPS.1.1.3.A1 Konzept für das Patch- und Änderungsmanagement [Administrator, Fachverantwortliche]

Wenn Änderungen an IT-Komponenten, Software oder Konfigurationsdaten umgesetzt werden sollen, MUSS es dafür Vorgaben geben, die auch Sicherheitsaspekte berücksichtigen. Alle Patches und Änderungen MÜSSEN geplant, getestet, genehmigt und dokumentiert werden. Wenn Patches und Änderungen durchgeführt werden, MÜSSEN Rückfall-Lösungen vorhanden sein. An größeren Änderungen MUSS zudem das Informationssicherheitsmanagement beteiligt sein. Insgesamt MUSS sichergestellt werden, dass das angestrebte Sicherheitsniveau während und nach den Änderungen erhalten bleibt.

OPS.1.1.3.A2 Festlegung der Verantwortlichkeiten [Leiter IT]

Für alle Organisationsbereiche MÜSSEN Verantwortliche für das Patch- und Änderungsmanagement festgelegt werden. Die definierten Zuständigkeiten MÜSSEN sich auch im Berechtigungskonzept widerspiegeln. Zudem SOLLTE ein dedizierter Änderungsmanager (Change Manager) benannt werden. Alle beteiligten Personen MÜSSEN mit den Begriffen des Patch- und Änderungsmanagements, der Informationssicherheit und der kryptografischen Verfahren vertraut sein.

OPS.1.1.3.A3 Konfiguration von Autoupdate-Mechanismen [Administrator]

Es MUSS innerhalb der Strategie zum Patch- und Änderungsmanagement definiert werden, wie mit integrierten Update-Mechanismen (Autoupdate) der eingesetzten Software umzugehen ist. Insbesondere MUSS festgelegt werden, wie diese Mechanismen abgesichert und passend konfiguriert werden. Außerdem SOLLTEN neue Komponenten daraufhin überprüft werden, ob und welche Update-Mechanismen diese haben.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Patch- und Änderungsmanagement. Sie SOLLTEN grundsätzlich umgesetzt werden.

OPS.1.1.3.A4 Planung des Änderungsmanagementprozesses [Änderungsmanager]

Es SOLLTE ein Änderungsmanagementprozess definiert werden, Institutionen können sich dabei am Change-Management-Prozess der "IT Infrastructure Library" (ITIL) orientieren. Alle Änderungen von Hard- und Softwareständen sowie von Konfigurationen SOLLTEN über den Prozess des Änderungsmanagements gesteuert und kontrolliert werden.

OPS.1.1.3.A5 Umgang mit Änderungsanforderungen [Änderungsmanager]

Anträge für Änderungen SOLLTEN nach einem festgelegten Verfahren eingereicht und bearbeitet werden. Es SOLLTEN alle Änderungsanforderungen (Request for Changes, RfCs) erfasst, dokumentiert und danach vom Änderungsmanager kontrolliert werden. Nachdem eine Änderungsanforderung akzeptiert wurde, SOLLTE sie priorisiert und kategorisiert werden. Dabei SOLLTE sichergestellt sein, dass für die jeweiligen Prioritäten auch die benötigten Ressourcen verfügbar sind.

OPS.1.1.3.A6 Abstimmung von Änderungsanforderungen [Änderungsmanager]

Wenn eine Änderung umgesetzt wird, SOLLTE der zugehörige Abstimmungsprozess alle relevanten Zielgruppen berücksichtigen. Die von der Änderung betroffenen Zielgruppen SOLLTEN sich nachweisbar dazu äußern können. Auch SOLLTE es ein festgelegtes Verfahren geben, durch das wichtige Änderungsanforderungen beschleunigt werden können.

OPS.1.1.3.A7 Integration des Änderungsmanagements in die Geschäftsprozesse [Änderungsmanager]

Der Änderungsmanagementprozess SOLLTE in die Geschäftsprozesse integriert werden. So SOLLTE bei geplanten Änderungen die aktuelle Situation der davon betroffenen Geschäftsprozesse berücksichtigt werden. Alle relevanten Fachabteilungen SOLLTEN über anstehende Änderungen informiert werden. Auch SOLLTE es eine Eskalationsebene geben, deren Mitglieder der Leitungsebene der Institution angehören und die in Zweifelsfällen über Priorität und Terminplanung einer Hard- oder Software-Änderung entscheidet.

OPS.1.1.3.A8 Sicherer Einsatz von Werkzeugen für das Patch- und Änderungsmanagement [Leiter IT]

Es SOLLTEN Anforderungen und Rahmenbedingungen definiert werden, nach denen Werkzeuge für das Patch- und Änderungsmanagement ausgewählt wird. Außerdem SOLLTE eine spezifische Sicherheitsrichtlinie für die eingesetzten Werkzeuge erstellt werden.

OPS.1.1.3.A9 Test- und Abnahmeverfahren für neue Hard- und Software [Leiter IT]

Neue Hard- und Software SOLLTE getestet werden, bevor sie eingesetzt wird. Dazu SOLLTEN ausschließlich isolierte Testsysteme verwendet werden. Auch SOLLTE es für Software ein Abnahmeverfahren und eine Freigabeerklärung geben. Der Verantwortliche SOLLTE die Freigabeerklärung an geeigneter Stelle schriftlich hinterlegen. Für den Fall, dass trotz der Abnahme- und Freigabe-Verfahren im laufenden Betrieb Fehler in der Software festgestellt werden, SOLLTE es ein Verfahren zur Fehlerbehebung geben.

OPS.1.1.3.A10 Sicherstellung der Integrität und Authentizität von Softwarepaketen [Administrator]

Während des gesamten Patch- und Änderungsprozesses SOLLTE die Authentizität und Integrität von Softwarepaketen sichergestellt werden. Dazu SOLLTE geprüft werden, ob für die eingesetzten Softwarepakete Prüfsummen oder digitale Signaturen verfügbar sind. Ebenso SOLLTE darauf geachtet werden, dass die notwendigen Programme zur Überprüfung vorhanden sind.

OPS.1.1.3.A11 Kontinuierliche Dokumentation der Informationsverarbeitung [Leiter IT, Änderungsmanager]

Änderungen SOLLTEN in allen Phasen, allen Anwendungen und allen Systemen dokumentiert werden. Dazu SOLLTEN entsprechende Regelungen erarbeitet werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.1.1.3.A12 Skalierbarkeit beim Änderungsmanagement (A)

Wenn ein Werkzeug zum Änderungsmanagement benutzt wird, SOLLTE vor der Inbetriebnahme die Umsetzungsgeschwindigkeit sorgfältig geprüft werden. Es SOLLTEN Unterbrechungspunkte definiert werden können, an denen die Verteilung einer fehlerhaften Änderung gestoppt wird.

OPS.1.1.3.A13 Erfolgsmessung von Änderungsanforderungen (IA)

Um zu überprüfen, ob eine Änderung erfolgreich war, SOLLTE der Änderungsmanager sogenannte Nachtests durchführen. Dazu SOLLTE er geeignete Referenzsysteme als Qualitätssicherungssysteme auswählen. Die Ergebnisse der Nachtests SOLLTEN im Rahmen des Änderungsprozesses dokumentiert werden.

OPS.1.1.3.A14 Synchronisierung innerhalb des Änderungsmanagements [Änderungsmanager] (CIA)

Wenn Institutionen Änderungen an der IT-Infrastruktur vornehmen, SOLLTE der Änderungsmanagementprozess darauf reagieren. Zeitweise oder permanent nicht erreichbare Geräte SOLLTEN im Änderungsmanagementprozess durch geeignete Mechanismen berücksichtigt werden.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Patch- und Änderungsmanagement" von Bedeutung.

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.33 Personalausfall

G 0.37 Abstreiten von Handlungen

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.09	G 0.18	G 0.19	G 0.20	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.33	G 0.37	G 0.39	G 0.40	G 0.45	G 0.46
OPS.1.1.3.A1		x													
OPS.1.1.3.A2		x						x		x	x				
OPS.1.1.3.A3	x		x	x	x	x	x		x			x	x		x
OPS.1.1.3.A4		x													
OPS.1.1.3.A5		x		x		x	x	x			x				
OPS.1.1.3.A6		x				x	x	x		x	x				
OPS.1.1.3.A7		x				x	x	x		x	x				
OPS.1.1.3.A8	x		x	x	x	x	x	x	x			x	x	x	x
OPS.1.1.3.A9	x					x	x		x						
OPS.1.1.3.A10			x	x	x				x			x	x		x
OPS.1.1.3.A11		x									x				
OPS.1.1.3.A12		x				x	x	x		x					
OPS.1.1.3.A13		x													
OPS.1.1.3.A14		x						x							

OPS.1.1: Kern-IT-Betrieb / Kernaufgaben

OPS.1.1.4 Schutz vor Schadprogrammen

1 Beschreibung

1.1 Einleitung

Schadprogramme sind Programme, die in der Regel ohne Wissen und Einwilligung des Benutzers oder Besitzers eines IT-Systems schädliche Funktionen auf diesem ausführen. Diese Funktionen können ein breites Feld abdecken, das von Spionagemöglichkeiten über Erpressung (sogenannte Ransomware) bis hin zur Sabotage und Zerstörung von Informationen oder gar Geräten reicht.

Schadprogramme können grundsätzlich auf allen Betriebssystemen und IT-Systemen auftreten. Dazu gehören neben klassischen IT-Systemen wie Clients und Servern auch mobile Geräte wie Smartphones. Netzkomponenten wie Router, Industriesteuerungsanlagen und sogar IoT-Geräte, wie vernetzte Kameras, sind heutzutage ebenfalls vielfach durch Schadprogramme gefährdet.

Schadprogramme verbreiten sich auf klassischen IT-Systemen zumeist über E-Mail-Anhänge, manipulierte Webseiten (Drive-by-Downloads) oder Datenträger. Smartphones werden in der Regel über die Installation von schädlichen Apps infiziert, auch Drive-by-Downloads sind möglich. Darüber hinaus sind offene Netzschnittstellen, fehlerhafte Konfigurationen und Softwareschwachstellen häufige Einfallstore auf allen IT-Systemen.

In diesem Baustein wird der Begriff "Viren-Schutzprogramm" verwendet. "Viren" stehen dabei als Synonym für alle Arten von Schadprogrammen. Gemeint ist also ein Programm zum Schutz vor jeglicher Art von Schadprogrammen.

1.2 Zielsetzung

Dieser Baustein beschreibt die Vorgehensweise, einen Schutz gegen Schadprogramme zu erstellen und umzusetzen, um eine Institution effektiv gegen Schadprogramme zu schützen.

1.3 Abgrenzung

In diesem Baustein werden die allgemeinen Anforderungen für den Schutz gegen Schadprogramme beschrieben. Spezifische Anforderungen, um bestimmte IT-Systeme der Institution vor Schadprogrammen zu schützen, finden sich in den jeweiligen Bausteinen insbesondere der Schicht SYS, etwa in SYS.2.2.3 Client unter Windows 10. Führt ein identifiziertes Schadprogramm zu einem Sicherheitsvorfall, sollten die Anforderungen des Bausteins DER.2.1. Behandlung von Sicherheitsvorfällen berücksichtigt werden. Die Anforderungen des Bausteins DER.2.3 Bereinigung helfen dabei, identifizierte Schadprogramme zu entfernen und einen bereinigten Zustand wieder herzustellen.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Schutz vor Schadprogrammen von besonderer Bedeutung:

2.1 Softwareschwachstellen und Drive-by-Downloads

Sind IT-Systeme nicht ausreichend vor Schadprogrammen geschützt, was unter anderem auch voraussetzt, dass Patches zeitnah eingespielt und Schutzmechanismen von Anwendungsprogrammen wie Browsern richtig konfiguriert sind, können Softwareschwachstellen ausgenutzt werden, um Schadcode auszuführen. Bei den sogenannten Drive-by-Downloads reicht es beispielsweise aus, eine schädliche Website zu besuchen. Eine Schwachstelle im Browser oder in einem installierten Plug-in wie Java oder Adobe Flash kann dann ausgenutzt werden, um das IT-System zu infizieren und dem Angreifer umfangreiche Kontrolle sowie einen Zugang zum Netz einer Institution zu verschaffen. Besonders gefährdet sind hier IT-Systeme, die nicht regelmäßig aktualisiert werden, etwa viele Smartphones.

2.2 Erpressung durch Ransomware

Eine weit verbreitete Art von Schadprogrammen ist die sogenannte Ransomware. Diese verschlüsselt die Daten des infizierten IT-Systems sowie häufig auch weitere Daten, die etwa über Netzfreigaben erreichbar sind. In der Regel verwenden die Angreifer dabei Verschlüsselungsmethoden, die ohne Kenntnis des Schlüssels nicht umkehrbar sind, und erpressen damit ihre Opfer um hohe Geldsummen. Besteht kein wirksamer Schutz gegen Schadprogramme und sind keine ergänzenden Vorkehrungen wie Datensicherungen getroffen, kann es zu erheblichen Einschränkungen der Verfügbarkeit von Informationen sowie zu massiven finanziellen sowie Image-Schäden kommen.

2.3 Gezielte Angriffe und Social Engineering

Institutionen werden häufig mit maßgeschneiderten Schadprogrammen angegriffen. Dabei werden z. B. Führungskräfte über Methoden des Social Engineerings dazu verleitet, schädliche E-Mail-Anhänge zu öffnen. Maßgeschneiderte Schadprogramme können häufig zudem nicht unmittelbar von Viren-Schutzprogrammen erkannt werden. Auch die Personalabteilung einer Institution kann beispielsweise ein Ziel sein, indem etwa maliziöse Bewerbungsunterlagen auf elektronischem Wege zugesendet werden. Hat der Angreifer auf diese Weise ein IT-System infizieren können, so kann er sich innerhalb der Institution ausbreiten und beispielsweise Informationen entwenden, manipulieren oder zerstören.

2.4 Infektionen durch mobile Datenträger

Sind die Benutzer nicht ausreichend sensibilisiert, können auch mobile Datenträger als Einfallstor für Schadprogramme dienen. Ein Angreifer kann z. B. bösartige USB-Sticks auf dem Gelände einer Institution platzieren, die dann von unbedarften Benutzern an IT-Systeme angeschlossen werden. Gibt es keinen ausreichenden Schutz vor Schadprogrammen, kann ein Angreifer auf diesem Wege ebenfalls Zugriff auf das Netz und die Daten der Institution erlangen.

2.5 Botnetze

Über Schadprogramme können IT-Systeme einer Institution Teil von sogenannten Botnetzen werden. Ein Angreifer, der in einem solchen Botnetz häufig tausende von Systemen kontrolliert, kann diese beispielsweise einsetzen, um Spam zu versenden oder verteilte Denial-of-Service-Angriffe (DDoS) auf Dritte zu starten. Auch wenn die eigene Institution möglicherweise nicht unmittelbar geschädigt wird, kann dies trotzdem negative Auswirkungen bezüglich der Verfügbarkeit und Integrität der eigenen Dienste und IT-Systeme haben und sogar rechtliche Probleme nach sich ziehen.

2.6 Infektion von Produktionssystemen und IoT-Geräten

Neben klassischen IT-Systemen werden vermehrt auch Geräte durch Schadprogramme angegriffen, die auf den ersten Blick nicht wie offensichtliche Ziele wirken. Ein Angreifer kann beispielsweise eine über das Internet erreichbare Überwachungskamera infizieren, um zu spionieren. Aber auch eine vernetzte

Glühbirne oder eine Kaffeemaschine mit App-Steuerung kann als Eintrittspunkt in das Netz der Institution oder als Teil eines Botnetzes dienen, wenn diese Geräte nicht ausreichend vor Schadprogrammen geschützt werden. Vernetzte Produktionssysteme oder Industriesteuerungen können ebenfalls mit Schadprogrammen manipuliert oder sogar zerstört werden, was Ausfälle und viele weitere Gefährdungen für die Institution und ihre Mitarbeiter, etwa durch Brände, nach sich ziehen kann.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz vor Schadprogrammen aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der ISB ist bei allen strategischen Entscheidungen zumindest einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten IT-Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Benutzer, Fachverantwortliche

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

OPS.1.1.4.A1 Erstellung eines Konzepts für den Schutz vor Schadprogrammen

Es MUSS ein Konzept erstellt werden, welche IT-Systeme vor Schadprogrammen geschützt werden müssen. Außerdem MUSS festgehalten werden, wie der Schutz zu erfolgen hat. Ist kein verlässlicher Schutz möglich, so SOLLTEN die identifizierten IT-Systeme NICHT betrieben werden. Das Konzept SOLLTE nachvollziehbar dokumentiert werden.

OPS.1.1.4.A2 Nutzung systemspezifischer Schutzmechanismen

Es MUSS geprüft werden, welche Schutzmechanismen die verwendeten IT-Systeme sowie die darauf genutzten Betriebssysteme und Anwendungen bieten, um einen Schutz vor Schadprogrammen zu ermöglichen bzw. zu unterstützen. Diese Mechanismen MÜSSEN genutzt werden, sofern es keinen mindestens gleichwertigen Ersatz gibt oder gute Gründe dagegen sprechen. Werden sie nicht genutzt, SOLLTE dies begründet und dokumentiert werden.

OPS.1.1.4.A3 Auswahl eines Viren-Schutzprogrammes für Endgeräte

In Abhängigkeit vom verwendeten Betriebssystem, anderen vorhandenen Schutzmechanismen sowie der Verfügbarkeit geeigneter Viren-Schutzprogramme MUSS für den konkreten Einsatzzweck ein solches Schutzprogramm ausgewählt und installiert werden. Es DÜRFEN NUR Produkte für den Enterprise-Bereich mit auf die Institution zugeschnittenen Service- und Supportleistungen eingesetzt werden. Produkte für reine Heimanwender oder Produkte ohne Herstellersupport DÜRFEN NICHT im professionellen Wirk-Betrieb eingesetzt werden. Es DÜRFEN NUR Cloud-Funktionen solcher Produkte verwendet werden, bei denen keine gravierenden, nachweisbaren Daten- oder Geheimschutzaspekte dagegen sprechen.

OPS.1.1.4.A4 Auswahl eines Viren-Schutzprogrammes für Gateways und IT-Systeme zum Datenaustausch [Fachverantwortliche]

Für Gateways und IT-Systeme, die dem Datenaustausch dienen, MUSS ein geeignetes Viren-Schutzprogramm ausgewählt und installiert werden. Es DÜRFEN NUR Produkte für den Enterprise-Bereich mit auf die Institution zugeschnittenen Service- und Supportleistungen eingesetzt werden. Produkte für reine Heimanwender oder Produkte ohne Herstellersupport DÜRFEN NICHT im professionellen Betrieb eingesetzt werden. Es DÜRFEN NUR Cloud-Funktionen solcher Produkte verwendet werden, bei denen keine gravierenden, nachweisbaren Daten- oder Geheimschutzaspekte dagegen sprechen.

OPS.1.1.4.A5 Betrieb von Viren-Schutzprogrammen

Das Viren-Schutzprogramm MUSS für seine Einsatzumgebung geeignet konfiguriert werden. Die Erkennungsleistung SOLLTE dabei im Vordergrund stehen, sofern nicht Datenschutz oder Leistungs-Gründe im jeweiligen Einzelfall schwerer wiegen. Wenn sicherheitsrelevante Funktionen des Viren-Schutzprogramms nicht genutzt werden, SOLLTE dies begründet und dokumentiert werden. Bei Schutzprogrammen, die speziell für Desktop-Virtualisierung optimiert sind, SOLLTE transparent sein, ob auf bestimmte Detektionsverfahren zu Gunsten der Leistung verzichtet wird.

OPS.1.1.4.A6 Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen

Auf den damit ausgestatteten IT-Systemen MÜSSEN die Scan-Engine des Viren-Schutzprogramms sowie die Signaturen für die Schadprogramme regelmäßig aktualisiert werden. Die Häufigkeit von qualitätsgesicherten Signatur-Updates MUSS dabei den Empfehlungen des Herstellers entsprechen.

Ein Update auf neue Programmversionen SOLLTE zeitnah nach Veröffentlichung erfolgen. Bei jedem Programmupdate des Viren-Schutzprogramms SOLLTE die Änderungsdokumentation des Herstellers auf relevante Änderungen hin überprüft werden. Nachdem das Update installiert wurde, MÜSSEN die Konfigurationseinstellungen überprüft und mit den dokumentierten Vorgaben abgeglichen werden.

OPS.1.1.4.A7 Sensibilisierung und Verpflichtung der Benutzer [Benutzer]

Benutzer MÜSSEN regelmäßig über die Bedrohung durch Schadprogramme aufgeklärt werden. Sie MÜSSEN die grundlegenden Verhaltensregeln einhalten, um die Gefahr eines Befalls durch Schadprogramme zu reduzieren. Dateien aus nicht vertrauenswürdigen Quellen SOLLTEN NICHT geöffnet werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Schutz vor Schadprogrammen. Sie SOLLTEN grundsätzlich umgesetzt werden.

OPS.1.1.4.A8 Nutzung von Cloud-Diensten

Cloud-Dienste zur Verbesserung der Detektionsleistung der Viren-Schutzprogrammen SOLLTEN genutzt werden. Dabei MÜSSEN die entsprechenden Vorgaben aus den Anforderungen OPS.1.1.4.A3 Auswahl eines Viren-Schutzprogrammes für Endgeräte sowie OPS.1.1.4.A4 Auswahl eines Viren-Schutzprogrammes für Gateways und IT-Systeme zum Datenaustausch beachtet werden.

OPS.1.1.4.A9 Meldung von Infektionen mit Schadprogrammen [Benutzer]

Eingesetzte Viren-Schutzprogramm SOLLTEN automatisch eine Infektion mit einem Schadprogramm blockieren und melden. Die automatische Meldung SOLLTE an einer zentralen Stelle angenommen werden. Dabei SOLLTEN die zuständigen Mitarbeiter je nach Sachlage über das weitere Vorgehen entscheiden. Unabhängig von einer automatischen Meldung SOLLTE sich jedoch auch der Benutzer an die ihm benannten Ansprechpartner wenden, wenn der Verdacht auf eine Infektion mit einem Schadprogramm besteht. Das Vorgehen bei Meldungen und Alarmen der Viren-Schutzprogramme SOLLTE geplant, dokumentiert und getestet werden. Es SOLLTE insbesondere geregelt sein, was im Falle einer bestätigten Infektion geschehen soll.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.1.1.4.A10 Nutzung spezieller Analyseumgebungen (CIA)

Automatisierte Analysen in einer speziellen Testumgebung (basierend auf Sandboxen bzw. separaten virtuellen oder physischen Systemen) SOLLTEN für eine Bewertung von verdächtigen Dateien ergänzend herangezogen werden.

OPS.1.1.4.A11 Einsatz mehrerer Scan-Engines (CIA)

Zur Verbesserung der Erkennungsleistung SOLLTEN für besonders schutzwürdige IT-Systeme, wie Gateways und IT-Systemen zum Datenaustausch, Viren-Schutzprogramme mit mehreren alternativen Scan-Engines eingesetzt werden.

OPS.1.1.4.A12 Einsatz von Datenträgerschleusen (CIA)

Bevor insbesondere Datenträger von Dritten mit den IT-Systemen der Institution verbunden werden, SOLLTEN diese durch eine Datenträgerschleuse geprüft werden.

OPS.1.1.4.A13 Umgang mit nicht vertrauenswürdigen Dateien (CIA)

Ist es notwendig, nicht vertrauenswürdige Dateien zu öffnen, SOLLTE dies nur auf einem isolierten IT-System geschehen. Die betroffenen Dateien SOLLTEN dort z. B. in ein ungefährliches Format umgewandelt oder ausgedruckt werden, wenn sich hierdurch das Risiko einer Infektion durch Schadsoftware verringert.

OPS.1.1.4.A14 Auswahl und Einsatz von Cyber-Sicherheitsprodukten gegen gezielte Angriffe (CIA)

Bei erhöhtem Schutzbedarf und entsprechender Bedrohungslage SOLLTE der Einsatz sowie der Mehrwert von Produkten und Services geprüft werden, die im Vergleich zu herkömmlichen Viren-Schutzprogrammen einen erweiterten Schutzumfang bieten, wie z. B. Ausführung von Dateien in speziellen Analyseumgebungen, Härtung von Clients oder Kapselung von Prozessen. Vor einer Kaufentscheidung SOLLTEN Schutzwirkung und Kompatibilität zur eigenen IT-Umgebung getestet werden.

OPS.1.1.4.A15 Externe Beratung (CIA)

Bei der Erstellung eines Konzepts zum Schutz vor Schadprogrammen SOLLTE externe Unterstützung in Anspruch genommen werden, wenn das eigene Know-how oder die Marktkenntnis nicht ausreichen. Um insbesondere Leistungsproblemen innerhalb der IT-Systeme und Netze vorzubeugen und den Schutz vor Schadprogrammen sinnvoll in ein Gesamtkonzept einzufügen, SOLLTE in komplexen IT-Infrastrukturen die Implementierung von Schutzprodukten nur durch erfahrene Experten vorgenommen werden. Nach der Installation von Schutzprogrammen SOLLTE die Konfiguration einem externen Expertenreview unterzogen werden.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [ISFTS1] The Standard of Good Practice - Area TS1 Security Solutions
  insbesondere Area TS1 Security Solutions, Information Security Forum (ISF), 06.2016

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Schutz vor Schadprogrammen" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.19 Offenlegung schützenswerter Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.32 Missbrauch von Berechtigungen

G 0.36 Identitätsdiebstahl

G 0.39 Schadprogramme

G 0.42 Social Engineering

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.14	G 0.19	G 0.23	G 0.32	G 0.36	G 0.39	G 0.42	G 0.46
OPS.1.1.4.A1	x	x	x	x	x	x	x	x
OPS.1.1.4.A2	x	x	x	x	x	x		x
OPS.1.1.4.A3	x	x	x	x	x	x		x
OPS.1.1.4.A4	x	x	x	x	x	x		x
OPS.1.1.4.A5	x	x	x	x	x	x	x	x
OPS.1.1.4.A6	x	x	x	x	x	x	x	x
OPS.1.1.4.A7	x	x	x	x		x		x
OPS.1.1.4.A8	x	x	x	x	x	x	x	x
OPS.1.1.4.A9	x	x	x	x	x	x		x
OPS.1.1.4.A10	x	x	x	x	x	x		x
OPS.1.1.4.A11	x	x	x	x	x		x	x
OPS.1.1.4.A12	x	x	x	x	x	x		x
OPS.1.1.4.A13	x	x	x	x	x	x		x
OPS.1.1.4.A14	x	x	x	x	x	x		x
OPS.1.1.4.A15	x	x	x	x	x	x	x	x

OPS.1.1: Kern-IT-Betrieb / Kernaufgaben

OPS.1.1.5 Protokollierung

1 Beschreibung

1.1 Einleitung

Für einen verlässlichen IT-Betrieb sollten IT-Systeme und Anwendungen alle oder ausgewählte betriebs- und sicherheitsrelevanten Ereignisse protokollieren, d. h. sie automatisch speichern und für die Auswertung bereitstellen. Eine Protokollierung wird in vielen Institutionen eingesetzt, um Hard- und Softwareprobleme sowie Ressourcenengpässe zeitnah entdecken zu können. Aber auch Sicherheitsprobleme und Angriffe auf die betriebenen Dienste können anhand von Protokollierungsdaten nachvollzogen werden. Ebenso können mit solchen Daten durch forensische Untersuchungen Beweise gesichert werden, nachdem ein Angriff auf IT-Systeme bekannt wurde.

In jedem Informationsverbund werden lokal Protokollierungsdaten von einer Vielzahl von IT-Systemen und Anwendungen generiert. Um jedoch einen Gesamtüberblick über einen Informationsverbund zu erhalten, können die von verschiedenen IT-Systemen und Anwendungen generierten Protokollinformationen an eine dedizierte Protokollierungsinfrastruktur gesendet und dort zentral gespeichert werden. Nur so lassen sich die Protokollierungsdaten an einer Stelle auswählen, filtern und systematisch auswerten.

1.2 Zielsetzung

Der Baustein enthält Anforderungen, mit denen die Protokollierung möglichst aller sicherheitsrelevanten Ereignisse umgesetzt werden kann. Ziel ist es, alle hierfür relevanten Daten sicher zu erheben, zu speichern und geeignet für die Auswertung bereitzustellen sowie deren ordnungsgemäße Entsorgung sicherzustellen.

1.3 Abgrenzung

Im vorliegenden Baustein werden nur übergreifende Aspekte betrachtet, die für eine angemessene Protokollierung erforderlich sind. Die Protokollierung spezifischer IT-Systeme oder Anwendungen wird hier nicht behandelt, sondern in den jeweiligen Bausteinen beschrieben.

In vielen Betriebssystemen oder Anwendungen sind Protokollierungsfunktionen bereits vorhanden oder können dort mittels Zusatzprodukten integriert werden. Um diese Funktionen und die gespeicherten Protokollierungsdaten abzusichern, muss das zugrundeliegende Betriebssystem geschützt sein. Das ist jedoch nicht Bestandteil dieses Bausteins. Dafür sind die betriebssystemspezifischen Bausteine umzusetzen, z. B. SYS.1.1 *Allgemeiner Server* und SYS.2.1 *Allgemeine Clients*.

Auch ist der Baustein abzugrenzen von der Detektion (siehe DER.1 *Detektion von sicherheitsrelevanten Ereignissen*) sowie der Reaktion auf Sicherheitsvorfälle (DER.2 *Incident Management*): Beide Aspekte werden im Baustein Protokollierung nicht oder nur am Rande behandelt.

Vorgaben, wie mit personenbezogenen Daten umzugehen ist, werden im Baustein CON.2 *Datenschutz* geregelt. Wie lang und umfangreich Protokollierungsdaten archiviert werden müssen, ist darüber hinaus im Baustein OPS.1.1.2 *Archivierung* erläutert.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich der Protokollierung von besonderer Bedeutung:

2.1 Fehlende oder unzureichende Protokollierung

In einem Informationsverbund gibt es häufig IT-Systeme oder Anwendungen, bei denen die Protokollierung in der Grundeinstellung nicht aktiviert wurde. Auch können einzelne IT-Systeme und Anwendungen manchmal gar nicht protokollieren. In beiden Fällen können wichtige Informationen verloren gehen und Angriffe nicht rechtzeitig erkannt werden. Das ist jedoch auch dann möglich, wenn die Protokollierung bei einzelnen IT-Systemen genutzt wird, aber die Protokolle nicht an einer zentralen Stelle zusammengeführt werden. In Informationsverbünden ohne zentrale Protokollierung ist es schwierig sicherzustellen, dass die relevanten Protokollinformationen aller IT-Systeme erhalten und ausgewertet werden.

Weiterhin müssen Protokollierungsdaten aussagekräftige Informationen enthalten. Welche Ereignisse protokolliert werden, hängt unter anderem auch vom Schutzbedarf der jeweiligen IT-Systeme bzw. Anwendungen ab. Wird dieser missachtet, indem beispielsweise bei der Protokollierung nur auf Standard-Einstellungen der IT-Systeme bzw. Anwendungen zurückgegriffen wird, kann dies dazu führen, dass besonders relevante Sicherheitsereignisse nicht protokolliert werden. Somit werden Angriffe eventuell nicht erkannt.

2.2 Fehlerhafte Auswahl von relevanten Protokollierungsdaten

Protokollierungsdaten liefern oft wichtige Informationen, um IT-Sicherheitsvorfälle zu erkennen. Die relevanten Meldungen aus der großen Menge der verschiedenen Protokollereignisse auszuwählen ist eine besondere Herausforderung. Denn viele protokollierte Meldungen haben nur informativen Charakter und lenken von den wirklich wichtigen Meldungen ab. Werden zu viele Protokollmeldungen ausgewählt, lässt sich die Fülle von Informationen nur schwer und mit hohem Zeitaufwand auswerten.

Des Weiteren können Protokollierungsdaten verworfen oder überschrieben werden, wenn der Arbeitsspeicher oder die Festplattenkapazität des IT-Systems bzw. der Protokollierungsinfrastruktur nicht ausreichen. Werden dadurch zu wenige oder nicht genug relevante Protokollmeldungen aufgezeichnet, könnten sicherheitskritische Vorfälle unerkannt bleiben.

2.3 Fehlende Zeitsynchronisation bei der Protokollierung

Wenn in einem Informationsverbund die Zeit nicht auf allen IT-Systemen synchronisiert wird, können die Protokollierungsdaten eventuell nicht miteinander korreliert werden bzw. kann die Korrelation zu eventuell fehlerhaften Aussagen führen, da die unterschiedlichen Zeitstempel von Ereignissen keine gemeinsame Basis aufweisen. Eine fehlende Zeitsynchronisation erschwert es somit, erhobene Protokollierungsdaten auszuwerten, insbesondere wenn diese auf einem zentralen Logserver gespeichert werden. Weiterhin kann eine fehlerhafte oder fehlende Zeitsynchronisation dazu führen, dass die Protokollierung nicht zur Beweissicherung herangezogen werden kann.

2.4 Fehlplanung bei der Protokollierung

Wird die Protokollierung nicht ausreichend geplant, kann dies dazu führen, dass IT-Systeme oder Anwendungen nicht überwacht und so sicherheitsrelevante Ereignisse nicht identifiziert und angemessen behandelt werden. Ebenso können Datenschutzverstöße nicht nachvollzogen werden.

2.5 Vertraulichkeits- und Integritätsverlust von Protokollierungsdaten

Einige IT-Systeme in einem Informationsverbund generieren Protokollierungsdaten wie Benutzernamen, IP-Adressen, E-Mail-Adressen und Rechnernamen, die konkreten Personen zugeordnet werden können. Solche Informationen lassen sich kopieren, abhören und manipulieren, wenn sie nicht verschlüsselt übertragen und gesichert gespeichert werden. Dies kann dazu führen, dass Angreifer auf ver-

trauliche Informationen zugreifen oder dass durch manipulierte Protokollierungsdaten Sicherheitsvorfälle bewusst verschleiert werden. Ebenso kann ein Angreifer, wenn er an eine größere Menge von Protokollierungsdaten gelangt, diese Informationen nutzen, um die interne Struktur des Informationsverbundes aufzudecken und dadurch seine Angriffe gezielter ausrichten.

2.6 Falsch konfigurierte Protokollierung

Wenn die Protokollierung in IT-Systemen falsch konfiguriert ist, werden wichtige Informationen gar nicht oder fehlerhaft aufgezeichnet. Auch kann es sein, dass zu viele oder falsche Informationen protokolliert werden. So können zum Beispiel personenbezogene Daten unberechtigt protokolliert und gespeichert werden und die Institution kann so gegen gesetzliche Anforderungen verstoßen.

Ebenso ist es durch eine falsch konfigurierte Protokollierung möglich, dass die Protokollierungsdaten in inkonsistenten oder proprietären Formaten vorliegen. Dadurch lassen sich die Protokolle eventuell nur schwer auswerten und IT-Sicherheitsvorfälle bleiben unentdeckt.

2.7 Ausfall von Datenquellen

Liefern IT-Systeme in einem Informationsverbund nicht mehr die notwendigen Protokollierungsdaten, lassen sich Sicherheitsvorfälle nicht mehr angemessen detektieren. Ursache für Ausfälle von Datenquellen können Fehler in der Hard- und Software oder auch fehlerhaft administrierte IT-Systeme sein. Besonders wenn nicht bemerkt wird, dass Datenquellen ausgefallen sind, kann das zu einem falschen Bild der Sicherheitslage in der Institution führen. Dadurch können Angreifer z. B. sehr lange unbemerkt bleiben und geschäftskritische Informationen abgreifen oder Produktionssysteme manipulieren.

2.8 Ungenügend dimensionierte Protokollierungsinfrastruktur

Aufgrund der komplexen Informationsverbünde und vielfältigen Angriffsszenarien steigen die Anforderungen an die Protokollierung, da sehr viele Protokollierungsdaten gespeichert und verarbeitet werden müssen. Weiterhin ist es bei Sicherheitsvorfällen üblich, die Intensität der Protokollierung zu erhöhen. Ist die Protokollierungsinfrastruktur dafür jedoch nicht ausgelegt, besteht die Gefahr, dass Protokollierungsdaten unvollständig gespeichert werden. Somit lassen sich sicherheitsrelevante Ereignisse nicht mehr oder nur unzureichend auswerten und Sicherheitsvorfälle bleiben unentdeckt.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Protokollierung aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Fachverantwortliche, Informationssicherheitsbeauftragter (ISB), Leiter IT

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

OPS.1.1.5.A1 Erstellung einer Sicherheitsrichtlinie für die Protokollierung [Informationssicherheitsbeauftragter (ISB), Fachverantwortliche]

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie erstellt werden, in der nachvollziehbar Anforderungen und Vorgaben beschrieben sind, wie die Protokollierung sicher geplant, aufgebaut und betrieben werden soll. In der Richtlinie MUSS geregelt werden, wie, wo und was protokolliert werden soll. Dabei SOLLTEN sich Art und Umfang der Protokollierung am Schutzbedarf der Informationen orientieren.

Die Richtlinie MUSS vom ISB gemeinsam mit den Fachverantwortlichen erstellt werden. Sie MUSS allen für die Protokollierung verantwortlichen Mitarbeitern bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies mit dem ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse MÜSSEN dokumentiert werden.

OPS.1.1.5.A2 Festlegung von Rollen und Verantwortlichkeiten [Leiter IT]

Für die in der Protokollierungsrichtlinie (siehe OPS.1.1.5.A1 *Erstellung einer Sicherheitsrichtlinie für die Protokollierung*) als relevant definierten IT-Systeme und Anwendungen MÜSSEN Verantwortliche benannt werden. Diese MÜSSEN sicherstellen, dass die Protokollierungsrichtlinie eingehalten wird.

OPS.1.1.5.A3 Konfiguration der Protokollierung auf System- und Netzebene

Alle sicherheitsrelevanten Ereignisse von IT-Systemen und Anwendungen MÜSSEN protokolliert werden. Sofern die in der Protokollierungsrichtlinie als relevant definierten IT-Systeme und Anwendungen über eine Protokollierungsfunktion verfügen, MUSS diese benutzt werden. Wenn die Protokollierung eingerichtet wird, MÜSSEN dabei die Herstellervorgaben für die jeweiligen IT-Systeme oder Anwendungen beachtet werden. Es MUSS in angemessenen Intervallen stichpunktartig überprüft werden, ob die Protokollierung noch korrekt funktioniert. Die Intervalle MÜSSEN in der Protokollierungsrichtlinie definiert werden. Sofern betriebs- und sicherheitsrelevante Ereignisse nicht auf einem IT-System protokolliert werden können, MÜSSEN weitere IT-Systeme zur Protokollierung (z. B. von Ereignissen auf Netzebene) integriert werden.

OPS.1.1.5.A4 Zeitsynchronisation der IT-Systeme

Die Systemzeit aller protokollierenden IT-Systeme und Anwendungen MUSS immer synchron sein. Es MUSS sichergestellt sein, dass das Datum und Zeitformat der Protokolldateien einheitlich ist. Weitere Hinweise hierzu finden sich im Baustein NET.1.2 *Netz-Management*.

OPS.1.1.5.A5 Einhaltung rechtlicher Rahmenbedingungen [Informationssicherheitsbeauftragter (ISB)]

Bei der Protokollierung MÜSSEN die gesetzlichen Bestimmungen aus den aktuellen Gesetzen zum Bundes-/Landesdatenschutz eingehalten werden (siehe CON.2 *Datenschutz*). Darüber hinaus MÜSSEN eventuelle Persönlichkeitsrechte bzw. Mitbestimmungsrechte der Mitarbeitervertretungen gewahrt werden. Ebenso MUSS sichergestellt sein, dass alle weiteren relevanten gesetzlichen Bestimmungen beachtet werden. Protokollierungsdaten MÜSSEN nach einem festgelegten Prozess gelöscht werden. Es MUSS technisch unterbunden werden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Protokollierung. Sie SOLLTEN grundsätzlich umgesetzt werden.

OPS.1.1.5.A6 Aufbau einer zentralen Protokollierungsinfrastruktur

Vor allem in größeren Informationsverbünden SOLLTEN alle gesammelten sicherheitsrelevanten Protokollierungsdaten an einer zentralen Stelle gespeichert werden. Dafür SOLLTE eine zentrale Protokollierungsinfrastruktur im Sinne eines Logserver-Verbunds aufgebaut und in einem hierfür eingerichteten

Netzsegment platziert werden. Der Logserver-Verbund SOLLTE die Protokollierungsdaten von IT-Systemen und Anwendungen ausschließlich nach dem Pull-Prinzip beziehen. Wird dies von IT-Systemen und Anwendungen nicht unterstützt, SOLLTEN die Protokollierungsdaten auf vorgelagerten IT-Systemen gesammelt und dort vom Logserver-Verbund abgeholt werden. Die hierfür erforderlichen Kommunikationsverbindungen SOLLTEN restriktiv erfolgen.

Zusätzlich zu sicherheitsrelevanten Ereignissen (siehe OPS.1.1.5.A3 *Konfiguration der Protokollierung auf System- und Netzebene*) SOLLTE eine zentrale Protokollierungsinfrastruktur auch allgemeine Betriebsereignisse protokollieren, die auf einen Fehler hindeuten, z. B.:

- Ausbleiben von Protokollierungsdaten bzw. Nichterreichbarkeit eines protokollierenden IT-Systems,
- Betriebsereignisse, die auf eine außergewöhnliche Auslastung bzw. Beanspruchung einzelner Dienste hindeuten.

Die Protokollierungsinfrastruktur SOLLTE ausreichend dimensioniert sein, sodass eine Skalierung im Sinne einer erweiterten Protokollierung berücksichtigt werden kann. Dafür SOLLTEN genügen technische, finanzielle und personelle Ressourcen verfügbar sein. Falls die Protokollierungsinfrastruktur extern aufgebaut und betrieben werden soll, SOLLTE ein spezialisierter Dienstleister beauftragt werden.

OPS.1.1.5.A7 Sichere Administration von Protokollierungsservern

Der Logserver-Verbund SOLLTE ausschließlich über ein separates Managementnetz (Out-of-Band-Management) administriert werden. Für die Administrationszugriffe SOLLTE ein Berechtigungskonzept erstellt werden. Es SOLLTEN nur Administratoren auf die Protokollierungsserver zugreifen können, die speziell dafür verantwortlich sind (siehe OPS.1.1.5.A2 *Festlegung von Rollen und Verantwortlichkeiten*).

OPS.1.1.5.A8 Archivierung von Protokollierungsdaten

Für Protokollierungsdaten SOLLTE ein Archivierungskonzept erstellt werden. Dabei SOLLTEN die gesetzlich vorgeschriebenen Regelungen berücksichtigt und im Konzept dokumentiert werden (siehe auch OPS.1.2.2 *Archivierung*).

OPS.1.1.5.A9 Bereitstellung von Protokollierungsdaten für die Auswertung

Die gesammelten Protokollierungsdaten SOLLTEN mithilfe einer Protokollierungsanwendung gefiltert, normalisiert, aggregiert und korreliert werden. Die so bearbeiteten Protokollierungsdaten SOLLTEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können. Damit sich die Daten automatisiert auswerten lassen, SOLLTEN die Protokollanwendungen über entsprechende Schnittstellen für die Auswertungsprogramme verfügen. Es SOLLTE sichergestellt sein, dass bei der Auswertung die in der Protokollierungsrichtlinie definierten Sicherheitsanforderungen eingehalten werden. Auch wenn die Daten bereitgestellt werden, SOLLTEN betriebliche und interne Vereinbarungen berücksichtigt werden. Die Protokollierungsdaten SOLLTEN in Originalform aufbewahrt werden.

OPS.1.1.5.A10 Zugriffsschutz für Protokollierungsdaten

Alle Protokollierungsdaten SOLLTEN so gespeichert werden, dass keine Unbefugten darauf zugreifen können. Es SOLLTE zudem ein Zugriffskonzept erstellt werden, das regelt, wer auf welche protokollierten Daten zugreifen darf. Dabei SOLLTEN die Berechtigungen so restriktiv wie möglich vergeben werden.

Es SOLLTE sichergestellt sein, dass auf die Protokollierungsdaten grundsätzlich nur zugegriffen wird, wenn sicherheitsrelevante Vorfälle aufzuklären sind. Dabei SOLLTE nach der im Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen* festgelegten Methode vorgegangen werden. Ein solcher Zugriff SOLLTE dokumentiert werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.1.1.5.A11 Steigerung des Protokollierungsumfangs (CIA)

Bei erhöhtem Schutzbedarf von Anwendungen oder IT-Systemen SOLLTE die Menge und Art der protokollierten Ereignisse erweitert werden, sodass sicherheitsrelevante Vorfälle möglichst lückenlos nachvollziehbar sind.

Um eine Echtzeitauswertung der Protokollierungsdaten zu ermöglichen, SOLLTEN in verkürzten Zeitabständen die Protokollierungsdaten von den protokollierenden IT-Systemen und Anwendungen zentral gespeichert werden (siehe auch OPS.1.1.5.A6 *Aufbau einer zentralen Protokollierungsinfrastruktur*). Die Protokollierung SOLLTE eine Auswertung über den gesamten Informationsverbund ermöglichen.

Anwendungen und IT-Systeme, mit denen eine zentrale Protokollierung nicht möglich ist, SOLLTEN bei einem erhöhten Schutzbedarf NICHT eingesetzt werden.

OPS.1.1.5.A12 Verschlüsselung (CI)

Um Protokollierungsdaten sicher übertragen zu können, SOLLTEN sie verschlüsselt werden. Weiterhin SOLLTEN alle gespeicherten Protokolle digital signiert werden. Auch archivierte und außerhalb der Protokollierungsinfrastruktur gespeicherte Protokollierungsdaten sollten immer verschlüsselt gespeichert werden. Weitere Hinweise und Anforderungen dazu führt Baustein CON.1 *Kryptokonzept* auf.

OPS.1.1.5.A13 Hochverfügbare Protokollierungssysteme [Informationssicherheitsbeauftragter (ISB)] (A)

Bei erhöhtem Schutzbedarf SOLLTE eine hochverfügbare Protokollierungsinfrastruktur aufgebaut werden.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [ISF] The Standard of Good Practice
  Information Security Forum (ISF), 06.2016

- [NISTSP800123] NIST Special Publication 800-123
  Guide to General Server Security, NIST, 07.2008
  https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Protokollierung" von Bedeutung.

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.37 Abstreiten von Handlungen

G 0.38 Missbrauch personenbezogener Daten

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.09	G 0.14	G 0.15	G 0.18	G 0.19	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.29	G 0.30	G 0.31	G 0.32	G 0.37	G 0.38	G 0.40	G 0.45	G 0.46
OPS.1.1.5.A1				x							x					x			
OPS.1.1.5.A2				x								x		x					
OPS.1.1.5.A3	x								x	x			x						
OPS.1.1.5.A4													x						x
OPS.1.1.5.A5											x					x			
OPS.1.1.5.A6	x			x		x	x	x			x	x						x	x
OPS.1.1.5.A7			x				x	x				x							x
OPS.1.1.5.A8				x			x				x							x	x
OPS.1.1.5.A9										x	x		x						
OPS.1.1.5.A10		x			x							x		x		x			x
OPS.1.1.5.A11						x		x	x	x			x		x			x	
OPS.1.1.5.A12		x	x		x		x											x	x
OPS.1.1.5.A13	x								x	x							x	x	

OPS.1.1: Kern-IT-Betrieb / Kernaufgaben

OPS.1.1.6 Software-Tests und -Freigaben

1 Beschreibung

1.1 Einleitung

Der Einsatz von IT zur Aufgabenbewältigung setzt voraus, dass die maschinelle Datenverarbeitung soweit wie möglich fehlerfrei arbeitet, da die Einzelergebnisse in den meisten Fällen nicht mehr kontrolliert werden können. Im Zuge der Software-Tests wird deshalb überprüft, ob die betrachtete Software fehlerfrei arbeitet. Hierfür muss die Software die erforderliche Funktionalität zuverlässig bereitstellen und darf darüber hinaus keine unerwünschten Nebeneffekte haben. Mit der anschließenden Freigabe der Software durch die fachlich zuständige Organisationseinheit wird die grundsätzliche Erlaubnis erteilt, die Software produktiv in der Institution zu nutzen. Gleichzeitig übernimmt diese Organisationseinheit damit auch die Verantwortung für das IT-Verfahren, das durch die Software unterstützt wird.

Software kann an unterschiedlichen Stellen des Lebenszyklus einer Software getestet werden. So können Software-Tests bereits bei der Entwicklung, vor der Freigabe für den Produktivbetrieb oder im Zuge des Patch- und Änderungsmanagements notwendig werden. Die Software-Tests und -Freigaben sind sowohl für Eigenentwicklungen als auch beim Einsatz von Standard-Software durchzuführen.

Dieser Baustein beschreibt den Test- und Freigabeprozess für selbst entwickelte oder angepasste Software sowie für Standardsoftware. Der Test- und Freigabeprozess zeichnet sich dadurch aus, dass dieser je nach Ergebnis mehrmals durchlaufen werden kann.

1.2 Zielsetzung

Mit der Umsetzung dieses Bausteins sorgt die Institution dafür, dass eingesetzte Software den technischen und organisatorischen Anforderungen sowie dem vorliegenden Schutzbedarf der gesamten Institution oder einzelner Organisationseinheiten entspricht. Ein wesentlicher Teilaspekt ist dabei, dass sicherheitskritische Software auf bestehende Schwachstellen systematisch und methodisch überprüft wird.

1.3 Abgrenzung

Während der Baustein CON.3 *Softwareentwicklung* auf den Softwareentwicklungsprozess und die darin enthaltenen Software-Tests, die während des Entwicklungsprozesses notwendig sind, eingeht, beschreibt dieser Baustein die speziellen Anforderungen, die an ein Test- und Freigabemanagement gestellt werden. Dabei bezieht sich dieses Test- und Freigabemanagement nicht ausschließlich auf selbst oder im Kundenauftrag entwickelte Software, sondern auch auf das Testen und die Freigabe von CON.4 *Auswahl und Einsatz von Standsoftware* und APP.1.1 *Office-Produkte*.

Für die Software-Tests werden unterschiedliche fachliche Methoden eingesetzt. Die Vorgehensweise bei Penetrationstests ist im Baustein DER.3.3 *Penetrationstests* genauer beschrieben.

Software-Tests können auch Bestandteil des Patch- oder Änderungsmanagements werden. Dieses ist im Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* näher spezifiziert.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Software-Tests und -Freigaben von besonderer Bedeutung:

2.1 Unvollständige Umsetzung von Anforderungen des Auftraggebers

Werden die Anforderungen unvollständig oder fehlerhaft eingearbeitet oder kommunizieren die an der Software-Entwicklung oder -Beschaffung beteiligten Parteien (z. B. Auftraggeber und Auftragnehmer) unzureichend miteinander, könnten die Anforderungen des Auftraggebers nur unvollständig erfüllt werden. Hieraus können Schwachstellen in der Software entstehen. Müssen beispielsweise die Anforderungen des Auftragnehmers nachträglich eingearbeitet werden, können sich Software-Entwicklungsprojekte verzögern und dadurch finanzielle Schäden entstehen.

2.2 Unzureichende Schulung der Entwickler und Software-Tester

Es wird häufig davon ausgegangen, dass ausgebildete Entwickler und Software-Tester aufgrund ihrer Ausbildung über ein ausreichendes Wissen für das Testen und Freigeben von Software verfügen. Entsprechend werden Entwickler und Software-Tester häufig zu wenig zu Neuerungen ihres Themengebiets oder zum Einsatzgebiet der Software geschult. Diese Unkenntnis kann zu gravierenden Sicherheitsproblemen führen, wenn z. B. Funktionen oder Methoden in der Programmierung verwendet werden, die bereits als unsicher eingestuft sind, dies aber bei den Entwicklern noch nicht bekannt ist.

2.3 Software-Test mit Produktivdaten

Software-Tests mit Produktivdaten oder im Produktivbetrieb sind notwendig, denn nur mit den Produktivdaten kann die Funktion und die Performance des Produktes beurteilt werden. Oft haben auch Entwickler einen anderen Blick auf das entwickelte Produkt, beispielsweise haben sie ein anderes Sicherheitsbewusstsein, vertrauen der entwickelten Software zu sehr und können mögliche Auswirkungen von Problemen nicht richtig deuten.

Obwohl Software-Tests mit Produktivdaten notwendig sind, können hierdurch Sicherheitsprobleme entstehen. Insbesondere vertrauliche Produktivdaten können für die Software-Tests so von unbefugten Mitarbeiter oder Dritten eingesehen werden, die mit dem jeweiligen Software-Test beauftragt wurden.

Durch Software-Tests im Produktivbetrieb könnte der Betrieb massiv gestört werden. Fehlfunktionen der zu testenden Software können Auswirkungen auf andere Anwendungen und IT-Systeme haben, die dadurch massiv gestört werden. Wird mit den "originalen" Produktivdaten im Produktivbetrieb getestet und nicht mit Kopien von den Daten, könnten diese ungewollt geändert oder gelöscht werden.

2.4 Fehlendes oder unzureichendes Testverfahren

Wird neue Software nicht oder nur unzureichend getestet und ohne Installationsvorschriften freigegeben, können Fehler in der Software unerkannt bleiben. Ebenso ist es möglich, dass dadurch erforderliche und einzuhaltende Installationsparameter nicht erkannt oder beachtet werden.

Diese Software- oder Installationsfehler, die aus einem fehlenden oder unzureichenden Software-Testverfahren resultieren, stellen eine erhebliche Gefährdung für den IT-Betrieb der Institution dar. So können beispielsweise Daten verloren gehen, wenn ein Update eines Datenbankmanagementsystems ohne vorherigem Test eingespielt wird.

2.5 Fehlendes oder unzureichendes Freigabeverfahren

Ein fehlendes oder unzureichendes Freigabeverfahren kann dazu führen, dass Software eingesetzt wird, die von der fachlichen Seite nicht abgenommen wurde. So kann die Software Funktionalitäten aufweisen, die sie nicht aufweisen sollte, oder Funktionalitäten können fehlen. Außerdem kann die Software zu anderen Anwendungen inkompatibel sein.

2.6 Fehlende oder unzureichende Dokumentation der Tests und Testergebnisse

Eine Software-Freigabe kann in der Regel erteilt werden, sobald alle Tests durchgeführt wurden und keine Abweichungen gefunden wurden. Sollte die Dokumentation der Software-Tests jedoch unvollständig sein, ist nachträglich nicht erkennbar, was getestet wurde. Wurden erkennbare Softwarefehler oder fehlende Funktionen ungenügend dokumentiert und damit bei der Freigabe nicht berücksichtigt, können durch diese Abweichungen die zu verarbeitenden Produktivdaten ungewollt gelöscht oder verändert sowie andere IT-Systeme und Anwendungen gestört werden.

2.7 Fehlende oder unzureichende Dokumentation der Freigabekriterien

Wenn Freigabekriterien nicht klar kommuniziert werden, kann dies dazu führen, dass die Freigabe voreilig erteilt wird oder keine Freigabe erfolgt, obwohl diese erteilt werden könnte. Dadurch können zum einen Versionen mit nicht erkannten Softwarefehlern freigegeben werden, die den Produktivbetrieb stören können und zum anderen kann dies zu einem Projektverzug mit finanziellen Schäden führen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Software-Tests und -Freigabe aufgeführt. Grundsätzlich ist der Leiter IT für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Leiter IT
Weitere Verantwortliche	Datenschutzbeauftragter, Fachverantwortliche, IT-Betrieb, Leiter Personal, Personalabteilung, Tester

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

OPS.1.1.6.A1 Planung der Software-Tests

Bevor die Software-Tests durchgeführt werden können, MÜSSEN die Rahmenbedingungen dafür innerhalb der Institution entsprechend der Schutzbedarfe, Organisationseinheiten, technischen Möglichkeiten und Test-Umgebungen festlegt sein. Die Software-Tests MÜSSEN auf den Angaben des Pflichtenhefts basieren.

Bei der Auswahl der Testfälle MUSS darauf geachtet werden, dass diese möglichst repräsentativ für die zu testenden Funktionen sind.

OPS.1.1.6.A2 Durchführung von funktionalen Software-Tests [Tester]

Funktionale Software-Tests MÜSSEN durchgeführt werden, um die ordnungsgemäße und vollständige Funktion der Software zu überprüfen. Die funktionalen Software-Tests MÜSSEN derart durchgeführt werden, dass diese den Produktivbetrieb nicht beeinflussen.

OPS.1.1.6.A3 Auswertung der Testergebnisse [Tester]

Die Ergebnisse der Software-Tests MÜSSEN ausgewertet werden. Es SOLLTE ein Soll- und Ist-Vergleich über den Abgleich mit definierter Vorgaben durchgeführt werden. Die Auswertung MUSS dokumentiert werden.

OPS.1.1.6.A4 Freigabe der Software [Fachverantwortliche]

Die fachliche Organisationseinheit MUSS die Software freigeben, sobald die Software-Tests erfolgreich durchgeführt wurden. Die Freigabe MUSS in Form einer Freigabeerklärung dokumentiert werden.

Die freigebende Organisationseinheit MUSS überprüfen, ob die Software gemäß den Anforderungen getestet wurde. Die Ergebnisse der Software-Tests MÜSSEN mit den vorher festgelegten Erwartungen übereinstimmen. Auch MUSS überprüft werden, ob die Einhaltung rechtlicher oder organisatorischer Vorgaben sichergestellt ist.

OPS.1.1.6.A5 Durchführung nicht-funktionaler Software-Tests [Tester]

Es MÜSSEN nicht-funktionale Tests durchgeführt werden. Insbesondere SOLLTEN sicherheitsspezifische Software-Tests durchgeführt werden, wenn die Anwendung sicherheitskritische Funktionen mitbringt. Die durchgeführten Testfälle als auch die Testergebnisse SOLLTEN dokumentiert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Software-Tests und -Freigaben. Sie SOLLTEN grundsätzlich umgesetzt werden.

OPS.1.1.6.A6 Geordnete Einweisung der Software-Tester [IT-Betrieb, Fachverantwortliche]

Ein Software-Tester SOLLTE über die durchzuführenden Testarten und die zu testenden Bereiche einer Software vom IT-Betrieb informiert werden. Darüber hinaus SOLLTE der Software-Tester über die Anwendungsfälle und mögliche weitere Anforderungen der Software informiert werden.

OPS.1.1.6.A7 Personalauswahl der Software-Tester [Personalabteilung]

Bei der Auswahl der Software-Tester SOLLTEN gesonderte Auswahlkriterien berücksichtigt werden. Die Personen SOLLTEN über die erforderliche berufliche Qualifikation verfügen. Es SOLLTEN ausreichende Kenntnisse der zu testenden Programmiersprache, Entwicklungsumgebung und den einzusetzenden Testmethoden vorhanden sein.

In öffentlichen Einrichtungen und geheimschutzbetreuten Institutionen SOLLTE geprüft werden, ob eine Sicherheitsüberprüfung erforderlich ist.

OPS.1.1.6.A8 Fort- und Weiterbildung der Software-Tester [Leiter Personal]

Die Software-Tester SOLLTEN entsprechend dem Baustein OPS.3 Sensibilisierung und Schulung geschult werden. Es SOLLTEN Verfahren etabliert werden, mit denen die Software-Tester über Neuerungen informiert werden, die für ihr jeweiliges Aufgabenspektrum relevant sind.

OPS.1.1.6.A9 Beschaffung von Test-Software [Tester, IT-Betrieb]

Die zu beschaffende Test-Software SOLLTE laut einem Anforderungskatalog beschafft werden. Sie SOLLTE ebenfalls dem Test- und Freigabeprozess unterzogen werden. Es SOLLTEN überprüft werden, ob die Hilfestellungs- und Supportleistungen des Softwareherstellers ausreichend sind.

OPS.1.1.6.A10 Erstellung eines Abnahmeplans

Im Abnahmeplan SOLLTEN die durchzuführenden Testarten, Testfälle und die erwarteten Ergebnisse dokumentiert sein. Außerdem SOLLTE der Abnahmeplan die Freigabekriterien beinhalten. Es SOLLTE die Vorgehensweise für die Ablehnung einer Freigabe definiert werden.

OPS.1.1.6.A11 Verwendung von anonymisierten oder pseudonymisierten Testdaten [Tester, Datenschutzbeauftragter]

Es SOLLTEN nur anonymisierte oder pseudonymisierte Testdaten für Software-Tests verwendet werden. Sofern die Produktivdaten einen Personenbezug aufweisen, SOLLTEN Institutionen ausschließlich anonymisierte Testdaten verwenden. Wenn ein Personenbezug von den Testdaten abgeleitet werden könnte, SOLLTEN der Datenschutzbeauftragte und unter Umständen die Personalvertretung hinzugezogen werden.

OPS.1.1.6.A12 Durchführung von Regressionstests [Tester]

Wenn Software-Tests nach einer Änderung der Software durchgeführt werden sollen, SOLLTEN Regressionstests durchgeführt werden. Regressionstests SOLLTEN vollständig durchgeführt werden. Die Auslassung von Testfällen SOLLTE begründet und dokumentiert werden. Die durchgeführten Testfälle und die Testergebnisse SOLLTEN dokumentiert werden.

OPS.1.1.6.A13 Trennung von Test- und Qualitätsmanagement-Umgebung von der Produktivumgebung [IT-Betrieb]

Software SOLLTE nur in einer hierfür vorgesehenen Test- und Qualitätsmanagement-Umgebung getestet werden. Die Test- und Qualitätsmanagement-Umgebungen SOLLTEN von der Produktivumgebung getrennt betrieben werden. Die in der Testlandschaft verwendeten Architekturen und Mechanismen SOLLTEN dokumentiert werden. Die Qualititätsmanagement-Umgebung SOLLTE der Produktivumgebung angepasst sein. Es SOLLTEN Verfahren dokumentiert werden, wie mit der Testlandschaft nach Abschluss des Software-Tests zu verfahren ist.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.1.1.6.A14 Durchführung von Penetrationstests [Tester] (CIA)

Es SOLLTEN für Anwendungen beziehungsweise IT-Systeme mit erhöhtem Schutzbedarf Penetrationstests als Testmethode durchgeführt werden. Es SOLLTE ein Penetrationstest-Konzept erstellt werden. Im Penetrationstest-Konzept SOLLTEN neben den zu verwendeten Testmethoden auch die Erfolgskriterien dokumentiert werden.

Der Penetrationstest SOLLTE nach den Rahmenbedingungen des Penetrationstest-Konzepts erfolgen. Die durch den Penetrationstest aufgefundenen Sicherheitslücken SOLLTEN klassifiziert und dokumentiert sein.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [29119] ISO/IEC 29119-2:2013-09
  Software and systems engineering - Software testing, ISO, 09.2013
  http://www.iso.org/iso/catalogue_detail.htm?csnumber=56736

- [BSIPEN] BSI Studie "Durchführungskonzept für Penetrationstests
  Bundesamt für Sicherheit in der Informationstechnik, 11.2013
  https://www.bsi.bund.de/DE/Publikationen/Studien/Pentest/index_htm.html

- [BSIWEB] BSI-Leitfäden zur Entwicklung sicherer Webanwendungen
  Bundesamt für Sicherheit in der Informationstechnik, 2013
  https://www.bsi.bund.de/DE/Publikationen/Studien/Webanwendungen/index_htm.html

- [CVSS] Common Vulnerability Scoring System
  CVSS, (zuletzt abgerufen am 28.09.2017)
  https://www.first.org/cvss

- [GLEN] The Art of Software Testing
  Glenford J. Myers, Corey Sandler, Tom Badgett, Todd M. Thomas John Wiley & Sons, 2004

- [ISF] The Standard of Good Practice
  Information Security Forum (ISF), 06.2016

- [NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations
  Special Publication 800-53, Revision 4, NIST, 04.2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an **grundschutz@bsi.bund.de** gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Software-Tests und -Freigaben" von Bedeutung.

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.38 Missbrauch personenbezogener Daten

G 0.42 Social Engineering

G 0.43 Einspielen von Nachrichten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen Anforderungen	G 0.18	G 0.19	G 0.21	G 0.22	G 0.23	G 0.28	G 0.29	G 0.30	G 0.31	G 0.38	G 0.42	G 0.43	G 0.45	G 0.46
OPS.1.1.6.A1	x													
OPS.1.1.6.A2	x													
OPS.1.1.6.A3	x													
OPS.1.1.6.A4								x						
OPS.1.1.6.A5		x	x	x	x	x				x		x	x	x
OPS.1.1.6.A6	x													
OPS.1.1.6.A7	x						x							
OPS.1.1.6.A8										x				
OPS.1.1.6.A9									x		x			
OPS.1.1.6.A10	x	x	x	x	x	x	x	x		x		x	x	x
OPS.1.1.6.A11		x								x				
OPS.1.1.6.A12		x	x	x	x	x				x		x	x	x
OPS.1.1.6.A13		x								x				
OPS.1.1.6.A14		x	x	x	x	x				x		x	x	x

OPS.1.2: Weiterführende Aufgaben

OPS.1.2.2 Archivierung

1 Beschreibung

1.1 Einleitung

Die Archivierung spielt im Dokumentenmanagement-Prozess eine besondere Rolle: Denn es wird erwartet, dass einerseits die Dokumente bis zum Ablauf einer vorgegebenen Aufbewahrungsfrist verfügbar sind und andererseits soll deren Vertraulichkeit und Integrität bewahrt bleiben. Zusätzlich muss der Kontext erhalten werden, damit der jeweilige gespeicherte Vorgang wieder rekonstruierbar ist.

Während der gesamten Dauer der Langzeitspeicherung müssen entsprechend Maßnahmen zur Informationserhaltung und, falls erforderlich, Maßnahmen zur Beweiswerterhaltung umgesetzt werden.

Im deutschen informationstechnischen Sprachgebrauch wird mitunter der Begriff elektronische Archivierung synonym zum Begriff elektronische Langzeitspeicherung verwendet. Zur besseren Verständlichkeit wird in diesem Baustein daher allgemein nur von Archivierung oder auch digitalem Langzeitarchiv gesprochen. Ein IT-Verfahren zur Aufbewahrung elektronischer Dokumente wird als Archivsystem bzw. digitales Archiv bzw. Langzeitspeicher bezeichnet. Die Aufbewahrungsdauer der Dokumente bemisst sich nach den rechtlichen und sonstigen Vorgaben sowie dem Anwendungszweck der Daten.

Der in diesem Baustein verwendete Begriff Dokumente subsumiert Daten und Dokumente, sofern sie nicht ausdrücklich in anderer Bedeutung gebraucht werden.

Aus rechtlicher Sicht ist der Begriff Archivierung in Deutschland durch die Archivgesetze des Bundes und der Länder konkretisiert und belegt. Daher ist er von der in diesem Dokument betrachteten zeitlich beschränkten Aufbewahrung zu unterscheiden. Archivierung im juristisch korrekten Sinne betrifft allein Unterlagen der öffentlichen Verwaltung und bezieht sich darauf, dass Unterlagen einer Behörde, sobald sie für die Zwecke der Behörde nicht mehr benötigt werden, ausgesondert und durch eine zuständige staatliche Einrichtung (Bundesarchiv) auf unbegrenzte Zeit verwahrt werden sollen (vgl. §§ 1 und 2 BArchG).

1.2 Zielsetzung

Der Baustein beschreibt, wie Dokumente langfristig, sicher, unveränderbar und wieder reproduzierbar archiviert werden können. Dazu werden Anforderungen definiert, mit denen sich ein Archivsystem sicher planen, umsetzen und betreiben lässt.

1.3 Abgrenzung

Der Baustein Archivierung beschreibt Sicherheitsmaßnahmen zur Aufbewahrung und Erhaltung von elektronischen Dokumenten für die Langzeitspeicherung im Rahmen von geltenden Aufbewahrungsfristen. Maßnahmen für eine operative Datensicherung werden nicht in diesem Baustein behandelt. Anforderungen dazu werden in OPS.1.1.6 Datensicherung dargestellt. dargestellt.

Ein digitaler Langzeitspeicher besteht aus einzelnen Komponenten, z. B. einer Datenbank. Wie sich solche Komponenten detailliert sicher betreiben lassen, ist jedoch ebenfalls nicht Thema des vorliegenden Bausteins. Dazu können z. B. zusätzlich die Anforderungen aus den Bausteinen APP.4.3 Relationale Datenbanksysteme, SYS.1.1 Allgemeiner Server sowie SYS.1.8 Speichersysteme ergänzt werden.systeme, SYS.1.1 Allgemeiner Server sowie SYS.1.8 Speichersysteme ergänzt werden., SYS.1.1 Allgemeiner Server sowie SYS.1.8 Speichersysteme ergänzt werden. sowie SYS.1.8 Speichersysteme ergänzt werden. ergänzt werden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Archivierung von besonderer Bedeutung:

2.1 Unzureichende Migration von Archivsystemen

Archivierte Daten sollen typischerweise über einen sehr langen Zeitraum gespeichert bleiben. Während dieses Zeitraums können die zugrundeliegenden technischen Systemkomponenten, Speichermedien und Datenformate physisch oder technisch altern und dadurch unbrauchbar werden. Außerdem können sich im Laufe der Zeit Probleme mit der Kompatibilität der verwendeten Datenformate ergeben.

Wenn auf die Alterung des bestehenden Systems nicht reagiert wird, ist langfristig damit zu rechnen, dass beispielsweise archivierte Rohdaten nicht mehr von den Archivmedien lesbar sind oder archivierte Daten durch physische Fehler an Archivsystem und -medien verändert werden.

2.2 Unzureichende Ordnungskriterien für Archive

Elektronische Archive können sehr große Datenmengen enthalten. Die einzelnen Datensätze werden dabei nach bestimmten Ordnungskriterien abgelegt, die in Indexdaten der Geschäftsanwendungen und Indexdaten des Archivsystems zu unterscheiden sind. Werden ungeeignete Ordnungskriterien verwendet, können archivierte Dokumente eventuell nicht oder nur sehr aufwändig wieder recherchiert werden oder die Semantik der Dokumente ist nicht eindeutig bestimmbar. Ebenso besteht die Gefahr, dass durch eine ungeeignete oder begrenzte Auswahl von Ordnungskriterien Aufbewahrungsziele verfehlt werden, z. B. die Nachweisfähigkeit gegenüber Dritten.

2.3 Unzureichende Dokumentation von Archivzugriffen

Unbefugte Archivzugriffe werden üblicherweise mithilfe von Protokolldateien aufgedeckt. Wurde jedoch nicht umfangreich genug protokolliert, besteht die Gefahr, dass solche Zugriffe nicht aufgedeckt werden. In der Folge könnten Angreifer unbemerkt an die dort gespeicherten Informationen gelangen und sie z. B. kopieren oder verändern.

2.4 Unzulängliche Übertragung von Papierdaten in ein elektronisches Archiv

Wenn Dokumente eingescannt werden, kann dabei das Erscheinungsbild oder die Semantik der aufgenommenen Daten verfälscht werden oder auch Dokumente verloren gehen. Dadurch kommt es zu falschen Interpretationen und Berechnungen, z. B. wenn wichtige Teile des Dokuments oder des Dokumentenstapel beim Scannen vergessen werden.

2.5 Unzureichende Erneuerung von kryptographischen Verfahren bei der Archivierung

Kryptographische Verfahren, die z. B. bei Signaturen, Siegeln, Zeitstempeln, technischen Beweisdaten (Evidence Records) oder Verschlüsselungen verwendet werden, müssen regelmäßig an den aktuellen Stand der Technik angepasst werden, damit die Schutzwirkung erhalten bleibt. Wird das versäumt, kann beispielsweise aufgrund einer veralteten unsicheren Signatur, die Integrität des Dokumentes angezweifelt werden, sodass die Datei nicht als Beweismittel vor Gericht zugelassen wird. Auch geht so die Vertraulichkeit eines verschlüsselten Dokumentes verloren.

2.6 Unzureichende Durchführung von Revisionen bei der Archivierung

Wenn der Archivierungsprozess zu selten oder zu ungenau überprüft wird, kann das mittelbar dazu führen, dass der gesamte Prozess nicht mehr ordnungsgemäß funktioniert. Damit kann die Integrität der archivierten Dokumente selbst angezweifelt werden. Hieraus können sich für die Institution rechtliche und wirtschaftliche Nachteile ergeben: So kann unter Umständen eine Datei nicht als Beweismittel vor Gericht zugelassen werden, weil nicht ausgeschlossen werden kann, dass sie manipuliert wurde.

2.7 Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivierung

Bei der Archivierung von elektronischen Dokumenten sind verschiedene rechtliche Rahmenbedingungen zu beachten. Werden diese nicht eingehalten, kann das zivil- oder strafrechtliche Konsequenzen haben, z. B. bei Mindestaufbewahrungsfristen, die sich aus steuerlichen, haushaltsrechtlichen oder sonstigen Gründen ergeben.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Archivierung aufgeführt. Grundsätzlich ist der Archivverwalter dafür zuständig, die Anforderungen zu erfüllen. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Archivverwalter
Weitere Verantwortliche	Benutzer, IT-Betrieb, Leiter IT

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

OPS.1.2.2.A1 Ermittlung von Einflussfaktoren für die elektronische Archivierung

Bevor entschieden wird, welche Verfahren und Produkte für die elektronische Archivierung eingesetzt werden, MÜSSEN die technischen, rechtlichen und organisatorischen Einflussfaktoren ermittelt und dokumentiert werden. Die Ergebnisse MÜSSEN in das Archivierungskonzept einfließen.

OPS.1.2.2.A2 Entwicklung eines Archivierungskonzepts

Es MUSS definiert werden, welche Ziele mit der Archivierung erreicht werden sollen. Hierbei MUSS insbesondere berücksichtigt werden, welche Regularien einzuhalten sind, welche Mitarbeiter verantwortlich sind und welcher Funktions- und Leistungsumfang angestrebt wird.

Die Ergebnisse MÜSSEN in einem Archivierungskonzept erfasst werden. Das Management MUSS in diesen Prozess einbezogen werden. Das Archivierungskonzept MUSS regelmäßig an die aktuellen Gegebenheiten der Institution angepasst werden.

OPS.1.2.2.A3 Geeignete Aufstellung von Archivsystemen und Lagerung von Archivmedien [Leiter IT, IT-Betrieb]

Da Archivsysteme schützenswerte Daten einer Institution zentral aufbewahren, MÜSSEN deren IT-Komponenten in gesicherten Räumen aufgestellt werden. Es MUSS sichergestellt sein, dass nur berechtigte Personen die Räume betreten dürfen. Damit Archiv-Speichermedien langfristig aufbewahrt werden können, MÜSSEN sie geeignet gelagert werden.

OPS.1.2.2.A4 Konsistente Indizierung von Daten bei der Archivierung [Leiter IT, IT-Betrieb, Benutzer]

Alle in einem Archiv abgelegten Daten, Dokumente und Datensätze MÜSSEN eindeutig indiziert werden, um sie bei späteren Suchanfragen schnell wiederfinden zu können. Dazu MUSS bereits während der Konzeption festgelegt werden, welche Struktur und welchen Umfang die Indexangaben für ein Archiv haben sollen.

OPS.1.2.2.A5 Regelmäßige Aufbereitung von archivierten Datenbeständen [Leiter IT]

Es MUSS über den gesamten Archivierungszeitraum hinweg sichergestellt werden, dass

- das verwendete Datenformat von den benutzten Anwendungen verarbeitet werden kann,
- die gespeicherten Daten auch zukünftig lesbar und so reproduzierbar sind, dass Semantik und Beweiskraft beibehalten werden können,
- das benutzte Dateisystem auf dem Speichermedium von allen beteiligten Komponenten verarbeitet werden kann,
- die Speichermedien jederzeit technisch einwandfrei gelesen werden können und
- die verwendeten kryptographischen Verfahren zur Verschlüsselung und zum Beweiswerterhalt mittels digitaler Signatur, Siegel, Zeitstempel oder technischen Beweisdaten (Evidence Records) dem Stand der Technik entsprechen.

OPS.1.2.2.A6 Schutz der Integrität der Indexdatenbank von Archivsystemen [Leiter IT, IT-Betrieb]

Die Integrität der Indexdatenbank MUSS sichergestellt und überprüfbar sein. Außerdem MUSS die Indexdatenbank regelmäßig gesichert werden. Die Datensicherungen MÜSSEN wiederherstellbar sein. Mittlere und große Archive MÜSSEN über redundante Indexdatenbanken verfügen.

OPS.1.2.2.A7 Regelmäßige Datensicherung der System- und Archivdaten [Leiter IT, IT-Betrieb]

Alle Archivdaten, die zugehörigen Indexdatenbanken sowie die Systemdaten MÜSSEN regelmäßig gesichert werden (siehe OPS.1.1.6 *Datensicherung).*).

OPS.1.2.2.A8 Protokollierung der Archivzugriffe [Leiter IT, IT-Betrieb]

Alle Zugriffe auf elektronische Archive MÜSSEN protokolliert werden. Dafür SOLLTEN Datum, Uhrzeit, Benutzer, Clientsystem und die ausgeführten Aktionen sowie Fehlermeldungen aufgezeichnet werden. Die Aufbewahrungsdauer der Protokolldaten SOLLTE im Archivierungskonzept festgelegt werden.

Die Protokolldaten der Archivzugriffe SOLLTEN regelmäßig ausgewertet werden. Dabei SOLLTEN die institutionsinternen Vorgaben beachtet werden.

Auch SOLLTE definiert sein, welche Ereignisse (z. B. Systemfehler, Timouts oder Datensätze kopieren) welchen Mitarbeitern angezeigt signalisiert werden. Kritische Ereignisse SOLLTEN sofort nach der Signalisierung geprüft und, falls nötig, weiter eskaliert werden.

OPS.1.2.2.A9 Auswahl geeigneter Datenformate für die Archivierung von Dokumenten [Leiter IT, IT-Betrieb]

Für die Archivierung MUSS ein geeignetes Datenformat ausgewählt werden. Es MUSS gewährleisten, dass sich Archivdaten sowie ausgewählte Merkmale des ursprünglichen Dokumentmediums langfristig und originalgetreu reproduzieren lassen.

Die Dokumentstruktur des ausgewählten Datenformats MUSS eindeutig interpretierbar und elektronisch verarbeitbar sein. Die Syntax und Semantik der verwendeten Datenformate SOLLTE dokumentiert und von einer Standardisierungsorganisation veröffentlicht sein. Es SOLLTE für eine beweis- und revisionssichere Archivierung ein verlustfreies Bild-Kompressionsverfahren benutzt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Archivierung. Sie SOLLTEN grundsätzlich umgesetzt werden.

OPS.1.2.2.A10 Erstellung einer Richtlinie für die Nutzung von Archivsystemen [Leiter IT, IT-Betrieb]

Es SOLLTE sichergestellt werden, dass Mitarbeiter das Archivsystem so benutzen, wie es im Archivierungskonzept vorgesehenen ist. Dazu SOLLTE eine Administrations- und eine Benutzerrichtlinie erstellt werden. Die Administrationsrichtlinie SOLLTE folgende Punkte enthalten:

- Festlegung der Verantwortung für Betrieb und Administration,
- Vereinbarungen über Leistungsparameter beim Betrieb (Service Level Agreements),
- Modalitäten der Vergabe von Zutritts- und Zugriffsrechten,
- Modalitäten der Vergabe von Zugangsrechten zu den vom Archiv bereitgestellten Diensten,
- Regelungen zum Umgang mit archivierten Daten und Archivmedien,
- Überwachung des Archivsystems und der Umgebungsbedingungen,
- Regelung zur Datensicherung
- Regelungen zur Protokollierung
- Trennung von Produzenten und Konsumenten (OAIS-Modell).

OPS.1.2.2.A11 Einweisung in die Administration und Bedienung des Archivsystems [Leiter IT, IT-Betrieb, Benutzer]

Die verantwortlichen IT-Betrieben und die Benutzer SOLLTEN für ihren Aufgabenbereich geschult werden.

Die Schulung der IT-Betrieben SOLLTE folgende Themen umfassen:

- Systemarchitektur und Sicherheitsmechanismen des verwendeten Archivsystems und des darunterliegenden Betriebssystems,
- Installation und Bedienung des Archivsystems und Umgang mit Archivmedien,
- Dokumentation der Administrationstätigkeiten und
- Eskalationsprozeduren.

Die Schulung der Benutzer SOLLTE folgende Themen umfassen:

- Umgang mit dem Archivsystem,
- Bedienung des Archivsystems,
- rechtliche Rahmenbedingungen der Archivierung.

Die Durchführung und Teilnahme an den Schulungen SOLLTEN dokumentiert werden.

OPS.1.2.2.A12 Überwachung der Speicherressourcen von Archivmedien [Leiter IT, IT-Betrieb]

Die auf den Archivmedien vorhandene freie Speicherkapazität MUSS kontinuierlich überwacht werden. Sobald ein definierter Grenzwert unterschritten wird, MUSS ein verantwortlicher Mitarbeiter automatisch alarmiert werden. Es SOLLTE darauf geachtet werden, dass die Alarmierung rollenbezogen erfolgt. Es MÜSSEN immer ausreichend leere Archivmedien verfügbar sein, um Speicherengpässen schnell vorbeugen zu können.

OPS.1.2.2.A13 Regelmäßige Revision der Archivierungsprozesse

ES SOLLTE regelmäßig überprüft werden, ob die Archivierungsprozesse noch korrekt und ordnungsgemäß funktionieren. Dazu SOLLTE eine Checkliste erstellt werden, die Fragen zu Verantwortlichkeiten, Organisationsprozessen, Einsatz der Archivierung, Redundanz der Archivdaten, Administration und

der technischen Beurteilung des Archivsystems enthält. Die Auditergebnisse SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTE nachgegangen werden.

OPS.1.2.2.A14 Regelmäßige Beobachtung des Markes für Archivsystemen [Leiter IT]

Der Markt für Archivsysteme SOLLTE regelmäßig und systematisch beobachtet werden. Dabei SOLLTEN unter anderem folgende Kriterien beobachtet werden: Veränderungen bei Standards, Technologiewechsel bei Herstellern von Hard- und Software, veröffentlichte Sicherheitslücken oder Schwachstellen sowie Verlust der Sicherheitseignung bei kryptographischen Algorithmen.

OPS.1.2.2.A15 Regelmäßige Aufbereitung von kryptographisch gesicherten Daten bei der Archivierung [Leiter IT, IT-Betrieb]

Es SOLLTE kontinuierlich beobachtet werden, wie sich das Gebiet der Kryptographie entwickelt, um beurteilen zu können, ob ein Algorithmus weiterhin zuverlässig und ausreichend sicher ist (siehe auch OPS.1.2.2.A20 Geeigneter Einsatz kryptographischer Verfahren).

Archivdaten, die mit kryptographischen Verfahren gesichert wurden, deren Sicherheitseignung in absehbarer Zeit verloren gehen wird, SOLLTEN rechtzeitig mit sicheren Verfahren neu gesichert, z.B. verschlüsselt bzw. signiert, werden.

OPS.1.2.2.A16 Regelmäßige Erneuerung technischer Archivsystem-Komponenten [Leiter IT, IT-Betrieb]

Archivsysteme SOLLTEN über lange Zeiträume auf dem aktuellen technischen Stand gehalten werden. Neue Hard- und Software SOLLTE vor der Installation in ein laufendes Archivsystem ausführlich getestet werden. Wenn neue Komponenten in Betrieb genommen oder neue Dateiformate eingeführt werden, SOLLTE ein Migrationskonzept erstellt werden. Darin SOLLTEN alle Änderungen, Tests und erwartete Testergebnisse beschrieben sein. Die Konvertierung der einzelnen Daten SOLLTE dokumentiert (Transfervermerk) werden.

Wenn Archivdaten in neue Formate konvertiert werden, SOLLTE geprüft werden, ob aufgrund rechtlicher Anforderungen zusätzlich die Daten in ihren ursprünglichen Formaten zu archivieren sind.

OPS.1.2.2.A17 Auswahl eines geeigneten Archivsystems [Leiter IT]

Ein neues Archivsystem SOLLTE immer aufgrund der im Archivierungskonzept beschriebenen Vorgaben ausgewählt werden. Es SOLLTE die dort formulierten Anforderungen erfüllen.

OPS.1.2.2.A18 Verwendung geeigneter Archivmedien [Leiter IT, IT-Betrieb]

Für die Archivierung SOLLTEN geeignete Medien ausgewählt und benutzt werden. Dabei SOLLTEN die Aspekte zu archivierendes Datenvolumen, mittlere Zugriffszeiten und mittlere gleichzeitige Zugriffe auf das Archivsystem beachtet werden. Ebenfalls SOLLTEN die Archivmedien die Anforderungen an eine Langzeitarchivierung hinsichtlich Revisionssicherheit und Lebensdauer erfüllen.

OPS.1.2.2.A19 Regelmäßige Funktions- und Recoverytests bei der Archivierung [Leiter IT, IT-Betrieb]

Für die Archivierung SOLLTE es regelmäßige Funktions- und Recoverytests geben. Die Archivierungsdatenträger SOLLTEN mindestens einmal jährlich überprüft werden, ob sie noch lesbar und integer sind. Für die Fehlerbehebung SOLLTEN geeignete Prozesse definiert werden.

Weiterhin SOLLTEN die Hardwarekomponenten des Archivsystems regelmäßig auf ihre einwandfreie Funktion hin geprüft werden. Es SOLLTE regelmäßig geprüft werden, ob alle Archivierungsprozesse fehlerfrei funktionieren.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.1.2.2.A20 Geeigneter Einsatz kryptographischer Verfahren bei der Archivierung [Leiter IT] (CI)

Um lange Aufbewahrungsfristen abdecken zu können, SOLLTEN Archivdaten nur mit kryptographischen Verfahren auf Basis aktueller Standards und Normen gesichert werden.

OPS.1.2.2.A21 Übertragung von Papierdaten in elektronische Archive (CI)

Werden Dokumente auf Papier und Gegenstände des Augenscheins digitalisiert und in ein elektronisches Archiv überführt, SOLLTE sichergestellt werden, dass die digitale Kopie mit dem Originaldokument bildlich und inhaltlich übereinstimmt.

4 Weiterführende Informationen

4.1 Literatur

- [AlgKat] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung
  Übersicht über geeignete Algorithmen, BNetzA, 2017
  https://www.bundesnetzagentur.de/DE/
  Service-Funktionen/ElektronischeVertrauensdienste/QES/
  WelcheAufgabenhatdieBundesnetzagentur/GeeigneteAlgorithmenfestlegen/geeignetealgorithmenfestlegen_node.html

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Archivierung" von Bedeutung.

G 0.02 Ungünstige klimatische Bedingungen

G 0.04 Verschmutzung, Staub, Korrosion

G 0.14 Ausspähen von Informationen (Spionage)

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.37 Abstreiten von Handlungen

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.02	G 0.04	G 0.14	G 0.18	G 0.19	G 0.22	G 0.25	G 0.26	G 0.28	G 0.29	G 0.30	G 0.31	G 0.37	G 0.45	G 0.46
OPS.1.2.2.A1				x						x			x		
OPS.1.2.2.A2				x							x				
OPS.1.2.2.A3	x	x													
OPS.1.2.2.A4				x			x	x							
OPS.1.2.2.A5				x						x					
OPS.1.2.2.A6							x	x	x						x
OPS.1.2.2.A7														x	x
OPS.1.2.2.A8			x			x				x					
OPS.1.2.2.A9														x	x
OPS.1.2.2.A10				x						x		x			
OPS.1.2.2.A11							x	x			x	x			
OPS.1.2.2.A12							x	x						x	x
OPS.1.2.2.A13				x						x					
OPS.1.2.2.A14															
OPS.1.2.2.A15				x			x	x	x						x
OPS.1.2.2.A16				x											x
OPS.1.2.2.A17							x	x							
OPS.1.2.2.A18				x					x	x					
OPS.1.2.2.A19				x			x	x							
OPS.1.2.2.A20							x	x	x					x	x
OPS.1.2.2.A21			x		x					x			x		

OPS.1.2: Weiterführende Aufgaben

OPS.1.2.3 Informations- und Datenträgeraustausch

1 Beschreibung

1.1 Einleitung

In diesem Baustein wird der sichere Austausch von Informationen betrachtet, mit dem Fokus auf digitale und analoge Datenträger als Transportmedien, aber auch der Informationsaustausch bei persönlichen Treffen oder über IT-Netze. Auch bei einer breitbandigen Netzanbindung kann es sinnvoll oder notwendig sein, für den Informationsaustausch Datenträger zu übermitteln. Ein Grund kann sein, dass es keine oder keine hinreichend vertrauenswürdige Vernetzung zwischen den betroffenen IT-Systemen gibt. Datenträger können bei persönlichen Treffen oder auch per Versand ausgetauscht werden.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, den Informationsaustausch zwischen verschiedenen Kommunikationspartnern und IT-Systemen abzusichern. Insbesondere wird dargestellt, was beim Datenträgeraustausch zu beachten ist, um die transportierten Daten angemessen zu schützen.

1.3 Abgrenzung

Dieser Baustein ist immer dann anzuwenden, wenn ein Informationsaustausch mit Stellen außerhalb der eigenen Institution bzw. Liegenschaft erfolgt und dabei nicht das interne Netz verwendet wird. Er ist vor allem anzuwenden, wenn

- neue Transportwege aufgebaut werden (neue Kommunikationspartner, neue Medien, neue Netze),
- der Informationsaustausch mit Hilfe von Datenträgern erfolgt. Hierbei sind neben der Übermittlung insbesondere auch die Speicherung und der Umgang mit den Datenträgern zu berücksichtigen.

Die Absicherung von Netzverbindungen wird in anderen Bausteinen des IT-Grundschutz-Kompendiums behandelt. Auch die Weiterverarbeitung im Ziel-IT-System wird nicht betrachtet. In diesem Baustein stehen die grundsätzlichen Regelungen für einen sicheren Informationsaustausch im Vordergrund, vor allem bei der Nutzung von mobilen Datenträgern. Nicht betrachtet werden die Gründe, warum es keine oder keine hinreichend vertrauenswürdige Vernetzung zwischen den betroffenen IT-Systemen gibt.

Daneben wird in diesem Baustein auch die Speicherung der Daten auf dem Sender- und Empfänger-System, soweit es in direktem Zusammenhang mit dem Datenträgeraustausch steht, sowie der Umgang mit den Datenträgern vor bzw. nach dem Transfer berücksichtigt. Dieser Baustein betrachtet mobile Datenträger wie z. B. Wechselplatten, optische Datenträger, USB-Sticks und -Festplatten und nicht zu vergessen Papierdokumente.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Informations- und Datenträgeraustausch von besonderer Bedeutung:

2.1 Defekte Datenträger

Bei allen Arten von Datenträgern können Beschädigungen, Fehler oder Ausfälle auftreten. Zum Problem werden sie dann, wenn die auf den Datenträgern gespeicherten Informationen an keiner anderen Stelle gespeichert sind und sich nicht schnell und einfach rekonstruieren lassen.

Unzulässige Temperatur und Luftfeuchte

Extreme Temperaturen und Feuchtigkeit können sich auf eine ordnungsgemäße Funktion von Datenträgern auswirken. Zu jeder Art von Datenträgern gibt es festgelegte Grenzwerte, innerhalb derer die ordnungsgemäße Funktion gewährleistet ist. Werden diese über- oder unterschritten, kann es zu Betriebsstörungen und zu Geräteausfällen kommen. Bei digitalen Speichermedien können zu große Temperaturschwankungen oder zu große Luftfeuchtigkeit zu Datenfehlern führen.

Unsachgemäß verpackte Datenträger

Beim Transport oder Versand sind Datenträger besonderen Belastungen ausgesetzt. Bei Datenträgern können bereits geringfügige Verunreinigungen zu Datenfehlern führen. Festplatten können durch den "Headcrash" des Schreib-/Lesekopfes, Bänder oder Kassetten durch direkte mechanische Einwirkung zerstört werden. CD-ROM s oder DVDs können durch Verkratzen der Oberfläche unbrauchbar werden.

Datenverlust durch starke Magnetfelder

Typische Datenträger mit magnetisierbaren Speichermedien sind Wechselplatten, Kassetten und Bänder. Diese Datenträger sind empfindlich gegenüber magnetischer Störstrahlung, so dass die Nähe zu solchen Strahlungsquellen vermieden werden sollte.

2.2 Nicht fristgerecht verfügbare Datenträger

Beim Datenträgeraustausch ist es bei vielen Geschäftsprozessen von besonderer Bedeutung, dass diese fristgerecht ihren Empfänger erreichen bzw. dort zeitnah genutzt werden können. Auch kleine Fehler in der Kennzeichnung können dazu führen, dass ein Datenträger nicht in der erforderlichen Zeit sein Ziel erreicht. Wenn vor Ort die notwendigen Schnittstellen bzw. Betriebsmittel nicht vorhanden sind, kann ein Datenträger unter Umständen nicht ausgelesen werden. Die resultierenden Verzögerungen können zu erheblichen Schäden führen.

2.3 Ungeregelte Weitergabe von Informationen oder Datenträgern

Bei einer ungeregelten Weitergabe bzw. ungeordneter Zustellung von Informationen oder Datenträgern besteht die Gefahr, dass vertrauliche Informationen in unbefugte Hände gelangen oder das gewünschte Ziel nicht rechtzeitig erreichen.

2.4 Unzureichendes Schlüsselmanagement bei Verschlüsselung

Werden zum Schutz der Vertraulichkeit zu übermittelnder Daten Verschlüsselungssysteme eingesetzt, so kann aufgrund eines unzureichenden Schlüsselmanagements der gewünschte Schutz unterlaufen werden, beispielsweise wenn leicht zu erratende Schlüssel gewählt wurden oder wenn die zur Verschlüsselung bzw. Entschlüsselung eingesetzten kryptographischen Schlüssel den Kommunikationspartner nicht auf einem sicheren Weg erreichen. Einfachstes Negativbeispiel ist der Versand der verschlüsselten Informationen und des benutzten Schlüssels auf oder mit demselben Datenträger. In diesem Fall kann jeder, der in den Besitz des Datenträgers gelangt, die Informationen entschlüsseln, vorausgesetzt, dass das bei der Verschlüsselung eingesetzte Verfahren bekannt ist.

2.5 Verlust von Datenträgern beim Versand

Werden Datenträger in nicht sonderlich stabilen Behältnissen (Briefumschlägen oder sonstigen Verpackungen) versandt, besteht die Gefahr, dass die Datenträger bei Beschädigung der Verpackung verloren gehen. Auch besteht die Gefahr des Verlustes beim Empfänger, auf dem Postweg oder durch Unachtsamkeit eines Boten. Datenträger werden immer kleiner, so dass sie auch leichter beim Transport verloren gehen können.

Wenn die Informationen auf den Datenträgern nicht verschlüsselt sind, können sie außerdem bei einem Verlust in die falschen Hände geraten.

2.6 Weitergabe falscher oder interner Informationen

Bei der Weitergabe von Informationen kommt es immer wieder vor, dass neben den gewünschten Informationen auch andere Informationen übermittelt werden. Dadurch geraten immer wieder vertrauliche oder nicht für die Veröffentlichung geeignete Informationen in die falschen Hände. So kommt es vor, dass Datenträger weitergegeben werden, ohne dass die vorher darauf gespeicherten Daten in geeigneter Weise gelöscht wurden. Ebenso kann es vorkommen, dass vertrauliche Unterlagen versehentlich an den falschen Empfänger versandt werden oder dass Briefe zusammen mit internen Kommentaren ausgedruckt und versandt werden.

2.7 Diebstahl, Manipulation oder Zerstörung von Datenträgern

Außentäter, aber auch Innentäter, können aus unterschiedlichen Beweggründen (Ausspähung, Rache, Böswilligkeit, Frust) heraus versuchen, Datenträger zu stehlen, zu manipulieren oder zu zerstören. Die Manipulationen reichen von der unerlaubten Einsichtnahme in schützenswerte Daten über inhaltliche Änderung von Daten bis hin zur Zerstörung von Datenträgern.

2.8 Schadprogramme in übertragenen Dateien oder auf Datenträgern

Wenn die Arbeitsumgebung unzureichend gegen Schadprogramme abgesichert ist, könnten sich auf Datenträger, die an Externe weitergegeben werden, Schadprogramme befinden. Dadurch könnten die gespeicherten Daten zerstört oder verfälscht werden, aber vor allem IT-Systeme auf Empfängerseite kompromittiert werden. Aber auch der Imageverlust und der finanzielle Schaden, der durch Schadprogramme entstehen kann, sind von großer Bedeutung.

2.9 Unberechtigtes Kopieren von Informationen oder der Datenträger

Werden Informationen oder Datenträger über einen unsicheren Transportweg ausgetauscht oder transportiert, besteht die Gefahr, dass die übermittelten Informationen bei der Beförderung durch Unbefugte kopiert werden. Ebenso könnten Angreifer versuchen, die Kommunikation über IT-Netze abzuhören.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz beim Informations- und Datenträgeraustausch aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte (ISB) für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt.

Bausteinverantwortlicher	Informationssicherheitsbeauftragter (ISB)
Weitere Verantwortliche	Benutzer, Fachverantwortliche, IT-Betrieb, Leiter Organisation, Poststelle

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

OPS.1.2.3.A1 Festlegung zulässiger Kommunikationspartner [Leiter Organisation]

In der Institution MUSS festgelegt werden, welche Kommunikationspartner welche Informationen erhalten und weitergeben dürfen. Dies MUSS für alle Einsatzzwecke in der Institution kommuniziert werden. Vor dem Austausch von Informationen MUSS geklärt werden, dass der Empfänger die notwendigen Berechtigungen für den Erhalt und die Weiterverarbeitung der Informationen besitzt.

OPS.1.2.3.A2 Regelung des Informationsaustausches [Leiter Organisation]

Werden Informationen ausgetauscht, MUSS im Vorfeld geklärt werden, wie schutzbedürftig die relevanten Informationen sind, mit wem die Informationen ausgetauscht werden dürfen und wie sie dabei konkret zu schützen sind. Die Mitarbeiter MÜSSEN dazu ausreichend sensibilisiert werden. Die Empfänger MÜSSEN darauf hingewiesen werden, dass die übermittelten Daten nur zu dem Zweck benutzt werden dürfen, zu dem sie weitergegeben wurden.

OPS.1.2.3.A3 Unterweisung des Personals zum Informationsaustausch [Fachverantwortliche]

Das Personal MUSS darüber informiert werden, welche Rahmenbedingungen für den Informationsaustausch gelten. Es MUSS wissen, welche Informationen sie wann, wo und wie weitergeben dürfen.

OPS.1.2.3.A4 Schutz vor Schadsoftware [Benutzer]

Digitale Daten MÜSSEN sowohl vom Sender vor Versand als auch vom Empfänger auf Schadsoftware überprüft werden. Die eingesetzten Virenschutz-Programme müssen dem aktuellen Stand der Technik entsprechen.

OPS.1.2.3.A5 Verlustmeldung [Benutzer]

Es MUSS umgehend gemeldet werden, wenn ein Datenträger beim Datenträgeraustausch verloren oder gestohlen wird oder der Verdacht auf Manipulation besteht. Hierfür MUSS es in jeder Institution klare Meldewege und Ansprechpartner geben.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Informations- und Datenträgeraustausch. Sie SOLLTEN grundsätzlich umgesetzt werden.

OPS.1.2.3.A6 Vereinbarungen zum Informationsaustausch mit Externen [Leiter Organisation]

Bei einem regelmäßigen Informationsaustausch mit externen Partnern SOLLTEN die Rahmenbedingungen hierfür formal vereinbart werden.

OPS.1.2.3.A7 Regelung des Datenträgeraustausches [Leiter Organisation]

Der ordnungsgemäße Datenträgeraustausch SOLLTE geregelt werden. Es SOLLTE festgelegt werden, wie die Datenträger in der eigenen Institution, beim Transport und beim Empfänger zu schützen sind. Bei der Wahl der Versandart SOLLTE die Art der Datenträger und der Schutzbedarf der Informationen berücksichtigt werden. Außerdem SOLLTE festgelegt werden, wann und wie Datenträger physikalisch gelöscht werden.

OPS.1.2.3.A8 Physikalisches Löschen von Datenträgern vor und nach Verwendung [Benutzer]

Vor und nach einem Datenträgeraustausch SOLLTEN zuvor anderweitig verwendete Datenträger physikalisch gelöscht werden. Den Mitarbeitern SOLLTEN geeignete Programme zum physikalischen Löschen zur Verfügung gestellt werden.

OPS.1.2.3.A9 Beseitigung von Restinformationen in Dateien vor Weitergabe [Benutzer]

Die Benutzer SOLLTEN hinsichtlich der Gefahren von Rest- und Zusatzinformationen in Dateien informiert werden. Den Benutzern SOLLTE vermittelt werden, wie sie Rest- und Zusatzinformationen in Dateien vermeiden können. Restinformationen SOLLTEN entsprechend beseitigt werden. Vor der Weitergabe von Dateien SOLLTEN stichprobenhafte Überprüfungen der Dateien auf enthaltene Restinformationen durchgeführt werden.

OPS.1.2.3.A10 Abschluss von Vertraulichkeitsvereinbarungen [Leiter Organisation]

Mit Externen SOLLTEN Vertraulichkeitsvereinbarungen getroffen werden, bevor sie Zugang und Zugriff auf vertrauliche Informationen erhalten. Durch die verwendeten Vertraulichkeitsvereinbarungen SOLLTEN alle wichtigen Aspekte zum Schutz von vertraulichen Informationen berücksichtigt werden.

OPS.1.2.3.A11 Kompatibilitätsprüfung des Sender- und Empfängersystems [IT-Betrieb]

Vor einem Informationsaustausch SOLLTEN die eingesetzten Systeme und Produkte auf Sender- und Empfängerseite auf ihre Kompatibilität geprüft werden.

OPS.1.2.3.A12 Angemessene Kennzeichnung der Datenträger beim Versand [Benutzer]

Bei der Kennzeichnung von Datenträgern SOLLTE sichergestellt werden, dass Absender und Empfänger unmittelbar zu identifizieren sind. Die Kennzeichnung der Datenträger bzw. deren Verpackung SOLLTE den Inhalt der Datenträger eindeutig für den Empfänger erkennbar machen. Die Kennzeichnung von Datenträgern mit schützenswerten Informationen SOLLTE KEINE Rückschlüsse auf Art und Inhalte der Informationen zulassen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.1.2.3.A13 Verschlüsselung und digitale Signaturen [Benutzer] (CI)

Vertrauliche Informationen SOLLTEN vor einem Informationsaustausch verschlüsselt werden. Informationen mit hohem Integritätsanspruch SOLLTEN digital signiert werden. Hierfür SOLLTEN geeignete Kryptoverfahren ausgewählt werden, die dem Schutzbedarf entsprechen und auf Sender- und Empfängerseite problemlos genutzt werden können. Für den Einsatz von kryptographischen Verfahren SOLLTE ein geeignetes Schlüsselmanagement etabliert werden.

OPS.1.2.3.A14 Datenträgerverwaltung [Leiter Organisation, IT-Betrieb] (CIA)

Bei höherem Schutzbedarf SOLLTE eine Datenträgerverwaltung eingerichtet werden, um den Zugriff auf Datenträger, deren Kennzeichnung und ordnungsgemäße Aufbewahrung zu regeln. Für alle Arten von Datenträgern SOLLTE der ordnungsgemäße Umgang inklusive Aufbewahrung, Weitergabe, Transport und Löschung geregelt sein. Es SOLLTE ein Bestandsverzeichnis erstellt werden. Die Datenträger SOLLTEN gemäß den Herstellerangaben sachgerecht behandelt werden.

OPS.1.2.3.A15 Sichere Versandart und Verpackung [Poststelle, Benutzer] (C)

Sofern Informationen einem erhöhten Schutzbedarf unterliegen, SOLLTE geprüft werden, wie diese bei einem Datenträgeraustausch angemessen geschützt werden können. Es SOLLTEN sichere Versandverpackungen für Datenträger verwendet werden, die Manipulationen durch Veränderungen an der Verpackung erkennen lassen. Der Versender SOLLTE die Poststelle auf notwendige Versand- und Verpackungsarten hinweisen. Grundsätzlich SOLLTEN die Daten verschlüsselt werden.

OPS.1.2.3.A16 Sichere Aufbewahrung der Datenträger vor und nach Versand [Benutzer, Poststelle] (CIA)

Beschriebene Datenträger SOLLTEN so aufbewahrt werden, dass nur berechtigte Benutzer darauf zugreifen können. Alle beteiligten Mitarbeiter SOLLTEN auf eine sachgerechte und sichere Aufbewahrung und Handhabung der Datenträger hingewiesen werden.

OPS.1.2.3.A17 Verifizieren von Datenträgern vor Versand [Benutzer] (CI)

Vor dem Versenden von Datenträgern SOLLTE überprüft werden,

- ob die gewünschten Informationen vollständig enthalten sind und
- ob keine zusätzlichen Informationen enthalten sind, die nicht weitergegeben werden sollen.

OPS.1.2.3.A18 Sicherungskopie der übermittelten Daten [Benutzer] (A)

Sind die zu übertragenden Daten nur zum Zweck der Datenübertragung erstellt bzw. zusammengestellt worden und nicht auf einem weiteren Medium gespeichert, SOLLTE eine Sicherungskopie dieser Daten vorgehalten werden. Bei Verlust oder Beschädigung der Daten auf dem Transportweg kann der Versand mit geringfügigem Aufwand erneut erfolgen.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [NIST800150] Guide to Cyber Threat Information Sharing
  Special Publication 800-150, National Institute of Standards and Technology (NIST), 10.2016
  http://dx.doi.org/10.6028/NIST.SP.800-150

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Informations- und Datenträgeraustausch" von Bedeutung.

G 0.02 Ungünstige klimatische Bedingungen

G 0.04 Verschmutzung, Staub, Korrosion

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.22 Manipulation von Informationen

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.38 Missbrauch personenbezogener Daten

G 0.39 Schadprogramme

G 0.42 Social Engineering

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen Anforderungen	G 0.02	G 0.04	G 0.14	G 0.16	G 0.17	G 0.18	G 0.19	G 0.20	G 0.22	G 0.24	G 0.25	G 0.26	G 0.29	G 0.38	G 0.39	G 0.42	G 0.45	G 0.46
OPS.1.2.3.A1							x	x	x				x	x		x		
OPS.1.2.3.A2			x				x	x					x	x		x		
OPS.1.2.3.A3			x				x						x	x	x	x	x	
OPS.1.2.3.A4												x			x		x	x
OPS.1.2.3.A5				x	x									x			x	
OPS.1.2.3.A6			x				x	x	x				x	x				
OPS.1.2.3.A7			x				x			x	x	x	x	x	x		x	
OPS.1.2.3.A8			x				x							x				
OPS.1.2.3.A9			x				x							x				
OPS.1.2.3.A10							x						x	x				
OPS.1.2.3.A11						x												
OPS.1.2.3.A12					x		x	x						x			x	
OPS.1.2.3.A13			x	x			x		x					x				x
OPS.1.2.3.A14										x	x	x					x	
OPS.1.2.3.A15	x	x	x	x			x			x	x	x		x				
OPS.1.2.3.A16	x	x	x	x			x							x				
OPS.1.2.3.A17							x							x				x
OPS.1.2.3.A18	x	x			x					x	x	x					x	

OPS.1.2: Weiterführende Aufgaben

OPS.1.2.4 Telearbeit

1 Beschreibung

1.1 Einleitung

Unter Telearbeit wird jede auf die Informations- und Kommunikationstechnik gestützte Tätigkeit verstanden, die ausschließlich außerhalb der Geschäftsräume und Gebäude des Arbeitgebers verrichtet wird. Es gibt verschiedene Formen der Telearbeit. Sie kann beispielsweise als heimbasierte Telearbeit in der Wohnung des Mitarbeiters erbracht werden. Es ist ebenfalls möglich, dass die Mitarbeiter im Rahmen der On-Site-Telearbeit bei Kunden oder Lieferanten eingesetzt werden und dort mit der Ausstattung des eigenen Arbeitgebers arbeiten. Eine weitere Möglichkeit ist die Telearbeit in sogenannten Telecentern, Satelliten- oder auch Nachbarschaftsbüros.

Bei der heimbasierten Telearbeit wird zwischen der ausschließlich zu Hause erbrachten Arbeit und der alternierenden Telearbeit unterschieden. Bei der alternierenden Telearbeit arbeiten die Arbeitnehmer wechselweise an ihrem Arbeitsplatz beim Arbeitgeber und am häuslichen Arbeitsplatz.

1.2 Zielsetzung

Ziel des Bausteins ist der Schutz der Informationen, die während der Telearbeit gespeichert, verarbeitet und übertragen werden. Dazu werden typische Gefährdungen aufgezeigt und spezielle Anforderungen an die Telearbeit definiert.

1.3 Abgrenzung

Dieser Baustein konzentriert sich auf die Formen der Telearbeit, die teilweise oder ganz im häuslichen Umfeld durchgeführt werden. Es wird davon ausgegangen, dass zwischen dem Telearbeitsplatz und der Institution eine Telekommunikationsverbindung besteht, die es ermöglicht, Informationen auszutauschen und falls erforderlich auf Daten in der Institution zuzugreifen. Die Anforderungen dieses Bausteins umfassen drei verschiedene Bereiche:

- die Organisation der Telearbeit,
- den Telearbeitsrechner des Telearbeiters und
- die Kommunikationsverbindung zwischen Telearbeitsrechner und Institution.

Sicherheitsanforderungen an die Infrastruktur des Telearbeitsplatzes werden im vorliegenden Baustein nicht berücksichtigt, sondern sind im Baustein INF.8 *Häuslicher Arbeitsplatz* beschrieben. Die Anforderungen aus dem themenüberschneidenden Baustein INF.10 *Mobiler Arbeitsplatz* sind zu beachten.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Telearbeit von besonderer Bedeutung:

2.1 Fehlende oder unzureichende Regelungen für den Telearbeitsplatz

Da ein Telearbeitsplatz räumlich außerhalb der Institution liegt, bedarf es für ihn individuell angepasster organisatorischer Absprachen. Gibt es solche Regelungen nicht, wissen Mitarbeiter mitunter nicht, dass sie z. B. selbstständig Datensicherungen durchführen müssen. Auch wissen sie unter Umständen nicht, wie sie mit sicherheitsrelevanten Vorkommnissen am Telearbeitsplatz umgehen sollen. Gelangen beispielsweise vertrauliche Informationen in fremde Hände, können diese von Unbefugten möglicherweise zum schwerwiegenden Nachteil der Institution verwendet werden.

2.2 Fehlende oder unzureichende Schulung der Telearbeiter

Telearbeiter sind am Arbeitsplatz weitgehend auf sich allein gestellt. Ist der Telearbeiter nicht ausreichend im Umgang mit der IT geschult, kann dies bei Problemen zu erhöhten Ausfallzeiten führen, da beispielsweise ein IT-Betreuer aus der Institution erst zum Telearbeitsplatz fahren muss, um dort die Probleme zu beseitigen.

2.3 Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners

Im häuslichen Bereich ist es einfacher, den dienstlichen Telearbeitsrechner privat zu benutzen, weil Kontrollen durch den Arbeitgeber nur bedingt möglich sind. Daher kann es dazu kommen, dass nicht geprüfte und freigegebene Software eingesetzt wird und durch unbedachtes Handeln Schadsoftware auf den Telearbeitsrechner gelangt. Dadurch könnten beispielsweise vertrauliche Informationen kompromittiert werden.

Aber nicht nur Telearbeiter können ihren Rechner unsachgemäß benutzen, sondern auch Angehörige oder Besucher. Schäden wie gelöschte Festplatten können Reinstallationskosten oder Nacherfassungsarbeiten nach sich ziehen.

2.4 Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Telearbeiter

Üblicherweise hat ein Telearbeiter keine festen Arbeitszeiten am Telearbeitsplatz. Es werden lediglich feste Zeiten vereinbart, an denen er erreichbar sein muss. Bei alternierender Telearbeit sind seine Arbeitszeiten zudem noch zwischen Telearbeitsplatz und dem innerbetrieblichen Arbeitsplatz verteilt.

Ist es notwendig, dass Informationen kurzfristig vom Telearbeiter eingeholt oder Informationen an den Telearbeiter übergeben werden können, kann es aufgrund der schwierigen Erreichbarkeit zu Verzögerungen kommen. Selbst wenn die Informationen über E-Mail übermittelt werden, verkürzt das nicht notwendigerweise die Reaktionszeit, da nicht sichergestellt werden kann, dass der Telearbeiter die E-Mail zeitnah liest.

Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Telearbeiter können sich dabei je nach Situation und Institution unterschiedlich auswirken und die Verfügbarkeit einschränken.

2.5 Mangelhafte Einbindung des Telearbeiters in den Informationsfluss

Da Telearbeiter nicht täglich in der Institution sind, haben sie weniger Gelegenheit, am direkten Informationsaustausch mit Vorgesetzten und Arbeitskollegen teilzuhaben. Hierdurch können sie vom betrieblichen Geschehen isoliert werden und sich dadurch z. B. weniger mit der Institution identifizieren. Aufgrund von fehlenden Informationen können sich auch Fehler in den Arbeitsabläufen und betrieblichen Prozessen ergeben, die die Produktivität des Telearbeiters einschränken. Ist der Informationsfluss zum Telearbeiter nicht gewährleistet, erreichen ihn eventuell auch wichtige Nachrichten zum Thema Informationssicherheit nicht rechtzeitig.

2.6 Unzureichende Vertretungsregelungen für Telearbeit

Die Aufgaben des Telearbeiters sind in der Regel so konzipiert, dass er weitestgehend selbständig arbeiten kann. Damit kann es im Krankheitsfall schwierig sein, eine entsprechende Vertretung für den Telearbeiter bereitzustellen. Insbesondere kann es zu Problemen führen, die erforderlichen Unterlagen oder die Daten aus dem Telearbeitsrechner für den Vertreter bereitzustellen, wenn keine Zutrittsmöglichkeiten zum häuslichen Arbeitsplatz des Telearbeiters bestehen.

2.7 Nichtbeachtung von Sicherheitsmaßnahmen

Besonders am Telearbeitsplatz kann es aufgrund fehlender Kontrollmöglichkeiten dazukommen, dass Mitarbeiter empfohlene oder angeordnete Sicherheitsmaßnahmen nicht oder nicht in vollem Umfang umsetzen. Es können Schäden entstehen, die sonst verhindert oder zumindest vermindert worden wären. Je nach der Funktion des Mitarbeiters und der Bedeutung der missachteten Maßnahme können sogar gravierende Schäden eintreten, z. B. können vertrauliche Informationen in fremde Hände geraten. Diese können dann möglicherweise zum schwerwiegenden Nachteil der Institution verwendet werden.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz von Telearbeit aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte (ISB) für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	Informationssicherheitsbeauftragter (ISB)
Weitere Verantwortliche	IT-Betrieb, Leiter IT, Leiter Organisation, Personalabteilung, Telearbeiter, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

OPS.1.2.4.A1 Regelungen für Telearbeit [Vorgesetzte, Personalabteilung]

Alle relevanten Aspekte der Telearbeit MÜSSEN geregelt werden. Zu Informationszwecken MÜSSEN den Telearbeitern die geltenden Regelungen oder ein dafür vorgesehenes Merkblatt ausgehändigt werden, das die zu beachtenden Sicherheitsmaßnahmen erläutert. Alle strittigen Punkte MÜSSEN entweder durch Betriebsvereinbarungen oder durch zusätzlich zum Arbeitsvertrag getroffene individuelle Vereinbarungen zwischen dem Telearbeiter und Arbeitgeber geregelt werden. Für jeden Telearbeiter MUSS ein Vertreter benannt werden. Der Vertretungsfall SOLLTE regelmäßig geprobt werden. Die Regelungen MÜSSEN regelmäßig aktualisiert werden.

OPS.1.2.4.A2 Sicherheitstechnische Anforderungen an den Telearbeitsrechner [Leiter IT, IT-Betrieb]

Es MÜSSEN alle sicherheitstechnischen Anforderungen festgelegt werden, die ein Telearbeitsrechner erfüllen muss. Alle Zugangs- und Zugriffsmöglichkeiten auf die Kommunikationsrechner der Institution MÜSSEN auf das notwendige Mindestmaß beschränkt sein.

Es MUSS sichergestellt werden, dass nur autorisierte Personen auf die Telearbeitsrechner zugreifen dürfen. Darüber hinaus MUSS der Telearbeitsrechner so abgesichert werden, dass er nur für autorisierte Zwecke benutzt werden kann.

OPS.1.2.4.A3 Sicherheitstechnische Anforderungen an die Kommunikationsverbindung [Telearbeiter, Leiter IT, IT-Betrieb]

Es MÜSSEN sicherheitstechnische Anforderungen an die Kommunikationsverbindung zwischen Telearbeitsrechner und Institution definiert werden. Dabei MUSS sichergestellt sein, dass die Vertraulichkeit, Integrität und Authentizität der übertragenen Daten gewährleistet ist.

Alle eingesetzten Kommunikationsprotokolle und Sicherheitsmechanismen MÜSSEN den definierten Anforderungen der Institution genügen. Die Stärke der dazu erforderlichen Sicherheitsmechanismen SOLLTE sich nach dem Schutzbedarf der übertragenen Daten richten. Zusätzlich MUSS die Authentizität der Kommunikationspartner gewährleistet sein.

OPS.1.2.4.A4 Datensicherung bei der Telearbeit [Telearbeiter, IT-Betrieb]

Alle Daten, die bei der Telearbeit bearbeitet werden, MÜSSEN zeitnah gesichert werden. Hierfür MÜSSEN entweder lokal auf externen Datenträgern oder zentral über die Anbindung an das Netz der Institution Datensicherungen durchgeführt werden.

Das gewählte Datensicherungsverfahren MUSS für das Volumen des Datenbestands geeignet und ausreichend sein. Für einen reibungslosen Prozessablauf MÜSSEN bei der Datensicherung möglichst wenig Aktionen vom Telearbeiter ausgehen. Es SOLLTE eine Generation der Backup-Datenträger in der Institution hinterlegt werden.

OPS.1.2.4.A5 Sensibilisierung und Schulung der Telearbeiter [Vorgesetzte, Leiter IT]

Anhand eines Merkzettels MÜSSEN die Telearbeiter über die Gefahren sensibilisiert werden, die mit der Telearbeit verbunden sind. Außerdem MÜSSEN sie in die entsprechenden Sicherheitsmaßnahmen der Institution eingewiesen und im Umgang mit diesen geschult werden. Die Schulungs- und Sensibilisierungsmaßnahmen für Telearbeiter SOLLTEN regelmäßig wiederholt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Telearbeit. Sie SOLLTEN grundsätzlich umgesetzt werden.

OPS.1.2.4.A6 Erstellen eines Sicherheitskonzeptes für Telearbeit [Vorgesetzte, Leiter Organisation, Leiter IT]

Es SOLLTE ein Sicherheitskonzept für Telearbeit erstellt werden, das Sicherheitsziele, Schutzbedarf, Sicherheitsanforderungen sowie Risiken beschreibt. Das Konzept SOLLTE regelmäßig aktualisiert und überarbeitet werden. Das Sicherheitskonzept zur Telearbeit SOLLTE mit dem übergreifenden Sicherheitskonzept der Institution abgestimmt werden.

OPS.1.2.4.A7 Geregelte Nutzung der Kommunikationsmöglichkeiten bei Telearbeit [Telearbeiter, IT-Betrieb]

Es SOLLTE klar geregelt werden, welche Kommunikationsmöglichkeiten bei der Telearbeit unter welchen Rahmenbedingungen benutzt werden dürfen. Die dienstliche und private Nutzung von Internet-Diensten bei der Telearbeit SOLLTE geregelt werden. Dabei SOLLTE auch geklärt werden, ob eine private Nutzung generell erlaubt oder unterbunden wird.

OPS.1.2.4.A8 Informationsfluss zwischen Telearbeiter und Institution [Vorgesetzte, Telearbeiter]

Es SOLLTE ein regelmäßiger innerbetrieblicher Informationsaustausch zwischen den Telearbeitern, den Arbeitskollegen und der Institution gewährleistet sein. Alle Telearbeiter SOLLTEN zeitnah Informationen über geänderte Sicherheitsanforderungen und andere sicherheitsrelevante Aspekte erhalten. Allen Kollegen des jeweiligen Telearbeiters SOLLTE bekannt sein, wann und wo dieser erreicht werden kann. Technische und organisatorische Telearbeitsregelungen zur Aufgabenbewältigung, zu Sicherheitsvorfällen und sonstigen Problemen SOLLTEN geregelt und an den Telearbeiter kommuniziert werden.

OPS.1.2.4.A9 Betreuungs- und Wartungskonzept für Telearbeitsplätze [Telearbeiter, Leiter IT, IT-Betrieb]

Für Telearbeitsplätze SOLLTE ein spezielles Betreuungs- und Wartungskonzept erstellt werden. Darin SOLLTEN folgende Aspekte geregelt werden: Ansprechpartner für den Benutzerservice, Wartungstermine, Fernwartung, Transport der IT-Geräte und Einführung von Standard-Telearbeitsrechnern. Damit die Telearbeiter einsatzfähig bleiben, SOLLTEN für sie Ansprechpartner für Hard- und Softwareprobleme benannt werden.

OPS.1.2.4.A10 Durchführung einer Anforderungsanalyse für den Telearbeitsplatz [Leiter IT, IT-Betrieb]

Bevor ein Telearbeitsplatz eingerichtet wird, SOLLTE eine Anforderungsanalyse durchgeführt werden. Daraus SOLLTE z. B. hervorgehen, welche Hard- und Software-Komponenten für den Telearbeitsplatz benötigt werden. Die Anforderungen an den jeweiligen Telearbeitsplatz SOLLTEN mit den IT-Verantwortlichen abgestimmt werden. Es SOLLTE immer festgestellt und dokumentiert werden, welchen Schutzbedarf die am Telearbeitsplatz verarbeiteten Informationen haben.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [ISF] The Standard of Good Practice
  Information Security Forum (ISF), 06.2016

- [NIST80046] NIST Special Publication 800-46 Revision 2
  Guide to Enterprise Telework, Remote Access and Bring Your Own Device (BYOD) Security, NIST, 07.2016
  http://dx.doi.org/10.6028/NIST.SP.800-46r2

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Telearbeit" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.25 Ausfall von Geräten oder Systemen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.33 Personalausfall

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.14	G 0.18	G 0.19	G 0.21	G 0.22	G 0.23	G 0.24	G 0.25	G 0.30	G 0.31	G 0.32	G 0.33	G 0.40	G 0.45	G 0.46
OPS.1.2.4.A1	x	x	x	x	x	x			x	x	x	x		x	x
OPS.1.2.4.A2	x		x	x	x	x			x	x			x	x	x
OPS.1.2.4.A3	x		x	x	x	x			x	x			x		x
OPS.1.2.4.A4	x			x	x	x	x		x		x		x	x	x
OPS.1.2.4.A5	x	x	x	x	x	x									x
OPS.1.2.4.A6		x					x	x				x		x	
OPS.1.2.4.A7	x	x	x	x	x	x			x	x	x				x
OPS.1.2.4.A8		x										x			x
OPS.1.2.4.A9		x						x							x
OPS.1.2.4.A10		x													

OPS.2: IT-Betrieb von Dritten

OPS.2.1 Outsourcing für Kunden

1 Beschreibung

1.1 Einleitung

Beim Outsourcing lagern Institutionen (Outsourcing-Kunden) Geschäftsprozesse und Dienstleistungen (z. B. Wach- oder Reinigungspersonal) ganz oder teilweise zu externen Dienstleistern (Outsourcing-Dienstleistern) aus. Der Betrieb von Hardware und Software kann ebenso als Dienstleistung ausgelagert werden. Unabhängig davon, was ausgelagert wird, bedingt jede Auslagerung eine enge Bindung an den externen Dienstleister und dessen Dienstleistungsquantität und -qualität. Dieses Verhältnis ist insbesondere für den Kunden nicht nur mit Chancen, sondern auch mit erheblichen Risiken verbunden, wie z. B. starken Abhängigkeiten, Verlust von eigenem Know-how sowie Verlust von Kontroll- und Steuerungsmöglichkeiten. Informationssicherheitsaspekte müssen daher während des kompletten Lebenszyklus einer Auslagerung angemessen berücksichtigt werden.

Den Schwerpunkt dieses Bausteins bilden Anforderungen, die die Outsourcing-Kunden im Rahmen jeder Phase eines Outsourcing-Vorhabens beachten bzw. umsetzen sollten.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, sicherzustellen, dass alle Sicherheitsziele des Outsourcing-Kunden auch nach der Auslagerung von Geschäftsprozessen oder Dienstleistungen an einen Outsourcing-Dienstleister erfüllt werden und das vereinbarte Sicherheitsniveau dauerhaft aufrechterhalten (bzw. verbessert) wird. Durch das Outsourcing darf es zu keinen unkontrollierbaren Risiken für die auslagernde Institution hinsichtlich Informationssicherheit kommen.

1.3 Abgrenzung

Dieser Baustein enthält Gefährdungen und Sicherheitsanforderungen aus Sicht der Kunden von Outsourcing und beschränkt sich einzig auf die Anforderungen des Schutzes für Informationen seitens der auslagernden Institution.

Übertragungswege zu Outsourcing-Dienstleistern können durch die Umsetzung der Anforderungen nicht abgesichert werden.

Die Begriffe Outsourcing und Cloud haben viele Parallelen. Für Kunden von Outsourcing sind in der Regel auch Anforderungen hinsichtlich Nutzen von Cloud-Services zusätzlich zu beachten.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Outsourcing von Kunden von besonderer Bedeutung:

2.1 Fehlende oder unzureichendeRegelungen zur Informationssicherheit

Im Rahmen eines Outsourcing-Vorhabens werden typischerweise große Mengen von Informationen zwischen dem Kunden und dem Outsourcing-Dienstleister übertragen. Abhängig vom Schutzbedarf der zu verarbeitenden Informationen können fehlende oder unzureichende Regelungen Schäden verursachen. Dies ist zum Beispiel dann der Fall, wenn bei technischen, organisatorischen oder personellen Änderungen die Regelungen und Anweisungen zur Steuerung des Dienstleisters nicht aktualisiert werden, etwa bei Änderung von Ansprechpartnern. Das Spektrum der Regelungsdefizite reicht dabei von Unklarheiten bei Zuständigkeiten und Kontrollfunktionen über unverständlich oder zusammenhanglos formulierte Regelungen, bis hin zu komplett fehlenden Regelungen.

2.2 Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten

Je nach Outsourcing-Vorhaben kann es erforderlich sein, dass die Mitarbeiter des Outsourcing-Kunden Zutritts-, Zugangs- und Zugriffsrechte zu IT-Systemen, Informationen, Gebäuden oder Räumen des Outsourcing-Dienstleisters benötigen. Wenn die Vergabe, Verwaltung und Kontrolle dieser Rechte schlecht geregelt ist und dadurch im Extremfall sogar unautorisiert Rechte vergeben werden, ist die Gewährleistung des notwendigen Schutzbedarfs der Informationen des Outsourcing-Kunden nicht mehr gegeben. Beispielsweise kann die unkontrollierte Vergabe von administrativen Berechtigungen an Mitarbeiter des Outsourcing-Dienstleisters zu gravierenden Sicherheitsrisiken führen. Diese könnten Berechtigungen ausnutzen und sensible Informationen kopieren oder manipulieren.

2.3 Fehlendes oder unzureichendes Test- und Freigabeverfahren

Hat ein Outsourcing-Kunde keine angemessenen Anforderungen zu Test- und Freigabeverfahren für den Outsourcing-Dienstleister definiert, werden vorhandene Fehler in der Hard- und Software oder Sicherheitslücken in der Konfiguration eventuell nicht oder nicht rechtzeitig erkannt. Dieser Mangel kann dazu führen, dass der notwendige Schutz der Informationen des Outsourcing-Kunden nicht mehr gewährleistet werden kann. Wenn sich bei Tests herausstellt, dass sich durch neue Komponenten oder Updates wesentliche Änderungen an Arbeitsabläufen ergeben oder für ein annehmbares Verarbeitungstempo mehr Ressourcen (z. B. Hauptspeicher, Prozessorkapazität) benötigt werden und dies dem Kunden nicht mitgeteilt wird, kann das zu erheblichen Fehl- oder Folgeinvestitionen führen.

2.4 Unzulängliche vertragliche Regelungen mit einem Outsourcing-Dienstleister

Aufgrund von unzulänglichen vertraglichen Regelungen mit einem Outsourcing-Dienstleister können vielfältige und auch schwerwiegende Sicherheitsprobleme auftreten. Wenn Aufgaben, Leistungsparameter oder Aufwände ungenügend oder missverständlich beschrieben wurden, kann die Folge sein, dass aus Unkenntnis oder wegen fehlender Ressourcen Sicherheitsmaßnahmen nicht umgesetzt werden. Dies kann eine Vielzahl negativer Auswirkungen nach sich ziehen wie die Nichterfüllung regulatorischer Anforderungen und Pflichten, die fehlende Einhaltung von Auskunftspflichten und Gesetzen bis hin zur fehlenden Übernahme von Verantwortung aufgrund des Verlusts vom fehlender Kontroll- und Steuerungsmöglichkeiten.

2.5 Unzulängliche Regelungen für das Ende eines Outsourcings

Ohne ausreichende und angemessene Regelungen für die Auflösung eines Outsourcing-Vertrags durch den Outsourcing-Kunden besteht die Gefahr, dass sich der Outsourcing-Kunde nur schwer vom Outsourcing-Dienstleister lösen kann. Ebenso kann es andersherum ebenso passieren, dass eine zu kurzfristig mögliche Kündigung des Outsourcing-Dienstleisters den Outsourcing-Kunden dazu zwingt, einen ungeeigneten neuen Outsourcing-Dienstleister auszuwählen zu müssen. In beiden Fällen kann es schwierig bis unmöglich sein, den ausgelagerten Bereich auf einen anderen Dienstleister zu übertragen oder ihn wieder in die eigene Institution einzugliedern. Dabei kann es zu verschiedensten Sicherheitsproblemen kommen, beispielsweise könnten während des Auflösungsprozesses Daten und Systeme nicht mehr ausreichend geschützt sein, da diese als "Alt-Systeme" angesehen werden. Unzureichende Regelungen für das Löschen von Datenbeständen, auch von Datensicherungen, können dazu führen, dass vertrauliche Daten Dritten bekannt werden.

2.6 Abhängigkeit von einem Outsourcing-Dienstleister

Durch die Entscheidung für Outsourcing begibt sich eine Institution immer in eine Abhängigkeit vom Outsourcing-Dienstleister. Mit dieser Abhängigkeit ist die Gefahr verbunden, dass Know-how verloren geht und keine vollständige Kontrolle über die ausgelagerten Prozesse und Komponenten mehr besteht. Außerdem kann es zu einer unterschiedlichen Einschätzung des Schutzbedarfs der ausgelagerten Geschäftsprozesse und Informationen kommen und damit zu unzureichenden Sicherheitsmaßnahmen. Dadurch, dass der Outsourcing-Dienstleister die vollständige Kontrolle über Geschäftsprozesse, schutzbedürftige Informationen, Ressourcen und IT-Systeme hat und gleichzeitig das Wissen über diese beim Outsourcing-Kunden weniger wird, werden unter Umständen Defizite der Informationssicherheit nicht mehr bemerkt.

Diese Situation könnte vom Outsourcing-Dienstleister beispielsweise durch drastische Preiserhöhungen und eine nicht ausreichende Dienstleistungsqualität ausgenutzt werden.

2.7 Störung des Betriebsklimas durch ein Outsourcing-Vorhaben

Outsourcing-Vorhaben werden aus Sicht der Mitarbeiter der auslagernden Institution oft als negative Veränderungen gesehen. Dies führt häufig zu einem schlechten Betriebsklima. Die Mitarbeiter des Outsourcing-Kunden befürchten oft für sie nachteilige Aufgabenänderungen oder sogar einen Stellenabbau durch Outsourcing-Vorhaben. Bei einer negativen Haltung gegenüber dem Outsourcing-Vorhaben könnten Mitarbeiter unabsichtlich oder mutwillig Sicherheitsmaßnahmen vernachlässigen, eine Boykott-Haltung einnehmen oder sogar Racheakte verüben. Außerdem könnten dadurch Know-how-Träger (wie beispielsweise IT-Leiter und der IT-Betrieb) während der Einführungsphase kündigen, so dass das Outsourcing-Vorhaben nicht wie geplant umgesetzt werden kann.

2.8 Mangelhafte Informationssicherheit in der Outsourcing-Einführungsphase

Die Einführungsphase von Outsourcing-Vorhaben ist oft geprägt von engen terminlichen und finanziellen Vorgaben. Dies kann zu fehlenden Sicherheitskontrollen und Audits führen oder Reviews und weitere qualitätssichernde Maßnahmen bleiben aus, zum Beispiel bei der Erstellung von Sicherheitskonzepten. Übergangsmaßnahmen mit Sicherheitsdefiziten werden mit der Zeit zur Gewohnheit und aufgrund von Ressourcenengpässen über Jahre beibehalten. Hieraus entsteht die konkrete Gefahr, dass sich dadurch ein "Projektklima" etabliert, das weitere gravierende Sicherheitsmängel entstehen lässt.

2.9 Ausfall der Systeme eines Outsourcing-Dienstleisters

Bei einem Outsourcing-Dienstleister können die dort betriebenen IT-Systeme und Prozesse teilweise oder ganz ausfallen, wodurch auch der Outsourcing-Kunde betroffen ist. Bei unzureichender Mandantentrennung kann unter Umständen auch der Ausfall eines Systems, das nicht dem Outsourcing-Kunde zugeordnet ist, trotzdem dazu führen, dass der Outsourcing-Kunde seine vertraglich zugesicherte Dienstleistung nicht mehr abrufen kann. Ähnliche Probleme ergeben sich, wenn die Anbindung zwischen Outsourcing-Dienstleister und -Kunde ausfällt.

2.10 Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister

Wenn bei einem Outsourcing-Vorhaben die IT-Anbindung zwischen dem Outsourcing-Dienstleister und dem Outsourcing-Kunden unzureichend abgesichert ist, kann die Vertraulichkeit und Integrität der übermittelten Daten gefährdet sein. Es könnten sich aber auch durch offene oder schlecht gesicherte Schnittstellen unautorisierte Zugangsmöglichkeiten für Außenstehende auf die Systeme der beteiligten Institutionen ergeben.

2.11 Fehlende Mandantenfähigkeit beim Outsourcing-Dienstleister

Outsourcing-Dienstleister haben in der Regel viele verschiedene Kunden, die auf die gleiche Ressourcenbasis (z. B. IT-Systeme, Netze, Personal) zurückgreifen. Wenn die IT-Systeme und Daten der verschiedenen Kunden nicht ausreichend sicher voneinander getrennt sind, besteht die Gefahr, dass ein Kunde auf den Bereich eines anderen Kunden zugreifen kann. Außerdem könnte es zu Interessenskonflikten

beim Outsourcing-Dienstleister kommen, wenn er parallel vergleichbare Ressourcenforderungen erfüllen muss. Wenn sich die jeweiligen Kunden in einer Konkurrenzsituation befinden, kann dies besonders problematisch sein.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Outsourcing für Kunden aufgeführt. Grundsätzlich ist der Leiter IT für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Leiter IT
Weitere Verantwortliche	Fachverantwortliche, ISB Outsourcing-Kunde, IT-Betrieb, Leiter Beschaffung, Leiter Organisation, Leiter Personal, Notfallbeauftragter, Änderungsmanager

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

OPS.2.1.A1 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben [ISB Outsourcing-Kunde]

Alle Sicherheitsanforderungen für ein Outsourcing-Vorhaben MÜSSEN auf Basis der Outsourcing-Strategie festgelegt sein. Es MÜSSEN beide Outsourcing-Parteien auf die Einhaltung von IT-Grundschutz oder eines vergleichbaren Schutzniveaus vertraglich verpflichtet sein. Es MÜSSEN alle Schnittstellen zwischen dem Outsourcing-Dienstleister und -Kunden identifiziert und entsprechende Sicherheitsanforderungen dafür definiert werden. Es MUSS in den Sicherheitsanforderungen festgelegt sein, welche Berechtigungen (Zutrittsrechte, Zugangsrechte, Zugriffsrechte) jeweils gegenseitig eingerichtet werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Outsourcing für Kunden. Sie SOLLTEN grundsätzlich umgesetzt werden.

OPS.2.1.A2 Rechtzeitige Beteiligung der Personalvertretung [Leiter Organisation]

Die Personalvertretung SOLLTE rechtzeitig über ein Outsourcing-Vorhaben informiert werden. Die Beteiligung der Personalvertretung SOLLTE schon in der Angebotsphase erfolgen. Je nach Outsourcing-Vorhaben SOLLTE das gesetzliche Mitspracherecht beachtet werden.

OPS.2.1.A3 Auswahl eines geeigneten Outsourcing-Dienstleisters [ISB Outsourcing-Kunde]

Zur Auswahl des Outsourcing-Dienstleisters SOLLTE ein Anforderungsprofil mit den Sicherheitsanforderungen für das Outsourcing-Vorhaben existieren. Es SOLLTEN Bewertungskriterien für den Outsourcing-Dienstleister und dessen Personal vorliegen, die auf diesem Anforderungsprofil basieren.

OPS.2.1.A4 Vertragsgestaltung mit den Outsourcing-Dienstleister [ISB Outsourcing-Kunde]

Es SOLLTEN alle Aspekte des Outsourcing-Vorhabens mit dem Outsourcing-Dienstleister schriftlich geregelt sein. Es SOLLTEN alle Rollen und Mitwirkungspflichten zur Erstellung, Prüfung und Änderung (z. B. von Personen) des Sicherheitskonzepts mit dem Outsourcing-Dienstleister geregelt sein. Die Rechte und Pflichten der Vertragsparteien SOLLTEN schriftlich geregelt sein. Für die regelmäßige Überprüfung der Anforderungen SOLLTE der Outsourcing-Dienstleister dem Outsourcing-Kunden die Möglichkeit von Audits gewährleisten.

OPS.2.1.A5 Festlegung einer Outsourcing-Strategie [ISB Outsourcing-Kunde]

Es SOLLTE eine Outsourcing-Strategie festgelegt werden, die neben den wirtschaftlichen, technischen, organisatorischen und rechtlichen Rahmenbedingungen auch die relevanten Aspekte für Informationssicherheit berücksichtigt. Es SOLLTE geklärt werden, welche Geschäftsprozesse, Aufgaben oder Anwendungen generell für ein Outsourcing in Frage kommen. Der Outsourcing-Kunde SOLLTE ausreichende Fähigkeiten, Kompetenzen und Ressourcen behalten, um in jedem Outsourcing-Vorhaben die Anforderungen an die Informationssicherheit bestimmen und kontrollieren zu können. In der Outsourcing-Strategie SOLLTEN die Ziele, Chancen und Risiken des Outsourcing-Vorhabens beschrieben werden.

OPS.2.1.A6 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben [Fachverantwortliche, ISB Outsourcing-Kunde]

Der Outsourcing-Kunde SOLLTE für jedes Outsourcing-Vorhaben ein Sicherheitskonzept basierend auf den zugehörigen Sicherheitsanforderungen erstellen. Ebenso SOLLTE jeder Outsourcing-Dienstleister ein individuelles Sicherheitskonzept für das jeweilige Outsourcing-Vorhaben vorlegen. Beide Sicherheitskonzepte SOLLTEN miteinander abgestimmt werden. Das Sicherheitskonzept des Outsourcing-Dienstleisters und der Umsetzung SOLLTEN in ein Gesamt-Sicherheitskonzept zusammengefügt und durch den Outsourcing-Kunden oder unabhängige Dritte regelmäßig auf deren Wirksamkeit überprüft werden.

OPS.2.1.A7 Festlegung der möglichen Kommunikationspartner [Leiter Organisation, ISB Outsourcing-Kunde]

Es SOLLTE festgelegt werden, welche internen und externen Kommunikationspartner welche Informationen über das jeweilige Outsoucing-Projekt übermitteln und erhalten dürfen. Es SOLLTE ein Prozess existieren, mit dem die Funktion der Kommunikationspartner auf beiden Seiten geprüft wird. Die zulässigen Kommunikationspartner mit den jeweiligen Berechtigungen MÜSSEN immer aktuell dokumentiert sein.

OPS.2.1.A8 Regelungen für den Einsatz des Personals des Outsourcing-Dienstleiters [Leiter Personal, ISB Outsourcing-Kunde]

Die Mitarbeiter des Outsourcing-Dienstleisters SOLLTEN schriftlich auf die Einhaltung der einschlägigen Gesetze, Vorschriften und der beim Outsourcing-Kunden gültigen Regelungen verpflichtet werden. Die Mitarbeiter des Outsourcing-Dienstleisters SOLLTEN geregelt in ihre Aufgaben eingewiesen und über bestehende Regelungen zur Informationssicherheit unterrichtet werden. Es SOLLTEN für die Mitarbeiter des Outsourcing-Dienstleisters Vertretungsregelungen existieren. Es SOLLTE ein geregeltes Verfahren für die Beendigung des Auftragsverhältnisses mit den Mitarbeitern des Outsourcing-Dienstleisters existieren. Kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal beim Outsourcing-Dienstleister SOLLTE wie Besucher behandelt werden.

OPS.2.1.A9 Vereinbarung über die Anbindung an Netze der Outsourcing-Partner [ISB Outsourcing-Kunde]

Vor der Anbindung des Netzes des Outsourcing-Kunden an das Netz des Outsourcing-Dienstleisters SOLLTEN alle sicherheitsrelevanten Aspekte in einer Vereinbarung schriftlich geregelt werden. In der Vereinbarung SOLLTE genau definiert sein, auf welche Bereiche und Dienste der Outsourcing-Dienstleister im Netz des Outsourcing-Kunden zugreifen darf. Die Einhaltung der Vereinbarungen für die Netz-

anbindung SOLLTE geprüft und dokumentiert werden. Es SOLLTEN auf beiden Seiten Ansprechpartner sowohl für organisatorische als auch technische Fragestellungen der Netzanbindung benannt werden. Das geforderte Sicherheitsniveau SOLLTE nachweislich beim Outsourcing-Dienstleister eingefordert und geprüft werden, bevor die Netzanbindung zum Outsourcing-Dienstleister aktiviert wird. Für den Fall von Sicherheitsproblemen auf einer der beiden Seiten SOLLTE festgelegt sein, wer darüber zu informieren ist und welche Eskalationsschritte einzuleiten sind.

OPS.2.1.A10 Vereinbarung über Datenaustausch zwischen den Outsourcing-Partnern [ISB Outsourcing-Kunde]

Für den regelmäßigen Datenaustausch mit festen Kommunikationspartnern SOLLTEN die erforderlichen Sicherheitsmaßnahmen vereinbart werden. Datenformate und Vorgehensweisen zum sicheren Datenaustausch SOLLTEN festgelegt werden. Ansprechpartner sowohl für organisatorische als auch technische Probleme und insbesondere für sicherheitsrelevante Ereignisse beim Datenaustausch mit Dritten SOLLTEN benannt werden. Verfügbarkeiten und Reaktionszeiten beim Datenaustausch mit Dritten SOLLTEN vereinbart werden. Es SOLLTE festgelegt werden, welche ausgetauschten Daten zu welchen Zwecken genutzt werden dürfen.

OPS.2.1.A11 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb [ISB Outsourcing-Kunde]

Es SOLLTE ein Betriebskonzept für das Outsourcing-Vorhaben erstellt werden, das auch die Sicherheitsaspekte berücksichtigt. Die Sicherheitskonzepte der Outsourcing-Partner SOLLTEN regelmäßig auf Aktualität und Konsistenz zueinander geprüft werden. Der Status der vereinbarten Sicherheitsmaßnahmen SOLLTE regelmäßig kontrolliert werden. Zwischen den Outsourcing-Partnern SOLLTE eine regelmäßige Kommunikation einschließlich Abstimmung zu Änderungen und Verbesserungen stattfinden.

Die Outsourcing-Partner SOLLTEN regelmäßig gemeinsame Übungen und Tests zur Aufrechterhaltung des Sicherheitsniveaus durchführen. Informationen über Sicherheitsrisiken und den Umgang damit SOLLTEN in regelmäßigen Abständen zwischen den Outsourcing-Partnern ausgetauscht werden. Es SOLLTE ein Prozess existieren, der den Informationsfluss im Umgang mit Sicherheitsvorfällen sicherstellt, welche die jeweiligen Vertragspartner betreffen.

OPS.2.1.A12 Änderungsmanagement [IT-Betrieb, Änderungsmanager]

Der Outsourcing-Kunde SOLLTE über größere Änderungen rechtzeitig vorab informiert werden. Eine Dokumentation aller wesentlichen Änderungen bezüglich Planung, Test, Genehmigung und Dokumentation SOLLTE vom Outsourcing-Kunden regelmäßig eingefordert werden. Bevor Änderungen durchgeführt werden, SOLLTEN gemeinsam mit dem Outsourcing-Dienstleister Rückfall-Lösungen erarbeitet werden.

OPS.2.1.A13 Sichere Migration bei Outsourcing-Vorhaben

Für die Migrationsphase SOLLTE ein Sicherheitsmanagement-Team aus qualifizierten Mitarbeitern des Outsourcing-Kunden und des Outsourcing-Dienstleisters eingerichtet werden. Es SOLLTE für die Migrationsphase ein vorläufiges Sicherheitskonzept erstellt werden, in dem auch die Test- und Einführungsphase betrachtet wird. Es SOLLTE sichergestellt sein, dass produktive Daten in der Migrationsphase nicht ungeschützt als Testdaten verwendet werden. Es SOLLTEN alle Änderungen dokumentiert werden. Nach Abschluss der Migration SOLLTE das Sicherheitskonzept aktualisiert werden. Es SOLLTE sichergestellt sein, dass alle Ausnahmeregelungen am Ende der Migrationsphase aufgehoben werden. Bei Änderungen in der Migrationsphase SOLLTE geprüft werden, inwieweit ein Anpassungsbedarf an den vertraglichen Grundlagen besteht.

OPS.2.1.A14 Notfallvorsorge beim Outsourcing [Notfallbeauftragter]

Es SOLLTE ein Notfallvorsorgekonzept zum Outsourcing existieren, das die Komponenten beim Outsourcing-Kunden, beim Outsourcing-Dienstleister sowie die zugehörigen Schnittstellen umfasst. Im Notfallvorsorgekonzept zum Outsourcing SOLLTEN die Zuständigkeiten, Ansprechpartner und Abläufe zwischen dem Outsourcing-Kunden und dem Outsourcing-Dienstleister geregelt sein. Der Outsour-

cing-Kunde SOLLTE die Umsetzung der Notfallmaßnahmen des Outsourcing-Dienstleisters kontrollieren. Es SOLLTEN dazu gemeinsame Notfallübungen von Outsourcing-Kunden und Outsourcing-Dienstleister durchgeführt werden.

OPS.2.1.A15 Geordnete Beendigung eines Outsourcing-Verhältnisses [Leiter Beschaffung]

Der Vertrag mit dem Outsourcing-Dienstleister SOLLTE alle Aspekte der Beendigung des Dienstleistungsverhältnisses regeln, sowohl für eine geplante als auch für eine ungeplante Beendigung des Vertrags. Es SOLLTE sichergestellt sein, dass eine Beendigung des Dienstleistungsverhältnisses mit dem Outsourcing-Dienstleister die Geschäftstätigkeit des Outsourcing-Kunden nicht beeinträchtigt.

Der Outsourcing-Kunde SOLLTE alle Informationen und Daten nach der Beendigung zurück erhalten. Der Outsourcing-Dienstleister SOLLTE alle Datenbestände nach erfolgter Rückgabe sicher löschen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.2.1.A16 Sicherheitsüberprüfung von Mitarbeitern (CI)

Mit externen Outsourcing-Dienstleistern SOLLTE vertraglich vereinbart werden, dass die Vertrauenswürdigkeit des eingesetzten Personals geeignet überprüft wird. Dazu SOLLTEN gemeinsam Kriterien festgelegt werden.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [BVIT2005] Buisiness Process Outsourcing Leitfaden
  Business Process Outsourcing Leitfaden - BPO als Chance für den Standort Deutschland, Bundesverband Informationswirtschaft Telekommunikation und neue Medien, Version 10.1, 2005
  https://www.bitkom.org/Bitkom/Publikationen/Leitfaden-Business-Process-Outsourcing.html

- [BVIT2008] Leitfaden rechtliche Asprekte von Outsourcing in der Praxis
  Rechtliche Aspekte von Outsourcing in der Praxis, Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V., 2008
  https://www.bitkom.org/Bitkom/Publikationen/Rechtliche-Aspekte-von-Outsourcing-in-der-Praxis.html

- [DIN37500] DIN ISO 37500:2015-08
  Leitfaden Outsourcing, DIN Deutsches Institut für Normung e.V., 08.2015

- [ISF] The Standard of Good Practice
  Information Security Forum (ISF), 06.2016

- [NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations
  Special Publication 800-53, Revision 4, NIST, 04.2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Outsourcing für Kunden" von Bedeutung.

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.25 Ausfall von Geräten oder Systemen

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.35 Nötigung, Erpressung oder Korruption

G 0.42 Social Engineering

Elementare Gefährdungen / Anforderungen	G 0.11	G 0.14	G 0.15	G 0.17	G 0.18	G 0.19	G 0.22	G 0.25	G 0.29	G 0.35	G 0.42
OPS.2.1.A1					x				x		
OPS.2.1.A2									x		
OPS.2.1.A3	x										
OPS.2.1.A4									x		
OPS.2.1.A5	x				x				x		
OPS.2.1.A6				x	x	x	x	x	x		
OPS.2.1.A7		x				x					x
OPS.2.1.A8						x			x		
OPS.2.1.A9	x		x		x						
OPS.2.1.A10		x	x	x		x	x				
OPS.2.1.A11						x					
OPS.2.1.A12					x						
OPS.2.1.A13					x	x					
OPS.2.1.A14	x							x			
OPS.2.1.A15	x										
OPS.2.1.A16									x	x	

OPS.2: IT-Betrieb von Dritten

OPS.2.4 Fernwartung

1 Beschreibung

1.1 Einleitung

Mit Fernwartung wird ein räumlich getrennter Zugriff auf IT-Systeme und die darauf laufenden Anwendungen zu Konfigurations-, Wartungs-, Reparatur- oder Kontrollzwecken bezeichnet. Die Fernwartung kann passiv durch einen ausschließlich betrachtenden Zugang auf das IT-System bzw. die Anwendungen erfolgen oder aktiv durch direkte administrative Eingriffe in das Betriebssystem oder laufende Anwendungen. Im Fall der passiven Fernwartung muss ein Benutzer vor Ort unter Anleitung durch einen Administrator die eigentlichen Aktionen durchführen. Bei der aktiven Fernwartung dagegen wird in ein Betriebssystem eingegriffen und dieses direkt durch einen Administrator bedient. Dabei werden unter anderem die Signale einer Maus und Tastaturbefehle, sowie Bildschirminhalte und Konsolenausgaben übertragen. Selbst wenn wirkungsvolle Mechanismen zur Absicherung des Fernwartungs-Zugangs implementiert werden, bestehen direkte Zugriffsmöglichkeiten von außerhalb auf das interne Netz und darin verarbeiteten Daten. Durch diese Schnittstellen können Externe die Institution gefährden und somit wirtschaftliche und betriebstechnische Schäden anrichten.

1.2 Zielsetzung

Ziel des Bausteins ist der Schutz der Informationen, die auf Basis der Fernwartung gespeichert, verarbeitet und übertragen werden. Zu diesem Zweck werden Anforderungen an die Fernwartung gestellt, die sich auf Funktionen der aktiven und passiven Fernwartung beziehen.

1.3 Abgrenzung

Dieser Baustein betrachtet Fernwartung aus der Sicht des IT-Betriebs und gibt Hinweise für Anwender, wie Fernwartung eingesetzt werden kann. Wichtig ist die ganzheitliche Gewährleistung der Informationssicherheit in allen Lebenszyklusphasen. Die Sicherheitsaspekte der eingesetzten Kommunikationsverbindungen, Authentisierungsmechanismen sowie die Absicherung der Fernwartungs-Zugänge sind dabei wichtige Bestandteile des Bausteins. Im Kontext des Bausteins Fernwratung werden nicht alle relevanten Aspekte der damit in Verbindung stehenden Geschäftsprozesse abgedeckt. Daher müssen vor allem Aspekte der Bausteine *OPS.1.1.3 Patch- und Änderungsmanagement*, *ORP.3 Sensibilisierung und Schulung, CON.1 Kryptokonzept* und CON.3 *Datensicherungskonzept* gesondert gewährleistet werden. Ebenso sind die Vorgaben der Bausteinschichten NET (Netze und Kommunikation), DER (Detektion & Reaktion),die Bausteine der Schicht *OPS.2 IT-Betrieb von Dritten* und die Bausteine der Schicht *OPS.3 IT-Betrieb für Dritte* umgesetzt werden, die direkt mit der Fernadministration in Verbindung stehen. Bei cloudbasierten Produkten muss der Baustein *OPS.2.2 Cloud-Nutzung* beachtet werden. Ebenso sind die Remote Procedure Calls von Windows 2010 nicht Bestandteil dieses Bauteins.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Fernwartung von besonderer Bedeutung:

2.1 Unzureichende Kenntnisse über Regelungen der Fernwartung

Sollten die Beteiligten wichtige Regelungen nur unzureichend kennen und darum nicht anwenden, ist der Schutz der Informationen im Rahmen einer Ferwartung gefährdet. Daher bestehen Gefahren für den IT-Betrieb, wenn geltende Regelungen nicht allgemein bekannt gemacht werden. Insbesondere Administratoren, die Fernwartung einrichten und nutzen, sind auf Regelungen, z. B. zu Konfiguationen, angewiesen , da sonst mit der Fernwartung zusätzliche Betriebsrisiken, aber auch Sicherheitslücken zum internen Netz entstehen und Angriffe über die Fernwartung nicht erkannt oder abgewehrt werden können.

2.2 Fehlende oder unzureichende Planung und Regelung der Fernwartung

Wird die Fernwartung nicht sorgfältig geplant, aufgebaut und geregelt, kann nicht nur die Sicherheit eines IT-Systems, sondern aller IT-Systeme einer Institution beeinträchtigt werden, wenn Sicherheitslücken ausgenutzt werden. Sicherheitslücken können an vielen Stellen entstehen und Kommunikationsprotokolle, Patch-Prozesse, Verschlüsselungsalgorithmen und Authentisierungsmechanismen betreffen. Über unzureichend gesicherte Fernwartungsschnittstellen kann auch ein gekoppeltes Netz eines Dritten kompromittiert werden.

2.3 Unerlaubtes Ausüben von Rechten bei der Fernwartung

Auf die jeweiligen Aufgaben zugeschnittene Zutritts-, Zugangs- und Zugriffsberechtigungen werden eingesetzt, um Informationen, Geschäftsprozesse und IT-Systeme vor unbefugtem Zugriff zu schützen. Werden solche Berechtigungen bei der Fernwartung an unberechtigte Personen vergeben oder werden Rechte unautorisiert aus der Ferne ausgeübt, können sich eine Vielzahl von Gefahren für die Vertraulichkeit und Integrität von Daten und die Verfügbarkeit z. B. von Rechenleistungen ergeben. Mögliche Schadensszenarien sind beispielsweise das Einschleusen von Schadsoftware, die Manipulation von Daten und Informationen und die unbefugte Informationsgewinnung. Auswirkungen können z. B. finanzielle und Wissensverluste, physische Zerstörungen von Sachgütern und Kompromittierungen von IT-Systemen und Netzen sein.

2.4 Ungeeignete Nutzung von Authentisierung bei der Fernwartung

Bei der Fernwartung werden Authentisierungsmechanismen verwendet, die auf einer Benutzerverwaltung mit gespeicherten Authentisierungsdaten beruhen. Erlangen unberechtigte Dritte administrative Berechtigungen auf Fernwartungsrechner bzw. für Fernwartungswerkzeuge, können weitreichende Schäden für die Institution entstehen. Dazu zählen z. B. unbefugte Konfigurationen an IT-Systemen und Anwendungen, Kompromittierungen sowie Informations- und Datenverluste.

2.5 Unsicherer und unkontrollierter Aufbau von Kommunikationsverbindungen

Für eine Fernwartung ist grundsätzlich ein Zugriff auf Kommunikationsschnittstellen des administrierten Rechners erforderlich. Dies beinhaltet immer auch ein Gefährdungspotential.

Ebenso ist bei Kommunikationsschnittstellen von IT-Systemen für den Benutzer nicht immer offensichtlich, was neben Benutzer- und Protokollinformationen zusätzlich übertragen wird. Eine manipulierte oder auch nur aktivierte Kommunikationsschnittstelle kann unter Umständen ohne Initiierung durch einen Benutzer eine Verbindung zu einer Gegenstelle aufbauen oder über eine dem Benutzer nicht bekannte Funktion durch Dritte angesprochen werden.

2.6 Fehlerhafte Fernwartung

Für die Gewährleistung der Sicherheit und Funktionsfähigkeit von IT-Systemen und Anwendungen, auf die nur aus der Ferne zugegriffen werden kann, ist eine professionelle und kontinuierliche Fernwartung erforderlich. Werden diese IT-Systeme und Anwendungen nicht ordnungsgemäß per Fernwartung kon-

figuriert, gewartet, repariert und kontrolliert, können sie im schlimmsten Fall nicht mehr genutzt werden. Sollten innerhalb der Fernwartungsprozesse Fehler entstehen, können daraus direkt Fehlfunktionen einzelner Betriebssystemfunktionen resultieren. Außerdem können durch verspätete oder fehlerhafte IT-Systemwartungen Sicherheitslücken entstehen.

2.7 Verwendung unsicherer Protokolle in der Fernwartung

Die Kommunikation über öffentliche und interne Netze mittels unsicherer Protokolle stellt eine potenzielle Gefahr dar. Werden z. B. veraltete Versionen von IPSec, SSH oder SSL/TLS eingesetzt, um einen Tunnel zwischen zwei Endpunkten bzw. Netzen herzustellen, kann die Sicherheit dieser Tunnel nicht ausreichend gewährleistet werden. Angreifer können Schwachstellen dieser Protokolle ausnutzen, um in geschützte Verbindungen eigene Inhalte einzuschleusen. Generell als unsicher gelten Protokolle, bei denen Informationen im Klartext übertragen werden.

2.8 Ungeeigneter Umgang mit Authentisierungsverfahren bei der Fernwartung

Die Sicherheit eines Authentisierungsverfahrens ist direkt abhängig vom sorgfältigen Umgang damit . Die Weitergabe von benutzergebundenen Authentisierungsdaten und die unsichere Aufbewahrung dieser Angaben stellen eine mögliche Gefahr dar. Es können Sicherheitslücken für den unbefugten Zugriff auf die Rechte- und Rollenprofile der Administratoren sowie auf IT-Systeme und Anwendungen entstehen.

2.9 Unsichere kryptographische Algorithmen bei der Fernwartung

Es kommt zu einem Sicherheitsverlust innerhalb der Fernwartung, wenn unsichere kryptographische Verfahren eingesetzt oder geheime Schlüssel nicht ausreichend geschützt werden. Nachlässigkeiten im Bereich der kryptographischen Algorithmen können zu Kompromittierungen kryptographischer Schlüssel führen. Zusätzlich können Angreifer leichter eindringen, wenn sie mit vertretbaren zeitlichen und technischen Ressourcen das eingesetzte kryptographische Verfahren analysieren oder brechen und anschließend dadurch in die Kommunikation eindringen können.

2.10 Unsichere und unkontrollierte Fremdnutzung der Fernwartungs-Zugänge

Wird Unbefugten bzw. Dritten ermöglicht, die Komponenten der Fernwartung ohne vertragliche Grundlage zu nutzen, indem z. B. Berechtigungskonzepte der Institution umgangen oder nicht sorgfältig umgesetzt werden, ist die Sicherheit der Fernwartung, der IT-Systeme und der Anwendungen nicht mehr gewährleistet.

2.11 Nutzung von Online-Diensten für die Fernwartung

Neben einer Fernwartung, bei der ein Administrator direkt eine Datenverbindung zu der zu administrierenden Institution aufbaut, können auch sogenannte Online-Dienste genutzt werden. Hierbei verbinden sich die zu administrierenden IT-Systeme mit den Servern eines Drittanbieters und die Administratoren können über einen Webbrowser oder Ähnlichem auf die zu administrierenden IT-Systeme zugreifen.

Da die Kommunikation nicht Ende-zu-Ende verschlüsselt wird und der Zugriff über einen Dritten stattfindet, könnte der Datenaustausch direkt mitgelesen werden. Zusätzlich könnten auch die IT-Systeme durch unberechtigte Personen administriert werden, indem die Datenverbindung verändert wird. Bauen die IT-Systeme automatisch beim Systemstart eine Datenverbindung zum Online-Dienst auf und sind die Zugangsdaten bekannt, könnte direkt auf das IT-System zugegriffen werden.

Um eine Verbindung zum Online-Dienst aufzubauen, werden oft keine administrativen Rechte auf den zu administrierenden IT-Systemen benötigt, der Administrator benötigt dann nur einen Browser. Benutzer ohne administrative Rechte können so unautorisiert einen Fernzugriff initiieren.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Fernwartung aufgeführt. Grundsätzlich ist der Leiter IT für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Leiter IT
Weitere Verantwortliche	Benutzer, IT-Betrieb

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

OPS.2.4.A1 Planung des Einsatzes der Fernwartung [IT-Betrieb]

Der Einsatz der Fernwartung MUSS an die Institution angepasst und bedarfsgerecht hinsichtlich technischer und organisatorischer Aspekte geplant werden. Es MUSS geklärt werden, ob In-Band und/oder Out-Band Administration genutzt wird, welche IT-Systemschnittstellen und Protokolle verwendet werden. Es MUSS geklärt werden, wie die Fernwartung abgesichert wird und wie dies auditiert wird.

OPS.2.4.A2 Sicherer Verbindungsaufbau bei der Fernwartung [Benutzer]

Die Initiierung des Fernwartungs-Zugriffs MUSS aus der Institution heraus erfolgen. Der Benutzer des fernadministrierten IT-Systems MUSS dem Fernzugriff explizit zustimmen.

OPS.2.4.A3 Absicherung der Kommunikationsverbindungen bei der Fernwartung [IT-Betrieb]

Die möglichen Zugänge und Kommunikationsschnittstellen für einen Verbindungsaufbau von außen MÜSSEN auf das notwendige Maß beschränkt werden. Ebenso MÜSSEN alle Kommunikationsverbindungen nach vollzogenem Fernzugriff getrennt werden (Deaktivierung). Für eine Fernwartung MÜSSEN notwendige Ports ständig bereitgestellt werden. Es MÜSSEN unter Berücksichtigung des erforderlichen Schutzbedarfes des IT-Systems oder der Anwendung sichere Authentisierungsmechanismen für die Administratoren eingesetzt werden.

OPS.2.4.A4 Regelungen zu Kommunikationsverbindungen [IT-Betrieb]

Unter Beachtung der Firewall-Anforderungen der Institution MUSS die Fernwartung in das Firewall-Regelwerk eingebunden werden. Hierbei MUSS darauf geachtet werden, dass bestehende Firewall-Infrastrukturen und deren Regelungen nicht umgangen werden.

Bei der Überprüfung der Netz-Konnektivität mittels ICMP MÜSSEN die Regelungen für die lokalen und entfernten Prüfungen beachtet werden.

OPS.2.4.A5 Einsatz von Online-Diensten [IT-Betrieb, Benutzer]

Es MUSS entschieden werden, ob eine Fernwartung über Online-Dienste erlaubt ist. Der Einsatz von Online-Diensten für die Fernwartung SOLLTE verboten werden. Es SOLLTEN technische und organisatorische Maßnahmen ergriffen werden, um das Verbot durchzusetzen.

Sofern der Einsatz nicht zu vermeiden ist, SOLLTE er auf möglichst wenige Fälle beschränkt werden. Die Bedingungen, unter denen eine Fernwartung über Online-Dienste erlaubt ist, SOLLTEN festgelegt werden. Die Clients SOLLTEN automatisiert keine Verbindungen zum zum Online-Dienst aufbauen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Fernwartung. Sie SOLLTEN grundsätzlich umgesetzt werden.

OPS.2.4.A6 Erstellung einer Richtlinie für die Fernwartung [IT-Betrieb]

Die Regelungen zur Fernwartung SOLLTEN in einer Richtlinie dokumentiert werden. Sollte eine eigenständige Richtlinie erstellt werden, SOLLTE in den bestehenden Richtlinien der Institution auf die Richtlinie für Fernwartung referenziert werden. Die Richtlinie SOLLTE allen Verantwortlichen, die an der Konzeption, dem Aufbau und dem Betrieb sowie der Aussonderung beteiligt sind, bekannt sein und die Grundlage für deren Arbeit bilden können.

OPS.2.4.A7 Dokumentation bei der Fernwartung [IT-Betrieb]

Es MUSS eine aktuelle Dokumentation der Fernwartung vorliegen. Vorhandene Stellvertreter SOLLTEN zu jeder Zeit die Aufgaben und Prozesse übernehmen können. Da die Dokumente meist vertrauliche Informationen und Daten beinhalten, SOLLTEN sie an geeigneten Orten gesichert abgelegt werden und auch im Rahmen des Notfallmanagements zur Verfügung stehen . Ebenso SOLLTE der Schutz vor unbefugtem Zugriff auf die Dokumentation sichergestellt sein. Sämtliche Fernzugriffsmöglichkeiten SOLLTEN erfasst und dokumentiert sein.

OPS.2.4.A8 Sichere Protokolle bei der Fernwartung [IT-Betrieb]

Es SOLLTEN aktuelle und als sicher eingestufte Kommunikationsprotokolle eingesetzt werden. Die Kommunikation SOLLTE verschlüsselt erfolgen. Dafür SOLLTEN ausgehend vom Schutzbedarf der Institution geeignete kryptographische Verfahren zur Realisierung eines Tunnels eingesetzt werden. Damit die eingesetzten Protokolle geeignet verwaltet werden können und die Sicherheitsanforderungen berücksichtigt werden, SOLLTEN Informationen zu Schwachstellen aus der Fachpresse bzw. aus einschlägigen Quellen beachtet und kontinuierlich aktualisiert werden.

OPS.2.4.A9 Auswahl geeigneter Fernwartungswerkzeuge [IT-Betrieb]

Die Auswahl geeigneter Fernwartungswerkzeuge SOLLTE sich aus den betrieblichen, sicherheitstechnischen und datenschutzrechtlichen Anforderungen der Institution ergeben. Alle Beschaffungsentscheidungen SOLLTEN mit den Verantwortlichen des Einkaufes, dem System- und Anwendungsverantwortlichen sowie dem Sicherheitsmanagement abgestimmt werden.

OPS.2.4.A10 Verwaltung der Fernwartungswerkzeuge [IT-Betrieb, Benutzer]

Es SOLLTEN organisatorische Verwaltungsprozesse zum Umgang mit den ausgewählten Werkzeugen etabliert werden. Es SOLLTE eine Bedienungsanleitung für den Umgang mit dem Fernwartungswerkzeug vorliegen. Musterabläufe für die passive und die aktive Fernwartung SOLLTEN erstellt und kommuniziert werden. Der IT-Betrieb SOLLTE im Umgang mit den Fernwartungswerkzeugen sensibilisiert und geschult werden. Es SOLLTE ein Ansprechpartner für alle fachlichen Fragen zu den Fernwartungswerkzeugen benannt werden.

OPS.2.4.A11 Einsatz von kryptographischen Verfahren bei der Fernwartung [IT-Betrieb]

Bei der Fernwartung SOLLTEN ausreichend starke kryptographische Verfahren genutzt werden, um die Kommunikation abzusichern und die Administrierenden zu authentisieren. Die Stärke der verwendeten kryptographischen Verfahren und Schlüssel SOLLTE im Rahmen der Fernwartung regelmäßig überprüft und falls erforderlich angepasst werden.

OPS.2.4.A12 Patch- und Änderungsmanagement bei der Fernwartung [IT-Betrieb]

Es SOLLTEN die allgemeinen Vorgaben zum Patch- und Änderungsmanagement der Institution für die Fernwartung umgesetzt werden. Die IT-Systeme und Administrationswerkzeuge SOLLTEN alle im Patch- und Änderungsmanagement berücksichtigt werden.

Die Fernwartungszugänge SOLLTEN geeignet aktiviert und deaktiviert werden. Alle Aktivierungen und Deaktivierungen der Fernwartungs-Zugänge SOLLTEN zusätzlich dokumentiert sein. Aus Sicherheitsgründen SOLLTEN alle durch die Fernwartung betreuten IT-Systeme und Anwendungen zeitnah gepatcht werden. Bevor Patches und Änderungen durch die Fernwartung in ein Produktivsystem eingespielt werden, SOLLTEN sie vorab in einer geeigneten eingerichteten Testumgebung geprüft werden.

OPS.2.4.A13 Datensicherung bei der Fernwartung [IT-Betrieb]

Zur Vermeidung von Datenverlusten innerhalb der Infrastruktur für die Fernwartung SOLLTEN regelmäßige Datensicherungen erfolgen. Es SOLLTEN Vorgaben der Datensicherung bei der Fernwartung anhand der Menge und Wichtigkeit der laufend neu gespeicherten Daten und des möglichen Schadens für die Institution bei Verlust dieser Daten getroffen werden.

Alle Datensicherungsanforderungen der Fernwartung SOLLTEN mit den allgemeinen Vorgaben der Institution zur Datensicherung korrespondieren.

OPS.2.4.A14 Dedizierte Systeme bei der Fernwartung [IT-Betrieb]

Innerhalb der Fernwartung SOLLTEN Komponenten eingesetzt werden, die ausschließlich diesem Anwendungszweck dienen. Alle weiteren Funktionen/Dienste SOLLTEN deaktiviert werden. Die Komponenten der Fernwartung SOLLTEN sicher konfiguriert und eingestellt werden.

OPS.2.4.A15 Absicherung der Fernwartung [IT-Betrieb]

Fernwartung SOLLTE nur aus dem internen Netz erfolgen.

Falls es dennoch nötig ist, von einem öffentlichen Datennetz auf interne IT-Systeme zuzugreifen, SOLLTE ein abgesichertes Virtuelles Privates Netz (VPN) genutzt werden. Für die Fernwartung per VPN SOLLTE eine geschützte Datenverbindung zu dem VPN-Endpunkt generiert werden. Neben diesen externen Fernwartungs-Zugängen SOLLTEN auch die internen Fernwartungs-Zugänge abgesichert werden. Die Benutzung von internen Fernwartungs-Zugängen SOLLTE so weit wie möglich eingeschränkt werden. Des Weiteren SOLLTEN alle Aktivitäten während einer Administrationssitzung protokolliert werden.

OPS.2.4.A16 Schulungen zur Fernwartung [IT-Betrieb]

Den Administratoren SOLLTEN ausreichende Kenntnisse im Umgang mit den Fernwartungskomponenten vermittelt werden. Diese Schulungsmaßnahmen SOLLTEN in die bereits etablierten Verfahren der Institution integriert werden.

Ebenso SOLLTEN die Mitarbeiter darauf hingewiesen werden, was sie bei der Fernwartung zu beachten haben.

OPS.2.4.A17 Authentisierungsmechanismen bei der Fernwartung [IT-Betrieb]

Für die Fernwartung SOLLTEN Zwei-Faktor-Verfahren zur Authentisierung eingesetzt werden.

Die Auswahl der Authentisierungsmethode und die Gründe, die zu der Auswahl geführt haben, SOLLTEN dokumentiert werden. Zur Erleichterung der Anmeldung bei der Fernwartung SOLLTE diese in einem Identitäts- und Berechtigungsmanagement und deren Infrastrukturen integriert werden.

OPS.2.4.A18 Passwortsicherheit bei der Fernwartung [IT-Betrieb]

Falls bei der Fernwartung passwortbasierte Authentisierungen verwendet werden, SOLLTEN Passwortregeln definiert, dokumentiert und den Administratoren bekannt gemacht werden. Für die Fernwartung SOLLTEN diese Passwortregeln technisch forciert werden.

OPS.2.4.A19 Fernwartung durch Dritte [IT-Betrieb]

Wenn es nicht möglich ist, auf externe Fernwartung zu verzichten, SOLLTEN alle Aktivitäten in diesem Rahmen von Internen beobachtet werden. Alle Fernwartungsvorgänge durch Dritte SOLLTEN aufgezeichnet werden. Mit externem Wartungspersonal MÜSSEN vertragliche Regelungen getroffen werden, vor allem über die Sicherheit der betroffenen IT-Systeme und Informationen. Die Pflichten und Kompetenzen des externen Wartungspersonals SOLLTEN vertraglich festgehalten werden.

OPS.2.4.A20 Betrieb der Fernwartung [IT-Betrieb]

Es SOLLTE ein Meldeprozess für Support- und Fernwartungsanliegen etabliert werden (z. B. Ticketsystem). Alle Zugriffe durch die Fernwartung SOLLTEN erst nach erfolgreicher Authentisierung gestattet werden.

Die zur Etablierung der Fernwartungszugänge erforderlichen Freischaltungen an der Sicherheitsinfrastruktur SOLLTEN in die etablierten Prozessefür Firewall-Regeln integriert werden. Es SOLLTEN Mechanismen zur Erkennung und Abwehr von hochvolumigen Angriffen, TCP-State-Exhaustion Angriffen und Angriffen auf Applikationsebene implementiert sein.

Alle Fernwartungsvorgänge SOLLTEN aufgezeichnet werden. Die anfallenden Protokolldaten SOLLTEN regelmäßig ausgewertet werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.2.4.A21 Erstellen eines Notfallplans für den Ausfall der Fernwartung (A)

Im Rahmen der Notfallvorsorge SOLLTE ein Konzept entwickelt werden, wie die Folgen eines Ausfalls von Fernwartungskomponenten minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind. Durch den Notfallplan SOLLTE sichergestellt sein, dass Störungen, Schäden und Folgeschäden minimiert werden sowie eine zeitnahe Wiederherstellung des Normalbetriebs erfolgt.

OPS.2.4.A22 Redundante Verwendung von mobilen Kommunikationsnetzen (A)

Für den Schutz der Kommunikationsnetze der Fernwartung bei Hochverfügbarkeitsanforderungen SOLLTEN redundante Verbindungs- bzw. Kommunikationsnetze eingerichtet werden.

OPS.2.4.A23 Planung des sicheren Einsatzes in einem abgesicherten Netzsegment [IT-Betrieb]

Für die Fernwartung SOLLTE ein abgesichertes Netzsegment eingesetzt werden. Dieses SOLLTE in der Art wie eine Demilitarized Zone (DMZ) realisiert und betrieben werden. Die Fernwartungszugänge SOLLTEN NICHT dazu führen, dass vorhandene Sicherheitsinfrastrukturen umgangen werden und so ein Zusammenschluss von vertrauenswürdigen und nicht vertrauenswürdigen Netzen erfolgt.

4 Weiterführende Informationen

4.1 Literatur

- [CSE108] Fernwartung im industriellen Umfeld
  BSI-Veröffentlichung zur Cyber-Sicherheit - Allianz für Cyber-Sicherheit, CSE 108, BSI, Version 1.0, 01.2015
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_108.pdf

- [CSE54] Grundregeln zur Absicherung von Fernwartungszugängen
  BSI-Veröffentlichung zur Cyber-Sicherheit- Allianze für Cyber-Sicherheit, BSI, 06.2013
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_054.pdf

- [TR02102] Kryptographische Verfahren- Empfehlungen und Schlüssellängen
  BSI, (zuletzt abgerufen am 27.09.2017)
  https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Fernwartung" von Bedeutung.

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

G 0.14 Ausspähen von Informationen (Spionage)

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.43 Einspielen von Nachrichten

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen Anforderungen	G 0.09	G 0.14	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.30	G 0.31	G 0.32	G 0.39	G 0.40	G 0.43	G 0.46
OPS.2.4.A1		x	x	x	x							x	x			x
OPS.2.4.A2																
OPS.2.4.A3			x					x			x		x			x
OPS.2.4.A4			x			x							x			x
OPS.2.4.A5				x		x		x						x	x	
OPS.2.4.A6			x													
OPS.2.4.A7		x	x	x												
OPS.2.4.A8		x	x	x			x	x					x			x
OPS.2.4.A9			x		x											
OPS.2.4.A10			x		x	x										
OPS.2.4.A11				x	x	x	x	x		x		x				x
OPS.2.4.A12			x		x				x				x	x	x	
OPS.2.4.A13		x							x							x
OPS.2.4.A14			x			x	x	x		x						
OPS.2.4.A15			x	x			x						x			x
OPS.2.4.A16			x		x							x				
OPS.2.4.A17		x		x		x	x	x								
OPS.2.4.A18		x		x		x	x	x		x		x			x	
OPS.2.4.A19				x		x	x			x	x	x				
OPS.2.4.A20			x			x	x	x		x	x	x	x			
OPS.2.4.A21	x		x				x		x				x	x		
OPS.2.4.A22			x	x			x				x					
OPS.2.4.A23		x	x			x				x						

OPS.3: IT-Betrieb für Dritte

OPS.3.1 Outsourcing für Dienstleister

1 Beschreibung

1.1 Einleitung

Beim Outsourcing übernehmen Outsourcing-Dienstleister Geschäftsprozesse und Dienstleistungen (z. B. Wach- oder Reinigungspersonal) ganz oder teilweise von auslagernden Institutionen (Outsourcing-Kunden). Der Betrieb von Hardware und Software kann ebenso als Dienstleistung übernommen werden. Unabhängig davon, welche Dienstleistungen übernommen werden, bedingt dies eine enge Bindung zwischen dem Outsourcing-Dienstleister und dem Outsourcing-Kunden. Der Outsourcing-Dienstleister bleibt nicht von den Risiken im Zuge der Outsourcing-Beziehung verschont. Er muss die in der Regel von Seiten des Outsourcing-Kunden festgelegten risikomindernden Sicherheitsanforderungen (siehe Baustein OPS.2.1 Outsourcing für Kunden) umsetzen. Es liegt nicht nur im Interesse des Outsourcing-Kunden, sondern auch in dem des Outsourcing-Dienstleisters, die vereinbarte Leistung zu erbringen und das vereinbarte Sicherheitsniveau einzuhalten. Bei einer Verfehlung der an ihn gestellten Anforderungen drohen mitunter hohe Vertragsstrafen und gegebenenfalls weitere juristische Folgen, die nicht nur finanzielle Auswirkungen haben, sondern auch die Reputation nachhaltig schädigen können. Den Schwerpunkt dieses Bausteins bilden daher Anforderungen, die sich mit der Planung, Umsetzung, Kontrolle und Steuerung von Informationssicherheitsaspekten im Rahmen eines Outsourcings aus Sicht des Dienstleisters beschäftigen.

1.2 Zielsetzung

Der Baustein beschreibt die Anforderungen für den Outsourcing-Dienstleister, damit er das Sicherheitsniveau der auslagernden Institution erfüllen bzw. für ihn unkontrollierbare Risiken , die sich aus der Geschäftsbeziehung ergeben, vermeiden kann.

1.3 Abgrenzung

Der Baustein enthält Sicherheitsanforderungen an Outsourcing, die Dienstleister erfüllen müssen. Er ergänzt die Anforderungen des Schutzes für Informationen der auslagernden Institution aus Sicht des Outsourcing-Dienstleisters.

Die Absicherung der Übertragungswege zwischen dem Dienstleister und dem Kunden von Outsourcing-Dienstleistungen wird in diesem Baustein nicht betrachtet.

Die Begriffe Outsourcing und Cloud haben viele Parallelen. Für Dienstleister von Outsourcing sind in der Regel auch Anforderungen hinsichtlich der Nutzung von Cloud-Services zusätzlich zu beachten.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Outsourcing von Dienstleister von besonderer Bedeutung:

2.1 Ausfall eines Weitverkehrsnetzes (WAN)

Outsourcing-Dienstleister, deren Leistungserbringung nicht vor Ort beim Kunden erfolgt, sind in hohem Maß abhängig von der Verfügbarkeit von Weitverkehrsnetzen (Wide Area Networks, WAN). Aus wirtschaftlichen Gründen werden die Dienstleistungen meistens von wenigen, zentralen Standorten aus erbracht. Die Anbindung zum Outsourcing-Kunden erfolgt über Weitverkehrsnetze. Der Ausfall eines Weitverkehrsnetzes kann also dazu führen, dass die ausgelagerte Dienstleistung nicht mehr erbracht werden kann.

2.2 Fehlende oder unzureichende Regelungen zur Informationssicherheit

Im Rahmen eines Outsourcings erhalten und verarbeiten Outsourcing-Dienstleister große Mengen an Informationen der Outsourcing-Kunden. Abhängig vom Schutzbedarf der zu verarbeitenden Informationen können fehlende oder unzureichende Regelungen Schäden verursachen, beispielsweise wenn Zuständigkeiten unklar sind. Dies ist zum Beispiel dann der Fall, wenn bei technischen, organisatorischen oder personellen Änderungen die Regelungen und Anweisungen nicht aktualisiert werden, etwa bei Änderung von Ansprechpartnern. Das Spektrum der Regelungsdefizite reicht dabei von Unklarheiten bei Zuständigkeiten und Kontrollfunktionen über unverständlich oder zusammenhanglos formulierte Regelungen, bis hin zu komplett fehlenden Regelungen.

2.3 Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten

Je nach Outsourcing-Vorhaben kann es erforderlich sein, dass die Mitarbeiter des Outsourcing-Kunden Zutritts-, Zugangs- und Zugriffsrechte zu IT-Systemen, Informationen, Gebäuden oder Räumen des Outsourcing-Dienstleisters benötigen. Wenn die Vergabe, Verwaltung und Kontrolle dieser Rechte beim Outsourcing-Dienstleister schlecht geregelt ist, kann das zu weitreichenden Sicherheitsproblemen führen. Wenn die Prozesse zur Rechtevergabe zu komplex sind, kann es zu lange dauern, bis die Mitarbeiter des Outsourcing-Kunden die dringend erforderlichen Rechte erhalten. Wenn der IT-Betrieb Mandanten zu viele Rechte einräumt, könnten diese dadurch auch auf Bereiche anderer Mandanten zugreifen.

2.4 Fehlendes oder unzureichendes Test- und Freigabeverfahren

Hat ein Outsourcing-Dienstleister kein ausreichendes Test- und Freigabeverfahren für Hard- und Software etabliert, so stellt dies eine erhebliche Gefährdung des IT-Betriebs dar. Vorhandene Fehler in der Hard- und Software oder Sicherheitslücken in der Konfiguration werden so eventuell nicht oder nicht rechtzeitig erkannt. Wenn neue Komponenten in die Betriebsumgebung eingebracht werden, ohne dass sie vorher ausreichend getestet wurden, kann dies auch dazu führen, dass Fehler oder Sicherheitslücken aus einem Mandantenbereich sich auch bei anderen Kunden negativ auswirken.

Wenn unzureichende Test- und Freigabeverfahren zu Sicherheitsvorfällen führen, ist der notwendige Schutz der Daten des Kunden nicht mehr gewährleistet und es kann zu Strafzahlungen oder Vertragskündigungen kommen und damit finanzielle Auswirkungen haben.

2.5 Ungesicherter Akten- und Datenträgertransport

Outsourcing-Dienstleister verarbeiten oft große Mengen an Daten der auslagernden Institution. Ist der Transport von Akten, Dokumenten und Datenträgern entsprechend dem Schutzbedarf der zu transportierenden Informationen nicht angemessen abgesichert, können durch Verlust, unautorisierte Kenntnisnahme oder Manipulation erhebliche Schäden für die auslagernde Institution, aber auch für den Outsourcing-Dienstleister entstehen. Das kann zu erheblichen Problemen in der Geschäftsbeziehung im Outsourcing führen. Schäden können eintreten, wenn Akten oder Datenträger auf unsicherem Wege zum Outsourcing-Kunden transportiert werden und diese unterwegs abgegriffen, manipuliert werden oder verloren gehen.

2.6 Unzureichendes Informationssicherheitsmanagement beim Outsourcing-Dienstleister

Ein unzureichend etabliertes oder nicht angemessen umgesetztes Informationssicherheitsmanagement seitens des Outsourcing-Dienstleisters birgt erhebliche Risiken. Die Probleme reichen von der fehlenden Gesamtverantwortung für das Thema Informationssicherheit über die mangelnde Unterstützung durch die Leitungsebene und unzureichende strategische und konzeptionelle Vorgaben hin zu einem intransparenten Sicherheitsprozess. Für Outsourcing-Dienstleister besteht nun das Risiko, dass die Anforderungen der auslagernden Institution nicht erfüllt werden, wenn die Gesamtorganisation hinsichtlich Informationssicherheit mangelhaft ist.

2.7 Unzulängliche vertragliche Regelungen mit einem Outsourcing-Kunden

Es kann passieren, dass ein Outsourcing-Dienstleister aufgrund von unzulänglichen vertraglichen Regelungen eine Dienstleistung nicht so erbringt, wie dies zur Aufrechterhaltung des Sicherheitsniveaus des Kunden erforderlich ist. Wenn der Schutzbedarf und die daraus resultierenden Anforderungen an die Sicherheit ausgelagerter Daten oder Systeme dem Outsourcing-Dienstleister unbekannt sind, können sie nicht angemessen geschützt werden.

2.8 Unzureichende Regelungen für das Ende eines Outsourcings

Ohne ausreichende und angemessene Regelung für die Auflösung des Outsourcing-Vertrags besteht die Gefahr, dass die Geschäftsbeziehung nicht konfliktfrei aufgelöst wird. So könnte es passieren, dass Informationen des Kunden unwiderruflich beim Outsourcing-Dienstleister gelöscht werden, bevor diese vollständig und korrekt zum Kunden übertragen wurden. Eine vorzeitige vollständige Löschung der Informationen des Kunden kann Strafzahlungen für den Dienstleister nach sich ziehen.

2.9 Unzureichendes Notfallvorsorgekonzept beim Outsourcing

Besitzt ein Outsourcing-Dienstleister nur ein unzureichendes Notfallvorsorgekonzept, stehen unter Umständen die vertraglich vereinbarten IT-Systeme und Anwendungen im Notfall nicht oder nur eingeschränkt zur Verfügung. Dies hat zur Folge, dass die darauf basierenden Geschäftsprozesse nicht zur Verfügung stehen und die vertraglich vereinbarte Dienstleistung nicht bereit gestellt werden.

2.10 Ausfall der Systme eines Outsourcing-Dienstleisters

Bei einem Outsourcing-Dienstleister können die dort betriebenen IT-Systeme und Prozesse teilweise oder ganz ausfallen, wodurch auch der Outsourcing-Kunde betroffen ist. Bei unzureichender Mandantentrennung kann unter Umständen auch der Ausfall eines Systems, das nicht dem Outsourcing-Kunden zugeordnet ist, trotzdem dazu führen, dass dieser seine vertraglich zugesicherte Dienstleistung nicht mehr abrufen kann. Ähnliche Probleme ergeben sich, wenn die Anbindung zwischen Outsourcing-Dienstleister und -Kunden ausfällt.

Dies kann für den Outsourcing-Dienstleister bedeuten, dass, falls vertraglich vereinbart, der Outsourcing-Kunde Schadensersatzansprüche geltend machen kann.

2.11 Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister

Wenn bei einem Outsourcing-Vorhaben die IT-Anbindung zwischen dem Outsourcing-Dienstleister und dem Outsourcing-Kunden unzureichend abgesichert ist, kann die Vertraulichkeit und Integrität der übermittelten Daten gefährdet sein. Es könnten sich aber auch durch offene oder schlecht gesicherte Schnittstellen unautorisierte Zugangsmöglichkeiten für Außenstehende auf die Systeme der beteiligten Institutionen ergeben.

2.12 Social Engineering

Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch "Aushorchen" von Mitarbeitern zu erlangen. Dadurch können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln. Mitarbeiter von Outsourcing-Dienstleistern können hier ein besonders lohnenswertes Ziel abgeben, da sie auf sehr viele Daten unterschiedlicher Unternehmen Zugriff haben.

2.13 Fehlende Mandantenfähigkeit beim Outsourcing-Dienstleister

Outsourcing-Dienstleister haben in der Regel viele verschiedene Kunden, die auf die gleiche Ressourcenbasis (IT-Systeme, Netze, Personal) zurückgreifen. Wenn die IT-Systeme und Daten der verschiedenen Kunden nicht ausreichend sicher voneinander getrennt sind, besteht die Gefahr, dass ein Kunde auf den Bereich eines anderen Kunden zugreifen kann. Außerdem könnte es zu Interessenskonflikten beim Outsourcing-Kunden kommen, wenn der Dienstleister parallel vergleichbare Ressourcenforderungen erfüllen muss. Wenn sich die jeweiligen Kunden in einer Konkurrenzsituation befinden, kann dies besonders problematisch sein.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Outsourcing für Dienstleister aufgeführt. Grundsätzlich ist der Leiter IT für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Leiter IT
Weitere Verantwortliche	Datenschutzbeauftragter, ISB Outsourcing-Dienstleister, IT-Betrieb, Institutionsleitung, Leiter Organisation, Leiter Personal, Notfallbeauftragter, Änderungsmanager

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

OPS.3.1.A1 Erstellung eines Grobkonzeptes für die Outsourcing-Dienstleistung

Es MUSS ein Grobkonzept für die angebotene Outsourcing-Dienstleistung erstellt werden. Dieses Grobkonzept MUSS Rahmenbedingungen des Outsourcings berücksichtigten (z. B. Sonderwünsche) und grundsätzliche Fragestellungen zum Sicherheitsniveau und zu den Sicherheitsanforderungen des Outsourcing-Kunden beantworten.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Outsourcing für Dienstleister. Sie SOLLTEN grundsätzlich umgesetzt werden.

OPS.3.1.A2 Vertragsgestaltung mit den Outsourcing-Kunden [ISB Outsourcing-Dienstleister]

Es SOLLTEN alle Aspekte des Outsourcing-Vorhabens mit dem Outsourcing-Kunden schriftlich geregelt sein, um den Auftrag wie gewünscht erfüllen zu können und das geforderte Sicherheitsniveau zu gewährleisten. Es SOLLTEN alle Verantwortlichkeiten und Mitwirkungspflichten zur Erstellung, Prüfung und Änderung (z. B. von Personen) im Rahmen des Vertragswerkes oder auch direkt im Sicherheitskonzept zwischen dem Outsourcing-Dienstleister und dem Outsourcing-Kunden geregelt sein.

OPS.3.1.A3 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben [ISB Outsourcing-Dienstleister]

Der Outsourcing-Dienstleister SOLLTE für seine Dienstleistungen ein Sicherheitskonzept besitzen. Für individuelle Outsourcing-Vorhaben SOLLTE er außerdem spezifische Sicherheitskonzepte basierend auf den zugehörigen Sicherheitsanforderungen des Outsourcing-Kunden erstellen. Zwischen Outsourcing-Dienstleister und Outsourcing-Kunden SOLLTEN gemeinsame Sicherheitsziele und eine gemeinsame Klassifikation für alle schutzbedürftigen Informationen erarbeitet werden. Die Umsetzung des Sicherheitskonzepts SOLLTE regelmäßig überprüft werden.

OPS.3.1.A4 Festlegung der möglichen Kommunikationspartner [Leiter Organisation, Datenschutzbeauftragter, ISB Outsourcing-Dienstleister]

Zwischen Outsourcing-Dienstleister und -Kunden SOLLTE festgelegt werden, welche internen und externen Kommunikationspartner welche Informationen über das jeweilige Outsourcing-Projekt übermitteln und erhalten dürfen. Es SOLLTE regelmäßig geprüft werden, ob die Kommunikationspartner noch aktuell in ihrer Funktion beschäftigt sind. Die Berechtigungen SOLLTEN bei Änderungen angepasst werden. Zwischen den Outsourcing-Partnern SOLLTE geregelt sein, nach welchen Kriterien welche Kommunikationspartner welche Informationen erhalten dürfen.

OPS.3.1.A5 Regelungen für den Einsatz des Personals des Outsourcing-Dienstleisters [Leiter Personal, ISB Outsourcing-Dienstleister]

Mitarbeiter des Outsourcing-Dienstleisters SOLLTEN geregelt in ihre Aufgaben eingewiesen und über bestehende Regelungen zur Informationssicherheit des Outsourcing-Kunden unterrichtet werden. Die Mitarbeiter des Outsourcing-Dienstleisters SOLLTEN schriftlich auf die Einhaltung der einschlägigen Gesetze, Vorschriften, Vertraulichkeitsvereinbarungen und internen Regelungen verpflichtet werden. Es SOLLTE Vertretungsregelungen in allen Bereichen geben.

OPS.3.1.A6 Regelungen für den Einsatz von Fremdpersonal [Leiter Personal, ISB Outsourcing-Dienstleister]

Setzt der Outsourcing-Dienstleister externes Personal ein, SOLLTE der Outsourcing-Kunde hierüber informiert werden. Externe Mitarbeiter mit Aufgaben in Bezug auf das Outsourcing SOLLTEN schriftlich auf die Einhaltung der einschlägigen Gesetze, Vorschriften und interne Regelungen verpflichtet werden. Sie SOLLTEN in ihre Aufgaben und vor allem in die Sicherheitsvorgaben eingewiesen werden. Kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal SOLLTE wie Besucher behandelt werden.

OPS.3.1.A7 Erstellung eines Mandantenkonzeptes durch den Outsourcing-Dienstleister [ISB Outsourcing-Dienstleister]

Durch ein geeignetes Mandantenkonzept SOLLTE sichergestellt werden, dass Anwendungs- und Datenkontexte verschiedener Kunden sauber getrennt sind. Das Mandantenkonzept SOLLTE durch den Outsourcing-Dienstleister erstellt und dem Outsourcing-Kunden zur Verfügung gestellt werden. Das Mandantenkonzept SOLLTE für den Schutzbedarf des Outsourcing-Kunden angemessene Sicherheit bieten. Die benötigten Mechanismen zur Mandantentrennung beim Outsourcing-Dienstleister SOLLTEN ausreichend umgesetzt sein.

OPS.3.1.A8 Vereinbarung über die Anbindung an Netze der Outsourcing-Partner [ISB Outsourcing-Dienstleister]

Vor der Anbindung eines eigenen Netzes an das Netz des Outsourcing-Dienstleisters SOLLTEN alle sicherheitsrelevanten Aspekte in einer Vereinbarung schriftlich festgelegt werden. Es SOLLTE definiert werden, wer aus dem einen Netz auf welche Bereiche und Dienste des jeweils anderen Netzes zugreifen darf. Es SOLLTEN auf jeder Seite Ansprechpartner sowohl für organisatorische als auch technische Fragestellungen der Netzanbindung benannt werden. Auf beiden Seiten SOLLTEN alle identifizierten

Sicherheitslücken beseitigt und das geforderte Sicherheitsniveau nachweislich erreicht sein, bevor die Netzanbindung aktiviert wird. Für den Fall von Sicherheitsproblemen auf einer der beiden Seiten SOLLTE festgelegt sein, wer darüber zu informieren ist und welche Eskalationsschritte einzuleiten sind.

OPS.3.1.A9 Vereinbarung über Datenaustausch zwischen den Outsourcing-Partnern [ISB Outsourcing-Dienstleister]

Für den regelmäßigen Datenaustausch mit festen Kommunikationspartnern der Outsourcing-Partner SOLLTEN die erforderlichen Sicherheitsmaßnahmen vereinbart werden. Datenformate und die sichere Form des Datenaustauschs SOLLTEN festgelegt werden. Ansprechpartner sowohl für organisatorische als auch technische Probleme und insbesondere für sicherheitsrelevante Ereignisse beim Datenaustausch mit Dritten SOLLTEN benannt werden. Verfügbarkeiten und Reaktionszeiten beim Datenaustausch mit Dritten SOLLTEN vereinbart werden. Es SOLLTE festgelegt werden, welche ausgetauschten Daten zu welchen Zwecken genutzt werden dürfen.

OPS.3.1.A10 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb [ISB Outsourcing-Dienstleister]

Der Outsourcing-Kunde SOLLTE ein Betriebskonzept erstellen, in dem alle relevanten Sicherheitsaspekte berücksichtigt werden. Die Sicherheitskonzepte der Outsourcing-Partner SOLLTEN regelmäßig auf Aktualität und Konsistenz zueinander geprüft werden. Der Status der vereinbarten Sicherheitsmaßnahmen SOLLTE regelmäßig kontrolliert werden. Zwischen den Outsourcing-Partnern SOLLTE eine regelmäßige Kommunikation einschließlich Abstimmung zu Änderungen und Verbesserungen stattfinden.

Die Outsourcing-Partner SOLLTEN regelmäßig gemeinsame Übungen und Tests zur Aufrechterhaltung des Sicherheitsniveaus durchführen. Informationen über Sicherheitsrisiken und der Umgang damit SOLLTEN in regelmäßigen Abständen zwischen den Outsourcing-Partnern ausgetauscht werden. Es SOLLTE ein Prozess existieren, welcher den Informationsfluss im Umgang mit Sicherheitsvorfällen sicherstellt, welche die jeweiligen Vertragspartner betreffen.

OPS.3.1.A11 Zutritts-, Zugangs- und Zugriffskontrolle [Leiter Organisation, ISB Outsourcing-Dienstleister]

Zutritts-, Zugangs- und Zugriffsberechtigungen SOLLTEN geregelt sein, sowohl für das Personal des Outsourcing-Dienstleisters als auch für Personal der Outsourcing-Kunden. Es SOLLTE ebenfalls geregelt sein, welche Berechtigungen Auditoren und andere Prüfer erhalten. Es SOLLTEN immer nur so viele Rechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist. Es SOLLTE ein geregeltes Verfahren für die Vergabe, die Verwaltung und den Entzug von Berechtigungen geben.

OPS.3.1.A12 Änderungsmanagement [IT-Betrieb, Änderungsmanager]

Es SOLLTEN Richtlinien für die Durchführung von Änderungen an IT-Komponenten, Software oder Konfigurationsdaten existieren. Es SOLLTE geregelt sein, dass bei der Durchführung von Änderungen auch Sicherheitsaspekte berücksichtigt werden. Es SOLLTEN alle Änderungen geplant, getestet, genehmigt und dokumentiert werden. Art und Umfang der Dokumentationen über die Änderungen SOLLTEN mit dem Outsourcing-Kunden abgestimmt und bereitgestellt werden. Es SOLLTEN Rückfall-Lösungen erarbeitet werden, bevor Änderungen durchgeführt werden. Bei größeren, sicherheitsrelevanten Änderungen SOLLTE das Informationssicherheitsmanagement der auslagernden Institution schon im Vorfeld beteiligt werden.

OPS.3.1.A13 Sichere Migration bei Outsourcing-Vorhaben

Für die Migrationsphase SOLLTE ein Sicherheitsmanagement-Team aus qualifizierten Mitarbeitern des Outsourcing-Kunden und des Outsourcing-Dienstleisters eingerichtet werden. Für die Migrationsphase SOLLTE eine Sicherheitskonzeption erstellt werden. Nach Abschluss der Migration SOLLTE das Sicherheitskonzept aktualisiert werden. Es SOLLTE sichergestellt sein, dass alle Ausnahmeregelungen am Ende der Migrationsphase aufgehoben werden. Bei Änderungen in der Migrationsphase SOLLTE geprüft werden, inwieweit ein Anpassungsbedarf an den vertraglichen Grundlagen und bestehenden Dokumenten besteht.

OPS.3.1.A14 Notfallvorsorge beim Outsourcing [Notfallbeauftragter]

Es SOLLTE ein Notfallvorsorgekonzept zum Outsourcing existieren, das die Komponenten beim Outsourcing-Kunden, beim Outsourcing-Dienstleister sowie die zugehörigen Schnittstellen umfasst. Im Notfallvorsorgekonzept zum Outsourcing SOLLTEN die Zuständigkeiten, Ansprechpartner und Abläufe zwischen Outsourcing-Kunden und Outsourcing-Dienstleister geregelt sein. Es SOLLTEN regelmäßig gemeinsame Notfallübungen vom Outsourcing-Kunden und Outsourcing-Dienstleister durchgeführt werden.

OPS.3.1.A15 Geordnete Beendigung eines Outsourcing-Verhältnisses [Institutionsleitung]

Es SOLLTE sichergestellt sein, dass eine Beendigung des Vertragsverhältnisses mit dem Outsourcing-Kunden weder dessen noch die eigene Geschäftstätigkeit beeinträchtigt. Der Outsourcing-Vertrag mit dem Outsourcing-Kunden SOLLTE alle Aspekte der Beendigung des Dienstleistungsverhältnisses regeln, sowohl für eine geplante als auch für eine ungeplante Beendigung des Vertragsverhältnisses. Der Outsourcing-Dienstleister SOLLTE alle Informationen und Daten des Outsourcing-Kunden an diesen übergeben. Beim Outsourcing-Dienstleister SOLLTEN danach alle Datenbestände des Kunden sicher gelöscht werden. Alle Berechtigungen, die im Rahmen des Outsourcing-Projekts eingerichtet wurden, SOLLTEN überprüft und, wenn erforderlich, gelöscht werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.3.1.A16 Sicherheitsüberprüfung von Mitarbeitern [Leiter Personal] (CI)

Die Vertrauenswürdigkeit von neuen Mitarbeitern und externem Personal beim Outsourcing-Dienstleister SOLLTE durch geeignete Nachweise überprüft werden. Hierzu SOLLTEN gemeinsam mit dem Outsourcing-Kunden Kriterien vertraglich vereinbart werden.

4 Weiterführende Informationen

4.1 Literatur

- [27001A15] ISO/IEC 27001;2013 - Annex A.15 Supplier relationship
  Information technology- Security techniques- Information security management systems- requirements, insbesondere Annex A, A.15 Supplier relationships, ISO, 2013

- [BVIT2005] Buisiness Process Outsourcing Leitfaden
  Business Process Outsourcing Leitfaden - BPO als Chance für den Standort Deutschland, Bundesverband Informationswirtschaft Telekommunikation und neue Medien, Version 10.1, 2005
  https://www.bitkom.org/Bitkom/Publikationen/Leitfaden-Business-Process-Outsourcing.html

- [BVIT2008] Leitfaden rechtliche Asprekte von Outsourcing in der Praxis
  Rechtliche Aspekte von Outsourcing in der Praxis, Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V., 2008
  https://www.bitkom.org/Bitkom/Publikationen/Rechtliche-Aspekte-von-Outsourcing-in-der-Praxis.html

- [DIN37500] DIN ISO 37500:2015-08
  Leitfaden Outsourcing, DIN Deutsches Institut für Normung e.V., 08.2015

- [ISFSC1.2] The Standard of Good Practice - Area SC1.2 Outsourcing insbesondere Area SC1.2 Outsourcing, Information Security Forum (ISF), 06.2016
- [NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations Special Publication 800-53, Revision 4, NIST, 04.2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Outsourcing für Dienstleister" von Bedeutung.

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

G 0.14 Ausspähen von Informationen (Spionage)

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.25 Ausfall von Geräten oder Systemen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.33 Personalausfall

G 0.38 Missbrauch personenbezogener Daten

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.09	G 0.14	G 0.17	G 0.18	G 0.19	G 0.22	G 0.25	G 0.30	G 0.33	G 0.38	G 0.41	G 0.42	G 0.45	G 0.46
OPS.3.1.A1				x										
OPS.3.1.A2							x	x	x					
OPS.3.1.A3					x								x	x
OPS.3.1.A4		x			x									x
OPS.3.1.A5								x	x					
OPS.3.1.A6								x	x					
OPS.3.1.A7					x									x
OPS.3.1.A8	x	x											x	
OPS.3.1.A9		x	x		x	x				x				x
OPS.3.1.A10					x									x
OPS.3.1.A11				x	x			x						
OPS.3.1.A12				x	x			x						
OPS.3.1.A13					x								x	x
OPS.3.1.A14	x						x		x				x	
OPS.3.1.A15					x								x	x
OPS.3.1.A16											x			

Bundesamt
für Sicherheit in der
Informationstechnik

DER: Detektion und Reaktion

DER.1	Detektion von sicherheitsrelevanten Ereignissen	**294**
DER.2.1	Behandlung von Sicherheitsvorfällen	**303**
DER.2.2	Vorsorge für die IT-Forensik	**314**
DER.2.3	Bereinigung weitreichender Sicherheitsvorfälle	**320**
DER.3.1	Audits und Revisionen	**327**
DER.3.2	IS-Revision für Bundesbehörden	**335**
DER.4	Notfallmanagement	**344**

IT-Grundschutz

DER: Detektion und Reaktion

DER.1 Detektion von sicherheitsrelevanten Ereignissen

1 Beschreibung

1.1 Einleitung

Um IT-Systeme schützen zu können, müssen sicherheitsrelevante Ereignisse rechtzeitig erkannt und behandelt werden. Dazu ist es notwendig, dass Institutionen im Vorfeld geeignete organisatorische, personelle und technische Maßnahmen planen, implementieren und regelmäßig üben. Denn wenn auf ein vorgegebenes und erprobtes Verfahren aufgesetzt werden kann, lassen sich Reaktionszeiten verkürzen und vorhandene Prozesse optimieren.

Als sicherheitsrelevantes Ereignis wird ein Ereignis bezeichnet, das sich auf die Informationssicherheit auswirkt und die Vertraulichkeit, Integrität und Verfügbarkeit beeinträchtigen kann. Typische Folgen solcher Ereignisse sind ausgespähte, manipulierte oder zerstörte Informationen. Die Ursachen hierfür sind dabei vielfältig: So spielen unter anderem Malware, veraltete Systeminfrastrukturen oder Innentäter eine Rolle. Angreifer nutzen aber auch oft Zero-Day-Exploits aus, also Sicherheitslücken in Programmen, bevor es für diese einen Patch gibt. Eine weitere erst zunehmende Gefährdung sind sogenannte Advanced Persistent Threats (APT). Dabei handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netz verschafft und diesen auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind oft schwer zu detektieren.

1.2 Zielsetzung

Dieser Baustein zeigt einen systematischen Weg auf, wie Informationen gesammelt, korreliert und ausgewertet werden können, um sicherheitsrelevante Ereignisse möglichst vollständig und zeitnah zu detektieren. Die aus der Detektion gewonnenen Erkenntnisse sollen die Fähigkeit von Institutionen verbessern, sicherheitsrelevante Ereignisse zu erkennen und darauf angemessen zu reagieren.

1.3 Abgrenzung

Der Baustein enthält grundsätzliche Anforderungen, die zu beachten und zu erfüllen sind, wenn sicherheitsrelevante Ereignisse detektiert werden. Voraussetzung hierfür ist jedoch, dass umfassend protokolliert wird. Die dafür notwendigen Maßnahmen werden nicht im vorliegenden Baustein beschrieben, sondern sind in OPS.1.1.5 *Protokollierung* enthalten.

Außerdem beschreibt der Baustein nicht, wie mit sicherheitsrelevanten Ereignissen umzugehen ist, nachdem sie detektiert worden. Empfehlungen dazu werden in DER.2.1 *Incident Management* und DER.2.2 *Forensik* aufgeführt. Ebenso wird nicht auf die Themen Datenschutz und Archivierung von Protokolldaten eingegangen, diese werden in CON.2 *Datenschutz* und OPS.1.1.2 *Archivierung* behandelt.

Um sicherheitsrelevante Ereignisse zu erkennen, sind oft zusätzliche Programme erforderlich, z. B. Antivirenprogramme, Firewalls oder Intrusion-Detection-/Intrusion-Prevention-Systeme (IDS/IPS). Sicherheitsaspekte dieser Systeme sind ebenfalls nicht Gegenstand des vorliegenden Bausteins. Sie werden z. B. in NET.3.4 *IDS/IPS*, OPS.1.1.5 *Schutz vor Schadprogrammen* und NET.3.2 *Firewall* thematisiert.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Detektion von sicherheitsrelevanten Ereignissen von besonderer Bedeutung:

2.1 Missachtung von gesetzlichen Vorschriften und betrieblichen Mitbestimmungsrechten

Programme, die sicherheitsrelevante Ereignisse detektieren und Protokolldaten auswerten, sammeln oft viele Informationen über die Netzstruktur und die internen Abläufe einer Institution. Darin können z. B. schützenswerte Daten, wie personenbezogene Daten, Verschlusssachen oder Arbeitsabläufe von Mitarbeitern enthalten sein. Dadurch, dass solche Daten jedoch gespeichert werden, können Persönlichkeitsrechte bzw. Mitbestimmungsrechte der Mitarbeiter verletzt werden. Auch verstößt die Institution unter bestimmten Voraussetzungen eventuell gegen die jeweiligen Landesdatenschutzgesetze bzw. das Bundesdatenschutzgesetz.

2.2 Unzureichende Qualifikation der Verantwortlichen

Im täglichen IT-Betrieb einer Institution können viele Störungen und Fehler auftreten (z. B. starke Zunahme ankommender Protokolldaten). Sind die verantwortlichen Mitarbeiter nicht ausreichend sensibilisiert und geschult, besteht die Gefahr, dass sie sicherheitsrelevante Ereignisse nicht als solche identifizieren und so ein Angriff unerkannt bleibt.

2.3 Fehlende oder unzureichende Protokollierung

Werden sicherheitsrelevante Ereignisse ungenügend oder gar nicht protokolliert, lässt sich nicht ausreichend und schnell genug feststellen, ob Sicherheitsvorgaben verletzt werden oder ob Angriffsversuche stattfinden. Auch kann im Schadenfall keine Fehleranalyse mehr durchgeführt werden und das Einfallstor eines Angriffs bleibt so eventuell bestehen. Auch werden Protokollinformationen dafür eingesetzt, Integritätsprüfungen durchzuführen. Fehlen die Protokolle jedoch, ist dies nicht möglich.

2.4 Fehlerhafte Administration der eingesetzten Detektionssysteme

Fehlerhafte Konfigurationen können dazu führen, dass eingesetzte Detektionssysteme nicht ordnungsgemäß funktionieren. Ist beispielsweise die Alarmierung falsch eingestellt, kann es zu vermehrten Fehlalarmen kommen. Die verantwortlichen Mitarbeiter können dann eventuell nicht mehr zwischen einem Fehlalarm und einem sicherheitsrelevanten Ereignis unterscheiden. Auch nehmen sie die Meldungen eventuell nicht zeitnah wahr, da zu viele Alarme generiert werden. Dadurch bleiben möglicherweise Angriffe unerkannt. Ebenso steigt der Aufwand stark an, die Menge der Meldungen auszuwerten.

2.5 Fehlende Informationen über den zu schützenden Informationsverbund

Sind keine oder nur ungenügende Informationen über den Informationsverbund vorhanden, besteht die Gefahr, dass wesentliche Bereiche des Informationsverbunds nicht ausreichend durch Detektionssysteme geschützt werden. Dadurch können Angreifer leicht in das Netz der Institution eindringen und zum Beispiel schützenswerte Informationen abgreifen. Auch ist es ihnen so möglich, lange unbemerkt im System zu bleiben und dauerhaft auf das Netz zuzugreifen.

2.6 Unzureichende Nutzung von Detektionssystemen

Wenn keine Detektionssysteme eingesetzt werden und auch die in IT-Systemen und Anwendungen vorhandenen Funktionen zur Detektion von sicherheitsrelevanten Ereignissen nicht benutzt werden, können Angreifer leichter unbemerkt in das Netz der Institution eindringen und unbefugt auf sensible Informationen zugreifen. Besonders kritisch ist es, wenn die Übergänge zwischen Netzgrenzen nur unzureichend überwacht werden.

2.7 Unzureichende personelle Ressourcen

Ist nicht genügend Personal vorhanden, um Protokolldaten auszuwerten, können sicherheitsrelevante Ereignisse nicht vollständig detektiert werden. So bleiben Angriffe eventuell lange verborgen bzw. werden erst entdeckt, wenn z. B. schon sehr viele schützenswerte Informationen abgeflossen sind. Auch wenn durch zu wenig Personal keine externen Informationsquellen ausgewertet werden, bleiben Sicherheitslücken eventuell zu lange offen und können von Angreifern ausgenutzt werden, um unerlaubt in die IT-Systeme der Institution einzudringen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen an die Detektion von sicherheitsrelevanten Ereignissen aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Benutzer, Fachverantwortliche, Informationssicherheitsbeauftragter (ISB), Leiter IT, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

DER.1.A1 Erstellung einer Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen [Informationssicherheitsbeauftragter (ISB)]

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie erstellt werden, in der nachvollziehbar Anforderungen und Vorgaben beschrieben sind, wie die Detektion von sicherheitsrelevanten Ereignissen sicher geplant, aufgebaut und betrieben werden kann. Die Richtlinie MUSS allen im Bereich Detektion verantwortlichen Mitarbeitern bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies mit dem verantwortlichen ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse MÜSSEN sinnvoll dokumentiert werden.

DER.1.A2 Einhaltung rechtlicher Bedingungen bei der Auswertung von Protokolldaten [Informationssicherheitsbeauftragter (ISB)]

Wenn Protokolldaten ausgewertet werden, MÜSSEN dabei die gesetzlichen Bestimmungen aus den aktuellen Gesetzen zum Bundes-/Landesdatenschutz eingehalten werden. Darüber hinaus MÜSSEN die Persönlichkeitsrechte bzw. Mitbestimmungsrechte der Mitarbeitervertretungen gewahrt werden, wenn Detektionssysteme eingesetzt werden. Ebenso MUSS sichergestellt sein, dass alle weiteren relevanten gesetzlichen Bestimmungen beachtet werden, z. B. Telemediengesetz (TMG), Betriebsverfassungsgesetz und Telekommunikationsgesetz.

DER.1.A3 Festlegung von Meldewegen für sicherheitsrelevante Ereignisse

Es MÜSSEN geeignete Melde- und Alarmierungswege festgelegt und dokumentiert werden. Dabei MUSS bestimmt werden, welche Stellen wann zu informieren sind. Auch MUSS aufgeführt sein, wie die jeweiligen Personen erreicht werden können. Je nach Dringlichkeit MUSS ein sicherheitsrelevantes Ereignis über verschiedene Kommunikationswege gemeldet werden.

Die Melde- und Alarmierungswege MÜSSEN den Mitarbeitern ausgedruckt vorliegen. Alle für die Meldung bzw. Alarmierung relevanten Personen MÜSSEN über ihre Aufgaben informiert sein. Es MÜSSEN alle Schritte des Melde- und Alarmierungsprozesses ausführlich beschrieben sein. Die eingerichteten Melde- und Alarmierungswege SOLLTEN regelmäßig geprüft, erprobt und falls erforderlich, aktualisiert werden.

DER.1.A4 Sensibilisierung der Mitarbeiter [Vorgesetzte, Leiter IT, Benutzer]

Damit Mitarbeiter mögliche Sicherheitsvorfälle schnell erkennen können, MÜSSEN sie entsprechend sensibilisiert werden. Dafür SOLLTEN regelmäßige Schulungen stattfinden, in denen gängige und aktuelle Bedrohungen sowie die Vorgehensweisen der Cyberkriminellen aufgezeigt werden.

Auch MÜSSEN die Mitarbeiter dahingehend sensibilisiert werden, dass sie Ereignismeldungen der Clients nicht einfach ignorieren oder schließen, sondern die Meldungen entsprechend der Alarmierungswege an das verantwortliche Incident Management weitergeben (siehe DER.2.1 *Incident Management*).

Jeder Mitarbeiter MUSS einen von ihm erkannten Sicherheitsvorfall unverzüglich dem Incident Management melden.

DER.1.A5 Einsatz von mitgelieferten Systemfunktionen zur Detektion [Fachverantwortliche]

Verfügen eingesetzte IT-Systeme oder Anwendungen über Funktionen, mit denen sich sicherheitsrelevante Ereignisse detektieren lassen , MÜSSEN diese aktiviert und benutzt werden.

Auf allen eingesetzten Komponenten MUSS die Protokollierung aktiviert werden (siehe OPS.1.1.5 *Protokollierung*). Liegt ein sicherheitsrelevanter Vorfall vor, MÜSSEN die Meldungen mindestens lokal ausgewertet werden. Zusätzlich MÜSSEN die protokollierten Ereignisse anderer IT-Systeme überprüft werden. Auch SOLLTEN die gesammelten Meldungen in verbindlich festgelegten Zeiträumen stichpunktartig kontrolliert werden.

Es MUSS geprüft werden, ob zusätzliche Schadcodescanner auf zentralen IT-Systemen installiert werden sollen (siehe auch SYS.1.1 *Allgemeiner Server*). Ist dies der Fall, MÜSSEN es diese über einen zentralen Zugriff ermöglichen, ihre Meldungen und Protokolle auszuwerten. Außerdem MÜSSEN sie regelmäßig aktualisiert werden. Es MUSS sichergestellt sein, dass die Schadcodescanner automatisch sicherheitsrelevante Ereignisse an die Verantwortlichen melden und die Meldungen auch ausgewertet und untersucht werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Detektion von sicherheitsrelevanten Ereignissen. Sie SOLLTEN grundsätzlich umgesetzt werden.

DER.1.A6 Kontinuierliche Überwachung und Auswertung von Protokolldaten [Benutzer]

Alle Protokolldaten SOLLTEN möglichst permanent aktiv überwacht und ausgewertet werden. Es SOLLTEN Mitarbeiter benannt werden, die dafür verantwortlich sind.

Müssen die verantwortlichen Mitarbeiter aktiv nach eingetretenen sicherheitsrelevanten Ereignissen suchen, z. B. wenn sie IT-Systeme kontrollieren oder testen, SOLLTEN solche Aufgaben in entsprechenden Verfahrensanleitungen dokumentiert sein.

Für die Detektion von sicherheitsrelevanten Ereignissen SOLLTEN genügend personelle Ressourcen bereitgestellt werden.

DER.1.A7 Schulung von Verantwortlichen [Vorgesetzte, Leiter IT]

Alle Verantwortlichen, die Ereignismeldungen kontrollieren, SOLLTEN weiterführende Schulungen und Qualifikationen erhalten. Wenn IT-Komponenten beschafft werden, SOLLTE ein Budget für Schulungen eingeplant und ein Schulungskonzept für die verantwortlichen Mitarbeiter erstellt werden.

DER.1.A8 Festlegung von zu schützenden Segmenten [Fachverantwortliche]

Anhand des Netzplans (siehe NET.1.1 *Netzarchitektur und -design*) SOLLTE festgelegt werden, welche Netzsegmente durch zusätzliche Detektionssysteme geschützt werden müssen (vgl. DER.1.A9 *Einsatz zusätzlicher Detektionssysteme*).

DER.1.A9 Einsatz zusätzlicher Detektionssysteme [Fachverantwortliche]

Um sicherheitsrelevante Ereignisse besser zu erkennen, SOLLTE der Informationsverbund um zusätzliche Detektionssysteme und Sensoren ergänzt werden. So SOLLTEN Schadcodedetektionssysteme eingesetzt und zentral verwaltet werden. Auch die im Netzplan definierten Übergange zwischen internen und externen Netzen SOLLTEN um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.

DER.1.A10 Einsatz von TLS/SSH-Proxies [Fachverantwortliche]

An den Übergängen zu externen Netzen SOLLTEN TLS/SSH-Proxies eingesetzt werden, die die verschlüsselte Verbindung unterbrechen und es so ermöglichen, die übertragenen Daten auf Malware zu prüfen. Alle TLS/SSH-Proxies SOLLTEN vor unbefugten Zugriffen geschützt werden. Außerdem SOLLTEN sicherheitsrelevante Ereignisse auf den TLS/SSH-Proxies automatisch detektiert werden. Es SOLLTE eine organisatorische Regelung erstellt werden, unter welchen datenschutzrechtlichen Voraussetzungen die Logdaten manuell ausgewertet werden dürfen.

DER.1.A11 Nutzung einer zentralen Protokollierungsinfrastruktur für die Auswertung sicherheitsrelevanter Ereignisse [Fachverantwortliche]

Die gesammelten Ereignismeldungen der IT-Systeme und Anwendungssysteme SOLLTEN auf einer zentralen Protokollinfrastruktur (siehe OPS1.1.5 *Protokollierung*) aufbewahrt werden. Die eingelieferten Ereignismeldungen SOLLTEN mithilfe eines Tools zentral gespeichert, ausgewertet und abgerufen werden können. Damit die Daten korreliert und abgeglichen werden können, SOLLTEN sie alle zeitlich synchronisiert werden. Die gesammelten Ereignismeldungen SOLLTEN regelmäßig auf Auffälligkeiten kontrolliert werden. Damit sicherheitsrelevante Ereignisse auch nachträglich erkannt werden können, SOLLTEN die Signaturen der Detektionssysteme durchgängig aktuell und auf dem gleichen Stand sein.

DER.1.A12 Auswertung von Informationen aus externen Quellen [Informationssicherheitsbeauftragter (ISB), Fachverantwortliche]

Um neue Erkenntnisse über sicherheitsrelevante Ereignisse für den eigenen Informationsverbund zu gewinnen, SOLLTEN externe Quellen herangezogen und ausgewertet werden. Da Meldungen über unterschiedliche Kanäle in eine Institution eingeliefert werden, SOLLTE sichergestellt sein, dass diese Meldungen von den Mitarbeitern auch als relevant erkannt und an die richtige Stelle weitergeleitet werden. Stammen Informationen aus qualifizierten Quellen, SOLLTEN sie grundsätzlich ausgewertet werden. Alle eingelieferten Informationen SOLLTEN bewertet werden, ob sie relevant für den eigenen Informationsverbund sind. Ist dies der Fall, SOLLTEN die Informationen entsprechend der Sicherheitsvorfallbehandlung eskaliert werden (siehe DER.2.1. *Incident Management*).

DER.1.A13 Regelmäßige Audits der Detektionssysteme

Die vorhandenen Detektionssysteme und getroffenen Maßnahmen SOLLTEN regelmäßig überprüft werden, ob sie noch aktuell und wirksam sind. Es SOLLTEN die Messgrößen ausgewertet werden, die beispielsweise anfallen, wenn sicherheitsrelevante Ereignisse aufgenommen, gemeldet und eskaliert werden. Die Auditergebnisse SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTE nachgegangen werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

DER.1.A14 Auswertung der Protokolldaten durch spezialisiertes Personal [Leiter IT] (CI)

Es SOLLTEN Mitarbeiter überwiegend dafür abgestellt werden, alle Protokolldaten zu überwachen. Das abgestellte Personal SOLLTE spezialisierte weiterführende Schulungen und Qualifikationen erhalten. Ein Personenkreis SOLLTE benannt werden, der ausschließlich für das Thema Auswertung von Protokolldaten, wie z. B. aus dem Bereich Forensik, verantwortlich ist.

DER.1.A15 Zentrale Detektion und Echtzeitüberprüfung von Ereignismeldungen (CIA)

Es SOLLTEN zentrale Komponenten eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten. Zentrale automatisierte Analysen mit Softwaremitteln SOLLTEN dazu eingesetzt werden, um alle in der Systemumgebung anfallenden Ereignisse aufzuzeichnen, in Bezug zueinander zu setzen und sicherheitsrelevante Vorgänge sichtbar zu machen. Alle eingelieferten Daten SOLLTEN lückenlos in der Protokollverwaltung einsehbar und auswertbar sein. Die tatsächlichen Daten SOLLTEN möglichst permanent ausgewertet werden. Werden definierte Schwellwerten überschritten, SOLLTE automatisch alarmiert werden. Durch das Personal SOLLTE sichergestellt werden, dass bei einem Alarm unverzüglich eine qualifizierte und dem Bedarf entsprechende Reaktion eingeleitet wird. In diesem Zusammenhang SOLLTE auch der betroffene Mitarbeiter sofort informiert werden.

Die Systemverantwortlichen SOLLTEN regelmäßig die Analyseparameter auditieren und, falls erforderlich, anpassen. Zusätzlich SOLLTEN bereits überprüfte Daten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden.

DER.1.A16 Einsatz von Detektionssystemen nach Schutzbedarfsanforderungen (CIA)

Anwendungen mit erhöhtem Schutzbedarf SOLLTEN durch zusätzliche Detektionsmaßnahmen geschützt werden. Dafür SOLLTEN z. B. solche Detektionssysteme eingesetzt werden, mit denen sich der erhöhte Schutzbedarf technisch auch sicherstellen lässt.

DER.1.A17 Automatische Reaktion auf sicherheitsrelevante Ereignisse (CI)

Bei einem sicherheitsrelevanten Ereignis SOLLTEN die eingesetzten Detektionssysteme das Ereignis automatisch melden und mit geeigneten Schutzmaßnahmen reagieren. Hierbei SOLLTEN Verfahren eingesetzt werden, die automatisch mögliche Angriffe, Missbrauchsversuche oder Sicherheitsverletzungen erkennen. Es SOLLTE möglich sein, automatisch in den Datenstrom einzugreifen, um einen möglichen Sicherheitsvorfall zu unterbinden.

DER.1.A18 Durchführung regelmäßiger Integritätskontrollen (CI)

Alle Detektionssysteme SOLLTEN regelmäßig daraufhin überprüft werden, ob sie noch integer sind. Auch SOLLTEN die Benutzerrechte kontrolliert werden. Zusätzlich SOLLTEN die Sensoren eine Integritätskontrolle von Dateien durchführen und bei sich ändernden Werten eine automatische Alarmierung auslösen.

4 Weiterführende Informationen

4.1 Literatur

- [BSILeit1] BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen,
  IDS, BSI, Version 1.0, 10.2002
  https://www.bsi.bund.de/DE/Publikationen/Studien/IDS02/index_htm.html

- [ISF] The Standard of Good Practice
  Information Security Forum (ISF), 06.2016

- [NISTSP800123] NIST Special Publication 800-123
  Guide to General Server Security, NIST, 07.2008
  https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Detektion von sicherheitsrelevanten Ereignissen" von Bedeutung.

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.33 Personalausfall

G 0.37 Abstreiten von Handlungen

G 0.38 Missbrauch personenbezogener Daten

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.41 Sabotage

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.09	G 0.11	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.29	G 0.30	G 0.31	G 0.32	G 0.33	G 0.37	G 0.38	G 0.39	G 0.40	G 0.41	G 0.46
DER.1.A1			x								x												
DER.1.A2				x									x					x	x				
DER.1.A3			x														x						
DER.1.A4			x							x					x								
DER.1.A5	x					x	x	x				x		x	x	x				x		x	
DER.1.A6			x					x	x	x	x			x		x				x			
DER.1.A7			x												x	x							
DER.1.A8	x		x																				
DER.1.A9	x					x		x						x	x	x				x		x	
DER.1.A10						x		x					x			x				x			
DER.1.A11	x			x		x		x	x	x	x	x		x	x	x		x		x			
DER.1.A12					x							x											
DER.1.A13			x	x	x	x	x	x		x	x			x		x				x			
DER.1.A14		x									x						x						
DER.1.A15	x			x		x		x	x	x	x	x		x	x	x		x		x			x
DER.1.A16			x			x		x						x		x					x	x	x
DER.1.A17	x							x			x	x		x		x				x	x		
DER.1.A18			x							x	x	x			x								x

DER.2: Security Incident Management

DER.2.1 Behandlung von Sicherheitsvorfällen

1 Beschreibung

1.1 Einleitung

Um Schäden zu begrenzen und um weitere Schäden zu vermeiden, müssen erkannte Sicherheitsvorfälle schnell und effizient bearbeitet werden. Dafür ist es notwendig, ein vorgegebenes und erprobtes Verfahren zur Behandlung von Sicherheitsvorfällen (*Security Incident Handling oder auch Security Incident Response)* zu etablieren.

Ein Sicherheitsvorfall kann sich sehr stark auf eine Institution auswirken und große Schäden nach sich ziehen. Solche Vorfälle sind beispielsweise Fehlkonfigurationen, die dazu führen, dass vertrauliche Informationen offengelegt werden oder kriminelle Handlungen, z. B. Hacking von Servern, Diebstahl von vertraulichen Informationen, Sabotage oder Erpressung mit IT-Bezug.

Die Ursachen für Sicherheitsvorfälle sind vielfältig: So spielen unter anderem Malware, veraltete Systeminfrastrukturen oder Innentäter eine Rolle. Angreifer nutzen aber auch oft Zero-Day-Exploits aus. Eine weitere erst zunehmende Gefährdung sind sogenannte Advanced Persistent Threats (APT).

Außerdem könnten sich Benutzer, Administratoren oder externe Dienstleister nicht korrekt verhalten, sodass Systemparameter sicherheitskritisch geändert werden oder dass gegen interne Richtlinien verstoßen wird. Weiter ist als Ursache denkbar, dass Zugriffsrechte verletzt werden, dass Software, Hardware geändert oder schutzbedürftiger Räume und Gebäude unzureichend gesichert werden.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, einen systematischen Weg aufzuzeigen, wie ein Konzept zur Behandlung von Sicherheitsvorfällen erstellt werden kann.

1.3 Abgrenzung

Der Fokus dieses Bausteins liegt auf der Behandlung von Sicherheitsvorfällen aus Sicht der Informationstechnik. Bevor Sicherheitsvorfälle behandelt werden können, müssen sie jedoch detektiert werden. Sicherheitsanforderungen dazu sind im Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen* enthalten und werden im vorliegenden Baustein vorausgesetzt. Die initiale forensische Untersuchung wird im Baustein DER.2.2 *Forensik* und die Bereinigung nach einem APT-Vorfall im Baustein DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle (APT-Responder)* behandelt. Ein besonderer Bereich der Behandlung von Sicherheitsvorfällen ist das Notfallmanagement, das im Baustein DER.4 *Notfallmanagement* thematisiert und hier nicht weiter betrachtet wird. Es ist jedoch zu beachten, dass die Entscheidung darüber, ob ein Notfall vorliegt oder nicht, im vorliegenden Baustein getroffen wird.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind bei der Behandlung von Sicherheitsvorfällen von besonderer Bedeutung:

2.1 Ungeeigneter Umgang mit Sicherheitsvorfällen

In der Praxis kann nie ausgeschlossen werden, dass Sicherheitsvorfälle auftreten. Das gilt auch dann, wenn eine Vielzahl von Sicherheitsmaßnahmen umgesetzt ist. Wird auf akute Sicherheitsvorfälle entweder nicht oder nicht angemessen reagiert, können sich daraus große Schäden bis hin zu Katastrophen entwickeln. Beispiele dafür sind:

- In den Protokolldateien einer Firewall finden sich auffällige Einträge. Wird nicht zeitnah untersucht, ob das erste Anzeichen für einen Einbruchsversuch sind, können Angreifer die Firewall mit einem erfolgreichen Angriff unbemerkt überwinden und in das interne Netz der Institution eindringen.
- Es werden Sicherheitslücken in den verwendeten IT-Systemen bzw. Anwendungen bekannt. Werden diese Informationen nicht rechtzeitig beschafft und notwendige Gegenmaßnahmen nicht zügig eingeleitet und umgesetzt, können diese Sicherheitslücken von Angreifern ausgenutzt werden.

Wenn für die Behandlung von Sicherheitsvorfällen keine geeignete Vorgehensweise vorgegeben ist, können in der Eile und unter Stress falsche Entscheidungen getroffen werden. Diese können z. B. dazu führen, dass die Presse falsch informiert und dadurch eine negative Außenwirkung erzielt wird, dass Dritte durch die eigenen IT-Systeme geschädigt werden und Schadenersatz fordern oder dass keinerlei Ausweich- oder Wiederherstellungsmaßnahmen vorgesehen sind und sich somit der Schaden für die Institution deutlich erhöht.

2.2 Nicht erkannte Sicherheitsvorfälle

Im täglichen Betrieb einer Institution können viele Störungen und Fehler auftreten. Dabei kann es passieren, dass Sicherheitsvorfälle durch das Personal nicht als solche identifiziert werden und ein Angriff bzw. Angriffsversuch unerkannt bleibt. Auch wenn die Mitarbeiter ausreichend für die Belange der Informationssicherheit sensibilisiert bzw. geschult sind, kann trotzdem nicht ausgeschlossen werden, dass sie Sicherheitsvorfälle nicht erkennen. Beispiele hierfür sind:

- Ein Benutzer, der seit längerer Zeit nicht im lokalen Netz seiner Institution angemeldet war, hält die seit einer Woche auftretende deutliche Verlangsamung seines Notebooks während des Internetzugangs für normal und bemerkt nicht, dass ein Schadprogramm im Hintergrund aktiv ist. Er wurde nicht oder nur unzureichend geschult, bei verdächtigen Auffälligkeiten den Sicherheitsverantwortlichen zu informieren.

- Ein Produktionsleiter bemerkt nicht, dass die Daten in den Produktionssystemen und auch die Steuerungsanzeigesysteme heimlich verändert wurden. Er schöpft keinen Verdacht, als die SCADA-Steuerung der Produktionsanlage seltsame Werte anzeigt, da dies nur kurzzeitig erfolgte. Der Vorfall wird nicht gemeldet, da alle Werte wieder den erwarteten Anzeigewerten entsprechen. Dass eine Schadsoftware die Anzeigewerte manipuliert hat, fällt somit niemandem auf.
- Ein Einbruchsdiebstahl in einer Filiale wird für einen Fall von Beschaffungskriminalität gehalten, da Notebooks und Flachbildschirme entwendet wurden. Der Tatsache, dass sich auf den Notebooks vertrauliche Informationen und Zugangsdaten für IT-Systeme im Intranet befunden haben, wird keine größere Bedeutung beigemessen und der ISB nicht informiert. Auf die nachfolgenden Angriffe auf die IT-Systeme anderer Standorte und der Firmenzentrale ist die Institution daher nicht vorbereitet. Für den Angriff werden die auf den gestohlenen Notebooks gefundenen Daten verwendet.

2.3 Zerstörung von Beweisspuren bei der Behandlung von Sicherheitsvorfällen

Wenn bei der Behandlung von Sicherheitsvorfällen unvorsichtig oder nicht nach Vorgaben agiert wird, kann das dazu führen, dass wichtige Beweisspuren für die Aufklärung oder spätere juristische Verfolgung unbeabsichtigt zerstört oder nicht gerichtsverwertbar gemacht werden.

Beispiele hierfür sind:

- Auf einem Arbeitsplatzrechner hat ein Angreifer eine Schadsoftware platziert, deren Arbeitsweise und Ziel nur im laufenden Zustand analysiert werden kann. Dafür müssten Informationen über die aktiven Prozesse und der Inhalt des Hauptspeichers gesichert und ausgewertet werden. Wird der Arbeitsplatzrechner nun voreilig heruntergefahren, können die Informationen aus dem laufenden Zustand nicht mehr für eine Analyse und Aufklärung des Sicherheitsvorfalls herangezogen werden.
- Ein Administrator findet auf einem Server einen laufenden Prozess, der eine überdurchschnittliche CPU-Auslastung verursacht. Zusätzlich erzeugt dieser Prozess temporäre Dateien und versendet unbekannte Informationen über das Internet. Wird der Prozess voreilig beendet und werden die temporären Dateien einfach gelöscht, kann nicht herausgefunden werden, ob vertrauliche Informationen erfolgreich entwendet werden konnten.
- Ein wichtiger Server wird kompromittiert, weil der Administrator durch die starke Arbeitsbelastung und ein fehlendes Wartungsfenster die letzten Sicherheitsupdates nicht wie geplant einspielen konnte. Um möglichen disziplinarischen Konsequenzen zu entgehen, spielt der Administrator die fehlenden Updates ein, bevor ein Sicherheitsteam die Einbruchsursache und den entstandenen Schaden analysieren kann. Mangelnde Fehlerkultur hat somit eine Analyse des Problems verhindert.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Behandlung von Sicherheitsvorfällen aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Informationssicherheitsbeauftragter (ISB)
Weitere Verantwortliche	Datenschutzbeauftragter, Fachverantwortliche, IT-Betrieb, Institutionsleitung, Leiter IT, Notfallbeauftragter, Pressestelle

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

DER.2.1.A1 Definition eines Sicherheitsvorfalls [Leiter IT]

In einer Institution MUSS klar definiert sein, was ein Sicherheitsvorfall ist. Ein Sicherheitsvorfall MUSS so weit wie möglich von Störungen im Tagesbetrieb abgegrenzt sein. Alle am Prozess zur Sicherheitsvorfallbehandlung beteiligten Mitarbeiter MÜSSEN die Definition eines Sicherheitsvorfalls kennen. Die Definition und die Eintrittsschwellen SOLLTEN auf dem Schutzbedarf der betroffenen Geschäftsprozesse, IT-Dienste, IT-Systeme bzw. IT-Anwendungen basieren.

DER.2.1.A2 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen

Es MUSS eine Richtlinie zur Behandlung von Sicherheitsvorfällen erstellt werden. Darin MÜSSEN der Zweck und das Ziel der Richtlinie definiert sowie alle Aspekte der Sicherheitsvorfallbehandlung geregelt werden. So MÜSSEN Verhaltensregeln für die verschiedenen Arten von Sicherheitsvorfällen beschrieben sein. Zusätzlich MUSS es für alle Mitarbeiter zielgruppenorientierte und praktisch anwendbare Handlungsanweisungen geben. Weiterhin SOLLTEN die Schnittstellen zu anderen Managementbereichen berücksichtigt werden, z. B. zum Notfallmanagement.

Die Richtlinie MUSS allen Mitarbeitern bekannt sein. Sie MUSS mit der IT-Leitung oder dem IT-Betrieb abgestimmt und durch die Institutionsleitung verabschiedet sein. Die Richtlinie MUSS regelmäßig geprüft und aktualisiert werden.

DER.2.1.A3 Festlegung von Verantwortlichkeiten und Ansprechpartnern bei Sicherheitsvorfällen [Leiter IT]

Es MUSS geregelt werden, wer bei auftretenden Sicherheitsvorfällen für was verantwortlich ist. Für alle Mitarbeiter MÜSSEN die Aufgaben und Kompetenzen bei Sicherheitsvorfällen festgelegt werden. Auch Mitarbeiter, die Sicherheitsvorfälle bearbeiten sollen, MÜSSEN über ihre Aufgaben und Kompetenzen unterrichtet werden. Dabei MUSS geregelt sein, wer die mögliche Entscheidung für eine forensische Untersuchung trifft, nach welchen Kriterien dies vorgenommen wird und wann sie erfolgen soll.

Die Ansprechpartner für alle Arten von Sicherheitsvorfällen MÜSSEN den Mitarbeiten bekannt sein. Kontaktinformationen MÜSSEN immer aktuell sein und in praktikabler Form vorliegen.

DER.2.1.A4 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen [Leiter IT, Notfallbeauftragter, Pressestelle, Datenschutzbeauftragter, Institutionsleitung]

Von einem Sicherheitsvorfall MÜSSEN alle betroffenen internen und externen Stellen zeitnah informiert werden. Dabei MUSS geprüft werden, ob der Datenschutzbeauftragte, der Betriebsrat/Personalrat sowie Mitarbeiter aus der Rechtsabteilung einbezogen werden müssen. Ebenso MÜSSEN die Meldepflichten für Behörden und regulierte Branchen berücksichtigt werden. Außerdem MUSS gewährleistet sein, dass betroffene Stellen über die erforderlichen Maßnahmen informiert werden.

DER.2.1.A5 Behebung von Sicherheitsvorfällen [Leiter IT, IT-Betrieb]

Damit ein Sicherheitsvorfall erfolgreich behoben werden kann, MUSS der Verantwortliche zunächst das Problem eingrenzen und die Ursache finden. Danach MUSS er die erforderlichen Maßnahmen zur Behebung auswählen und sich eine Freigabe vom Leiter IT holen, bevor er sie umsetzt. Anschließend MUSS die Ursache beseitigt und ein sicherer Zustand hergestellt (siehe DER.2.1.A6 *Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen*) werden.

Es MUSS eine aktuelle Liste von internen und externen Sicherheitsexperten vorhanden sein, die bei Sicherheitsvorfällen für Fragen aus den verschiedenen erforderlichen Themenbereichen hinzugezogen werden können. Es MÜSSEN sichere Kommunikationsverfahren mit diesen internen und externen Stellen etabliert werden.

DER.2.1.A6 Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen [Leiter IT, IT-Betrieb]

Um die Auswirkungen der Sicherheitsvorfälle zu beseitigen, MÜSSEN die betroffenen Komponenten vom Netz genommen und alle erforderlichen Daten gesichert werden, die Aufschluss über die Art und Ursache des aufgetretenen Problems geben könnten. Auf allen betroffenen Komponenten MÜSSEN das Betriebssystem und alle Applikationen auf Veränderungen untersucht werden.

Die Originaldaten MÜSSEN von schreibgeschützten Datenträgern wieder eingespielt werden. Dabei MÜSSEN alle sicherheitsrelevanten Konfigurationen und Patches mit aufgespielt werden. Wenn Daten aus Datensicherungen wieder eingespielt werden, MUSS sichergestellt sein, dass diese vom Sicherheits-

vorfall nicht betroffen waren. Vor der Wiederinbetriebnahme nach einem Angriff MÜSSEN alle Passwörter auf den betroffenen Komponenten geändert werden. Die betroffenen Komponenten SOLLTEN einem Penetrationstest unterzogen werden, bevor sie wieder eingesetzt werden.

Bei der Wiederherstellung der sicheren Betriebsumgebung MÜSSEN die Benutzer in die Anwendungsfunktionstests einbezogen werden. Nachdem alles wiederhergestellt wurde, MÜSSEN die Komponenten inklusive der Netzübergänge gezielt überwacht werden, um erneute Angriffsversuche feststellen zu können.

Wird auf externe Dienstleister zurückgegriffen, um Störungen zu beheben, MUSS geregelt werden, welche Informationen über den Sicherheitsvorfall wem zugänglich gemacht werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Behandlung von Sicherheitsvorfällen. Sie SOLLTEN grundsätzlich umgesetzt werden.

DER.2.1.A7 Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen

Damit Institutionen angemessen auf Sicherheitsvorfälle reagieren können, SOLLTE eine geeignete Vorgehensweise zur Behandlung von Sicherheitsvorfällen definiert werden. Die Abläufe, Prozesse und Vorgaben für die verschiedenen Sicherheitsvorfälle SOLLTEN dabei eindeutig geregelt und geeignet dokumentiert werden. Die Institutionsleitung SOLLTE die fertige Vorgehensweise in Kraft setzen und veröffentlichen. Die Vorgehensweise SOLLTE regelmäßig geprüft und aktualisiert werden.

DER.2.1.A8 Aufbau von Organisationsstrukturen zur Behandlung von Sicherheitsvorfällen

Für den Umgang mit Sicherheitsvorfällen SOLLTEN geeignete Organisationsstrukturen festgelegt werden. So SOLLTE ein Sicherheitsvorfall-Team aufgebaut werden, dessen Mitglieder je nach Art des Vorfalls einberufen werden können. Auch wenn das Sicherheitsvorfall-Team nur für einen konkreten Sicherheitsvorfall zusammentritt, SOLLTEN bereits im Vorfeld geeignete Mitglieder benannt und in ihre Aufgaben eingewiesen sein. Der Aufbau des Sicherheitsvorfall-Teams SOLLTE regelmäßig aktualisiert werden.

DER.2.1.A9 Festlegung von Meldewegen für Sicherheitsvorfälle [Leiter IT]

Für die verschiedenen Arten von Sicherheitsvorfällen SOLLTEN die jeweils passenden Meldewege aufgebaut sein. Es SOLLTE dabei sichergestellt sein, dass Mitarbeiter Sicherheitsvorfälle über verlässliche und vertrauenswürdige Kanäle schnell und einfach melden können.

Wird eine zentrale Anlaufstelle für die Meldung von Störungen oder Sicherheitsvorfällen eingerichtet, SOLLTE auch das an alle Mitarbeiter kommuniziert werden.

Es SOLLTE eine Kommunikations- und Kontaktstrategie vorliegen. Darin SOLLTE geregelt sein, wer grundsätzlich informiert werden muss und wer informiert werden darf, durch wen das in welcher Reihenfolge erfolgt und in welcher Tiefe informiert wird. Es SOLLTE definiert sein, wer Informationen über Sicherheitsvorfälle an Dritte weitergibt. Ebenso SOLLTE sichergestellt sein, dass keine unautorisierten Personen Informationen über den Sicherheitsvorfall weitergeben.

DER.2.1.A10 Eindämmen der Auswirkung von Sicherheitsvorfällen [Notfallbeauftragter, Leiter IT, IT-Betrieb]

Parallel zur Analyse der Ursachen eines Sicherheitsvorfalls SOLLTE entschieden werden, ob es wichtiger ist, den aufgetretenen Schaden einzudämmen oder ihn aufzuklären. Um die Auswirkung eines Sicherheitsvorfalls abschätzbar zu machen, SOLLTEN ausreichend Informationen vorliegen. Für ausgewählte Sicherheitsvorfallsszenarien SOLLTEN bereits im Vorfeld Worst-Case-Betrachtungen durchgeführt werden.

DER.2.1.A11 Einstufung von Sicherheitsvorfällen [Leiter IT, IT-Betrieb]

Es SOLLTE ein einheitliches Verfahren festgelegt werden, um Sicherheitsvorfälle und Störungen einzustufen. Das Einstufungsverfahren für Sicherheitsvorfälle SOLLTE zwischen Sicherheitsmanagement und der Störungs- und Fehlerbehebung (Incident Management) abgestimmt sein.

DER.2.1.A12 Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung [Notfallbeauftragter]

Die Schnittstellen zwischen Störungs- und Fehlerbehebung, Notfallmanagement und Sicherheitsmanagement SOLLTEN analysiert werden. Dabei SOLLTEN auch eventuell gemeinsam benutzbare Ressourcen identifiziert werden.

Die bei der Störungs- und Fehlerbehebung beteiligten Mitarbeiter SOLLTEN für Belange der Sicherheitsvorfallbehandlung sowie des Notfallmanagements sensibilisiert werden. Das Sicherheitsmanagement SOLLTE lesenden Zugriff auf eingesetzte Incident-Management-Werkzeuge haben.

DER.2.1.A13 Einbindung in das Sicherheits- und Notfallmanagement [Notfallbeauftragter]

Als Teil des Sicherheitsmanagements SOLLTE die Behandlung von Sicherheitsvorfällen in der Sicherheitsleitlinie bzw. im Sicherheitskonzept der Institution geregelt werden. Die Behandlung von Sicherheitsvorfällen SOLLTE außerdem mit dem Notfallmanagement abgestimmt werden. Falls es in der Institution eine spezielle Rolle für Störungs- und Fehlerbehebung gibt, SOLLTE auch diese mit einbezogen werden.

DER.2.1.A14 Eskalationsstrategie für Sicherheitsvorfälle [Leiter IT]

Über die Kommunikations- und Kontaktstrategie (siehe DER.2.1.A9 *Festlegung von Meldewegen für Sicherheitsvorfälle*) hinaus SOLLTE eine Eskalationsstrategie formuliert werden. Diese SOLLTE zwischen den Verantwortlichen für Störungs- und Fehlerbehebung und dem Informationssicherheitsmanagement abgestimmt werden.

Die Eskalationsstrategie SOLLTE eindeutige Handlungsanweisungen enthalten, wer, auf welchem Wege, bei welcher Art von erkennbaren oder vermuteten Sicherheitsstörungen, in welchem Zeitraum zu involvieren ist. Es SOLLTE geregelt sein, zu welchen Maßnahmen eine Eskalation führt und welche Aktivitäten ausgelöst werden sollen.

Für die festgelegte Eskalationsstrategie SOLLTEN geeignete Werkzeuge ausgewählt werden. Diese SOLLTEN auch für vertrauliche Informationen geeignet sein. Es SOLLTE sichergestellt sein, dass die Werkzeuge auch während eines Sicherheitsvorfalls bzw. Notfalls verfügbar sind.

Die Eskalationsstrategie SOLLTE regelmäßig überprüft und gegebenenfalls aktualisiert werden. Die Checklisten (Matching Szenarios) für Störungs- und Fehlerbehebung SOLLTEN regelmäßig um sicherheitsrelevante Themen ergänzt bzw. aktualisiert werden. Die festgelegten Eskalationswege SOLLTEN in Übungen erprobt werden.

DER.2.1.A15 Schulung der Mitarbeiter der zentralen Anlaufstelle des IT-Betriebs zur Behandlung von Sicherheitsvorfällen [Leiter IT]

Die Mitarbeiter des Service Desk SOLLTEN die Richtlinien für die Behandlung von Sicherheitsvorfällen kennen. Ihnen SOLLTEN geeignete Hilfsmittel zur Verfügung stehen, damit sie solche Vorfälle erkennen können. Sie SOLLTEN in deren Bedienung ausreichend geschult sein. Die Mitarbeiter des Service Desk SOLLTEN den Schutzbedarf der betroffenen Systeme kennen. Die Checklisten des Service Desk SOLLTEN auch Fragen beinhalten, um Sicherheitsvorfälle identifizieren zu können.

DER.2.1.A16 Dokumentation der Behandlung von Sicherheitsvorfällen

Die Behebung von Sicherheitsvorfällen SOLLTE nach einem standardisierten Verfahren dokumentiert werden. Es SOLLTEN sowohl alle durchgeführten Aktionen inklusive der Zeitpunkte, als auch die Protokolldaten der betroffenen Komponenten dokumentiert werden. Dabei SOLLTE die Vertraulichkeit bei der Dokumentation und Archivierung der Berichte gewährleistet sein.

Die benötigten Informationen SOLLTEN in die jeweiligen Dokumentationssysteme eingepflegt werden, bevor die Störung als beendet und abgeschlossen markiert wird. Dafür SOLLTEN die erforderlichen Qualitätssicherungsanforderungen im Vorfeld mit dem Sicherheitsmanagement definiert werden.

DER.2.1.A17 Nachbereitung von Sicherheitsvorfällen

Sicherheitsvorfälle SOLLTEN standardisiert nachbereitet werden. Dabei SOLLTE untersucht werden, wie schnell Sicherheitsvorfälle erkannt und behoben wurden, ob die Meldewege funktionierten, ausreichend Informationen für die Bewertung verfügbar und ob die Detektionsmaßnahmen wirksam waren. Ebenso SOLLTE geprüft werden, ob die ergriffenen Maßnahmen und Aktivitäten wirksam und effizient waren.

Die Erfahrungen aus vergangenen Sicherheitsvorfällen SOLLTEN genutzt werden, um daraus Handlungsanweisungen für vergleichbare Sicherheitsvorfälle zu erstellen. Diese Handlungsanweisungen SOLLTEN den relevanten Personengruppen bekanntgegeben und auf Basis neuer Erkenntnisse regelmäßig aktualisiert werden.

Außerdem SOLLTE die Leitungsebene jährlich über die Sicherheitsvorfälle unterrichtet werden. Allerdings SOLLTE die Leitungsebene gleich unterrichtet werden, wenn es sofortigen Handlungsbedarf gibt.

DER.2.1.A18 Weiterentwicklung der Prozesse durch Erkenntnisse aus Sicherheitsvorfällen und Branchenentwicklungen [Fachverantwortliche]

Die Reaktionen auf Sicherheitsvorfälle SOLLTEN analysiert und daraufhin untersucht werden, ob die Prozesse und Abläufe geändert oder weiterentwickelt werden müssen. Dabei SOLLTEN die in Reaktionen auf Sicherheitsvorfälle involvierten als auch die zuständigen Beteiligten über ihre jeweiligen Erfahrungen berichten.

Es SOLLTE geprüft werden, ob neue Entwicklungen im Incident Management und in der Forensik existieren und in die jeweiligen Dokumente und in die Abläufe eingebracht werden können.

Werden Hilfsmittel und Checklisten z. B. für Service-Desk-Mitarbeiter eingesetzt, SOLLTE geprüft werden, ob diese um erforderliche relevante Fragestellungen und Informationen zu erweitern sind.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

DER.2.1.A19 Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen (CIA)

Um die Ursachen von Sicherheitsvorfällen und die entstandenen Schäden effizient und in einer sinnvollen Reihenfolge beheben zu können, SOLLTEN die Prioritäten vorab festgelegt und regelmäßig aktualisiert werden. Dabei SOLLTE auch die vorgenommene Einstufung von Sicherheitsvorfällen berücksichtigt werden (siehe DER.2.1.A11 *Einstufung von Sicherheitsvorfällen*).

Die Prioritäten SOLLTEN von der Institutionsleitung genehmigt und in Kraft gesetzt werden. Sie SOLLTEN allen Entscheidungsträgern bekannt sein, die mit der Behandlung von Sicherheitsvorfällen zu tun haben. Die festgelegten Prioritätsklassen SOLLTEN außerdem im Incident Management hinterlegt sein.

DER.2.1.A20 Einrichtung einer internen Meldestelle für Sicherheitsvorfälle (CIA)

Es SOLLTE eine interne Stelle zur Meldung von Sicherheitsvorfällen eingerichtet werden. Es SOLLTE gewährleistet sein, dass die Meldestelle zu den üblichen Arbeitszeiten erreichbar ist. Allerdings SOLLTE es zusätzlich möglich sein, dass Sicherheitsvorfälle auch außerhalb der üblichen Arbeitszeiten von Mitarbeitern gemeldet werden können. Die Mitarbeiter der Meldestelle SOLLTEN ausreichend geschult und für die Belange der Informationssicherheit sensibilisiert sein. Alle Informationen über Sicherheitsvorfälle SOLLTEN bei der Meldestelle vertraulich behandelt werden.

DER.2.1.A21 Einrichtung eines Expertenteams für die Behandlung von Sicherheitsvorfällen (CIA)

Um Sicherheitsvorfälle durch den gesamten Lebenszyklus des Sicherheitsvorfallbehandlungsprozesses kompetent begleiten zu können, SOLLTE hierfür ein Team mit erfahrenen und vertrauenswürdigen Spezialisten zusammengestellt werden. Neben dem technischen Verständnis SOLLTEN die Teammitglieder auch Kompetenzen in der Kommunikationsfähigkeit besitzen. Die Vertrauenswürdigkeit der Mitglieder des Expertenteams SOLLTE überprüft werden. Der Aufbau des Expertenteams SOLLTE regelmäßig aktualisiert werden.

Die Mitglieder des Expertenteams SOLLTEN in die Eskalations- und Meldewege eingebunden sein. Das Expertenteam SOLLTE für die Analyse von Sicherheitsvorfällen an den in der Institution eingesetzten Systemen ausgebildet werden. Die Mitglieder des Expertenteams SOLLTEN sich regelmäßig weiterbilden, sowohl zu den eingesetzten Systemen als auch zu Detektion und Reaktion auf Sicherheitsvorfälle. Dem Expertenteam SOLLTEN alle vorhandenen Dokumentationen sowie finanzielle und technische Ressourcen zur Verfügung stehen, um Sicherheitsvorfälle schnell und diskret zu behandeln.

Das Expertenteam SOLLTE geeignet in den Organisationsstrukturen berücksichtigt und integriert werden (siehe DER.2.1.A8 *Aufbau von Organisationsstrukturen zur Behandlung von Sicherheitsvorfällen*). Die Verantwortlichkeiten des Expertenteams SOLLTEN vorher mit denen des Sicherheitsvorfall-Teams abgestimmt werden (siehe DER.2.1.A4 *Festlegung von Verantwortlichkeiten und Ansprechpartnern bei Sicherheitsvorfällen*).

DER.2.1.A22 Überprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen (CIA)

Das Managementsystem zur Behandlung von Sicherheitsvorfällen SOLLTE regelmäßig geprüft werden, ob es noch aktuell und wirksam ist. Dazu SOLLTEN sowohl angekündigte als auch unangekündigte Übungen durchgeführt werden. Die Übungen SOLLTEN vorher mit der Leitungsebene abgestimmt sein. Es SOLLTEN die Messgrößen ausgewertet werden, die beispielsweise anfallen, wenn Sicherheitsvorfälle aufgenommen, gemeldet und eskaliert werden.

Außerdem SOLLTEN Planspiele zur Behandlung von Sicherheitsvorfällen durchgeführt werden, um die notwendige Praxis zu fördern.

4 Weiterführende Informationen

4.1 Literatur

- [27001A16] ISO/IEC 27001: 2013 - Annex A.16 Information security incident management
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013, insbesondere Annex A, A.16 Information security incident management
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [27035] ISO/IEC 27035:2016
  Information technology- Security techniques- Information security management system- Requirements, ISO, 09.2011
  https://www.iso.org/standard/44379.html

- [ISFSATS14] The Standard of Good Practice - Area SA System Access und TS1.4 Technical Security Management
  Information Security Forum (ISF), insbesondere Area SA (System Access) und TS1.4 (Technical Security Management; Identiy and Access Management), 06.2016

- [NIST80061] NIST Special Publication 800-61 Revision 2
  NIST, Computer Security Incident Handling Guide, 08.2012
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

- [NST80083] NIST Special Publication 800-83 Revision 1
  NIST, Guide to Malware incident Prevention and Handling vor Desktops and Laptops, 07.2013
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an **grundschutz@bsi.bund.de** gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Behandlung von Sicherheitsvorfällen" von Bedeutung.

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.22 Manipulation von Informationen

G 0.25 Ausfall von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.33 Personalausfall

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen Anforderungen	G 0.11	G 0.18	G 0.19	G 0.20	G 0.22	G 0.25	G 0.27	G 0.29	G 0.30	G 0.32	G 0.33	G 0.45	G 0.46
DER.2.1.A1		x	x	x				x					
DER.2.1.A2		x					x	x					
DER.2.1.A3		x					x	x			x		
DER.2.1.A4			x	x				x					
DER.2.1.A5	x	x	x			x	x	x					
DER.2.1.A6	x	x	x			x		x	x	x		x	x
DER.2.1.A7		x					x	x					
DER.2.1.A8		x					x	x			x		
DER.2.1.A9		x	x	x	x		x	x			x		
DER.2.1.A10		x				x		x				x	x
DER.2.1.A11		x	x					x					
DER.2.1.A12		x	x				x						x
DER.2.1.A13		x											x
DER.2.1.A14		x	x	x	x			x					x
DER.2.1.A15		x	x	x				x					
DER.2.1.A16		x						x					
DER.2.1.A17		x	x	x	x			x				x	x
DER.2.1.A18		x	x	x				x				x	x
DER.2.1.A19		x				x	x				x	x	x
DER.2.1.A20		x	x	x	x		x	x		x		x	x
DER.2.1.A21		x	x	x			x	x		x	x	x	x
DER.2.1.A22	x	x	x	x	x	x	x	x			x	x	x

DER.2: Security Incident Management

DER.2.2 Vorsorge für die IT-Forensik

1 Beschreibung

1.1 Einleitung

IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems.

IT-Sicherheitsvorfälle forensisch zu untersuchen, ist immer dann notwendig, wenn eingetretene Schäden bestimmt, Angriffe abgewehrt und künftig vermieden sowie Angreifer identifiziert werden sollen. Ob ein IT-Sicherheitsvorfall forensisch untersucht wird, entscheidet sich während der Vorfall behandelt wird. Eine IT-forensische Untersuchung im Sinne dieses Bausteins besteht aus den folgenden Phasen:

- strategische Vorbereitung: In dieser Phase werden Prozesse geplant und aufgebaut, die sicherstellen, dass eine Institution IT-Sicherheitsvorfälle forensisch analysieren kann. Sie ist auch dann notwendig, wenn die Institution über keine eigenen Forensik-Experten verfügt.
- Initialisierung: Nachdem die verantwortlichen Mitarbeiter entschieden haben, einen IT-Sicherheitsvorfall forensisch zu untersuchen, werden die vorher geplanten Prozesse angestoßen. Weiterhin wird der Untersuchungsrahmen festgelegt und es werden Erstmaßnahmen durchgeführt.
- Spurensicherung: Hier werden die zu sichernden Beweismittel ausgewählt und die Daten forensisch gesichert. Dabei wird zwischen Live-Forensik und Post-Mortem-Forensik unterschieden: Die Live-Forensik stellt sicher, dass flüchtige Daten (z. B. Netzverbindungen, RAM) von einem laufenden IT-System gesichert werden. Bei der Post-Mortem-Forensik hingegen werden forensische Kopien von Datenträgern erstellt.
- Analyse: Die gesammelten Daten werden forensisch analysiert. Dabei werden die Daten sowohl für sich als auch im Gesamtzusammenhang betrachtet.
- Ergebnisdarstellung: Die relevanten Untersuchungsergebnisse werden zielgruppengerecht aufbereitet und vermittelt.

1.2 Zielsetzung

Der Baustein zeigt auf, welche Vorsorgemaßnahmen notwendig sind, um IT-forensische Untersuchungen zu ermöglichen. Dabei wird vor allem darauf eingegangen, wie die Spurensicherung vorbereitet und durchgeführt werden kann. Führen Forensik-Dienstleister Spurensicherung ganz oder teilweise durch, gelten die Anforderungen auch für die Dienstleister. Durch vertragliche Vereinbarungen und Prüfungen, kann dabei sichergestellt werden, dass sich der Dienstleister auch daran hält.

1.3 Abgrenzung

Der Baustein beschreibt keine Anforderungen, die sicherstellen, dass Angriffe erkannt werden. Diese sind im Baustein DER.1 *Detekction von sicherheitsrelevanten Ereignissen* enthalten und werden im vorliegenden Baustein vorausgesetzt. Auch werden keine Kriterien und Prozesse erläutert, anhand derer die Verantwortlichen entscheiden können, ob ein IT-Sicherheitsvorfall forensisch untersucht werden muss oder nicht. Die Entscheidung darüber wird getroffen, während der Sicherheitsvorfall behandelt wird (siehe DER.2.1 *Incident Management*).

Weiterhin befasst sich der Baustein nur mit Vorsorgemaßnahmen, die grundlegend für spätere IT-forensische Untersuchungen sind. Wie die eigentliche forensische Analyse durchgeführt wird, ist daher nicht Thema dieses Bausteins.

Letztlich geht der Baustein auch nicht darauf ein, wie sich IT-Infrastrukturen bereinigen lassen, nachdem sie angegriffen worden sind (siehe dazu DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle*). Die dort beschriebenen Tätigkeiten können jedoch durch die Ergebnisse von IT-forensischen Untersuchungen maßgeblich unterstützt werden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für die Vorsorge für die IT-Forensik von besonderer Bedeutung:

2.1 Verstoß gegen rechtliche Rahmenbedingungen

Für IT-forensische Untersuchungen werden oft alle als notwendig erachteten Daten kopiert, sichergestellt und ausgewertet. Darunter befinden sich meistens auch personenbezogene Daten von Mitarbeitern oder Partnern. Wird darauf z. B. unbegründet und ohne dass der Datenschutzbeauftragte miteinbezogen wird, zugegriffen, verstößt die Institution gegen gesetzliche Regelungen, z. B. wenn dabei die Zweckbindung missachtet wird. Auch ist es möglich, dass aus den erhobenen Daten beispielsweise abgeleitet werden kann, wie sich Mitarbeiter verhalten, oder es kann ein Bezug zu ihnen hergestellt werden. Dadurch besteht die Gefahr, dass auch gegen interne Regelungen verstoßen wird.

2.2 Verlust von Beweismitteln durch fehlerhafte oder unvollständige Beweissicherung

Werden Beweismittel falsch oder nicht schnell genug gesichert, können dadurch wichtige Daten verlorengehen, die später auch nicht wiederherstellbar sind. Schlimmstenfalls führt das zu einer ergebnislosen forensischen Untersuchung. Mindestens ist jedoch die Beweiskraft eingeschränkt.

Die Gefahr wichtige Beweismittel zu verlieren, steigt stark an, wenn Mitarbeiter Forensik-Werkzeuge fehlerhaft benutzen, Daten zu langsam sichern oder zu wenig üben. Oft gehen auch Beweismittel verloren, wenn die Verantwortlichen flüchtige Daten nicht als relevant erkennen und sichern.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Vorsorge für die IT-Forensik aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	Informationssicherheitsbeauftragter (ISB)
Weitere Verantwortliche	Datenschutzbeauftragter, Ermittler, Ermittlungsleiter, Institutionsleitung

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

DER.2.2.A1 Prüfung rechtlicher und regulatorischer Rahmenbedingungen zur Erfassung und Auswertbarkeit [Institutionsleitung, Datenschutzbeauftragter]

Werden Daten für forensische Untersuchungen erfasst und ausgewertet, MÜSSEN alle rechtlichen und regulatorischen Rahmenbedingungen identifiziert und eingehalten werden (siehe ORP.5 *Anforderungsmanagement*). Auch DARF NICHT gegen interne Regelungen und Mitarbeitervereinbarungen verstoßen werden. Im Einzelfall kann es jedoch notwendig sein, das Interesse der Institution gegen das der Mitarbeiter abzuwägen. Dabei MUSS der Betriebs- oder Personalrat sowie der Datenschutzbeauftragte einbezogen werden.

DER.2.2.A2 Erstellung eines Leitfadens für Erstmaßnahmen bei einem IT-Sicherheitsvorfall

Es MUSS ein Leitfaden erstellt werden, der für die eingesetzten IT-Systeme beschreibt, welche Erstmaßnahmen bei einem IT-Sicherheitsvorfall durchgeführt werden müssen, um möglichst wenig Spuren zu zerstören. Darin MUSS auch beschrieben sein, durch welche Handlungen potenzielle Spuren vernichtet werden können und wie sich das vermeiden lässt.

DER.2.2.A3 Vorauswahl von Forensik-Dienstleistern

Verfügt eine Institution nicht über ein eigenes Forensik-Team, MÜSSEN bereits in der Vorbereitungsphase mögliche geeignete Forensik-Dienstleister identifiziert werden. Welche Forensik-Dienstleister infrage kommen, MUSS dokumentiert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Vorsorge für die IT-Forensik. Sie SOLLTEN grundsätzlich umgesetzt werden.

DER.2.2.A4 Festlegung von Schnittstellen zum Krisen- und Notfallmanagement

Die Schnittstellen zwischen IT-forensischen Untersuchungen und dem Krisen- und Notfallmanagement SOLLTEN definiert und dokumentiert werden. Hierzu SOLLTE geregelt werden, welche Mitarbeiter für was verantwortlich sind und wie mit ihnen kommuniziert werden soll. Darüber hinaus SOLLTE sichergestellt werden, dass Ansprechpartner erreichbar sind.

DER.2.2.A5 Erstellung eines Leitfadens für Beweissicherungsmaßnahmen bei IT-Sicherheitsvorfällen

Es SOLLTE ein Leitfaden erstellt werden, in dem beschrieben wird, wie Beweise gesichert werden sollen. Darin SOLLTEN Vorgehensweisen, technische Werkzeuge, rechtliche Rahmenbedingungen und Dokumentationsvorgaben aufgeführt werden.

DER.2.2.A6 Schulung des Personals für die Umsetzung der forensischen Sicherung

Alle verantwortlichen Mitarbeiter SOLLTEN wissen, wie sie Spuren korrekt sichern und Forensik-Werkzeuge richtig einsetzen. Dafür SOLLTEN geeignete Schulungen angeboten werden.

DER.2.2.A7 Auswahl von Forensik-Werkzeugen

Es SOLLTE sichergestellt werden, dass Werkzeuge, mit denen Spuren forensisch gesichert und analysiert werden, auch dafür geeignet sind. Bevor ein Forensik-Werkzeug eingesetzt wird, SOLLTE zudem geprüft werden, ob es richtig funktioniert. Auch SOLLTE überprüft und dokumentiert werden, dass es nicht manipuliert wurde.

DER.2.2.A8 Auswahl und Reihenfolge der zu sichernden Beweismittel [Ermittlungsleiter]

Eine forensische Untersuchung SOLLTE immer damit beginnen, die Ziele bzw. den Arbeitsauftrag zu definieren. Die Ziele SOLLTEN möglichst konkret formuliert sein. Danach SOLLTEN alle notwendigen Datenquellen identifiziert werden. Auch SOLLTE festgelegt werden, in welcher Reihenfolge die Daten gesichert werden und wie genau dabei vorgegangen werden soll. Die Reihenfolge SOLLTE sich danach richten, wie flüchtig (volatil) die zu sichernden Daten sind. So SOLLTEN schnell flüchtige Daten zeitnah gesichert werden. Erst danach SOLLTEN beispielsweise Festspeicherinhalte und schließlich Backups folgen.

DER.2.2.A9 Vorauswahl forensisch relevanter Daten [Ermittlungsleiter]

Es SOLLTE festgelegt werden, welche sekundären Daten (z. B. Logdaten oder Verkehrsmitschnitte) auf welche Weise und wie lange im Rahmen der rechtlichen Rahmenbedingungen für mögliche forensische Beweissicherungsmaßnahmen vorgehalten werden.

DER.2.2.A10 IT-forensische Sicherung von Beweismitteln [Ermittler, Ermittlungsleiter]

Um Beweismittel zu sichern, SOLLTEN möglichst die kompletten Datenträger forensisch dupliziert werden. Wenn das nicht möglich ist, z. B. bei flüchtigen Daten im RAM oder in SAN-Partitionen, SOLLTE eine Methode gewählt werden, die möglichst wenig Daten verändert.

Um nachweisen zu können, dass die Daten integer sind, SOLLTEN die Originaldatenträger versiegelt aufbewahrt werden. Existieren kryptografische Prüfsummen von forensischen Kopien oder Originalen, kann die Integrität auch darüber nachgewiesen werden. Dazu SOLLTEN die schriftlich dokumentierten kryptografischen Prüfsummen von den Datenträgern getrennt und in mehreren Kopien aufbewahrt werden. Zudem SOLLTE sichergestellt sein, dass die so dokumentierten Prüfsummen nicht verändert werden können. Damit die Daten gerichtlich verwertbar sind, SOLLTE ein Zeuge bestätigen, wie dabei vorgegangen wurde und die erstellen Prüfsummen beglaubigen.

Es SOLLTE ausschließlich geschultes Personal (siehe DER.2.2.A6 *Schulung des Personals für die Umsetzung der forensischen Sicherung*) oder ein Forensik-Dienstleister (siehe DER.2.2.A3 *Vorauswahl von Forensik-Dienstleistern*) eingesetzt werden, um Beweise forensisch zu sichern.

DER.2.2.A11 Dokumentation der Beweissicherung [Ermittler, Ermittlungsleiter]

Wenn Beweise forensisch gesichert werden, SOLLTEN alle dafür durchgeführten Schritte dokumentiert werden. Die Dokumentation SOLLTE lückenlos nachweisen, wie mit den gesicherten Originalbeweismitteln umgegangen wurde. Auch SOLLTE dokumentiert werden, welche Methoden eingesetzt wurden und warum sich die Verantwortlichen dafür entschieden haben.

DER.2.2.A12 Sichere Verwahrung von Originaldatenträgern und Beweismitteln [Ermittler, Ermittlungsleiter]

Alle sichergestellten Originaldatenträger SOLLTEN physisch so gelagert werden, dass nur ermittelnde und namentlich bekannte Mitarbeiter darauf zugreifen können. Wenn Originaldatenträger und Beweismittel eingelagert werden, SOLLTE festgelegt werden, wie lange sie aufzubewahren sind. Nachdem die Frist abgelaufen ist, SOLLTE geprüft werden, ob die Datenträger und Beweise noch weiter aufbewahrt werden müssen. Nach der Aufbewahrungsfrist SOLLTEN Beweismittel sicher gelöscht oder vernichtet und Originaldatenträger zurückgegeben werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

DER.2.2.A13 Rahmenverträge mit externen Dienstleistern (CIA)

Damit IT-Sicherheitsvorfälle schneller forensisch untersucht werden können, SOLLTE die Institution Abrufvereinbarungen bzw. Rahmenverträge mit Forensik-Dienstleistern abschließen.

DER.2.2.A14 Festlegung von Standardverfahren für die Beweissicherung (CIA)

Für Anwendungen, IT-Systeme bzw. IT-Systemgruppen mit hohem Schutzbedarf sowie für verbreitete Systemkonfigurationen SOLLTEN Standardverfahren erstellt werden, die es erlauben, flüchtige und nichtflüchtige Daten möglichst vollständig forensisch zu sichern.

Die jeweiligen systemspezifischen Standardverfahren SOLLTEN durch erprobte und möglichst automatisierte Prozesse umgesetzt werden. Sie SOLLTEN zudem durch Checklisten und technische Hilfsmittel unterstützt werden, z. B. durch Software, Software-Tools auf mobilen Datenträgern und IT-forensischer Hardware wie Schreibblockern.

DER.2.2.A15 Durchführung von Übungen zur Beweissicherung (CIA)

Alle an forensischen Analysen beteiligten Mitarbeiter SOLLTEN regelmäßig üben, wie Beweise bei einem IT-Sicherheitsvorfall zu sichern sind.

4 Weiterführende Informationen

4.1 Literatur

- [BSIFor] BSI Leitfaden IT-Forensik
  BSI, Version 1.0.1, 03.2011
  https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/IT-Forensik/forensik_node.html

- [ISFTM24] Information Security Forum (ISF), insbesondere Area TM 2.4 Forensic Investigations
  ISF, insbesondere Area TM 2.4 Forensic Investigations, 06.2016

- [ISO27042] ISO/IEC 27042:2015
  Information technology- Security techniques- Guidelines for the analysis and interpretation of digital evidence, ISO, 06.2015
  https://www.iso.org/standard/44406.html

- [ISO27043] DIN EN ISO/IEC 27043
  Informationstechnik- IT- Sicherheitsverfahren- Grundsätze und Prozesse für die Untersuchung von Vorfällen (ISO/IEC 27043:2015); Deutsche Fassung EN ISO/IEC27043:2016

- [NIST80086] NIST Special Publikaton 800-86
  NIST, Guide to Integrating Forensic Techniques into Incident Response, 08.2006
  https://csrc.nist.gov/publications/detail/sp/800-86/final

- [RFC3227] Guidelines for Evidence Collection and Archiving
  RFC, 02.2002
  https://tools.ietf.org/html/rcf3227

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Vorsorge für die IT-Forensik" von Bedeutung.

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.22 Manipulation von Informationen

G 0.25 Ausfall von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.37 Abstreiten von Handlungen

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.17	G 0.20	G 0.22	G 0.25	G 0.27	G 0.29	G 0.31	G 0.37	G 0.45	G 0.46
DER.2.2.A1						x			x	
DER.2.2.A2	x	x	x	x			x		x	x
DER.2.2.A3					x		x		x	
DER.2.2.A4				x					x	x
DER.2.2.A5	x	x	x	x			x		x	x
DER.2.2.A6		x					x		x	x
DER.2.2.A7							x		x	x
DER.2.2.A8	x		x				x	x	x	x
DER.2.2.A9	x		x				x	x	x	x
DER.2.2.A10	x		x				x	x	x	x
DER.2.2.A11	x		x	x			x	x	x	x
DER.2.2.A12	x		x					x	x	x
DER.2.2.A13					x		x		x	
DER.2.2.A14	x		x	x			x	x	x	x
DER.2.2.A15	x		x	x			x	x	x	x

DER.2: Security Incident Management

DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle

1 Beschreibung

1.1 Einleitung

Bei Advanced Persistent Threats (APT) handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netz verschafft und diesen in der Folge auf weitere IT-Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind in der Regel schwierig zu detektieren.

Nachdem ein APT-Angriff entdeckt wurde, stehen die Verantwortlichen in den betroffenen Institutionen vor der Herausforderung, eine Bereinigung durchführen zu müssen, die über das übliche Vorgehen zur Behandlung von IT-Sicherheitsvorfällen hinausgeht. Denn es ist davon auszugehen, dass die entdeckten Angreifer bereits seit geraumer Zeit auf die betroffene IT-Infrastruktur zugreifen können und komplexe Angriffswerkzeuge benutzen, um die Standard-Sicherheitsmechanismen zu umgehen und diverse Hintertüren zu etablieren. Außerdem besteht die Gefahr, dass die Angreifer die infizierte Umgebung genau beobachten und auf Bereinigungsversuche reagieren, indem sie ihre Spuren verwischen und die Untersuchung sabotieren.

Allgemein geht der Baustein von einer hohen Bedrohungslage durch einen gezielten, motivierten Angreifer mit überdurchschnittlichen Ressourcen aus. Grundsätzlich sollte bei einem solchen Vorfall immer auch ein (zertifizierter) Forensikdienstleister hinzugezogen werden, wenn die Institution selbst nicht über entsprechende eigene Forensik-Experten verfügt. Forensik-Dienstleister sollten dabei bereits in der Phase der forensischen Analyse herangezogen werden, der Dienstleister sollte jedoch auch bei der Bereinigung zumindest beratend hinzugezogen werden

1.2 Zielsetzung

Dieser Baustein beschreibt, wie eine Institution vorgehen sollte, um nach einem APT-Angriff die IT-Systeme zu bereinigen und den regulären und sicheren Betriebszustand des Informationsverbunds wiederherzustellen.

1.3 Abgrenzung

Ein Informationsverbund kann nur bereinigt werden, wenn der APT-Vorfall vorher erfolgreich detektiert und forensisch analysiert wurde. Detektion und Forensik sind jedoch nicht Thema dieses Bausteins, sondern werden in DER.1 *Detektion von sicherheitsrelevanten Ereignissen* und DER.2.2 *Vorsorge für die IT-Forensik* behandelt.

Im vorliegenden Baustein wird ausschließlich die Bereinigung von APT-Vorfällen betrachtet. Übliche Vorfälle werden im Baustein DER.2.1 *Incident Management* behandelt. Auch beschreibt der Baustein nicht, wie sogenannte Indicators of Compromise (IOCs), also Einbruchsspuren, abzuleiten sind

und wie diese benutzt werden können, um wiederkehrende Angreifer zu erkennen. Ebenso wird nicht darauf eingegangen, wie sich eventuell bei der Analyse und Bereinigung übersehene Hintertüren finden lassen. Weiterhin ist der Baustein abzugrenzen vom übergeordneten Incident-Management-Prozess (siehe DER.2.1 *Incident Management*), in den die Bereinigung eingebettet ist.

Außerdem werden keine Angriffe betrachtet, mit denen sich Angreifer physischen Zugriff auf eine IT-Umgebung verschaffen. So fallen Angriffsformen wie in Rechenzentren einbrechen, Administratoren bestechen, neu beschaffte Hardware abfangen und manipulieren oder elektromagnetische Strahlung abhören nicht in diesen Baustein. Es werden ausschließlich Cyber-Angriffe berücksichtigt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Bereinigung weitreichender Sicherheitsvorfälle von besonderer Bedeutung:

2.1 Unvollständige Bereinigung

APT-Angreifer wollen üblicherweise einen Informationsverbund dauerhaft infiltrieren. Sie verfügen über die dafür notwendigen Ressourcen und sind in der Lage, langfristige Angriffskampagnen durchzuführen. Dafür benutzen sie Werkzeuge und Methoden, die auf ein Angriffsziel abgestimmt sind. Auch wenn ein APT-Vorfall entdeckt wird, kann nicht davon ausgegangen werden, dass sämtliche Zugangswege der Angreifer gefunden, alle Infektionen und Kommunikationswege von Schadsoftware beseitigt und alle Hintertüren entfernt wurden. Bei einer unvollständigen Bereinigung ist es jedoch sehr wahrscheinlich, dass ein Angreifer zu einem späteren Zeitpunkt, z. B. nach einer längeren Ruhephase, erneut auf die IT-Systeme zugreift und seinen Zugang wieder ausbaut. Das kann er beispielsweise, indem er Hintertüren nicht nur in Betriebssystemen und Anwendungssoftware platziert, sondern auch hardwarenahe Komponenten, wie etwa Firmware, manipuliert. Solche Modifikationen sind nur sehr schwierig zu identifizieren und das notwendige Wissen, um sie zu extrahieren und zu analysieren, ist nur wenig verbreitet. Versuchen die Verantwortlichen z. B., die IT-Komponenten zu bereinigen, indem sie die Firmware überschreiben oder aktualisieren, kann es trotzdem passieren, dass der Angreifer auch die Update-Routinen modifiziert hat und somit auf diesem Weg wieder ins System kommt.

2.2 Vernichtung von Spuren

Nach einem APT-Vorfall werden IT-Systeme oft neu installiert oder ganz ausgemustert. Wurde jedoch zuvor von den IT-Systemen keine forensische Kopie angefertigt, können Spuren vernichtet werden, die für eine weitere Aufklärung des Vorfalls oder sogar für ein Gerichtsverfahren notwendig wären.

2.3 Vorzeitige Alarmierung des Angreifers

Üblicherweise wird vor der Bereinigung eines APT-Vorfalls der Angriff über längere Zeit hinweg beobachtet und forensisch analysiert, um so alle Zugangswege und verwendeten Werkzeuge und Methoden zu identifizieren. Bemerkt der Angreifer während dieser Phase, dass er entdeckt wurde, greift er eventuell zu Gegenmaßnahmen. Beispielsweise kann er versuchen, seine Spuren zu verwischen oder er sabotiert noch schnell weitere IT-Systeme. Auch könnte er aufhören oder weitere Hintertüren einrichten, um einfach später den Angriff fortzuführen.

Da bei einem APT-Angriff grundsätzlich davon ausgegangen werden muss, dass die gesamte IT-Infrastruktur der Institution kompromittiert wurde, ist das Risiko hoch, dass der Angreifer die Bereinigungsaktivitäten entdeckt. Das gilt insbesondere, wenn die kompromittierte IT-Infrastruktur benutzt wird, um die Bereinigung zu planen und zu koordinieren. Finden die wesentlichen Schritte zur Bereinigung nicht in der korrekten Reihenfolge statt bzw. werden kritische Maßnahmen nicht gleichzeitig und aufeinander abgestimmt durchgeführt, erhöht sich die Gefahr, dass der Angreifer alarmiert wird. Isolieren die Verantwortlichen beispielsweise das Netz schrittweise statt auf einmal, wird der Angreifer eventuell gewarnt, bevor sein Zugriff effektiv beendet ist.

2.4 Datenverlust und Ausfall von IT-Systemen

Bei der Bereinigung eines APT-Vorfalls werden verschiedene IT-Systeme neu installiert und auch Netze temporär isoliert. Hierdurch fallen zwangsweise IT-Systeme aus und Dienste sind damit z. B. nur noch eingeschränkt oder gar nicht mehr verfügbar. Dauert die Bereinigung sehr lange, kann es hierdurch zu erheblichen Produktivitätsausfällen kommen. Das kann wiederum signifikante wirtschaftliche Einbußen zur Folge haben, die sogar die Unternehmensexistenz bedrohen können. Dies ist auch insbesondere dann der Fall, wenn keine oder keine ausreichende Dokumentation für einen Wiederaufbau verfügbar ist.

2.5 Fehlender Netzumbau nach einem APT-Angriff

Bei einem APT-Angriff erlangt der Angreifer detaillierte Kenntnisse darüber, wie die Zielumgebung aufgebaut und konfiguriert ist. Zum Beispiel kennt er die existierenden Netzsegmente, Namensschemata für IT-Systeme, Benutzer- und Dienstkonten, eingesetzte Software und Services. Durch dieses Wissen kann sich derselbe Angreifer unter Umständen nach einer Bereinigung erneut Zugang auf die Zielumgebung verschaffen. Somit kann er sich sehr gezielt, effizient und unauffällig innerhalb des Netzes bewegen und in kurzer Zeit erneut einen hohen Infektionsgrad erreichen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Bereinigung weitreichender Sicherheitsvorfälle (APT-Responder) aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Informationssicherheitsbeauftragter (ISB), Leiter IT

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

DER.2.3.A1 Einrichtung eines Leitungsgremiums [Informationssicherheitsbeauftragter (ISB)]

Um einen APT-Vorfall zu bereinigen, MUSS ein Leitungsgremium eingerichtet werden, dass alle notwendigen Aktivitäten plant, koordiniert und überwacht. Dem Gremium MÜSSEN alle für die Aufgaben erforderlichen Weisungsbefugnisse übertragen werden.

Wenn ein solches Leitungsgremium bereits eingerichtet wurde, als der APT-Vorfall detektiert und klassifiziert wurde, SOLLTE dasselbe Gremium auch die Bereinigung planen und leiten. Wurde schon ein spezialisierter Forensik-Dienstleister hinzugezogen, um den APT-Vorfall zu analysieren, SOLLTE auch dieser bei der Vorfallsbereinigung miteinbezogen werden.

Ist die IT zu stark kompromittiert oder sind die notwendigen Bereinigungsmaßnahmen sehr umfangreich, SOLLTE geprüft werden, ob ein Krisenstab eingerichtet werden soll. In diesem Fall MUSS das Leitungsgremium die Bereinigungsmaßnahmen überwachen. Das Leitungsgremium MUSS dann dem Krisenstab berichten.

DER.2.3.A2 Entscheidung für eine Bereinigungsstrategie [Leiter IT, Informationssicherheitsbeauftragter (ISB)]

Bevor ein APT-Vorfall tatsächlich bereinigt wird, MUSS das Leitungsgremium eine Bereinigungsstrategie festlegen. Hierbei MUSS insbesondere entschieden werden, ob die Schadsoftware von kompromittierten IT-Systemen entfernt werden kann, ob IT-Systeme neu installiert werden müssen oder ob IT-Systeme inklusive der Hardware komplett ausgetauscht werden sollen. Weiterhin MUSS festgelegt werden, welche IT-Systeme bereinigt werden. Grundlage für diese Entscheidungen MÜSSEN die Ergebnisse einer zuvor durchgeführten forensischen Untersuchung sein.

Es SOLLTEN alle betroffenen IT-Systeme neu installiert werden. Danach MÜSSEN die Wiederanlaufpläne der Institution benutzt werden. Bevor jedoch Backups wieder eingespielt werden, MUSS durch forensische Untersuchungen sichergestellt sein, dass hierdurch keine manipulierten Daten oder Programme auf das neu installierte IT-System übertragen werden.

Entscheidet sich eine Institution dagegen alle IT-Systeme neu zu installieren, MUSS eine gezielte APT-Bereinigung umgesetzt werden. Um das Risiko übersehener Hintertüren zu minimieren, MÜSSEN nach der Bereinigung die IT-Systeme gezielt daraufhin überwacht werden, ob sie noch mit dem Angreifer kommunizieren.

DER.2.3.A3 Isolierung der betroffenen Netzabschnitte

Die von einem APT-Vorfall betroffenen Netzabschnitte MÜSSEN vollständig isoliert werden (Cut-Off). Insbesondere DÜRFEN die betroffenen Netzabschnitte NICHT mit dem Internet verbunden sein. Um den Angreifer effektiv auszusperren und zu verhindern, dass er seine Spuren verwischt oder noch IT-Systeme sabotiert, MÜSSEN die Netzabschnitte auf einen Schlag isoliert werden.

Welche Netzabschnitte isoliert werden müssen, MUSS vorher durch eine forensische Analyse bestimmt werden. Es MÜSSEN dabei sämtliche betroffenen Abschnitte identifiziert werden. Kann das nicht sichergestellt werden, MÜSSEN alle verdächtigen sowie alle auch nur theoretisch infizierten Netzabschnitte isoliert werden.

Um Netzabschnitte effektiv isolieren zu können, MÜSSEN sämtliche lokalen Internetanschlüsse, z. B. zusätzliche DSL-Anschlüsse in einzelnen Subnetzen, möglichst vollständig erfasst und mitberücksichtigt werden.

DER.2.3.A4 Sperrung und Änderung von Zugangsdaten und kryptografischen Schlüsseln

Da davon ausgegangen werden muss, dass der Angreifer sich sämtliche auf den kompromittierten IT-Systemen vorhandenen Zugangsdaten angeeignet hat, MÜSSEN alle Zugangsdaten geändert werden, nachdem das Netz isoliert wurde. Weiterhin MÜSSEN auch zentral verwaltete Zugangsdaten zurückgesetzt werden, z. B. in Active-Directory-Umgebungen oder wenn das Lightweight DirectoryAccess Protocol (LDAP) benutzt wurde.

Ist der zentrale Authentisierungsserver (Domaincontroller oder LDAP-Server) kompromittiert, MÜSSEN sämtliche dort vorhandenen Zugänge gesperrt und ihre Passwörter ausgetauscht werden. Dies MÜSSEN erfahrene Administratoren umsetzen, falls erforderlich mithilfe interner oder externer Forensikexperten.

Wurden TLS-Schlüssel oder eine interne Certification Authority (CA) durch den APT-Angriff kompromittiert, MÜSSEN entsprechende Schlüssel und Infrastrukturen neu erzeugt und verteilt werden. Auch MÜSSEN die kompromittierten Schlüssel zuverlässig gesperrt werden.

DER.2.3.A5 Schließen des initialen Einbruchswegs

Wurde durch eine forensische Untersuchung herausgefunden, dass der Angreifer durch eine technische Schwachstelle in das Netz der Institution eingedrungen ist, MUSS diese Schwachstelle geschlossen werden. Konnten die Angreifer die IT-Systeme durch menschliche Fehlhandlungen kompromittieren, MÜSSEN organisatorische, personelle und technische Maßnahmen ergriffen werden, um ähnliche Vorfälle zukünftig zu verhindern.

DER.2.3.A6 Rückführung in den Produktivbetrieb

Nachdem das Netz erfolgreich bereinigt wurde, MÜSSEN die IT-Systeme geordnet in den Produktivbetrieb zurückgeführt werden. Dabei MÜSSEN sämtliche zuvor angeschafften IT-Systeme und installierten Programme, mit denen der Angriff beobachtet und analysiert wurde, entweder entfernt oder aber in den Produktivbetrieb überführt werden. Dasselbe MUSS mit Kommunikations- und Kollaborationssystemen erfolgen, die für die Bereinigung angeschafft wurden. Beweismittel und ausgesonderte IT-Systeme MÜSSEN entweder sicher gelöscht bzw. vernichtet oder aber geeignet archiviert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Bereinigung weitreichender Sicherheitsvorfälle. Sie SOLLTEN grundsätzlich umgesetzt werden.

DER.2.3.A7 Gezielte Systemhärtung

Nach einem APT-Angriff SOLLTEN alle betroffenen IT-Systeme gehärtet werden. Grundlage hierfür SOLLTEN die Ergebnisse der forensischen Untersuchungen sein (siehe DER.2.X *IT-Forensische Analysen*). Zusätzlich SOLLTE erneut geprüft werden, ob die betroffene Umgebung noch sicher ist, z. B. mit den Ergebnissen der ausführlichen forensischen Analysen.

Wenn möglich, SOLLTEN IT-Systeme bereits während der Bereinigung gehärtet werden. Maßnahmen, die sich nicht kurzfristig durchführen lassen, SOLLTEN in einen Maßnahmenplan aufgenommen und mittelfristig umgesetzt werden. Der ISB SOLLTE dafür verantwortlich sein, den Plan aufzustellen und zu prüfen, ob er korrekt umgesetzt wurde.

DER.2.3.A8 Etablierung sicherer, unabhängiger Kommunikationskanäle

Es SOLLTEN sichere Kommunikationskanäle für das Leitungsgremium und die mit der Bereinigung beauftragen Mitarbeiter etabliert werden. Es SOLLTE darauf geachtet werden, dass ein möglichst sicherer Kommunikationskanal ausgewählt wird.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

DER.2.3.A9 Hardwaretausch betroffener IT-Systeme (CIA)

Bei IT-Systemen mit hohem Schutzbedarf SOLLTE erwogen werden, nach einem APT-Vorfall die Hardware komplett auszutauschen. Auch wenn nach einer Bereinigung bei einzelnen IT-Systemen noch verdächtiges Verhalten beobachtet wird, z. B. unerklärlicher Netzverkehr, SOLLTE das betroffene IT-System ausgetauscht werden.

DER.2.3.A10 Umbauten zur Erschwerung eines erneuten Angriffs durch denselben Angreifer (CI)

Damit derselbe Angreifer nicht noch einmal einen APT-Angriff auf die IT-Systeme der Institution durchführen kann, SOLLTE der interne Aufbau der Netzumgebung abgeändert werden. Außerdem SOLLTEN Mechanismen etabliert werden, mit denen sich ein wiederkehrender Angreifer schnell detektieren lässt.

4 Weiterführende Informationen

4.1 Literatur

- [CS072] Erste Hilfe bei einem APT Angriff
  Bundesamt für Sicherheit in der Informationstechnik, Version 3.0, 01.2016
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_072_TLP-White.pdf

- [DRP] Data Breach Response Guide
  Experian Data Breach Resolution, 2013
  https://www.experian.com/assets/data-breach/brochures/response-guide.pdf

- [KGT] Protection from Kerberos Golden Ticket
  CERT-EU, 06.2014
  https://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_14_07_PassTheGolden_Ticket_v1_1.pdf

- [ReCoBS] Common Criteria Protection Profile for Remote-Controlled Browsers System (ReCoBS)
  BSI, BSI-PP-0040; Version 1.0, 2008
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/recobslanginfo_pdf.pdf?_blob=publicationBundesamt

- [SANS1] When Breaches Happen: Top Five Questions to Prepare For
  SANS Institute, 2000
  https://www.sans.org/reading-room/whitepapers/analyst/breaches-happen-top-questions-prepare-35220

- [SANS2] Detection and Recovery from a Major security Breach
  SANS Institute, 2000
  https://giac.org/paper/gcux/50/detection-recovery-major-security-breach/100810

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Bereinigung weitreichender Sicherheitsvorfälle" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.43 Einspielen von Nachrichten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.14	G 0.15	G 0.16	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.24	G 0.28	G 0.29	G 0.31	G 0.32	G 0.39	G 0.40	G 0.41	G 0.42	G 0.43	G 0.45	G 0.46
DER.2.3.A1	x				x											x	x	x		x	x
DER.2.3.A2	x	x	x		x		x	x	x	x				x	x		x		x	x	x
DER.2.3.A3	x				x			x	x					x						x	x
DER.2.3.A4	x	x	x		x		x	x	x	x				x	x	x	x		x	x	x
DER.2.3.A5	x	x			x				x		x			x			x	x			
DER.2.3.A6				x	x						x	x	x								
DER.2.3.A7	x	x	x		x	x	x	x	x	x	x			x	x	x	x		x	x	x
DER.2.3.A8	x	x	x		x			x											x	x	x
DER.2.3.A9	x	x	x		x		x	x	x						x		x		x		x
DER.2.3.A10	x	x	x		x		x	x	x	x	x			x	x		x		x		x

DER.3: Sicherheitsprüfungen

DER.3.1 Audits und Revisionen

1 Beschreibung

1.1 Einleitung

Audits und Revisionen sind grundlegend für jedes erfolgreiche Informationssicherheits- Managementsystem (ISMS). Nur wenn etablierte Sicherheitsmaßnahmen und -prozesse regelmäßig überprüft werden, ob sie wirksam, vollständig, angemessen und noch aktuell sind, lässt sich der Gesamtzustand der Informationssicherheit beurteilen. Audits und Revisionen sind somit ein Werkzeug, um ein angemessenes Sicherheitsniveau festzustellen, zu erreichen und aufrechtzuerhalten. Durch sie ist es möglich, Fehlentwicklungen und bestehende Sicherheitsmängel zu erkennen und entsprechende Gegenmaßnahmen einzuleiten.

Als Audit (lat. audire = hören, zuhören) wird eine systematische, unabhängige Prüfung von Aktivitäten und deren Ergebnissen bezüglich der Einhaltung von definierten Anforderungen (zum Beispiel Normen, Standards oder Richtlinien) verstanden. In einer Revision (revidieren = kontrollieren, prüfen) wird geprüft, ob Dokumente, Zustände, Gegenstände oder Vorgehensweisen korrekt, wirksam und angemessen sind. Im Gegensatz zum Audit muss die Revision nicht unbedingt unabhängig erfolgen. Zudem kann die Revision im Sinne einer Wartung auch bereits die Berichtigung beinhalten.

1.2 Zielsetzung

Der Baustein definiert Anforderungen an Audits und Revision mit dem Ziel, die Informationssicherheit in einer Institution zu verbessern, Fehlentwicklungen auf diesem Gebiet zu vermeiden und Sicherheitsmaßnahmen und -prozesse zu optimieren.

1.3 Abgrenzung

Der Baustein beschreibt, wie sich Audits und Revisionen aus Sicht des ISMS planen, durchführen und nachbereiten lassen. Das betrifft demnach interne Audits (sogenannte Erstparteien-Audits) und Revisionen sowie Audits bei Dienstleistern und Partnern (sogenannte Zweitparteien-Audits) der Institution. Zertifizierungsaudits (sogenannte Drittparteien-Audits) werden in diesem Baustein nicht berücksichtigt.

Ebenso wird die für Bundesbehörden verpflichtende IS-Revision nicht betrachtet. Diese wird im Baustein DER 3.2: *IS-Revision* behandelt. Weiterhin wird nicht berücksichtigt, wie Audits und Revisionen in eine eventuell existierende, übergeordnete Prüforganisation einer Institution integriert werden können.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Audit und Revision von besonderer Bedeutung:

2.1 Unzureichende oder nicht planmäßige Umsetzung von Sicherheitsmaßnahmen

Das Schutzniveau einer Institution hängt davon ab, dass Sicherheitsmaßnahmen vollständig und korrekt umgesetzt werden. Insbesondere in der kritischen Phase von Projekten oder unter bestimmten Rahmenbedingungen kann es vorkommen, dass Sicherheitsmaßnahmen temporär ausgesetzt werden. Teilweise wird jedoch vergessen, sie wieder zu reaktivieren, sodass ein zu niedriges Sicherheitsniveau entsteht.

2.2 Wirkungslose oder nicht wirtschaftliche Umsetzung von Sicherheitsmaßnahmen

Werden Sicherheitsmaßnahmen umgesetzt, ohne dabei bestimmte Praxisaspekte zu berücksichtigen, sind die Maßnahmen eventuell wirkungslos. Beispielsweise ist es sinnlos, den Eingangsbereich mit Drehkreuzen abzusperren, wenn die Mitarbeiter das Gebäude einfach durch einen offenen Seiteneingang betreten können.

Ebenso können Einzelmaßnahmen ergriffen werden, die wirtschaftlich nicht sinnvoll sind. So ist für den Schutz von Informationen mit einer normalen Vertraulichkeit ein sauber implementiertes Rechte- und Rollenkonzept sinnvoller und wirtschaftlicher als eine Certificate Authority und die anschließende zertifikatsbasierte Verschlüsselung des Fileservers aufzubauen.

2.3 Unzureichende Umsetzung des ISMS

In vielen Institutionen überprüft der Informationssicherheitsbeauftragten selbst, ob Sicherheitsmaßnahmen umgesetzt wurden. Oft wird darüber die Prüfung des eigentlichen ISMS vergessen. Insbesondere da dies durch einen unabhängigen Dritten erfolgen sollte. Hierdurch könnten die Prozesse eines ISMS ineffizient oder nicht angemessen umgesetzt sein. In der Folge kann das Sicherheitsniveau der Institution beeinträchtigt sein.

2.4 Unzureichende Qualifikation des Prüfers

Ist ein Auditor oder ein Revisor nicht ausreichend qualifiziert oder bereitet er sich ungenügend auf die Prüfungen vor, schätzt er während des Audits bzw. der Revision eventuell den Sicherheitszustand einer Institution falsch ein. Dadurch veranlasst er in seinem Prüfbericht nicht die nötigen oder sogar die falschen Korrekturmaßnahmen. Im schlimmsten Fall hat das eine zu hohe und damit nicht wirtschaftliche bzw. zu niedrige und damit sehr risikobehaftete Absicherung von Informationen zur Folge.

2.5 Fehlende langfristige Planung

Werden Audits und Revisionen nicht langfristig und zentral geplant, kann es passieren, dass einzelne Bereiche sehr häufig und andere überhaupt nicht geprüft werden. Dadurch ist es nur sehr schwer oder gar nicht möglich, den Sicherheitszustand des Informationsverbunds einzuschätzen.

2.6 Fehlende Planung und Abstimmung bei der Durchführung eines Audits

Wenn ein Audit mangelhaft geplant und nicht mit allen betroffenen Mitarbeitern der Institution abgestimmt wurde, sind während der Vor-Ort-Prüfung eventuell nicht die benötigten oder die falschen Ansprechpartner verfügbar. Dadurch lassen sich dann möglicherweise einzelne Bereiche überhaupt nicht auditieren. Auch wenn der Auditor die Termine für die einzelnen Bereiche zu eng gesetzt hat, könnte die geplante Untersuchung nur oberflächlich durchgeführt wird, wenn zu wenig Zeit verfügbar ist.

2.7 Fehlende Abstimmung mit der Personalvertretung

In Audits und Revisionen können auch Aspekte geprüft werden, aus denen sich Rückschlüsse auf die Leistung von Mitarbeitern ziehen lassen. Somit könnten diese Prüfungen als Leistungsbeurteilung gewertet werden. Wird die Personalvertretung nicht beteiligt, kann dies zu Verstößen gegen das geltende Mitbestimmungsrecht führen.

2.8 Absichtliches Verschweigen von Abweichungen

Mitarbeiter könnten befürchten, dass bei der Prüfung Fehler aufgedeckt werden, und darum versuchen, Sicherheitsprobleme zu kaschieren. Hierdurch könnte ein falsches Bild über den tatsächlichen Status Quo vermittelt werden.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Audit und Revision aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte (ISB) dafür zuständig, die Anforderungen zu erfüllen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	Informationssicherheitsbeauftragter (ISB)
Weitere Verantwortliche	Auditteam, Auditteamleiter, Institutionsleitung

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

DER.3.1.A1 Definition von Verantwortlichkeiten [Institutionsleitung]

Die Institutionsleitung MUSS einen Mitarbeiter benennen, der dafür verantwortlich ist, Audits bzw. Revisionen zu planen und zu initiieren. Dabei MUSS darauf geachtet werden, dass keine Interessenskonflikte entstehen, z. B. wenn die eigene Abteilung überprüft werden soll. Der Verantwortliche MUSS überwachen, dass die Ergebnisse der Audits und Revisionen bearbeitet werden.

DER.3.1.A2 Vorbereitung eines Audits oder einer Revision

Vor einem Audit oder einer Revision MÜSSEN der Prüfgegenstand und die Prüfungsziele festgelegt werden. Auch MÜSSEN die betroffenen Ansprechpartner unterrichtet werden. Abhängig vom Untersuchungsgegenstand MUSS die Personalvertretung über das geplante Audit oder die geplante Revision informiert werden.

DER.3.1.A3 Durchführung eines Audits

Bei einem Audit MUSS geprüft werden, ob die Anforderungen aus Richtlinien, Normen, Standards etc. erfüllt sind. Die Anforderungen MÜSSEN der geprüften Institution bekannt sein.

Ein Audit MUSS eine Dokumentenprüfung sowie eine Vor-Ort-Prüfung beinhalten. Beim Vor-Ort-Audit MUSS sichergestellt werden, dass die Auditoren niemals selbst aktiv in IT-Systeme eingreifen und auch keine Handlungsanweisungen zu Änderungen am Prüfgegenstand erteilen.

Sämtliche Ergebnisse eines Audits MÜSSEN schriftlich dokumentiert und in einem Auditbericht zusammengefasst werden. Der Auditbericht MUSS dem Ansprechpartner der Institution zeitnah übermittelt werden.

DER.3.1.A4 Durchführung einer Revision

Bei einer Revision MUSS geprüft werden, ob die Anforderungen vollständig, korrekt, angemessen und aktuell umgesetzt sind. Festgestellte Abweichungen MÜSSEN, wenn das möglich ist, sofort korrigiert werden. Die jeweiligen Revisionen MÜSSEN mit einer Änderungsverfolgung dokumentiert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Audits und Revisionen. Sie SOLLTEN grundsätzlich umgesetzt werden.

DER.3.1.A5 Integration in den Informationssicherheitsprozess

Es SOLLTEN eine Richtlinie zur internen ISMS-Auditierung und eine Richtlinie zur Lenkung von Korrekturmaßnahmen erstellt werden. Die Richtlinien SOLLTEN vorgeben, dass regelmäßige Audits und Revisionen ein Teil des Sicherheitsprozesses sind und durch diesen initiiert werden.

Außerdem SOLLTE sichergestellt werden, dass die Ergebnisse der Audits und Revisionen in das ISMS zurückfließen und zu dessen Verbesserung beitragen. Weiter SOLLTEN die durchgeführten Audits und Revisionen, die Ergebnisse sowie die Aktivitäten zur Mängelbeseitigung und Qualitätsverbesserung in den regelmäßigen Bericht des Informationssicherheitsbeauftragten an die Institutionsleitung aufgenommen werden.

DER.3.1.A6 Definition der Prüfungsgrundlage und eines einheitlichen Bewertungsschemas

Es SOLLTE eine einheitliche Prüfgrundlage für Audits festgelegt werden. Für die Bewertung der Umsetzung von Anforderungen SOLLTE ein einheitliches Bewertungsschema festgelegt und dokumentiert sein.

DER.3.1.A7 Erstellung eines Auditprogramms

Es SOLLTE ein Auditprogramm für mehrere Jahre aufgestellt werden, das alle durchzuführenden Audits und Revisionen erfasst. Für das Auditprogramm SOLLTEN Ziele definiert werden, die sich insbesondere aus den Institutionszielen sowie den Informationssicherheitszielen ableiten.

Für unvorhergesehene Ereignisse SOLLTEN Reserven in der jährlichen Ressourcenplanung vorgesehen werden. Das Auditprogramm SOLLTE einem eigenen kontinuierlichen Verbesserungsprozess unterliegen.

DER.3.1.A8 Erstellung einer Revisionsliste

Es SOLLTEN ein oder mehrere Revisionslisten gepflegt werden, die den aktuellen Stand der Revisionsobjekte sowie die geplanten Revisionen dokumentieren.

DER.3.1.A9 Auswahl eines geeigneten Audit- oder Revionsteams

Es SOLLTE für jedes Audit bzw. für jede Revision ein geeignetes Team zusammengestellt werden. Es SOLLTE ein leitender Auditor (Auditteamleiter) bzw. leitender Revisor benannt werden, der die Gesamtverantwortung für die Durchführung der Audits bzw. der Revisionen trägt.

Die Größe des Audit- bzw. Revisionsteams SOLLTE dem Prüfbereich entsprechen. Hierbei SOLLTEN insbesondere die Kompetenzanforderungen der Prüfthemen sowie die Größe und örtliche Verteilung des Prüfbereichs berücksichtigt werden. Die Mitglieder des Audit- bzw. Revisionsteams SOLLTEN angemessen qualifiziert sein.

Die Neutralität des Auditteams SOLLTE sichergestellt werden. Darüber hinaus SOLLTEN auch die Revisoren unabhängig sein. Werden externe Dienstleister als Auditoren oder Revisoren eingesetzt, SOLLTEN diese auf ihre Unabhängigkeit überprüft und zur Verschwiegenheit verpflichtet werden.

DER.3.1.A10 Erstellung eines Audit- oder Revisionsplans [Auditteamleiter]

Vor einem Audit oder einer größeren Revision SOLLTE der Auditteamleiter bzw. leitende Revisor einen Audit- bzw. Revisionplan erstellen. Bei Audits SOLLTE der Auditplan Teil des abschließenden Auditberichts sein. Der Auditplan SOLLTE während des gesamten Audits fortgeschrieben und bei Bedarf angepasst werden. Kleinere Revisionen SOLLTEN anhand der Revisionsliste geplant werden.

Es SOLLTEN genügend Ressourcen für das Audit- bzw. Revisionsteam vorgesehen werden.

DER.3.1.A11 Kommunikation und Verhalten während der Prüfungen [Auditteamleiter]

Es SOLLTEN klare Regelungen dafür aufgestellt werden, wie das Audit- bzw. Revisionsteam und die Mitarbeiter der zu prüfenden Institution bzw. Abteilung miteinander Informationen austauschen dürfen. So SOLLTE durch geeignete Maßnahmen sichergestellt werden, dass die bei einem Audit ausgetauschten Informationen auch vertraulich und integer bleiben.

Personen, die das Audit begleiten, SOLLTEN NICHT die Prüfungen beeinflussen. Zudem SOLLTEN sie zur Vertraulichkeit verpflichtet werden.

DER.3.1.A12 Durchführung eines Auftaktgesprächs [Auditteamleiter]

Es SOLLTE ein Auftaktgespräch zwischen dem Auditteam bzw. dem Revisionsteam und den betroffenen Ansprechpartnern durchgeführt werden. Dabei SOLLTEN das Audit- bzw. Revisionsverfahren erläutert und die Rahmenbedingungen der Vor-Ort-Prüfung abgestimmt und durch die jeweiligen Verantwortlichen bestätigt werden.

DER.3.1.A13 Sichtung und Prüfung der Dokumente [Auditteam]

Die Dokumentenprüfung im Rahmen von Audits SOLLTE anhand der im Prüfplan festgelegten Anforderungen erfolgen. Alle relevanten Dokumente SOLLTEN daraufhin geprüft werden, ob sie aktuell, vollständig und nachvollziehbar sind. Die Ergebnisse der Dokumentenprüfung SOLLTEN dokumentiert werden. Diese SOLLTEN in die Vor-Ort-Prüfung einfließen, soweit das sinnvoll ist.

DER.3.1.A14 Auswahl von Stichproben [Auditteam]

Das Auditteam SOLLTE die Stichproben für die Vor-Ort-Prüfung risikoorientiert auswählen und nachvollziehbar begründen sowie dokumentieren. Wird das Audit auf der Basis von Baustein-Zielobjekten und Maßnahmen durchgeführt, SOLLTEN diese anhand eines vorher definierten Verfahrens ausgewählt werden. Bei der Auswahl von Stichproben SOLLTEN auch die Ergebnisse vorangegangener Audits berücksichtigt werden.

DER.3.1.A15 Auswahl von geeigneten Prüfmethoden [Auditteam]

Das Auditteam SOLLTE für die jeweils zu prüfenden Sachverhalte geeignete Methoden benutzen, z. B. Interviews (siehe DER.3.1.A8 *Durchführung von Interviews*) oder Dokumentenprüfungen. Außerdem SOLLTE darauf geachtet werden, dass alle Prüfungen verhältnismäßig sind.

DER.3.1.A16 Ablaufplan der Vor-Ort-Prüfung [Auditteam]

Gemeinsam mit den Ansprechpartnern SOLLTE das Auditteam den Ablaufplan für die Vor-Ort-Prüfung erarbeiten. Die Ergebnisse SOLLTEN im Auditplan dokumentiert werden.

DER.3.1.A17 Durchführung der Vor-Ort-Prüfung [Auditteam]

Zu Beginn der Vor-Ort-Prüfung SOLLTE das Auditteam ein Eröffnungsgespräch mit den Verantwortlichen der betroffenen Institution führen. Danach SOLLTEN alle im Prüfplan festgelegten Anforderungen mit den vorgesehenen Prüfmethoden überprüft werden. Weicht eine ausgewählte Stichprobe vom dokumentierten Status ab, SOLLTE die Stichprobe bedarfsorientiert erweitert werden bis der Sachverhalt geklärt ist. Nach der Prüfung SOLLTE das Auditteam ein Abschlussgespräch führen, in dem kurz die Ergebnisse ohne Bewertung sowie die weitere Vorgehensweise dargestellt werden. Das Gespräch SOLLTE protokolliert werden.

DER.3.1.A18 Durchführung von Interviews [Auditteam]

Interviews SOLLTEN strukturiert erfolgen. Fragen SOLLTEN knapp, präzise und leicht verständlich formuliert werden. Zudem SOLLTEN geeignete Fragetechniken eingesetzt werden.

DER.3.1.A19 Überprüfung des Risikobehandlungsplans [Auditteam]

Das Auditorteam SOLLTE prüfen, ob die verbleibenden Restrisiken für den Informationsverbund angemessen und tragbar sind. Er SOLLTE außerdem prüfen, ob sie verbindlich durch die Geschäftsführung getragen werden. Maßnahmen, die grundlegend zur Informationssicherheit der gesamten Institution beitragen, DÜRFEN NICHT in die Risikoübernahme einfließen.

Der Auditor SOLLTE stichprobenartig verifizieren, ob bzw. wie weit die im Risikobehandlungsplan festgelegten Maßnahmen umgesetzt sind.

DER.3.1.A20 Abschlussbesprechung [Auditteam]

Das Auditteam SOLLTE mit den jeweiligen Verantwortlichen der auditierten Institution eine Abschlussbesprechung durchführen. Darin SOLLTEN die vorläufigen Auditergebnisse dargelegt und die weiteren Tätigkeiten vorgestellt werden.

DER.3.1.A21 Auswertung der Prüfungen [Auditteam]

Nach der Vor-Ort-Prüfung SOLLTEN die erhobenen Informationen weiter konsolidiert und ausgewertet werden. Nachdem die eventuell nachgeforderten Dokumentationen und zusätzlichen Informationen ausgewertet wurden, SOLLTEN die geprüften Maßnahmen endgültig bewertet werden. Um die nachgeforderten Dokumentationen bereitzustellen, SOLLTE ein ausreichendes Zeitfenster gewährt werden. Dokumente, die bis zum vereinbarten Enddatum nicht eingegangen sind, SOLLTEN als nicht existent gewertet werden.

DER.3.1.A22 Erstellung eines Auditberichts [Auditteam]

Das Auditteam SOLLTE die gewonnenen Ergebnisse in einen Auditbericht überführen und dort nachvollziehbar dokumentieren. Die Ergebnisse des Audits SOLLTEN den Verantwortlichen in einer Präsentation erläutert werden.

Die geprüfte Institution SOLLTE sicherstellen, dass alle betroffenen Stellen innerhalb einer angemessenen Frist die für sie wichtigen und notwendigen Passagen des Auditberichts erhalten.

DER.3.1.A23 Dokumentation der Revisionsergebnisse

Die Ergebnisse einer Revision SOLLTEN einheitlich dokumentiert werden.

DER.3.1.A24 Abschluss des Audits oder der Revision [Auditteam]

Nach dem Audit bzw. der Revision SOLLTEN alle relevanten Dokumente, Datenträger und IT-Systeme zurückgegeben oder vernichtet werden. Das SOLLTE mit der geprüften Institution abgestimmt werden. Aufbewahrungspflichten aus gesetzlichen oder anderen verbindlichen Anforderungen SOLLTEN hierbei entsprechend berücksichtigt werden. Weiter SOLLTE der ISB alle für das Audit- oder Revisionsteam genehmigten Zugriffe wieder deaktivieren oder löschen lassen.

Mit den Auditoren bzw. Revisoren SOLLTE vereinbart werden, wie mit den Ergebnissen umzugehen ist. Hierbei SOLLTE auch festgelegt werden, dass die Auditergebnisse nicht ohne Genehmigung der geprüften Institution an andere Institutionen weitergeleitet werden dürfen.

DER.3.1.A25 Nachbereitung und Einleitung des Follow-up

Die im Auditbericht oder bei einer Revision festgestellten Abweichungen oder Mängel SOLLTEN in einer angemessenen Zeit abgestellt werden. Damit sich der Umsetzungsstatus leicht nachvollziehen lässt, SOLLTEN die durchzuführenden Korrekturmaßnahmen inklusive Zeitpunkt und Zuständigkeiten dokumentiert werden. Auch abgeschlossene Korrekturmaßnahmen SOLLTEN dokumentiert werden. Dafür SOLLTE im ISMS bereits ein etabliertes Verfahren existieren, das zu benutzen ist.

Gab es schwerwiegende Abweichungen oder Mängel, SOLLTE das Audit- bzw. Revisionsteam überprüfen, ob die Korrekturmaßnahmen durchgeführt wurden.

DER.3.1.A26 Überwachen und Anpassen des Auditprogramms

Das Auditprogramm SOLLTE kontinuierlich überwacht und angepasst werden, sodass Termine, Auditziele, Auditinhalte und die Auditqualität eingehalten werden.

Mithilfe der bestehenden Anforderungen an das Auditprogramm und mit den Ergebnissen der durchgeführten Audits SOLLTE überprüft werden, ob das Auditprogramm angemessen ist. Eventuell sollte es angepasst werden.

DER.3.1.A27 Aufbewahrung und Archivierung von Unterlagen zu Audits und Revisionen

Auditprogramme sowie Unterlagen zu Audits und Revisionen SOLLTEN entsprechend den gesetzlichen oder weiteren regulatorischen Anforderungen nachvollziehbar und revisionssicher abgelegt und aufbewahrt werden. Dabei SOLLTE sichergestellt werden, dass lediglich berechtigte Personen auf Auditprogramme und Unterlagen (insbesondere Auditberichte) zugreifen können. Nach Ablauf der Archivierungsfristen SOLLTEN die Auditprogramme und Unterlagen sicher vernichtet werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

DER.3.1.A28 Sicherheitsüberprüfung der Auditoren (CI)

Sofern Auditoren auf besonders schützenswerte Informationen zugreifen müssen, SOLLTEN Nachweise über ihre Integrität und Reputation eingefordert werden. Handelt es sich dabei um nach Geheimschutz klassifizierte Verschlusssachen, SOLLTEN sich die Mitglieder des Auditteams einer Sicherheitsüberprüfung nach Sicherheitsüberprüfungsgesetz (SÜG) unterziehen. Diesbezüglich SOLLTE der ISB den Geheimschutzbeauftragten bzw. Sicherheitsbevollmächtigten der Institution einbeziehen.

4 Weiterführende Informationen

4.1 Literatur

- [19011] DIN EN ISO 19011 Guidelines for auditing management systems
  http://www.bsi.bund.de/cyberglossar

- [27007] ISO/IEC 27007:2011
  Information technology - Security techniques - Guidelines for information security management systems auditing, 11.2011
  http://www.iso.org/iso/catalogue_detail?csnumber=42506

- [ISF] The Standard of Good Practice
  Information Security Forum (ISF), 06.2016

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Audits und Revisionen" von Bedeutung.

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.18	G 0.19	G 0.27	G 0.29	G 0.46
DER.3.1.A1	x		x		x
DER.3.1.A2	x			x	
DER.3.1.A3	x				
DER.3.1.A4	x				
DER.3.1.A5	x	x			x
DER.3.1.A6	x				
DER.3.1.A7	x			x	x
DER.3.1.A8	x			x	x
DER.3.1.A9	x		x		x
DER.3.1.A10	x				
DER.3.1.A11	x	x			
DER.3.1.A12	x	x			
DER.3.1.A13	x				
DER.3.1.A14	x			x	
DER.3.1.A15	x				
DER.3.1.A16	x				
DER.3.1.A17	x	x			
DER.3.1.A18	x	x			
DER.3.1.A19	x			x	
DER.3.1.A20	x				
DER.3.1.A21	x				
DER.3.1.A22	x			x	x
DER.3.1.A23	x			x	x
DER.3.1.A24	x	x		x	x
DER.3.1.A25	x			x	
DER.3.1.A26	x		x	x	x
DER.3.1.A27	x				x
DER.3.1.A28	x		x	x	x

DER.3: Sicherheitsprüfungen

DER.3.2 IS-Revision für Bundesbehörden

1 Beschreibung

1.1 Einleitung

Im "Umsetzungsplan für die Gewährleistung der IT-Sicherheit in der Bundesverwaltung" (UP Bund) wird festgelegt, dass Bundesbehörden den IT-Grundschutz vollständig umsetzen müssen. Auch sind sie verpflichtet, mindestens alle 3 Jahre eine umfassende Informationssicherheitsrevision (IS-Revision) durchzuführen. Allerdings sind Behörden davon befreit, wenn sie ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz besitzen.

IS-Revisionen sind grundlegend für jedes erfolgreiche Informationssicherheitsmanagement. Nur wenn etablierte Sicherheitsmaßnahmen und -prozesse regelmäßig überprüft werden, ob sie wirksam, vollständig, angemessen und noch aktuell sind, lässt sich der Gesamtzustand der Informationssicherheit beurteilen. IS-Revisionen sind somit ein Werkzeug, um ein angemessenes Sicherheitsniveau festzustellen, zu erreichen und aufrechtzuerhalten. Durch sie ist es möglich, Fehlentwicklungen und bestehende Sicherheitsmängel zu erkennen und entsprechende Gegenmaßnahmen einzuleiten.

1.2 Zielsetzung

Der Baustein definiert Anforderungen an die IS-Revision für Bundesbehörden mit dem Ziel, die Informationssicherheit in einer Behörde zu verbessern, Fehlentwicklungen auf diesem Gebiet zu vermeiden und die Sicherheitsmaßnahmen und -prozesse zu optimieren.

1.3 Abgrenzung

Der Baustein beschreibt, wie sich IS-Revisionen in Bundesbehörden anhand des "*Leitfadens für Informationssicherheitsrevision*" planen, durchführen und nachbereiten lassen. Der Baustein stellt jedoch nur die Pflichten im Rahmen der IS-Revision zusammen. Das für die IS-Revision verbindliche Regelwerk ist der "*Leitfaden für die Informationssicherheitsrevision*" in der jeweils aktuellen Version

Audits und Revisionen im Rahmen des Informationssicherheits-Managementsystems (ISMS) werden im Baustein DER.3.1 *Audit und Revision* betrachtet und sind somit nicht Bestandteil dieses Bausteins. Auch wird nicht berücksichtigt, wie sich die IS-Revision in eine bereits bestehende, übergeordnete Prüforganisation einer Behörde (zum Beispiel interne Revision) integrieren lässt.

Der Baustein richtet sich insbesondere an Bundesbehörden. Grundsätzlich können die Inhalte jedoch auch für weitere Behörden (z. B. Landesbehörden), Unternehmen oder andere Organisationen relevant sein. Sofern diese nicht durch gesetzliche, vertragliche oder anderweitige Regelungen ebenfalls zur IS-Revision verpflichtet sind, sind die Inhalte des vorliegenden Bausteins als Empfeh-

lungen anzusehen. Beispielsweise könnte eine IS-Revision im Sinne dieses Bausteins auch für andere Institutionen als Bundesbehörden für die Vorbereitung einer ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz sinnvoll sein.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich *IS-Revision für Bundesbehörden* von besonderer Bedeutung:

2.1 Verstoß gegen die Vorgaben des UP Bund

Der UP Bund sieht unter anderem vor, dass sich alle Bundesbehörden, die noch keine vollumfängliche ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz haben, einer regelmäßigen IS-Revision unterziehen. Führen Bundesbehörden nicht regelmäßig IS-Revisionen durch, verstoßen sie gegen diese Vorgaben.

2.2 Außer Kraft setzen von Sicherheitsmaßnahmen

Das Sicherheitsniveau einer Behörde hängt davon ab, dass Sicherheitsmaßnahmen vollständig und korrekt umgesetzt werden. Insbesondere in der kritischen Phase von Projekten oder unter bestimmten Rahmenbedingungen kann es vorkommen, dass Sicherheitsmaßnahmen temporär ausgesetzt werden. Teilweise wird jedoch vergessen, sie wieder zu reaktivieren, sodass ein zu niedriges Sicherheitsniveau entsteht.

2.3 Wirkungslose oder nicht wirtschaftliche Umsetzung von Sicherheitsmaßnahmen

Werden Sicherheitsmaßnahmen umgesetzt, ohne dabei bestimmte Praxisaspekte zu berücksichtigen, sind die Maßnahmen eventuell wirkungslos. Beispielsweise ist es sinnlos, den Eingangsbereich mit Drehkreuzen abzusperren, wenn die Mitarbeiter das Gebäude einfach durch einen offenen Seiteneingang betreten können.

Ebenso können Einzelmaßnahmen ergriffen werden, die wirtschaftlich nicht sinnvoll sind. So ist für den Schutz von Informationen mit einer normalen Vertraulichkeit ein sauber implementiertes Rechte- und Rollenkonzept sinnvoller und wirtschaftlicher als eine Certificate Authority und die anschließende zertifikatsbasierte Verschlüsselung des Fileservers aufzubauen.

2.4 Unzureichende Umsetzung des Informationssicherheitsmanagementsystems

In vielen Behörden überprüft der Informationssicherheitsbeauftragte selbst, ob Sicherheitsmaßnahmen umgesetzt wurden. Oft wird darüber die Prüfung des eigentlichen ISMS vergessen. Insbesondere da dies durch einen unabhängigen Dritten erfolgen sollte. Hierdurch besteht die Gefahr, dass die Prozesse eines ISMS ineffizient sind oder nicht angemessen umgesetzt wurden. In der Folge ist das Sicherheitsniveau der Institution beeinträchtigt.

2.5 Unzureichende Qualifikation des Prüfers

Ist ein IS-Revisor nicht ausreichend qualifiziert oder bereitet er sich ungenügend auf die Prüfungen vor, schätzt er während der IS-Revision eventuell den Sicherheitszustand einer Behörde falsch ein. Dadurch veranlasst er in seinem Prüfbericht nicht die nötigen oder sogar die falschen Korrekturmaßnahmen. Im schlimmsten Fall hat das eine zu hohe und damit nicht wirtschaftliche bzw. zu niedrige und damit sehr risikobehaftete Absicherung von Informationen zur Folge.

2.6 Fehlende langfristige Planung

Werden IS-Revisionen nicht langfristig und zentral geplant, kann es passieren, dass einzelne Bereiche einer Behörde sehr häufig und andere überhaupt nicht geprüft werden. Dadurch ist es nur sehr schwer oder gar nicht möglich, den Sicherheitszustand des Informationsverbunds einzuschätzen.

2.7 Fehlende Planung und Abstimmung bei der Durchführung von IS-Revisionen

Wenn eine IS-Revision mangelhaft geplant und nicht mit allen betroffenen Mitarbeitern der Behörde abgestimmt wurde, sind während der Vor-Ort-Prüfung eventuell nicht die benötigten oder die falschen Ansprechpartner verfügbar. Dadurch lassen sich dann möglicherweise einzelne Bereiche überhaupt nicht prüfen. Auch wenn der IS-Revisor die Termine für die einzelnen Bereiche zu eng gesetzt hat, besteht die Gefahr, dass die geplante Untersuchung nur oberflächlich durchgeführt wird, da zu wenig Zeit verfügbar ist.

2.8 Fehlende Abstimmung mit der Personalvertretung

In IS-Revisionen können auch Aspekte geprüft werden, aus denen sich Rückschlüsse auf die Leistung von Mitarbeitern ziehen lassen. Somit könnten diese Prüfungen als Leistungsbeurteilung gewertet werden. Wird die Personalvertretung nicht beteiligt, kann dies zu Verstößen gegen das geltende Mitbestimmungsrecht führen.

2.9 Absichtliches Verschweigen von Abweichungen oder Problemen

Mitarbeiter könnten befürchten, dass bei einer IS-Revison Fehler aufgedeckt werden, und darum versuchen, Sicherheitsprobleme zu kaschieren und ein falsches Bild über den tatsächlichen Status Quo zu vermitteln.

2.10 Vertraulichkeitsverlust von schützenswerten Informationen

Während einer IS-Revision werden diverse vertrauliche Informationen durch die Revisoren erhoben. Auch werden Defizite in der Informationssicherheit der geprüften Behörde benannt. Werden diese Mängel jedoch unberechtigten Dritten bekannt, könnten sie dazu benutzt werden, die Behörde anzugreifen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich IS-Revision für Bundesbehörden aufgeführt. Grundsätzlich ist der Verantwortliche für die IS-Revision für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Verantwortlicher für die IS-Revision
Weitere Verantwortliche	IS-Revisionsteam, Informationssicherheitsbeauftragter (ISB)

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

DER.3.2.A1 Definition von Verantwortlichkeiten für die IS-Revision

Die Institution MUSS einen Verantwortlichen benennen, der IS-Revisionen plant, initiiert und die Ergebnisse nachverfolgt.

DER.3.2.A2 Erstellung eines IS-Revisionshandbuches

Es MUSS ein IS-Revisionshandbuch erstellt werden. Das Handbuch MUSS von der Leitungsebene verabschiedet werden.

DER.3.2.A3 Definition der Prüfungsgrundlage und eines einheitlichen Bewertungsschemas [IS-Revisionsteam]

Die Prüfungsgrundlagen für die IS-Revision MÜSSEN der UP Bund, der Leitfaden für die Informationssicherheitsrevision, die BSI-Standards zur Informationssicherheit sowie das IT-Grundschutz-Kompendium sein. Dies MUSS zudem allen Beteiligten bekannt sein. Für die Bewertung der Maßnahmenumsetzung MUSS das Bewertungsschema aus *Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz* - benutzt werden (siehe 4. *Weiterführende Informationen*).

DER.3.2.A4 Erstellung einer Planung für die IS-Revision

Bundesbehörden, die noch keine ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz haben, MÜSSEN mindestens alle 3 Jahre eine umfassende IS-Revision durchführen lassen. Darüber hinaus SOLLTEN weitere Revisionen für kritische Geschäftsprozesse eingeplant werden. Der Verantwortliche für die IS-Revision SOLLTE daher eine mehrjährige Grobplanung (sinnvollerweise über mindestens 3 Jahre) für das Revisionsvorhaben anhand des Leitfadens für die Informationssicherheitsrevision erstellen. Diese SOLLTE dann durch eine jährliche Detailplanung konkretisiert werden.

DER.3.2.A5 Auswahl eines geeigneten IS-Revisionsteams

Für IS-Revisionen MUSS ein geeignetes Team zusammengestellt oder beauftragt werden. Dem IS-Revisionsteam MUSS ein uneingeschränktes Informations- und Einsichtnahmerecht für seine Tätigkeit eingeräumt werden.

DER.3.2.A6 Vorbereitung einer IS-Revision [IS-Revisionsteam]

Die Behördenleitung MUSS das IS-Revisionsverfahren durch Auftragserteilung an das IS-Revisionsteam initiieren.

Für die Dokumentenprüfung MUSS die zu prüfende Behörde die erforderlichen Referenzdokumente entsprechend dem Leitfaden für die Informationssicherheitsrevision an das IS-Revisionsteam übergeben.

DER.3.2.A7 Durchführung einer IS-Revision [IS-Revisionsteam]

Bei einer IS-Kurzrevision MUSS die verbindliche Prüfthemenliste aus *Verbindliche Prüfthemen für die IS-Kurzrevision* (siehe 4. *Weiterführende Informationen*) verwendet werden. Alle erstellten Grundlagen müssen während der IS-Revision fortgeschrieben und bei Bedarf angepasst werden.

Es MUSS im Rahmen einer IS-Revision sowohl eine Dokumentenprüfung als auch eine Inspektion vor Ort durchgeführt werden. Sämtliche Ergebnisse der beiden Phasen MÜSSEN schriftlich dokumentiert und in einem IS-Revisionsbericht zusammengefasst werden.

DER.3.2.A8 Aufbewahrung von IS-Revisionsberichten

Der IS-Revisionsbericht und die diesem zugrunde liegenden Referenzdokumente MÜSSEN von der geprüften Behörde mindestens für 10 Jahre ab Zustellung des Berichts revisionssicher aufbewahrt werden, sofern keine anders lautenden Gesetze oder Verordnungen gelten. Hierbei MUSS sichergestellt werden, dass lediglich berechtige Personen auf die IS-Revisionsberichte und die Referenzdokumente zugreifen können.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich IS-Revision für Bundesbehörden. Sie SOLLTEN grundsätzlich umgesetzt werden.

DER.3.2.A9 Integration in den Informationssicherheitsprozess [Informationssicherheitsbeauftragter (ISB)]

Es SOLLTE sichergestellt werden, dass IS-Revisionen ein Teil des Sicherheitsprozesses sind und durch diesen initiiert werden. Außerdem SOLLTEN die Ergebnisse von IS-Revisionen in das ISMS zurückfließen und zu dessen Verbesserung beitragen.

Weiter SOLLTEN die IS-Revisionen, die Ergebnisse sowie die Aktivitäten zur Mängelbeseitigung und Qualitätsverbesserung in den regelmäßigen Bericht des ISB an die Behördenleitung aufgenommen werden.

DER.3.2.A10 Kommunikationsabsprache

Es SOLLTEN klare Regelungen getroffen werden, wie zwischen dem IS-Revisionsteam und der zu prüfenden Bundesbehörde Informationen auszutauschen sind. So SOLLTE durch geeignete Maßnahmen sichergestellt werden, dass die bei einer IS-Revision ausgetauschten Informationen auch vertraulich und integer bleiben.

DER.3.2.A11 Durchführung eines Auftaktgeprächs für eine Querschnittsrevision [IS-Revisionsteam]

Für eine Querschnittsrevision SOLLTE zwischen dem IS-Revisionsteam und den Ansprechpartnern ein Auftaktgespräch durchgeführt werden. Darin SOLLTEN folgenden Inhalte besprochen werden:

- Erläuterung und Darstellung des IS-Revisionsverfahrens,
- Vorstellung der Institution: Erläuterung der Aufgabenschwerpunkte und Überblick über die eingesetzte IT,
- Übergabe der Referenzdokumente an das IS-Revisionsteam.

DER.3.2.A12 Erstellung eines Prüfplans [IS-Revisionsteam]

Vor einer IS-Revision SOLLTE das IS-Revisionsteam einen IS-Prüfplan erstellen, der den gesamten zeitlichen und organisatorischen Ablauf der Prüfung sowie alle zugehörigen Tätigkeiten und Regelungen koordiniert und beschreibt. Ist es während der IS-Revision notwendig, die geplanten Abläufe zu erweitern oder anderweitig anzupassen, SOLLTE der IS-Prüfplan entsprechend angepasst werden. Der Prüfplan SOLLTE zudem Teil des abschließenden IS-Revisionsberichts sein.

Bei der IS-Kurzrevision SOLLTE die verbindlich festgelegte Prüfthemenliste aus *Verbindliche Prüfthemen für die IS-Kurzrevision* (siehe 4. *Weiterführende Informationen*) an die Stelle des Prüfplans treten.

DER.3.2.A13 Sichtung und Prüfung der Dokumente [IS-Revisionsteam]

Die Dokumentenprüfung SOLLTE auf Basis der im Prüfplan festgelegten Maßnahmen erfolgen. Das IS-Revisionsteam SOLLTE überprüfen, ob alle relevanten Dokumente aktuell und vollständig sind. Bei der Prüfung der Aktualität SOLLTE die Granularität der Dokumente berücksichtigt werden. Bei der Prüfung der Vollständigkeit SOLLTE darauf geachtet werden, dass alle wesentlichen Aspekte erfasst wurden bzw. dass die geeigneten Rollen zugewiesen wurden.

Weiter SOLLTE geprüft werden, ob die vorliegenden Dokumente und die darin getroffenen Entscheidungen nachvollziehbar sind. Die Ergebnisse der Dokumentenprüfung SOLLTEN dokumentiert werden und soweit sinnvoll in die Vor-Ort-Prüfung einfließen.

DER.3.2.A14 Auswahl der Zielobjekte und Maßnahmen [IS-Revisionsteam]

In einer IS-Querschnittsrevision oder IS-Partialrevision SOLLTE das IS-Revisionsteam anhand der Ergebnisse der Dokumentenprüfung die Baustein-Zielobjekte für die Vor-Ort-Prüfung auswählen. Der Baustein zum Informationssicherheitsmanagement (siehe ISMS.1 *Sicherheitsmanagement*) einschließlich aller zugehörigen Anforderungen SOLLTE jedoch immer vollständig geprüft werden. Weitere Bau-

steinzielobjekte SOLLTEN risikoorientiert nach dem im *Leitfaden für die Informationssicherheitsrevision* definierten Verfahren ausgewählt werden. Die Auswahl SOLLTE nachvollziehbar schriftlich dokumentiert werden.

Darüber hinaus SOLLTEN bei der Auswahl die bemängelten Anforderungen aus vorhergehenden IS-Revisionen berücksichtigt werden. Alle Maßnahmen mit schwerwiegenden Sicherheitsmängeln aus vorhergehenden IS-Revisionen SOLLTEN berücksichtigt werden.

DER.3.2.A15 Auswahl von geeigneten Prüfmethoden [IS-Revisionsteam]

Es SOLLTE sichergestellt werden, dass geeignete Methoden eingesetzt werden, um die jeweiligen Sachverhalte zu ermitteln. Außerdem SOLLTEN grundsätzlich alle Prüfungen verhältnismäßig sein.

DER.3.2.A16 Ablaufplan der Vor-Ort-Prüfung [IS-Revisionsteam]

Gemeinsam mit dem Ansprechpartner der zu prüfenden Behörde SOLLTE das IS-Revisionsteam einen Ablaufplan für die Vor-Ort-Prüfung erarbeiten. Die Ergebnisse SOLLTEN im IS-Prüfplan dokumentiert werden.

DER.3.2.A17 Durchführung der Vor-Ort-Prüfung [IS-Revisionsteam]

Die Vor-Ort-Prüfung SOLLTE sicherstellen, dass durch die gewählten Maßnahmen die Informationssicherheit in angemessener und praxistauglicher Form gewährleistet wird. Die Prüfung SOLLTE mit einem Eröffnungsgespräch beginnen.

Danach SOLLTEN alle Maßnahmen des Prüfplans bzw. alle Themenfelder der Prüfthemenliste getestet werden. Dafür SOLLTEN, sofern sinnvoll, die vorgesehenen Prüfmethoden benutzt werden. Stellt das IS-Revisionsteam bei einer ausgewählten Stichprobe Abweichungen zum dokumentierten Status fest, SOLLTE die Stichprobe bedarfsorientiert erweitert werden, bis der Sachverhalt geklärt ist.

Während der Vor-Ort-Prüfung SOLLTEN die IS-Revisoren niemals selbst aktiv in Systeme eingreifen und auch keine Handlungsanweisungen zu Änderungen am Revisionsgegenstand erteilen.

Alle wesentlichen Sachverhalte und Angaben über Quellen-, Auskunfts- und Vorlage-Ersuche sowie durchgeführte Besprechungen SOLLTEN schriftlich festgehalten werden.

Das IS-Revisionsteam SOLLTE den Ansprechpartnern der geprüften Behörde die getroffenen Feststellungen in einem Abschlussgespräch kurz darstellen. Dabei SOLLTE keine konkrete Bewertung erfolgen, aber ein Hinweis auf etwaige Mängel und den weiteren Verfahrensgang. Auch dieses Abschlussgespräch ist zu protokollieren.

DER.3.2.A18 Durchführung von Interviews [IS-Revisionsteam]

Interviews SOLLTEN strukturiert erfolgen. Fragen SOLLTEN knapp, präzise und leicht verständlich formuliert werden. Zudem SOLLTEN geeignete Fragetechniken eingesetzt werden.

DER.3.2.A19 Überprüfung des Risikobehandlungsplans [IS-Revisionsteam]

Das IS-Revisionsteam SOLLTE prüfen, ob die verbleibenden Restrisiken für den Informationsverbund angemessen und tragbar sind und verbindlich durch die Behördenleitung getragen werden. Maßnahmen, die grundlegend zur Informationssicherheit der gesamten Bundesbehörde beitragen, DÜRFEN NICHT in die Risikoübernahme einfließen.

Das IS-Revisionsteam SOLLTE stichprobenartig verifizieren, ob bzw. wie weit die im Risikobehandlungsplan festgelegten Maßnahmen umgesetzt sind.

DER.3.2.A20 Nachbereitung der Vor-Ort-Prüfung [IS-Revisionsteam]

Nach der Vor-Ort-Prüfung SOLLTEN die erhobenen Informationen weiter konsolidiert und ausgewertet werden. Nachdem die eventuell nachgeforderten Dokumentationen und zusätzlichen Informationen ausgewertet wurden, SOLLTEN die geprüften Maßnahmen endgültig bewertet werden.

Um die nachgeforderten Dokumentationen bereitzustellen, SOLLTE ein ausreichendes Zeitfenster gewährt werden. Dokumente, die bis zum vereinbarten Enddatum nicht eingegangen sind, SOLLTEN als nicht existent gewertet werden.

DER.3.2.A21 Erstellung eines IS-Revisionsberichts [IS-Revisionsteam]

Das IS-Revisionsteam SOLLTE die gewonnenen Ergebnisse in einen IS-Revisionsbericht überführen und dort nachvollziehbar dokumentieren.

Eine Entwurfsversion des Berichts SOLLTE der geprüften Bundesbehörde vorab übermittelt werden, um zu verifizieren, ob die durch das Prüfteam festgestellten Sachverhalte richtig aufgenommen wurden. Es SOLLTE überlegt werden, dass das IS-Revisionsteam den Verantwortlichen die Ergebnisse der IS-Revision in einer Präsentation erläutert.

Die geprüfte Bundesbehörde SOLLTE sicherstellen, dass alle betroffenen Stellen in der Bundesbehörde innerhalb einer angemessenen Frist die für sie wichtigen und notwendigen Passagen des IS-Revisionsberichts erhalten. Insbesondere SOLLTEN die Inhalte an die Behördenleitung, an den Verantwortlichen für die IS-Revision sowie den ISB kommuniziert werden.

IS-Revisionsberichte SOLLTEN mindestens als Verschlusssache "Nur für den Dienstgebrauch" (VS-NfD) eingestuft werden.

DER.3.2.A22 Nachbereitung und Einleitung des Follow-up [Informationssicherheitsbeauftragter (ISB)]

Die im IS-Revisionsbericht festgestellten Abweichungen SOLLTEN in einer angemessenen Zeit abgestellt werden. Die durchzuführenden Korrekturmaßnahmen SOLLTEN mit Zuständigkeiten, Umsetzungstermin und dem jeweiligen Status dokumentiert sein. Die Umsetzung SOLLTE kontinuierlich nachverfolgt und der Umsetzungsstatus fortgeschrieben werden.

Grundsätzlich SOLLTE geprüft werden, ob ergänzende IS-Revisionen notwendig sind. Der Verantwortliche für die IS-Revision SOLLTE die Grob- und Detailplanung zur IS-Revision anpassen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

DER.3.2.A23 Sicherheitsüberprüfung der IS-Revisoren (CI)

Sofern die IS-Revisoren auf besonders schützenswerte Informationen zugreifen, SOLLTEN Nachweise über ihre Integrität und Reputation eingefordert werden, zum Beispiel ein polizeiliches Führungszeugnis oder Referenzen.

Handelt es sich dabei um nach Geheimschutz klassifizierte Verschlusssachen, SOLLTEN sich die IS-Revisoren einer Sicherheitsüberprüfung nach Sicherheitsüberprüfungsgesetz (SÜG) unterziehen. Diesbezüglich SOLLTE der ISB den Geheimschutzbeauftragten bzw. Sicherheitsbevollmächtigten seiner Behörde einbeziehen.

4 Weiterführende Informationen

4.1 Literatur

- [ISKR] Verbindliche Prüfthemen für die IS-Kurzrevision
  BSI, Version 1.1, 11.2010
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Pruefthemen_IS-Kurzrevision_pdf.pdf

- [ISR] Informationssicherheitsrevision
  Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz, BSI, Version 2.0, 03.2010
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Leitfaden_IS-Revision-v1_pdf.pdf

- [RH] Revisionshandbuch zur Informationssicherheit nach UP Bund (Muster)
  BSI, Version 1.0, 09.2008
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Muster_ISRevisionshandbuch-v1_pdf.pdf

- [VSA] Allgemeine Verwaltungsvorschrift des Bundesministerium des Inneren zum materiellen und organisatorischen Schutz von Verschlußsachen
  (VS-Anweisung - VSA), 31.03.2006

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "IS-Revision für Bundesbehörden" von Bedeutung.

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.18	G 0.19	G 0.27	G 0.29	G 0.46
DER.3.2.A1	x		x		x
DER.3.2.A2	x			x	
DER.3.2.A3	x				
DER.3.2.A4	x			x	x
DER.3.2.A5	x		x		x
DER.3.2.A6	x			x	
DER.3.2.A7	x				
DER.3.2.A8	x				x
DER.3.2.A9	x	x			x
DER.3.2.A10	x	x			
DER.3.2.A11	x	x			
DER.3.2.A12	x				
DER.3.2.A13	x				
DER.3.2.A14	x			x	
DER.3.2.A15	x				
DER.3.2.A16	x				
DER.3.2.A17	x	x			
DER.3.2.A18	x	x			
DER.3.2.A19	x			x	
DER.3.2.A20	x				
DER.3.2.A21	x			x	x
DER.3.2.A22	x			x	
DER.3.2.A23	x		x	x	x

DER: Detektion und Reaktion

DER.4 Notfallmanagement

1 Beschreibung

1.1 Einleitung

In Notfallsituationen ist ein Zugriff auf Informationen zur Wiederherstellung eines Geschäftsprozesses, eines IT-Systems oder einer Fachaufgabe unentbehrlich. Hierzu sollten die entsprechenden Prozesse zur Aufrechterhaltung der Informationssicherheit in einem Notfall geplant, etabliert und überprüft werden.

Nur wenn geplant und organisiert vorgegangen wird, ist eine optimale Notfallvorsorge und Notfallbewältigung möglich. Ein professioneller Prozess zum Notfallmanagement reduziert deren Auswirkungen und sichert somit den Betrieb und Fortbestand der Institution. Es sind geeignete Maßnahmen zu identifizieren und umzusetzen, durch die Geschäftsprozesse und Fachaufgaben zum einen robuster und ausfallsicherer werden und die es zum anderen ermöglichen, den Notfall schnell und zielgerichtet zu bewältigen.

Die Aufrechterhaltung der Informationssicherheit ist deshalb in ein übergreifendes Notfallmanagement einzubinden. Das Notfallmanagement hat jedoch einen eigenen Prozessverantwortlichen (den Notfallbeauftragten), mit dem sich der Informationssicherheitsbeauftragte abstimmt.

1.2 Zielsetzung

Ziel des Bausteins Notfallmanagement ist es, Anforderungen zu beschreiben, durch die die Informationssicherheit selbst in kritischen Situationen gewährleistet wird. Dazu sind die entsprechenden Maßnahmen in ein ganzheitliches Kontinuitätsmanagement einzubetten und alle Aspekte zu betrachten, die erforderlich sind, um die Informationssicherheit auch bei Eintritt eines Schadensereignisses aufrechterhalten zu können. Dies reicht von der Planung bis zur Überprüfung aller Prozesse.

1.3 Abgrenzung

Bei Eintritt eines Schadensereignisses müssen die richtigen Informationen vollständig und korrekt zur Verfügung stehen. Im vorliegenden Baustein werden weder Kriterien noch Prozesse erläutert, anhand derer die Verantwortlichen entscheiden können, ob ein Notfall vorliegt oder nicht. Die Entscheidung darüber wird getroffen, während der Sicherheitsvorfall behandelt wird (siehe DER.2.1 *Behandlung von Sicherheitsvorfällen*).

Krisen werden im Rahmen eines eigenen Krisenmanagements betrachtet und in diesem Baustein nur als Schnittstelle, z. B. im Rahmen der weiteren Eskalation von Notfällen behandelt. Weiterführende Informationen zu den einzelnen Phasen des Notfallmanagements sowie der Abgrenzung des Notfallmanagements zum Krisenmanagement sind im BSI-Standard 100-4 enthalten.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Notfallmanagement von besonderer Bedeutung:

2.1 Personalausfall

Wenn Mitarbeiter ausfallen, z. B. durch Keime in der Kantine, Pandemie, Tod oder Streik, könnte die eigene Institution ihre Fachaufgaben und Geschäftsprozesse nicht mehr ausführen und zudem könnten relevante Informationen zum Wiederanlauf des Geschäftsprozesses oder der IT-Systeme nicht mehr zugänglich sein. Vielfach besitzen einzelne Personen spezifisches Fachwissen (Kopfmonopole), sodass ein Schaden auch dann eintreten kann, wenn der Personalausfall zahlenmäßig nur sehr gering ist.

2.2 Ausfall von IT-Systemen

Wenn Komponenten eines IT-Systems ausfallen, z. B. durch defekte Hardware oder Stromausfall, kann der gesamte IT-Betrieb gestört werden. Dadurch ist die Verfügbarkeit der jeweiligen Informationen und damit auch des jeweiligen Geschäftsprozesses gefährdet. Zudem können wichtige Informationen, die für Wiederanlaufmaßnahmen benötigt werden, nicht zur Verfügung stehen.

2.3 Ausfall eines Weitverkehrsnetzes (WAN)

Die Ursachen für den Ausfall eines Weitverkehrsnetzes (Wide Area Network, WAN) können vielfältig sein. Daher ist es möglich, dass sich ein Netzausfall lediglich auf einzelne Benutzer, einen Anbieter oder eine bestimmte Region auswirkt. Häufig stören solche Ausfälle nur kurz und betreffen dann nur die Geschäftsprozesse und Fachaufgaben, die eine entsprechend hohe Verfügbarkeit des WAN benötigen. Es gibt aber auch immer wieder längere Ausfälle, die massive Probleme in der Kommunikation und Erreichbarkeit nach sich ziehen können.

2.4 Ausfall eines Gebäudes

Gebäude können unvorhergesehen unbenutzbar werden, z. B. weil sie durch Feuer, Sturm, Hochwasser, Erdbeben oder eine Explosion teilweise oder vollständig zerstört wurden. Ein Ausfall eines Gebäudes kann jedoch auch dadurch verursacht werden, dass wegen Sperrungen von Polizei oder Feuerwehr das Umfeld nicht mehr betreten werden kann oder das Gebäude verlassen werden muss, weil Strom, Wasser, Abwasser, Heizung oder Klimatisierung über einen gewissen Zeitraum nicht mehr funktionieren.

2.5 Ausfall eines Lieferanten oder Dienstleisters

Wenn Organisationseinheiten von Dienstleistern abhängig sind, kann sich der teilweise oder vollständige Ausfall eines Outsourcing-Dienstleisters oder eines Lieferanten erheblich auf die betriebliche Kontinuität auswirken, insbesondere bei kritischen Geschäftsprozessen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Notfallmanagement aufgeführt. Grundsätzlich ist der Notfallbeauftragte für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	Notfallbeauftragter
Weitere Verantwortliche	Informationssicherheitsbeauftragter (ISB), Institutionsleitung, Leiter Personal, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Notfallmanagement. Sie SOLLTEN grundsätzlich umgesetzt werden.

DER.4.A1 Erstellung eines Notfallhandbuchs [Informationssicherheitsbeauftragter (ISB)]

Es SOLLTE ein Notfallhandbuch erstellt werden, in dem die wichtigsten Informationen zu

- Rollen,
- Sofortmaßnahmen,
- Alarmierung und Eskalation,
- Kommunikations-, grundsätzliche Geschäftsfortführungs-, Wiederanlauf und
- Wiederherstellungspläne

enthalten sind. Zuständigkeiten und Befugnisse SOLLTEN zugewiesen, kommuniziert und im Notfallhandbuch festgehalten werden. Es SOLLTE sichergestellt sein, dass im Notfall entsprechend geschultes Personal zur Verfügung steht. Es SOLLTE regelmäßig durch Tests und Übungen überprüft werden, ob die im Notfallhandbuch beschriebenen Maßnahmen auch wie Vorgesehen funktionieren.

Das Notfallhandbuch SOLLTE regelmäßig geprüft und, falls erforderlich, aktualisiert werden. Es SOLLTE auch im Notfall zugänglich sein. Ergänzt werden SOLLTE das Notfallhandbuch um Verhaltensregeln für Fälle (z. B. Brand), die allen Mitarbeitern bekannt gegeben werden sollten.

DER.4.A2 Integration von Notfallmanagement in organisationsweite Abläufe und Prozesse [Institutionsleitung]

Die Prozesse im Sicherheitsmanagement SOLLTEN mit dem Notfallmanagement (siehe DER.2.1 *Behandlung von Sicherheitsvorfällen*) abgestimmt werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

DER.4.A3 Festlegung des Geltungsbereichs und der Notfallmanagementstrategie [Institutionsleitung] (CIA)

Der Geltungsbereich für das Notfallmanagement-System SOLLTE eindeutig festgelegt werden. Die Institutionsleitung SOLLTE eine Notfallmanagement-Strategie festlegen, die die angestrebten Ziele und das Risikoakzeptanzniveau darlegen.

DER.4.A4 Leitlinie zum Notfallmanagement und Übernahme der Gesamtverantwortung durch die Leitungsebene [Institutionsleitung] (CIA)

Es SOLLTE eine Leitlinie zum Notfallmanagement von der Leitungsebene verabschiedet werden. Diese SOLLTE die wesentlichen Eckpunkte des Notfallmanagements enthalten. Die Leitlinie zum Notfallmanagement SOLLTE regelmäßig überprüft und gegebenenfalls überarbeitet werden. Die Leitlinie zum Notfallmanagement SOLLTE allen Mitarbeitern bekannt gegeben werden.

DER.4.A5 Aufbau einer geeigneten Organisationsstruktur für das Notfallmanagement [Institutionsleitung] (CIA)

Es SOLLTEN die Rollen für das Notfallmanagement den Gegebenheiten der Institution angemessen festgelegt werden. Dies SOLLTE mit den Aufgaben, Pflichten und Kompetenzen der Rollen schriftlich dokumentiert werden. Es SOLLTEN für alle Rollen im Notfallmanagement qualifizierte Mitarbeiter benannt werden. Die Organisationsstruktur im Notfallmanagement SOLLTE regelmäßig darauf überprüft werden, ob sie praxistauglich, effektiv und effizient ist.

DER.4.A6 Bereitstellung angemessener Ressourcen für das Notfallmanagement [Institutionsleitung] (CIA)

Die finanziellen, technischen und personellen Ressourcen für die angestrebten Ziele des Notfallmanagements SOLLTEN angemessen sein. Der Notfallbeauftragte bzw. das Notfallmanagement-Team SOLLTE über genügend Zeit für die Aufgaben im Notfallmanagement verfügen.

DER.4.A7 Erstellung eines Notfallkonzepts [Institutionsleitung] (CIA)

Alle kritischen Geschäftsprozesse und Ressourcen SOLLTEN identifiziert werden (beispielsweise mit einer Business Impact Analyse (BIA)). Es SOLLTEN die wichtigsten, relevanten Risiken für die kritischen Geschäftsprozesse und Ressourcen identifiziert werden. Für jedes identifizierte Risiko SOLLTE entscheiden werden, welche Risikostrategien zur Risikobehandlung eingesetzt werden sollen. Es SOLLTEN Kontinuitätsstrategien entwickelt werden, die einen Wiederanlauf und eine Wiederherstellung der kritischen Geschäftsprozesse in der geforderten Zeit ermöglichen. Ein Notfallkonzept SOLLTE erstellt werden. Notfallpläne und Maßnahmen SOLLTEN entwickelt und implementiert werden, die eine effektive Notfallbewältigung und eine schnelle Wiederaufnahme der kritischen Geschäftsprozesse ermöglichen. Im Notfallkonzept SOLLTE die Informationssicherheit berücksichtigt und entsprechende Sicherheitskonzepte für die Notfalllösungen entwickelt werden.

DER.4.A8 Integration der Mitarbeiter in den Notfallmanagement-Prozess [Vorgesetzte, Leiter Personal] (CIA)

Alle Mitarbeiter SOLLTEN regelmäßig für das Thema Notfallmanagement sensibilisiert werden. Zum Notfallmanagement SOLLTE es ein Schulungs- und Sensibilisierungskonzept geben. Die Mitarbeiter im Notfallmanagement-Team SOLLTEN regelmäßig entsprechend der benötigten Kompetenzen geschult werden.

DER.4.A9 Integration von Notfallmanagement in organisationsweite Abläufe und Prozesse [Institutionsleitung] (CIA)

Es SOLLTE sichergestellt werden, dass Aspekte des Notfallmanagements in allen Geschäftsprozessen der Institution berücksichtigt werden. Die Prozesse, Vorgaben und Verantwortlichkeiten im Notfallmanagement SOLLTEN mit dem Risikomanagement und Krisenmanagement abgestimmt werden.

DER.4.A10 Tests und Notfallübungen [Institutionsleitung] (CIA)

Es SOLLTE eine Übungsplanung erstellt werden, sodass alle wesentlichen Pläne und Maßnahmen des Notfallmanagements regelmäßig und anlassbezogen getestet und geübt werden. Im Notfallmanagement SOLLTEN ausreichend Ressourcen für die Planung, Konzeption, Durchführung und Auswertung der Tests und Übungen bereitgestellt werden.

DER.4.A11 Überprüfung und Aufrechterhaltung der Maßnahmen zur Notfallvorsorge und -reaktion (CIA)

Es SOLLTEN die identifizierten Maßnahmen zur Notfallvorsorge und -reaktion regelmäßig und anlassbezogen überprüft werden. Die Überprüfungen SOLLTEN so geplant werden, dass kein relevanter Teil ausgelassen wird. Die Ergebnisse der Überprüfungen SOLLTEN ausgewertet und gegebenenfalls in Korrekturmaßnahmen umgesetzt werden. Die Korrekturmaßnahmen SOLLTEN geplant und die Umsetzung kontrolliert werden.

DER.4.A12 Dokumentation im Notfallmanagement-Prozess (CIA)

Der Ablauf des Notfallmanagement-Prozesses, die Arbeitsergebnisse der einzelnen Phasen und wichtige Entscheidungen SOLLTEN dokumentiert werden. Es SOLLTE ein Verfahren etabliert werden, das gewährleistet, dass regelmäßige Dokumente aktualisiert werden. Hierüber hinaus SOLLTE der Zugriff auf die Dokumentation nur auf autorisierte Personen eingeschränkt werden.

DER.4.A13 Überprüfung und Steuerung des Notfallmanagement-Systems [Institutionsleitung] (CIA)

Die Leitungsebene SOLLTE ihre Aufgabe, das Notfallmanagement-System regelmäßig zu überprüfen, zu bewerten und gegebenenfalls zu korrigieren, wahrnehmen. Die Leitungsebene SOLLTE regelmäßig über den Stand des Notfallmanagements durch Management-Berichte informiert werden.

DER.4.A14 Regelmäßige Überprüfung und Verbesserung der Notfallmaßnahmen [Institutionsleitung] (IA)

Es SOLLTEN alle Notfallmaßnahmen regelmäßig oder bei größeren Änderungen daraufhin überprüft werden, ob sie noch eingehalten sowie korrekt umgesetzt werden und ob sie noch geeignet sind, die definierten Ziele zu erreichen.

Hierbei SOLLTE untersucht werden, ob technische Maßnahmen korrekt implementiert und konfiguriert wurden und ob organisatorische Maßnahmen effektiv und effizient umgesetzt sind. Bei Abweichungen SOLLTEN die Ursachen für Mängel ermittelt und Verbesserungsmaßnahmen veranlasst werden. Diese Ergebnisübersicht SOLLTE durch die Leitungsebene freigegeben werden. Es SOLLTE zudem ein Prozess initiiert werden, der steuert und überwacht, ob und wie die Verbesserungsmaßnahmen umgesetzt werden. Bei Verzug SOLLTE dies frühzeitig an die Leitungsebene eskaliert werden.

Es SOLLTE in der Institutionsleitung festgelegt sein, wie die Überprüfungstätigkeiten koordiniert werden. Insbesondere SOLLTEN die im Bereich der Revision, der IT, des Sicherheitsmanagements, des Informationssicherheitsmanagements und des Notfallmanagements durchgeführten Überprüfungen miteinander koordiniert werden. Dazu SOLLTE geregelt werden, welche Maßnahmen wann und von wem überprüft werden.

DER.4.A15 Bewertung der Leistungsfähigkeit des Notfallmanagement-Systems [Institutionsleitung] (IA)

Es SOLLTE regelmäßig bewertet werden, wie leistungsfähig und effektiv das Notfallmanagement-System ist. Als Grundlage SOLLTEN Mess- und Bewertungskriterien, wie z. B. Leistungskennzahlen (engl.: Key Performance Indicators) definiert werden. Diese Messgrößen SOLLTEN regelmäßig ermittelt und mit den Vorjahreswerten verglichen werden. Weichen die Werte negativ ab, SOLLTEN die Ursachen ermittelt und Verbesserungsmaßnahmen definiert werden. Die Ergebnisse der Bewertung SOLLTEN an die Leitung berichtet werden.

Die Leitung SOLLTE entscheiden, mit welchen Maßnahmen das Notfallmanagement weiterentwickelt werden soll. Alle Entscheidungen der Leitungsebene SOLLTEN dokumentiert und die bisherigen Aufzeichnungen aktualisiert werden.

DER.4.A16 Notfallvorsorge- und Notfallreaktionsplanung für ausgelagerte Komponenten [Institutionsleitung] (IA)

Bei der Notfallvorsorge- und Notfallreaktionsplanung für ausgelagerte Komponenten SOLLTE in den unterzeichneten Verträgen das Notfallmanagement des Lieferanten oder Dienstleisters geprüft werden. Diese Prüfung SOLLTE regelmäßig ein Verantwortlicher der Institutionsleitung durchführen. Auch SOLLTEN die Abläufe in Notfalltests und -übungen mit dem Lieferanten oder Outsourcing-Dienstleister abgestimmt und ggf. gemeinsam durchgeführt werden.

Die Ergebnisse und Auswertungen SOLLTEN regelmäßig zwischen der Institutionsleitung und dem Lieferanten oder Dienstleister ausgetauscht werden. Darin SOLLTEN auch eventuelle Verbesserungsmaßnahmen enthalten sein.

4 Weiterführende Informationen

4.1 Literatur

- [22301] ISO 22301:2012
  Scietal security - Business continuity management systems - Requirements, ISO, 2012
  https://www.iso.org/standard/50038.html

- [27001A17] ISO/IEC 27001:2013 - Annex A.17 Information security aspects of buisiness continuity management
  Information technology - Security techniques - Information security management systems - Requirements, insbesonder A.17 Information security aspects of business continuity management, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [27031] ISO/IEC 27031:2011
  Information technology - Security techniques - Guidelines for information and communications technology readiness for business continuity, 02.2011
  https://www.iso.org/standard/44374.html

- [BSI3] Risikoanalyse auf der Basis IT-Grundschutz, BSI-Standard 200-3
  BSI, 2017
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/IT-Grundschutz-Modernisierung/GS_Standards/gs_standards_node.html

- [BSI4] Notfallmanagement, BSI-Standard 100-4
  BSI, (zuletzt aubgerufen am 28.09.2017)
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard04/ITGStandard04_node.html

- [BWV] Bericht des bundesbeauftragten für die Wirtschaftlichkeit in der Verwaltung
  Modell eines Risikomanagements für die Bundesverwaltung, Bundesrechnungshof, 04.2017
  https://www.bundesrechnungshof.de/de/veroeffentlichungen/gutachten-berichte-bwv/berichte/sammlung/2017-bwv-bericht-modell-eines-risikomanagements-fuer-die-bundesverwaltung

- [ISFBC] The Standard of Good Practice- Area BC Business Continuity
  ISF, insbesonder Area BC Business Continuity, Juni 2016

- [LFKK] Krisenkommunikation - Leitfaden für Behörden und Unternehmen
  BMI, 2014
  https://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2014/leitfaden-krisenkommunikation.pdf

- [LFKRITIS] Schutz kritischer Infrastrukturen - Risiko- und Krisenmanagement (Leitfaden für Unternehmen und Behörden)
  BMI, 05.2011
  https://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2011/leitfaden_schutz-kritischer-infrastrukturn.pdf

- [NIST80034] NIST Special Publication 800-34
  Contingency Planning Guide for Federal Information Systems, Revision 1, 05.2010
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

- [UMRA] Umsetzungsrahmenwerk zum Notfallmanagement nach BSI-Standard 100-4
  BSI, (zuletzt aufgerufen am 28.09.2017)
  https://www.bsi.bund.de/DE/
  Themen/ITGrundschutz/ITGrundschutzStandards/Umsetzungsrahmenwerk/umra.html

- [WKN] Webkurs Notfallmanagement nach BSI-Standard 100-4
  BSI, (zuletzt aufgerufen am 28.09.2017)
  https://www.bsi.bund.de/DE/
  Themen/ITGrundschutz/ITGrundschutzSchulung/Webkurs1004/0_Startseite/nfm00_Start.html

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Notfallmanagement" von Bedeutung.

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.27 Ressourcenmangel

G 0.33 Personalausfall

Elementare Gefährdungen / Anforderungen	G 0.18	G 0.27	G 0.33
DER.4.A1	x	x	x
DER.4.A2	x		
DER.4.A3	x		
DER.4.A4	x		
DER.4.A5	x		
DER.4.A6	x	x	x
DER.4.A7	x		
DER.4.A8	x	x	x
DER.4.A9	x	x	
DER.4.A10	x		
DER.4.A11	x		
DER.4.A12	x	x	x
DER.4.A13	x		
DER.4.A14	x		
DER.4.A15	x		
DER.4.A16	x		

APP: Anwendungen

APP.2.2	Active Directory	376
APP.2.1	Allgemeiner Verzeichnisdienst	368
APP.4.3	Relationale Datenbanksysteme	430
APP.3.1	Webanwendungen	386
APP.3.6	DNS-Server	421
APP.3.3	Fileserver	406
APP.3.4	Samba	414
APP.3.2	Webserver	397
APP.1.2	Web-Browser	361
APP.1.1	Office-Produkte	353
APP.5.2	Microsoft Exchange und Outlook	450
APP.5.1	Allgemeine Groupware	440

APP.1: Client-Anwendungen

APP.1.1 Office-Produkte

1 Beschreibung

1.1 Einleitung

Die Gruppe der Office-Produkte umfasst alle Anwendungen, die dazu dienen, Dokumente zu erstellen, zu bearbeiten und zu betrachten. Dazu zählen unter anderem die freie Anwendung LibreOffice und die proprietäre Anwendung Microsoft Office, die in vielen Institutionen genutzt werden. Office-Produkte gehören für die meisten Institutionen zur notwendigen IT-Grundausstattung. Sie umfassen unter anderem Programme zur Textverarbeitung, Tabellenkalkulation und Erstellung von Präsentationen sowie Zeichenprogramme und einfache Datenbanksysteme. Die Nutzung von Office-Anwendungen ermöglicht und vereinfacht es, Informationen zu erheben und zu verarbeiten.

1.2 Zielsetzung

Ziel des vorliegenden Bausteins ist der Schutz der Informationen, die bei der Nutzung von Office-Produkten verarbeitet und genutzt werden. Dazu werden spezielle Anforderungen an die Funktionsweise der Komponenten von Office-Produkten gestellt. Der Baustein zeigt Anforderungen auf, die zur Absicherung von Office-Produkten vor spezifischen Gefährdungen umgesetzt werden sollten.

1.3 Abgrenzung

Dieser Baustein betrachtet den Einsatz von Office-Produkten aus Sicht des IT-Betriebs und gibt Hinweise für Benutzer, wie Office-Produkte eingesetzt werden sollten. Es werden spezifische Anforderungen gestellt, die beim Einsatz von Office-Produkten zu beachten sind. Ergänzend zu den Anforderungen dieses Bausteins muss die Umsetzung der Anforderungen des übergeordneten Bausteins CON.4 *Auswahl und Einsatz von Standardsoftware* gewährleistet werden. E-Mail- und PIM-Anwendungen werden in diesem Baustein ausgeklammert, die entsprechenden Anforderungen sind im Baustein APP.1.4 *Groupware* dokumentiert. Bei E-Mail- und PIM-Anwendungen der Firma Microsoft ist zusätzlich der Baustein APP.1.1 *Microsoft Exchange/Outlook* zu beachten. Bei der Verwendung von integrierten Datenbanksystemen wie Base in LibreOffice oder Access in Microsoft Office muss der Baustein APP.4.3 *Datenbank* berücksichtigt werden. Ebenfalls im vorliegenden Baustein ausgenommen sind reine Cloud-Office-Anwendungen wie Googles G Suite (Docs, Sheets und so weiter). Anforderungen an Cloud-Anwendungen sind in den Bausteinen OPS.2.2 *Cloud-Nutzung* und APP.5.3 *Cloud-Anwendungen aus Client-Sicht* festgelegt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich von Office-Produkten von besonderer Bedeutung:

2.1 Fehlende Anpassung der Office-Produkte an den Bedarf der Institution

Durch mangelnde Beachtung von Anforderungen an Office-Produkte bei der Beschaffung oder beim Anpassen der Software kann der Betrieb erheblich gestört werden. Gründe hierfür können beispielsweise fehlende Kompatibilität mit vorhandenen Vorlagen und Dokumenten, mangelnder Funktionsumfang der eingesetzten Version oder fehlende Interoperabilität mit Anwendungen von Geschäftspartnern sein. Sollten Office-Produkte nicht an den Bedarf der Institution angepasst werden, kann dies zu Performance-Verlusten, Störungen oder Fehlern innerhalb der Geschäftsprozesse führen.

2.2 Fehlendes oder unzureichendes Test- und Freigabeverfahren bei Office-Produkten

Werden neue Office-Produkte sowie ihre Integration in die Institution nicht oder nur unzureichend getestet und ohne Installationsvorschriften freigegeben, kann es vorkommen, dass Fehler nicht erkannt werden oder dass die notwendigerweise einzuhaltenden Installationsparameter nicht erkannt bzw. nicht beachtet werden. Fehler in Office-Produkten, die aus einem fehlenden oder unzureichenden Test- und Freigabeverfahren resultieren, stellen eine erhebliche Gefährdung für den IT-Betrieb dar. Arbeitsabläufe können durch Office-Produkt-Fehler maßgeblich behindert werden. Fehlerhafte Updates der Office-Produkte können zu Datenverlusten führen oder die Verfügbarkeit von genutzten Datenbanken einschränken.

2.3 Schützenswerte Daten in Restinformationen in Office-Dokumenten

Office-Dokumente speichern in der Regel Meta-Informationen zum Dokument selbst, sowie Informationen zum Autor und zur Institution. Diese Meta-Informationen lassen sich um beliebige, benutzerdefinierte Einträge erweitern, unterstützen die Arbeitsabläufe der Geschäftsprozesse und sorgen für eine geeignete Transparenz. Zusätzlich bieten Office-Produkte die Möglichkeit, Kommentare im Dokument anzulegen und im Überarbeiten-Modus Informationen hinzuzufügen oder zu ändern. Diese und weitere Restinformationen können vertrauliche Informationen enthalten, die Dritten nicht zugänglich gemacht werden dürfen. Dies kann andernfalls zu einem Verlust der Vertraulichkeit und zur späteren Verfälschung der Restinformationen führen und finanzielle, prozessuale und Image-Schäden verursachen.

2.4 Bezug von Office-Produkten und Updates aus unzuverlässiger Quelle

Werden Installationsquellen oder Updates von Office-Produkten aus inoffiziellen Quellen bezogen, besteht keine Garantie, dass die Software einwandfrei funktioniert und frei von Schadcode ist. Das gilt sowohl für die Office-Produkte an sich, als auch für Funktionen, die als Plug-in bzw. Add-on oder als Makro in Dokumenten vorliegen. Dies kann dazu führen, dass Berechnungen falsche Ergebnisse liefern oder die Integrität und Verfügbarkeit von Systemen beeinträchtigt wird.

2.5 Manipulation von Office-Dokumenten

Unter der Manipulation von Office-Dokumenten ist die Veränderung von Informationen zu verstehen. Office-Dokumente können in der Regel verschiedene Aktive Inhalte enthalten, die mitunter für komplexe Automatisierungen genutzt werden. Aktive Inhalte können aber auch Schadcode enthalten, der beim Öffnen des Dokuments mit den Rechten des Benutzers ausgeführt wird. Solche Schadprogramme in Office-Dokumenten können neben Manipulationen des betroffenen Dokumentes weitere Dokumente unerkannt verändern oder sich in weitere Dokumente verbreiten. Alle betroffenen Geschäftsprozesse der Institution können in ihren Funktionen gestört oder blockiert werden. Im schlimmsten Fall bleibt die Manipulation unerkannt und führt zu Sicherheitslücken und zur Verarbeitung von verfälschten Informationen.

2.6 Mangelnde Verbindlichkeit von Office-Dokumenten

Je nach Einsatzzweck kann es notwendig sein, Office-Dokumente verbindlich einem oder mehreren Autoren zuordnen zu können oder nachweisen zu können, dass jemand ein Dokument zur Kenntnis genommen hat. Kann diese Funktion leicht umgangen werden bzw. ist sie gar nicht vorgesehen oder entspricht sie nicht den gesetzlichen Anforderungen, können ungültige Verträge entstehen oder die Rechtmäßigkeit bestehender Verträge angefochten werden.

2.7 Integritätsverlust von Office-Dokumenten

Die Integrität von Office-Dokumenten kann durch unbeabsichtigte Änderungen oder durch vorsätzliche Manipulationen der Dokumenteninhalte verfälscht werden. Durch einen unbedachten Umgang mit Office-Produkten oder durch Unkenntnis der Benutzer im Umgang mit Office-Dokumenten kann es zu unerkannten Änderungen an Dokumenten kommen. Dies ist dann besonders problematisch, wenn es sich um Dokumente im produktiven Einsatz handelt. Wird mit Dokumenten weitergearbeitet, die unerkannt verfälscht wurden, werden möglicherweise falsche geschäftliche Entscheidungen getroffen oder es kann ein Image-Schaden für die Institution entstehen.

2.8 Software-Schwachstellen in Office-Produkten

Software-Schwachstellen in Office-Produkten werden trotz intensiver Tests meist nicht vollständig vor der Auslieferung an die Kunden entdeckt. Werden diese Software-Schwachstellen nicht rechtzeitig erkannt, können Abstürze und Fehler der Anwendungen resultieren. Zu den Folgen nicht behobener Fehler können unter anderem falsche Berechnungsergebnisse oder Integritätsverlust in Dokumenten gehören. Durch Software-Schwachstellen bzw. -fehler kann es außerdem zu schwerwiegenden Sicherheitslücken in Office-Produkten kommen. Solche Sicherheitslücken können unter Umständen von Angreifern ausgenutzt werden, um Schadcode einzuschleusen.

2.9 Einsatz von unlizenzierten Office-Produkten

Unlizenzierte Office-Produkte sind eine mögliche finanzielle Gefahrenquelle für Institutionen. Werden Office-Produkte ohne gültige Software-Lizenz eingesetzt, weil beispielsweise das Lizenzvolumen unbemerkt überschritten wurde, kann dies bei Bekanntwerden Vertragsstrafen zur Folge haben. Umgekehrt werden möglicherweise zu hohe Lizenzkosten entrichtet, da Office-Produkte an Arbeitsplätzen installiert sind, an denen sie nicht benötigt werden.

2.10 Datenverlust durch Passwortschutz von Office-Dokumenten

Datenverluste bei Office-Dokumenten können Geschäftsprozesse blockieren. In der Regel bieten Office-Produkte die Möglichkeit, Dokumente beim Speichern mit einem Passwort zu versehen, welches für das Öffnen oder Bearbeiten des Dokuments benötigt wird. Bei unvorsichtigem Einsatz dieser Funktion ist es möglich, dass vergebene Dokumenten-Passwörter nicht mehr bekannt oder nicht mehr auffindbar sind. Dadurch können wichtige Dokumente nicht mehr gelesen oder nur mit erhöhtem Aufwand weiter bearbeitet werden. Dieser Mehraufwand muss technisch und organisatorisch kompensiert werden, was wiederum zu einer erhöhten Arbeitslast führt.

2.11 Unerlaubtes Ausüben von Rechten bei Office-Produkten

Zugriffsrechte werden als organisatorische Maßnahmen eingesetzt, um Informationen, Geschäftsprozesse und IT-Systeme vor unbefugtem Zugriff zu schützen. Wenn unautorisierte Personen durch falsch gesetzte Berechtigungen auf Office-Produkte zugreifen können, kann dies die Vertraulichkeit und Integrität der Informationen gefährden, indem Informationen verändert, gelöscht oder unsachgemäß erstellt werden. Solche Sicherheitslücken entstehen meist durch fehlerhafte Rechtevergaben. Betroffene Geschäftsprozesse können korrumpiert werden sowie unbeabsichtigt fehlerhafte Informationen verarbeiten oder schützenswerte Informationen offenlegen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz von Office-Produkten aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Benutzer

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

APP.1.1.A1 Sicherstellen der Integrität von Office-Produkten

Bei der Installation von Office-Produkten MUSS sichergestellt werden, dass ausschließlich unveränderte Kopien der freigegebenen Originalsoftware verwendet werden. Updates MÜSSEN ausschließlich aus sicheren Quellen bezogen werden. Falls zu einem Office-Produkt Prüfsummen angeboten werden, SOLLTEN diese vor der Installation überprüft werden. Falls zu einem Office-Produkt digitale Signaturen verfügbar sind, SOLLTEN diese vor der Installation des Pakets überprüft werden. Die Administratoren SOLLTEN über die Bedeutung und Aussagekraft von Prüfsummen und digitalen Signaturen informiert werden. Ebenso wie bei einer Neuinstallation MUSS bei der Installation von Updates sichergestellt werden, dass die Update-Pakete unverändert sind.

APP.1.1.A2 Einschränken von Aktiven Inhalten [Benutzer]

Das automatische Ausführen von eingebetteten Aktiven Inhalten, wie beispielsweise Makros oder ActiveX-Elementen, MUSS in den Einstellungen aller verwendeten Office-Produkte deaktiviert werden. Ist die Ausführung Aktiver Inhalte für einen Geschäftsprozess notwendig, MUSS darauf geachtet werden, dass nur Aktive Inhalte von vertrauenswürdigen Quellen ausgeführt werden. Alle Benutzer MÜSSEN in Schulungen bezüglich der Gefährdungen durch Aktive Inhalte sensibilisiert werden und hinsichtlich der Funktionen zum Einschränken Aktiver Inhalten eingewiesen werden.

APP.1.1.A3 Öffnen von Dokumenten aus externen Quellen

Alle aus externen Quellen bezogenen Dokumente MÜSSEN vor dem Öffnen auf Schadsoftware überprüft werden. Alle als problematisch eingestuften und zusätzlich alle innerhalb der Institution nicht benötigten Dateiformate MÜSSEN verboten werden. Die Benutzer MÜSSEN zum Umgang mit Dokumenten aus externen Quellen geschult und sensibilisiert werden. Die Prüfung von Dokumenten aus externen Quellen SOLLTE durch technische Maßnahmen erzwungen werden.

APP.1.1.A4 Absichern des laufenden Betriebs von Office-Produkten

IT-Betrieb und ISB MÜSSEN sich regelmäßig über bekannt gewordene Sicherheitslücken der Office-Produkte informieren. Vorhandene Patches MÜSSEN zeitnah eingespielt werden.

Die Benutzer SOLLTEN über die Möglichkeiten und Grenzen von Sicherheitsfunktionen der eingesetzten Software und der genutzten Speicherformate informiert werden. Die Vorgaben für die sichere Nutzung von Office-Produkten SOLLTEN in der Sicherheitsrichtlinie integriert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Office-Produkte. Sie SOLLTEN grundsätzlich umgesetzt werden.

APP.1.1.A5 Auswahl geeigneter Office-Produkte

Im Rahmen der Beschaffung von Office-Anwendungen SOLLTEN die Anforderungen der Institution an Office-Produkte durch die Fach- und IT-Abteilung erhoben werden. Diese sollten in einem Anforderungskatalog dokumentiert werden. Sind alle Anforderungen an das zu beschaffende Office-Produkt dokumentiert, SOLLTEN die am Markt erhältlichen Produkte dahingehend untersucht werden, inwieweit sie diese Anforderungen der Institution erfüllen. Bei der Auswahl zwischen mehreren Alternativen SOLLTEN auch zusätzliche Aufwände berücksichtigt werden; zu diesen zählen beispielsweise Mehraufwänden für die Schulung von Administratoren und Benutzern oder für die Migration.

APP.1.1.A6 Testen neuer Versionen von Office-Produkten

Neue Versionen von Office-Produkten SOLLTEN vor dem produktiven Einsatz auf Kompatibilität mit etablierten Arbeitsmitteln (z. B. Dokumentenvorlagen, Formulare) der Institution geprüft werden. Zu diesem Zweck SOLLTEN Testmethoden für die Einzeltests (Testarten, -verfahren und -werkzeuge) entwickelt und freigegeben werden. Es SOLLTE sichergestellt sein, dass wichtige Arbeitsmittel auch mit der neuen Software-Funktion einwandfrei funktionieren. Bei entdeckten Inkompatibilitäten SOLLTE ein Migrationsplan für die betroffenen Dokumente erstellt werden.

APP.1.1.A7 Installation und Konfiguration von Office-Produkten

Für die eingesetzten Office-Produkte SOLLTE eine an den Bedarf der Institution angepasste Standardkonfiguration erstellt und genutzt werden. Diese Konfiguration SOLLTE in einer Installations- und Konfigurationsanweisung dokumentiert werden. Die Installation und Konfiguration SOLLTE gemäß der Anweisung erfolgen und die Standardeinstellungen anwenden. Alle notwendigen Abweichungen von der definierten Standardkonfiguration SOLLTEN nachvollziehbar dokumentiert werden und bedürfen für den Gebrauch einer Zustimmung durch eine geeignete Freigabeinstanz. Im Falle von Pilot-Installationen gilt, dass diese immer durch die IT-Abteilung begleitet werden SOLLTEN. Vor und nach den Installationen SOLLTEN Datensicherungen der Office-Produkte auf allen betroffenen IT-Systemen durchgeführt werden.

APP.1.1.A8 Versionskontrolle von Office-Produkten

Es SOLLTE eine regelmäßige Kontrolle der installierten Versionen von Office-Produkten erfolgen. Diese Bestandsführung der Software-Lizenzen SOLLTE bei jeder Installation oder Deinstallation aktualisiert werden. Darüber hinaus SOLLTEN die verschiedenen Konfigurationen der installierten Office-Produkte dokumentiert werden.

APP.1.1.A9 Beseitigung von Restinformationen vor Weitergabe von Dokumenten [Benutzer]

Vor der Weitergabe von Dokumenten an Dritte SOLLTEN alle nicht benötigten und vertraulichen Restinformationen aus Office-Dokumenten entfernt werden. Zusätzlich SOLLTEN die Metadaten bereinigt werden. Alle Benutzer SOLLTEN bezüglich der Risiken durch Restinformationen sowie der Möglichkeiten zur Beseitigung in den eingesetzten Office-Produkten sensibilisiert und geschult werden. Die Übermittlung von Dokumenten SOLLTE in einem nicht-veränderbaren Format erfolgen, falls eine Bearbeitung durch den Empfänger nicht erforderlich ist.

APP.1.1.A10 Regelung der Software-Entwicklung durch Endbenutzer [Benutzer]

Es SOLLTEN verbindliche Regelungen für die Softwareentwicklung auf Basis von Office-Anwendungen (z. B. Makros, Tabellenkalkulation) durch Endbenutzer getroffen werden, siehe auch APP.5.2.A2 Einschränken von Aktiven Inhalten. Zunächst SOLLTE in jeder Institution die Grundsatz-Entscheidung getroffen werden, ob solche Eigenentwicklungen erwünscht sind oder nicht. Die Entscheidung SOLLTE in den betroffenen Sicherheitsrichtlinien dokumentiert werden. Werden Eigenentwicklungen erlaubt, SOLLTE ein Verfahren für den Umgang mit entsprechenden Funktionen der Office-Produkte für die Endbenutzer entwickelt werden. Verantwortlichkeiten SOLLTEN klar definiert werden. Alle Informationen über die erstellten Anwendungen SOLLTEN dokumentiert werden. Aktuelle Versionen SOLLTEN allen betroffenen Benutzern zeitnah zugänglich gemacht werden.

APP.1.1.A11 Geregelter Einsatz von Erweiterungen für Office-Produkte

Alle Erweiterungen von Office-Produkten SOLLTEN vor dem produktiven Einsatz analog zum Testvorgehen von neuen Versionen getestet werden. Die durchzuführenden Tests SOLLTEN ausschließlich auf isolierten Testsystemen durchgeführt werden. Die Tests SOLLTEN prüfen, dass Erweiterungen keine negativen Auswirkungen für die Office-Produkte und laufenden IT-Systeme haben. Die Tests der eingesetzten Erweiterungen SOLLTEN einem definierten Testplan folgen, der die Nachvollziehbarkeit für Dritte gewährleistet.

APP.1.1.A12 Verzicht auf Cloud-Speicherung [Benutzer]

Die in einigen Office-Produkten integrierten Cloud-Speicher-Funktionen SOLLTEN grundsätzlich deaktiviert werden. Alle Cloud-Laufwerke SOLLTEN deaktiviert werden. Alle Dokumente SOLLTEN auf zentral verwalteten File-Servern der Institution gespeichert werden. Um Dokumente für Dritte zur Sichtung oder Bearbeitung freizugeben, SOLLTEN spezialisierte Anwendungen wie beispielsweise geeignete Datenräume eingesetzt werden, die über Sicherheitsfunktionen wie eine verschlüsselte Datenablage und -versendung und ein geeignetes System zur Benutzer- und Rechteverwaltung verfügen.

APP.1.1.A13 Verwendung von Viewer-Funktionen [Benutzer]

Daten aus potentiell unsicheren Quellen wie dem Internet oder Anhänge von E-Mail-Nachrichten SOLLTEN automatisch in einem geschützten Modus geöffnet werden, in dem sie nicht unmittelbar bearbeitet werden können. Nur eine allgemeine Navigation SOLLTE ermöglicht werden. Diese Funktion SOLLTE NICHT durch den Benutzer deaktivierbar sein. Es SOLLTEN entsprechende Viewer-Anwendungen verwendet werden, wenn diese verfügbar sind. Es kann eine Liste vertrauenswürdiger Orte definiert werden, von denen Inhalte unmittelbar geöffnet und bearbeitet werden können.

APP.1.1.A14 Schutz gegen nachträgliche Veränderungen von Informationen [Benutzer]

In Abhängigkeit vom geplanten Verwendungszweck von Dokumenten SOLLTEN die in Anwendungsprogrammen vorhandenen Sicherheitsmechanismen genutzt werden, um den weiteren Umgang mit den erstellten Dateien einzuschränken. Die Mitarbeiter SOLLTEN darauf hingewiesen werden, wie diese Sicherheitsmechanismen funktionieren und wie sie anzuwenden sind.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

APP.1.1.A15 Einsatz von Verschlüsselung und Digitalen Signaturen (CI)

Daten mit erhöhtem Schutzbedarf SOLLTEN vor einer Übertragung oder Speicherung verschlüsselt werden, um die Vertraulichkeit sicherzustellen. Vor der Nutzung eines in ein Office-Produkt integrierten Verschlüsselungsverfahrens SOLLTE geprüft werden, ob es einen ausreichenden Schutz bietet, das gilt besonders für ältere Produktversionen. Die IT-Systeme von Absender und Empfänger SOLLTEN den Zugriffsschutz auf die verwendete Methode zur Verschlüsselung gewährleisten. Benutzer SOLLTEN im Umgang mit den Verschlüsselungsfunktionen geschult und sensibilisiert werden. Zusätzlich SOLLTE ein Verfahren eingesetzt werden, mit dem Makros und Dokumente digital signiert werden können. Die Gültigkeit der verwendeten Zertifikate SOLLTE zeitlich begrenzt werden.

APP.1.1.A16 Integritätsprüfung von Dokumenten (I)

Zum Schutz vor zufälliger Veränderung von Daten mit erhöhtem Schutzbedarf bei einer Übertragung und/oder Speicherung SOLLTEN Prüfsummen-Verfahren eingesetzt werden. Es SOLLTE ein Verfahren ausgewählt werden, das dazu in der Lage ist, die Daten selbstständig zu korrigieren. Zum Schutz vor Manipulation SOLLTEN darüber hinaus kryptographische Prüfsummen-Verfahren eingesetzt werden.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [LIBRE] LibreOffice
  The Document Foundation - LibreOffice, (zuletzt abgerufen am 28.09.2017)
  https://de.libreoffice.org

- [MSTN] Microsoft Technet
  Microsoft, (zuletzt abgerufen am 28.09.2017)
  https://technet.microsoft.com/de-de

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Office-Produkte" von Bedeutung.

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.37 Abstreiten von Handlungen

G 0.39 Schadprogramme

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.28	G 0.29	G 0.37	G 0.39	G 0.45	G 0.46
APP.1.1.A1			x	x					x		
APP.1.1.A2		x			x				x		
APP.1.1.A3							x		x		
APP.1.1.A4		x				x			x		x
APP.1.1.A5	x										
APP.1.1.A6	x		x	x		x				x	x
APP.1.1.A7	x		x								
APP.1.1.A8	x						x				
APP.1.1.A9		x									
APP.1.1.A10	x					x					
APP.1.1.A11			x	x		x	x		x	x	
APP.1.1.A12	x	x					x				x
APP.1.1.A13			x			x			x		
APP.1.1.A14		x			x			x			x
APP.1.1.A15		x	x		x			x			x
APP.1.1.A16			x		x				x		x

APP.1: Client-Anwendungen

APP.1.2 Web-Browser

1 Beschreibung

1.1 Einleitung

Web-Browser sind Anwendungsprogramme, die (Hypertext-)Dokumente, Bilder, Video-, Audio- und andere Datenformate aus dem Internet abrufen, verarbeiten, darstellen, ausgeben und auf lokale IT-Systeme speichern können. Ebenso können Web-Browser auch Daten ins Internet übertragen. Stationäre und mobile Client-Systeme sind heute ohne Web-Browser nicht vorstellbar, weil sehr viele private und geschäftliche Anwendungen entsprechende Inhalte nutzen.

Gleichzeitig werden diese Inhalte im Internet immer vielfältiger. Immer weniger Websites kommen ohne eingebettete Videos, animierte Elemente und andere aktive Inhalte aus. Moderne Web-Browser decken zudem eine große Bandbreite an Zusatzfunktionen ab, indem sie Plug-ins und externe Bibliotheken einbinden. Hinzu kommen Erweiterungen für bestimmte Funktionen, Datenformate und Inhalte. Die Komplexität moderner Web-Browser bietet ein hohes Potential für gravierende konzeptionelle Fehler und programmtechnische Schwachstellen. Sie erhöht nicht nur die möglichen Gefahren für Angriffe aus dem Internet, sondern birgt zusätzliche Risiken durch Programmier- und Bedienungsfehler.

Die Folgen für die Vertraulichkeit und Integrität von Daten sind erheblich. Ebenso ist die Verfügbarkeit des gesamten IT-Systems durch solche Schwachstellen bedroht. Internetinhalte müssen demzufolge aus Sicht des Web-Browsers grundsätzlich als nicht vertrauenswürdig angesehen werden.

1.2 Zielsetzung

Dieser Baustein beschreibt Sicherheitsanforderungen für Web-Browser, die auf Client-Systemen, also auf stationären und mobilen Computern sowie teilweise auch auf Tablets und Smartphones, eingesetzt werden. Es werden sowohl zentral verwaltete als auch einzelne Betriebsumgebungen betrachtet.

1.3 Abgrenzung

Dieser Baustein enthält grundsätzliche Sicherheitsanforderungen, die bei der Installation und dem Betrieb von Web-Browsern für den Zugriff auf Daten aus dem Internet zu beachten und zu erfüllen sind. Browser für den Zugriff auf rein lokale oder Daten in internen Datennetzen ohne Internetzugriff werden in diesem Baustein nicht behandelt.

Web-Browser sind in eng mit dem Betriebssystem des Client-Systems verzahnt und greifen auf dort bereitgestellte Schnittstellen und Funktionen zurück. Um die Betriebssysteme abzusichern, sollten daher die Anforderungen der Bausteine der Schichten SYS.2.2 *Desktop-Systeme* und SYS.3.2 *Tablet und Smartphone* erfüllt werden.

Viele Plug-ins wie Java werden durch die Web-Browser-Instanzen ausgeführt und laufen in der Regel in separaten Ausführungsumgebungen ab. Anforderungen hierzu sind im Baustein SYS.2.7 *Internet-PC* zu finden.

Mit Browsern genutzte Web-Anwendungen sowie zuständige Server werden in den Bausteinen APP.3.1 *Web-Anwendungen* und APP.3.2 *Webserver* behandelt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Web-Browser von besonderer Bedeutung:

2.1 Ausführung von Schadcode durch Web-Browser

Web-Browser können Daten aus nicht vertrauenswürdigen oder möglicherweise sogar kompromittierten Quellen laden. Solche Daten können ausführbaren Code mit Schadfunktion enthalten, der Schwachstellen ausnutzen kann und das Gerät des Benutzers ohne dessen Kenntnis und somit unbemerkt infiziert.

Dabei kann es sich um Code handeln, der durch den Web-Browser direkt ausgeführt werden kann, wie etwa JavaScript. Ebenso kann es auch ausführbarer Code eines Plug-ins oder einer Erweiterung im Kontext des Browsers sein, wie etwa Adobe Flash, Java oder Bestandteile von PDF-Dokumenten. Schließlich kann es sich auch um Code handeln, der vom Web-Browser auf den Client geladen und dort außerhalb des Browser-Prozesses ausgeführt wird. Vielfach wird auch durch den Schadcode weitere Schadsoftware nachgeladen, die dann auf dem Client mit den Rechten des Nutzers ausgeführt wird. Werden die grundlegenden Schutzmechanismen moderner Web-Browser nicht ausreichend angewendet, werden die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder Diensten des Clients oder der möglicherweise verbundenen Netze bedroht.

2.2 Exploit Kits

Schwachstellenlisten und sogenannte Exploit Kits erleichtern die Entwicklung individueller Schadsoftware erheblich. Cyberangriffe können automatisiert werden, um Drive-by-Downloads oder andere Verbreitungswege leicht und ohne Expertenwissen zu nutzen. Angreifer können ihnen bekannte Schwachstellen des Web-Browsers oder einer verbundenen Ressource oder Erweiterung ausnutzen, um Folgeangriffe vorzubereiten oder Code mit Schadfunktion auf den Client zu laden und zu installieren.

2.3 Mitlesen der Internetkommunikation

Die grundlegende Sicherheit der Kommunikation im Internet hängt ganz wesentlich vom eingesetzten Authentisierungsverfahren und von der Verschlüsselung der Daten auf dem Transportweg ab. Die nötigen Verfahren sind oft schlecht implementiert.

Schwache Implementierungen der nötigen Verfahren sind weit verbreitet und verhindern eine wirkungsvolle Authentisierung und Verschlüsselung. Viele Webdienste wenden außerdem immer noch veraltete Verschlüsselungsverfahren an. Somit kann ein Angreifer die Authentisierung von Servern unterlaufen oder die Kommunikation bzw. die Daten werden nicht wirkungsvoll verschlüsselt. Hierdurch können Informationen auf dem Übertragungsweg mitgelesen oder verändert werden. In der Vergangenheit wurden außerdem Zertifizierungsstellen kompromittiert, hierdurch konnten Angreifer an Zertifikate für fremde Websites gelangen.

2.4 Integritätsverlust in Web-Browsern

Werden Browser, Plug-ins oder Erweiterungen aus nicht vertrauenswürdigen Quellen bezogen, können unabsichtlich und unbemerkt Schadfunktionen ausgeführt werden. Angreifer können beispielsweise Komponenten wie Toolbars von Web-Browsern fälschen, um die Benutzer auf manipulierte Kopien von Webseiten zu locken, mit deren Hilfe Phishing-Angriffe durchgeführt werden. Bösartige Erweiterungen können Inhalte der betrachteten Webseiten manipulieren oder Daten ausspionieren und an den Angreifer senden.

2.5 Verlust der Privatsphäre

Werden Browser unsicher konfiguriert, können so vertrauenswürdige Daten zufällig oder böswillig unbefugten Dritten zugänglich gemacht werden. Auch Passwörter können ungewollt weitergegeben werden. Werden Cookies, Passwörter, Historien, Eingabedaten und Suchanfragen gespeichert oder unnötige Erweiterungen aktiviert, können Daten von Dritten oder von Schadprogrammen leichter missbräuchlich ausgelesen werden.

2.6 Fehler bei Administration und Betrieb

Fehler in der Administration des Web-Browsers können zu einer unsicheren Konfiguration und zu unsicherem Betrieb führen. Ein wesentliches Bedrohungspotential erwächst in der mangelhaften Aktualität und Pflege des verwendeten Web-Browsers. Browserhersteller bieten zudem oftmals Sicherheitsupdates nicht zeitnah genug an. Dadurch steigt die Verbreitungsrate von ausnutzbaren Schwachstellen signifikant.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen für Web-Browser aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der Informationssicherheitsbeauftragte dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Benutzer

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

APP.1.2.A1 Verwendung von Sandboxing

Der eingesetzte Web-Browser MUSS über sicherstellen, das jede Instanz und jeder Verarbeitungsprozess nur auf die eigenen Ressourcen zugreifen kann (Sandboxing). Web-Seiten MÜSSEN als eigenständige Prozesse oder mindestens als eigene Threads voneinander isoliert werden. Plug-ins und Erweiterungen MÜSSEN ebenfalls in isolieren Bereichen ausgeführt werden. Der verwendete Web-Browser SOLLTE die Content Security Policy gemäß den W3C-Spezifikationen umsetzen.

APP.1.2.A2 Verschlüsselung der Kommunikation

Der Web-Browser MUSS Transport Layer Security (TLS) in einer sicheren Version unterstützen. Unsichere Versionen von TLS Version SOLLTEN deaktiviert werden. Der Web-Browser MUSS den Sicherheitsmechanismus HTTP Strict Transport Security (HSTS) gemäß RFC 6797 unterstützen. Für alle wichtigen öffentlichen TLS-verschlüsselten Web-Dienste SOLLTEN die Domains in die HSTS-Preload-Liste des Browsers eingefügt werden.

APP.1.2.A3 Verwendung von Zertifikaten [Benutzer]

Der Web-Browser MUSS eine Liste vertrauenswürdiger Wurzelzertifikats-Aussteller bereitstellen sowie die von der Institution selbst bereitgestellte Zertifikate akzeptieren. Der Web-Browser MUSS Extended-Validation-Zertifikate unterstützen. Wurzelzertifikate DÜRFEN NUR mit Administrationsrechten hinzugefügt, geändert, oder gelöscht werden. Zertifikate MÜSSEN durch den Web-Browser (lokal) widerrufen werden können.

Der Web-Browser MUSS die Gültigkeit der Server-Zertifikate mit Hilfe des öffentlichen Schlüssels und des Gültigkeitszeitraums vollständig prüfen. Der Sperrstatus der Server-Zertifikate MUSS vom Web-Browser geprüft werden. Die Zertifikatskette einschließlich des Wurzelzertifikats MUSS verifiziert werden.

Der Web-Browser MUSS dem Benutzer eindeutig und gut bemerkbar darstellen, ob die Kommunikation im Klartext oder verschlüsselt erfolgt. Der Web-Browser SOLLTE dem Benutzer auf Anforderung das verwendete Serverzertifikat anzeigen können. Der Web-Browser MUSS dem Benutzer signalisieren, wenn Zertifikate fehlen, ungültig sind oder widerrufen wurden. Die verschlüsselte Verbindung DARF in einem solchen Fall NUR nach ausdrücklicher Bestätigung durch den Benutzer hergestellt werden.

APP.1.2.A4 Versionsprüfung und Aktualisierung des Web-Browsers

Der Web-Browser MUSS über einen Mechanismus verfügen, der den eigenen Versionsstand sowie denjenigen aller geladenen oder aktivierten Erweiterungen und Plug-ins zuverlässig erkennen und anzeigen kann.

Updates für den Web-Browser, Plug-ins und Erweiterungen MÜSSEN unverzüglich eingespielt werden. Der Web-Browser SOLLTE Updates automatisch einspielen können. Ist kein Update für eine bekannt gewordene kritische Schwachstelle verfügbar, MÜSSEN zeitnah Maßnahmen zur Mitigation ergriffen werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Web-Browser. Sie SOLLTEN grundsätzlich umgesetzt werden.

APP.1.2.A5 Basiskonfiguration

Der Browser SOLLTE zentral konfiguriert werden können. Zentral vorgegebene Einstellungen DÜRFEN NICHT von den Benutzern verändert werden können. Der Web-Browser SOLLTE NICHT dauerhaft mit erweiterten Rechten ausgeführt werden.

APP.1.2.A6 Kennwortmanagement im Web-Browser [Benutzer]

Wird ein Kennwortmanager im Browser verwendet, SOLLTE er eine direkte und eindeutige Beziehung zwischen Webseite und hierfür gespeichertem Kennwort herstellen. Der Kennwortspeicher SOLLTE geschützt sein. Auf die im Kennwortmanager gespeicherten Passwörter SOLLTE nur nach Eingabe eines Master-Kennwortes zugegriffen werden können. Die Authentisierung für den kennwortgeschützten Zugriff SOLLTE nur für die aktuelle Sitzung gültig sein. Der Kennwortmanager SOLLTE die Qualität der Kennwörter entsprechend der Sicherheitsrichtlinie der Institution vorgegeben. Die gespeicherten Kennwörter SOLLTEN durch den Benutzer gelöscht werden können.

APP.1.2.A7 Schutz von Daten [Benutzer]

Cookies von Drittanbietern SOLLTEN abgelehnt werden. Gespeicherte Cookies SOLLTEN durch den Benutzer gelöscht werden können.

Die Funktion zur Auto-Vervollständigung von Daten SOLLTE deaktiviert werden. Wird die Funktion doch genutzt, SOLLTE der Benutzer die Vervollständigungsdaten löschen können. Der Benutzer SOLLTE außerdem die Historiendaten des Browsers löschen können.

Sofern vorhanden, SOLLTE eine Synchronisationen des Browsers mit Cloud-Diensten deaktiviert werden. Telemetriefunktionen sowie das automatische Senden von Absturzberichten an den Hersteller SOLLTEN soweit wie möglich deaktiviert werden.

Sind Peripheriegeräte wie Mikrofon oder Webcam angeschlossen, SOLLTEN diese im Browser deaktiviert werden. Der Browser SOLLTE eine Möglichkeit bieten, um WebRTC, HSTS und JavaScript zu konfigurieren bzw. abzuschalten.

APP.1.2.A8 Verwendung von Plug-ins und Erweiterungen [Benutzer]

Es SOLLTEN nur unbedingt notwendige Plug-ins und Erweiterungen installiert werden. Plug-ins und Erweiterungen für den Browser SOLLTEN nur mit Administrationsrechten installiert werden dürfen. Die Ausführung von Plug-ins SOLLTE immer vom Benutzer bestätigt werden müssen. Der Browser SOLLTE die Möglichkeit bieten, Erweiterungen zu konfigurieren und abzuschalten.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

APP.1.2.A9 Einsatz einer isolierten Browser-Umgebung

Bei erhöhtem Schutzbedarf SOLLTEN Web-Browser eingesetzt werden, die in einer isolierten Umgebung (wie ReCoBS) oder auf dedizierten IT-Systemen laufen.

APP.1.2.A10 Verwendung des privaten Modus [Benutzer]

Der Browser SOLLTE bei erhöhten Anforderungen bezüglich der Vertraulichkeit im sogenannten privaten Modus ausgeführt werden, sodass keinerlei Informationen oder Inhalte persistent auf dem IT-System des Benutzers gespeichert werden. Der Browser SOLLTE so konfiguriert werden, dass lokale Inhalte beim Beenden gelöscht werden.

APP.1.2.A11 Überprüfung auf schädliche Inhalte

Aufgerufene Internetadressen SOLLTEN durch den Browser auf potentiell schädliche Inhalte geprüft werden. Der Browser SOLLTE den Benutzer in geeigneter Form warnen, wenn Informationen über schädliche Inhalte vorliegen. Eine als schädlich klassifizierte Verbindung SOLLTE nicht aufgerufen werden können. Das verwendete Verfahren zur Überprüfung DARF NICHT gegen Datenschutz- oder Geheimschutz-Vorgaben verstoßen.

APP.1.2.A12 Zwei-Browser-Strategie

Für den Fall von ungelösten Sicherheitsproblemen mit dem verwendeten Web-Browser SOLLTE ein alternativer Browser eines anderen Herstellers installiert sein, um als Ausweichmöglichkeit dienen zu können.

4 Weiterführende Informationen

4.1 Literatur

- [AbWeB] Absicherungsmöglichkeiten beim Einsatz von Web-Browsern
  Bundesamt für Sicherheit in der Informationstechnik, Version 1.0, 2013
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_047.pdf

- [ACSDB] SSL Cipher Suite Details of Your Browser
  Aktive Cipher Suites Detais des Browsers, Check Möglichkeiten, (zuletzt abgerufen am 28.09.2017)
  https://cc.dcsec.uni-hannover.de/

- [CSP] Content Security Polic W3C
  W3, Version 1.0, 2012
  https://www.w3.org/TR/2012/CR-CSP-20121115/

- [HSTS] HTTP Strict Security Policy (HSTS), RFC 6797
  IETF, 2012
  https://tools.ietf.org/html/rfc6797

- [MDST8SSL] Mindeststandard des BSI nach §8 Absatz 1 Satz 1 BSIG für den Einsatz des SSL/ TLS-Protokoll in der Bundesverwaltung
  Bundesamt für Sicherheit in der Informationstechnik, Version 1.0, 2015
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf

- [MDST8Web] Mindeststandard des BSI nach §8 Absatz 1 Satz 1 BSIG für den sicheren Einsatz von Web-Browsern in der Bundesverwaltung
  Bundesamt für Sicherheit in der Informationstechnik, Version 1.0, 2017
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Sichere_Web-Browser.pdf

- [OWASPList] OWASP List of the 10 Most Critical Web Application Security Risks
  OWASP, (zuletzt abgerufen am 28.09.2017)
  https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

- [ReCoBS] Common Criteria Protection Profile for Remote-Controlled Browsers System (ReCoBS)
  BSI, BSI-PP-0040; Version 1.0, 2008
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/recobslanginfo_pdf.pdf?_blob=publicationBundesamt

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Web-Browser" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.14	G 0.15	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.28	G 0.30	G 0.31	G 0.39	G 0.40	G 0.45	G 0.46
APP.1.2.A1				x				x			x			x			
APP.1.2.A2	x		x	x			x										x
APP.1.2.A3	x		x		x		x										x
APP.1.2.A4					x	x		x		x	x			x			
APP.1.2.A5			x			x						x	x				
APP.1.2.A6			x	x								x	x				
APP.1.2.A7	x	x		x								x	x			x	
APP.1.2.A8			x				x				x	x	x				
APP.1.2.A9								x		x	x			x			
APP.1.2.A10	x			x													
APP.1.2.A11								x			x						
APP.1.2.A12			x						x	x	x				x		

APP.2: Verzeichnisdienst

APP.2.1 Allgemeiner Verzeichnisdienst

1 Beschreibung

1.1 Einleitung

Ein Verzeichnisdienst stellt in einem Datennetz Informationen über beliebige Objekte in einer definierten Art zur Verfügung. Mit einem Objekt können zugehörige Attribute gespeichert werden, zum Beispiel zu einer Benutzerkennung Namen und Vornamen des Benutzers, die Personalnummer und der Rechnername. Diese Daten können dann gleichermaßen von verschiedenen Applikationen verwendet werden. Der Verzeichnisdienst und seine Daten werden in der Regel von zentraler Stelle aus verwaltet.

Einige typische Anwendungsgebiete von Verzeichnisdiensten sind:

- Verwaltung von Adressbüchern, z. B. für Telefonnummern, E-Mail-Adressen, Zertifikate für elektronische Signaturen
- Ressourcen-Verwaltung, z. B. für Computer, Drucker, Scanner und andere Peripherie-Geräte
- Benutzer-Verwaltung, z. B. zur Verwaltung von Benutzerkonten und Benutzerberechtigungen
- Authentisierung, z. B. zur Anmeldung an Betriebssystemen oder Anwendungen

Verzeichnisdienste sind auf Lesezugriffe hin optimiert, da Daten aus dem Verzeichnisdienst typischerweise abgerufen werden. Schreibzugriffe, wie das Erstellen, Ändern oder Löschen von Einträgen, sind seltener notwendig.

1.2 Zielsetzung

Ziel des Bausteins ist es, allgemeine Verzeichnisdienste sicher zu betreiben sowie die damit verarbeiteten Informationen angemessen zu schützen.

1.3 Abgrenzung

Dieser Baustein betrachtet allgemeine Sicherheitsaspekte von Verzeichnisdiensten unabhängig vom eingesetzten Produkt. Für produktspezifische Sicherheitsaspekte existieren im IT-Grundschutz-Kompendium weitere Bausteine, die zusätzlich auf den jeweiligen Verzeichnisdienst anzuwenden sind.

Ein Beispiel hierfür ist Active Directory von Microsoft (siehe APP.2.2 *Active Directory*). Andere Verzeichnisdienste basieren auf dem frei verfügbaren OpenLDAP (siehe APP.2.3 *OpenLDAP*), das in vielen Unix-basierten Systemen verwendet und beispielsweise auch von Apples macOS genutzt wird. Bausteine zu Server-Systemen, auf denen Verzeichnisdienste üblicherweise betrieben werden, sind in der Schicht SYS.1 *Server* des IT-Grundschutz-Kompendiums aufgeführt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Allgemeiner Verzeichnisdienst von besonderer Bedeutung:

2.1 Fehlende oder unzureichende Planung des Einsatzes von Verzeichnisdiensten

Die Sicherheit von Verzeichnisdiensten stützt sich stark auf die Sicherheit des Basisbetriebssystems und hierbei vor allem auf die Dateisystemsicherheit. Verzeichnisdienste lassen sich auf einer Vielzahl von Betriebssystemen installieren und betreiben, wodurch sich eine große Vielfalt der vorzunehmenden Sicherheitseinstellungen ergeben kann. Diese Vielfalt erhöht die Anforderungen an die Planung und setzt entsprechende Kenntnisse des als Basis dienenden Betriebssystems voraus. Sollte die entstehende Gesamtlösung sehr heterogen oder komplex sein, kann ein nicht ausreichend geplanter Einsatz des Verzeichnisdienstes im Wirkbetrieb zu Sicherheitslücken führen. Da bei Verzeichnisdiensten außerdem eine rollenbasierte Administration der Verzeichnisdatenbank üblich ist sowie einzelne Administrationsaufgaben delegiert werden können, besteht bei fehlerhafter Planung der Administrationsaufgaben die Gefahr, dass das System unsicher oder unzulänglich administriert wird.

2.2 Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Verzeichnisdienst

Bei der Partitionierung handelt es sich um eine Aufteilung der Verzeichnisdaten eines Verzeichnisdienstes in einzelne Teilbereiche (Partitionen). Die Replizierung von Partitionen des Verzeichnisdienstes dient in der Regel zur Lastverteilung. Weiter wird durch die Redundanz in der Datenhaltung die Ausfallsicherheit verbessert und somit die Verfügbarkeit erhöht. Von entscheidender Bedeutung ist deshalb auch hier eine geeignete Planung, da nachträgliche Änderungen an den Partitions- und Replikationseinstellungen zwar möglich sind, aber unter Umständen Probleme nach sich ziehen können. Wird die Partitionierung und die Replizierung des Verzeichnisdienstes fehlerhaft oder unzureichend geplant, kann dies zu Datenverlusten sowie Inkonsistenzen in der Datenhaltung, zu einer mangelhaften Verfügbarkeit des Verzeichnisdienstes und zu einer insgesamt schlechten Systemperformance bis hin zu Ausfällen führen.

2.3 Fehlerhafte oder unzureichende Planung des Zugriffs auf den Verzeichnisdienst

Zugangs- und Zugriffsrechten im Kontext eines Verzeichnisdienstes zu verwalten, ist eine äußerst arbeitsintensive Aufgabe, bei der im Extremfall viele manuelle Arbeitsschritte erforderlich sind, die zu Fehlern und Mängeln im Überblick über durchgeführte Arbeiten führen können. Eine unzureichende Planung, ob und welche Daten im Klartext übertragen werden dürfen, kann Inkonsistenzen oder Widersprüche zu organisationsinternen Sicherheitsrichtlinien hervorrufen. Auch kann eine fehlerhafte Planung der Sicherheitsmaßnahmen und -techniken des Verzeichnisdienstes zum Schutz vertraulicher Daten zu Inkompatibilitäten bis hin zum Ausfall der Verschlüsselung führen, was sich unmittelbar auf die Vertraulichkeit und die Integrität auswirken kann.

2.4 Fehlerhafte Administration von Zugangs- und Zugriffsrechten

Zugangsrechte zu einem IT-System und Zugriffsrechte auf gespeicherte Daten und IT-Anwendungen dürfen nur in dem Umfang eingeräumt werden, wie sie für die durchzuführenden Aufgaben erforderlich sind. Dies gilt auch für die Berechtigungen, die über einen Verzeichnisdienst verwaltete Benutzer und Gruppen erhalten. Werden diese Rechte fehlerhaft administriert, so kommt es zu Betriebsstörungen, falls erforderliche Rechte nicht zugewiesen wurden. Andererseits kann es zu Sicherheitslücken kommen, falls über die notwendigen Rechte hinaus weitere vergeben werden. Sofern die Zugriffsrechte im Verzeichnisdienst falsch oder inkonsistent vergeben werden, ist dadurch die Sicherheit des Gesamtsystems erheblich gefährdet. Ein besonders kritischer Punkt sind auch die Administrationsrechte. Werden diese Rechte falsch vergeben, kann das gesamte Administrationskonzept in Frage gestellt oder unter Umständen sogar die Administration des Verzeichnissystems selbst blockiert werden.

2.5 Fehlerhafte Konfiguration des Zugriffs auf Verzeichnisdienste

In vielen Einsatzszenarien müssen weitere Applikationen, wie Internet- oder Intranet-Anwendungen, auf den Verzeichnisdienst zugreifen. Eine Fehlkonfiguration kann dazu führen, dass Zugriffsrechte falsch vergeben werden oder unautorisiert auf den Verzeichnisdienst zugegriffen werden kann, oder dass Daten zur Authentisierung im Klartext übermittelt und somit unverschlüsselte Informationen ausgespäht werden können.

2.6 Ausfall von Verzeichnisdiensten und Verschlüsselung

Durch technisches Versagen aufgrund von Hardware- oder Software-Problemen können Verzeichnisdienste oder Teile davon ausfallen. Als Folge sind die im Verzeichnis gehaltenen Daten temporär nicht mehr zugänglich. Im Extremfall können Daten verloren gehen. Dadurch können Geschäftsprozesse und interne Arbeitsabläufe behindert werden. Sind funktionsfähige Kopien der ausgefallenen Systemteile vorhanden, so ist der Zugriff zwar weiterhin möglich, jedoch unter Umständen je nach gewählter Netztopologie nur mit eingeschränkter Leistungsfähigkeit.

2.7 Kompromittierung von Verzeichnisdiensten durch unbefugten Zugriff

Wenn es einem Angreifer gelungen ist, eine notwendige Authentisierung gegenüber dem Verzeichnisdienst erfolgreich zu umgehen, kann er danach im Allgemeinen auf eine Vielzahl von Daten zugreifen, für die er keine Berechtigung besitzen sollte. Somit kann der gesamte Verzeichnisdienst kompromittiert werden. Außerdem könnten Unbefugten durch erweiterte Berechtigungen auf Netzressourcen oder Dienste zugreifen. Dies kann dazu führen, dass ein Angreifer alle Verteidigungsmaßnahmen des Verzeichnisdienstes umgeht. Dadurch könnte das betroffene System beeinträchtigt oder gar zerstört werden. Die Sicherheit eines Verzeichnisdienstes kann ebenfalls gefährdet werden, wenn anonyme Benutzer zugelassen werden. Dadurch, dass deren Identität nicht überprüft wird, können anonyme Benutzer zunächst beliebige Abfragen an den Verzeichnisdienst richten, durch die sie zumindest Teilinformationen über dessen Struktur und Inhalt erlangen. Wenn anonyme Zugriffe zugelassen werden, sind außerdem DoS-Attacken auf den Verzeichnisdienst leichter durchführbar, da Angreifer mehr Zugriffsmöglichkeiten haben, die nur schlecht kontrollierbar sind.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Allgemeiner Verzeichnisdienst aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Datenschutzbeauftragter, Fachverantwortliche

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

APP.2.1.A1 Erstellung einer Sicherheitsrichtlinie für Verzeichnisdienste

Es MUSS eine Sicherheitsrichtlinie für den Verzeichnisdienst erstellt werden. Diese SOLLTE mit dem übergreifenden Sicherheitskonzept der gesamten Institution abgestimmt sein.

APP.2.1.A2 Planung des Einsatzes von Verzeichnisdiensten [Datenschutzbeauftragter, Fachverantwortliche]

Der Einsatz von Verzeichnisdiensten MUSS sorgfältig geplant werden. Neben der Festlegung der Nutzung des Verzeichnisdienstes MUSS ein Modell aus Objektklassen und Attributtypen entwickelt werden, das den Ansprüchen der vorgesehenen Nutzungsarten genügt. Bei der Planung des Verzeichnisdienstes MÜSSEN Personalvertretung und Datenschutzbeauftragter beteiligt werden. Ein bedarfsgerechtes Berechtigungskonzept zum Verzeichnisdienst MUSS entworfen werden. Generell SOLLTE die geplante Verzeichnisdienst-Struktur vollständig dokumentiert werden. Es SOLLTEN Maßnahmen geplant werden, die das unbefugte Sammeln von Daten aus dem Verzeichnisdienst unterbinden.

APP.2.1.A3 Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste [Fachverantwortliche]

Die administrativen Aufgaben für die Administration des Verzeichnisdienstes selbst sowie für die eigentliche Verwaltung der Daten MÜSSEN strikt getrennt werden. Die administrativen Tätigkeiten SOLLTEN so delegiert werden, dass sich möglichst keine Überschneidungen ergeben. Alle administrativen Aufgabenbereiche und Berechtigungen SOLLTEN ausreichend dokumentiert werden.

Die Zugriffsrechte der Benutzer- und Administratorengruppen MÜSSEN anhand der erstellten Sicherheitsrichtlinie konfiguriert und umgesetzt werden. Bei einer eventuellen Zusammenführung mehrerer Verzeichnisdienst-Bäume MÜSSEN die resultierenden effektiven Rechte kontrolliert werden.

APP.2.1.A4 Sichere Installation von Verzeichnisdiensten

Es MUSS ein Konzept für die Installation erstellt werden, nach dem Administrations- und Zugriffsberechtigungen bereits bei der Installation des Verzeichnisdienstes konfiguriert werden.

APP.2.1.A5 Sichere Konfiguration und Konfigurationsänderungen von Verzeichnisdiensten

Der Verzeichnisdienst MUSS sicher konfiguriert werden. Für die sichere Konfiguration einer Verzeichnisdienstes-Infrastruktur MÜSSEN neben dem Server auch die Clients (Rechner und Programme) einbezogen werden.

Administrative Zugänge zum Verzeichnisdienst MÜSSEN geschützt werden. Bei der Durchführung von Konfigurationsänderungen der vernetzten IT-Systeme SOLLTEN die Benutzer rechtzeitig über Wartungsarbeiten informiert werden. Vor den Konfigurationsänderungen SOLLTEN von allen betroffenen Dateien und Verzeichnissen Datensicherungen angefertigt werden.

APP.2.1.A6 Sicherer Betrieb von Verzeichnisdiensten

Die Sicherheit des Verzeichnisdienstes MUSS im Betrieb permanent aufrechterhalten werden. Alle für den Betrieb eines Verzeichnisdienst-Systems betreffenden Richtlinien, Regelungen und Prozesse SOLLTEN dokumentiert werden. Der Zugriff auf alle Administrationswerkzeuge MUSS für normale Benutzer unterbunden werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Allgemeiner Verzeichnisdienst. Sie SOLLTEN grundsätzlich umgesetzt werden.

APP.2.1.A7 Erstellung eines Sicherheitskonzepts für den Einsatz von Verzeichnisdiensten

Durch das Sicherheitskonzept für Verzeichnisdienste SOLLTEN sämtliche sicherheitsbezogenen Themenbereiche eines Verzeichnisdienstes geregelt werden. Die daraus entwickelten Sicherheitsrichtlinien SOLLTEN schriftlich festgehalten und im erforderlichen Umfang den Benutzern des Verzeichnisdienstes mitgeteilt werden.

APP.2.1.A8 Planung einer Partitionierung und Replikation im Verzeichnisdienst

Bei einer Partitionierung SOLLTE auf die Verfügbarkeit und den Schutzbedarf des Verzeichnisdienstes geachtet werden. Die Partitionierung des Verzeichnisdienstes SOLLTE schriftlich dokumentiert werden, so dass sie manuell wieder rekonstruiert werden kann. Um die Replikationen zeitgerecht ausführen zu können, SOLLTE eine ausreichende Bandbreite sichergestellt werden.

APP.2.1.A9 Geeignete Auswahl von Komponenten für Verzeichnisdienste [Fachverantwortliche]

Für den Einsatz eines Verzeichnisdienstes SOLLTEN geeignete Komponenten identifiziert werden. Es SOLLTE ein Kriterienkatalog erstellt werden, aufgrund dessen die Komponenten für den Verzeichnisdienst ausgewählt und beschafft werden. Im Rahmen der Planung und Konzeption des Verzeichnisdienstes SOLLTEN Anforderungen an dessen Sicherheit in Abhängigkeit vom Einsatzzweck formuliert werden.

APP.2.1.A10 Schulung zu Administration und Betrieb von Verzeichnisdiensten

Die Administratoren SOLLTEN mit allen Sicherheitsmechanismen und -aspekten von Verzeichnisdiensten in ihrem Tätigkeitsbereich vertraut sein. Sie SOLLTEN vor der Einrichtung sowie anschließend regelmäßig hierzu geschult werden.

APP.2.1.A11 Einrichtung des Zugriffs auf Verzeichnisdienste

Der Zugriff auf den Verzeichnisdienst SOLLTE entsprechend der Sicherheitsrichtlinie konfiguriert werden. Wird der Verzeichnisdienst als Server im Internet eingesetzt, so SOLLTEN er entsprechend durch ein Sicherheitsgateway geschützt werden. Sollen anonymen Benutzern auf einzelne Teilbereiche des Verzeichnisbaums weitergehende Zugriffe eingeräumt werden, so SOLLTE ein gesondertes Benutzerkonto, ein sogenannter Proxy-User, für den anonymen Zugriff eingerichtet werden. Des Weiteren SOLLTEN die Zugriffsrechte für diesen Proxy-User hinreichend restriktiv vergeben werden. Sie SOLLTEN wieder komplett entzogen werden, wenn der Account nicht mehr gebraucht wird. Um die unnötige Herausgabe sicherheitssensitiver Informationen zu verhindern, SOLLTE die Suchfunktion des Verzeichnisdienstes dem Einsatzzweck angemessen eingeschränkt werden.

APP.2.1.A12 Überwachung von Verzeichnisdiensten

Zur Überwachung von Verzeichnisdiensten SOLLTE ein Überwachungskonzept entworfen und umgesetzt werden. Verzeichnisdienst-spezifische Ereignisse und Ereignisse des Betriebssystems SOLLTEN beobachtet, protokolliert und ausgewertet werden.

APP.2.1.A13 Absicherung der Kommunikation mit Verzeichnisdiensten

Der Datenaustausch zwischen Client und Verzeichnisdienst-Server SOLLTE abgesichert werden, dies gilt insbesondere bei Außenanbindungen. Es SOLLTE definiert werden, auf welche Daten zugegriffen werden darf. Im Falle einer serviceorientierten Architektur (SOA) SOLLTEN zum Schutz von Service-Einträgen in einer Service-Registry sämtliche Anfragen an die Registratur auf Gültigkeit des Benutzers überprüft werden.

APP.2.1.A14 Geregelte Außerbetriebnahme eines Verzeichnisdienstes [Fachverantwortliche]

Bei einer Außerbetriebnahme des Verzeichnisdienstes SOLLTE sichergestellt sein, dass weiterhin benötigte Rechte bzw. Informationen in ausreichendem Umfang zur Verfügung stehen, alle anderen aber gelöscht werden. Zudem SOLLTEN die Benutzer darüber informiert werden, wenn ein Verzeichnisdienst außer Betrieb genommen wird. Bei der Außerbetriebnahme einzelner Partitionen eines Verzeichnisdienstes SOLLTE darauf geachtet werden, dass dadurch andere Partitionen nicht beeinträchtigt werden.

APP.2.1.A15 Migration von Verzeichnisdiensten

Bei einer geplanten Migration von Verzeichnisdiensten SOLLTE vorab ein Migrationskonzept erstellt werden. Die Schema-Änderungen, die am Verzeichnisdienst vorgenommen wurden, SOLLTEN dokumentiert werden. Weitreichende Berechtigungen, die zur Durchführung der Migration des Verzeichnisdienstes verwendet wurden, SOLLTEN wieder zurückgesetzt werden. Die Zugriffsrechte für Verzeichnisdienst-Objekte bei Systemen, die von Vorgängerversionen aktualisiert bzw. von anderen Verzeichnissystemen übernommen wurden, SOLLTEN aktualisiert werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

APP.2.1.A16 Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes (CIA)

Im Rahmen der Notfallvorsorge SOLLTE eine bedarfsgerechte Notfallplanung für Verzeichnisdienste durchgeführt werden. Für den Ausfall wichtiger Verzeichnisdienst-Systeme SOLLTEN Notfallpläne vorliegen. Alle Notfall-Prozeduren für die gesamte Systemkonfiguration der Verzeichnisdienst-Komponenten SOLLTEN dokumentiert werden.

4 Weiterführende Informationen

4.1 Literatur

- [ISFTM12] The Standard of Good Practice - Area TM 1.2 Security Event Logging
  insbesondere Area TM 1.2 Security Event Logging, Information Security Forum (ISF), 06.2016

- [NISTSP800123] NIST Special Publication 800-123
  Guide to General Server Security, NIST, 07.2008
  https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

- [TKOM1] Telekom - Privacy and Security Assessment Verfahren
  Proxyserver, Deutsche Telekom, 10.2016
  https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/sicherheit/sicherheit/privacy-and-security-assessment-verfahren-342724

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Allgemeiner Verzeichnisdienst" von Bedeutung.

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.33 Personalausfall

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.38 Missbrauch personenbezogener Daten

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.42 Social Engineering

G 0.43 Einspielen von Nachrichten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.11	G 0.14	G 0.15	G 0.18	G 0.19	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.29	G 0.30	G 0.31	G 0.32	G 0.33	G 0.36	G 0.37	G 0.38	G 0.39	G 0.40	G 0.42	G 0.43	G 0.45	G 0.46
APP.2.1.A1				x				x						x	x											
APP.2.1.A2	x	x	x	x	x	x		x		x	x					x		x				x			x	x
APP.2.1.A3	x	x	x	x	x	x	x	x						x	x	x		x		x				x	x	x
APP.2.1.A4								x				x														
APP.2.1.A5	x			x					x	x				x	x					x						
APP.2.1.A6	x	x	x		x	x	x	x	x	x				x	x	x		x							x	x
APP.2.1.A7				x							x															
APP.2.1.A8	x			x					x		x															x
APP.2.1.A9				x							x															
APP.2.1.A10	x			x	x			x		x	x	x	x	x	x	x	x	x		x			x		x	x
APP.2.1.A11				x					x				x	x						x					x	x
APP.2.1.A12				x				x	x	x	x			x	x	x			x		x	x	x			
APP.2.1.A13		x	x					x						x	x			x		x					x	x
APP.2.1.A14				x					x						x							x			x	
APP.2.1.A15				x					x					x	x							x			x	
APP.2.1.A16	x			x						x																

APP.2: Verzeichnisdienst

APP.2.2 Active Directory

1 Beschreibung

1.1 Einleitung

Active Directory Services (oft als AD oder ADS abgekürzt) ist ein von Microsoft entwickelter Verzeichnisdienst, der mit dem Betriebssystem Windows 2000 Server erstmalig eingeführt wurde. Ausgehend von den Active Directory-Funktionen des Betriebssystems Microsoft Windows 2000 Server wurden dem Active Directory-Dienst mit jedem Release der Windows-Server-Familie weiteren Schlüsselfunktionen hinzugefügt.

Active Directory wird hauptsächlich in IT-Netzen mit überwiegend Microsoft-Komponenten eingesetzt. Active Directory speichert Informationen über Objekte innerhalb eines IT-Netzes, z. B. über Benutzer oder Computer, und erleichtert es Anwendern und Administratoren, diese Informationen bereitzustellen, zu organisieren, zu nutzen und zu überwachen. Als ein objektbasierter Verzeichnisdienst ermöglicht Active Directory die Verwaltung von Objekten und deren Beziehung untereinander, die die eigentliche Netzumgebung ausmachen. Active Directory stellt zentrale Steuerungs- und Kontrollmöglichkeiten des jeweiligen Netzes bereit. Der Einsatz eines solchen Verzeichnisdienstes bietet sich vor allem dort an, wo z. B. die Anzahl der im Netz eingesetzten Clients eine dezentrale Verwaltung erschwert. Ohne einen Verzeichnisdienst könnte die Zuverlässigkeit lokal vorzunehmender Einstellungen, wie z. B. Umsetzung der Vorgaben aus Sicherheitsrichtlinien, aufgrund des hohen personellen Aufwandes nicht mehr gewährleistet werden. Verwaltungsaufgaben innerhalb des Netzes wie z. B. Passwortänderungen, Kontenerstellung und Zugriffsrechte können durch den Einsatz eines Verzeichnisdienstes effizienter durchgeführt werden.

1.2 Zielsetzung

Dieser Baustein hat die Absicherung von Active Directory im Regelbetrieb einer Institution (Behörde oder Unternehmen) zum Ziel, die ADS zur Verwaltung ihrer Infrastruktur von Windows-Systemen (Client und Server) einsetzt.

1.3 Abgrenzung

In diesem Baustein werden die für Active Directory spezifischen Gefährdungen und Maßnahmen betrachtet. Allgemeine Sicherheitsempfehlungen zu Verzeichnisdiensten finden sich im Baustein APP.2.1 Allgemeiner Verzeichnisdienst. Die dort beschriebenen allgemeinen Maßnahmen werden im vorliegenden Baustein konkretisiert und ergänzt. Dieser Baustein wiederholt nicht die Anforderungen der Absicherung der Betriebssysteme der Server und Clients, die für den Betrieb und die Verwaltung des AD genutzt werden (z. B. SYS.1.2.2 Windows Server 2012 oder SYS.2.2.3 Client unter Windows 10) sowie der zugrundeliegenden Netzinfrastruktur. Auch Prozesse wie Datensicherung und Patchmanagement werden nur insofern behandelt, wie im Bereich AD Besonderheiten zu beachten sind.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Active Directory von besonderer Bedeutung:

2.1 Unzureichende Planung der Sicherheitsgrenzen

Eine AD-Instanz erzeugt einen Wald (Forest) als Container auf höchster Ebene für alle Domänen dieser Instanz. Ein Wald kann einen oder mehrere Domänen-Containerobjekte enthalten, die über eine gemeinsame logische Struktur, einen Global Catalog, ein Schema und automatische transitive Vertrauensbeziehungen verfügen. Der Wald stellt also die Sicherheitsgrenze dar, innerhalb derer Informationen standardmäßig im AD weitergegeben werden, nicht ein einzelner Baum. Wird diese Grenzen nicht bewusst und strukturiert geplant, kann es dazu kommen, dass Informationen ungewollt abfließen und das Sicherheitskonzept der Institution versagt. Daher kann es notwendig sein, weitere Forests aufzubauen, wenn für Teile der Infrastruktur unterschiedliche Sicherheitsanforderungen gelten. Dies bedeutet jedoch zusätzliche Komplexität in Einrichtung und Verwaltung.

2.2 Zu viele oder zu laxe Vertrauensbeziehungen

Werden die Vertrauensbeziehungen zwischen Wäldern und Domänen nicht regelmäßig daraufhin evaluiert, ob sie weiterhin benötigt und gerechtfertigt sind, ob sie den korrekten Typ haben (d. h. vor allem, ob eine zweiseitige Vertrauensbeziehung wirklich notwendig ist) und ob die Sicherheitskontrollen zu ihrer Gewährleistung ausreichend sind, können Probleme mit Berechtigungen auftreten und Informationen abfließen. Insbesondere wenn die standardmäßig aktive SID-(Security Identifier-)Filterung deaktiviert wird, können komplexe, schwer zu durchschauende Schwachstellen auftreten. Gleiches gilt für den Verzicht auf Selective Authentication bei Vertrauensbeziehungen zwischen Forests.

2.3 Fehlende Sicherheitsfunktionen durch ältere Betriebssysteme und Domain Functional Level

Jede neue Generation des Betriebssystems Windows Server bringt zusätzliche Sicherheitsfunktionen und -erweiterungen auch in Bezug auf AD mit. Außerdem werden in der Regel die Standardeinstellungen mit jedem neuen Release immer sicherer gesetzt. Einige davon sind verwendbar, sobald das neue System installiert ist, andere erst dann, wenn das Domänen-/Wald-Functional-Level angehoben wurde. Der Einsatz älterer Betriebssysteme als (primärer) Domänencontroller bzw. veralteter Domain Functional Level verhindert also die Nutzung zeitgemäßer Sicherheitsfunktionen und erhöht die Gefahr unsicherer Standardeinstellungen. Eine unsicher konfigurierte Domäne gefährdet die darin verarbeiteten Informationen und erleichtert Angriffe durch Dritte.

2.4 Betrieb weiterer Rollen und Dienste auf Domänencontrollern

Jeder weitere auf einem Domänencontroller betriebene Dienst, außer dem AD selbst sowie weniger dafür unbedingt benötigter Hilfsdienste wie etwa DNS, erhöht die Angriffsfläche dieser zentralen Infrastrukturkomponenten durch mögliche zusätzliche Schwachstellen und Fehlkonfigurationen. Diese können bewusst oder unbewusst missbraucht werden, um z. B. Informationen unberechtigt zu kopieren oder zu verändern.

2.5 Missbrauch der Gruppe der Domänenadministratoren

Das AD selbst sollte nur von einer sehr kleinen Zahl von Administratoren verwaltet werden. Häufig werden jedoch sehr viel mehr Konten als DA (Domänenadministrator) geführt. Diese haben volle administrative Rechte auf allen Domänencontrollern, Workstations, Gruppenrichtlinien etc. Dies eröffnet Angreifern unnötig viel Spielraum, wenn einer dieser Accounts übernommen werden kann. Häufig enthält die Gruppe der DA Dienstkonten und andere Gruppen, die nicht direkt mit der Verwaltung des AD selbst zu tun haben.

2.6 Unzureichende Überwachung und Dokumentation von delegierten Rechten

Wenn die Bildung unternehmensspezifischer Gruppen und die Delegation von Rechten an diese nicht systematisch geplant und umgesetzt wird, kann die Delegation außer Kontrolle geraten und viel mehr Zugriff einräumen als vorgesehen, was durch Dritte missbraucht werden kann. Ohne regelmäßige Auditierung der Gruppen und ihrer Zugriffsrechte drohen diese Rechte mit der Zeit auszuufern. Auch die Nutzung von Standardgruppen und Delegation derer Rechte an eigene Gruppen (etwa durch Delegation von "Account Operators" an Helpdesk-Mitarbeiter) gewähren in der Regel mehr Rechte als tatsächlich benötigt.

2.7 Unsichere Authentisierung

Sogenannte "Legacy" (also historische) Authentisierungsmechanismen im Bereich AD wie LM (LAN Manager) und NTLM (NT LAN Manager) v1 gelten heute als unsicher und können von Angreifern unter bestimmten Bedingungen leicht umgangen werden. Dadurch kann ein Angreifer Rechte erhalten und missbrauchen, ohne Benutzerpasswörter zu kennen, zu erraten oder anderweitig zu brechen und so die Domäne oder Teile von dieser kompromittieren.

2.8 Anmeldung von AD-Administratoren an Systemen niedriger Vertrauensstufen

Es muss davon ausgegangen werden, dass Schadcode auf verschiedene Systeme wie etwa normale Workstations oder Server gelangt. Ein Angreifer, der hierüber Zugriff erhält, wird nach weiteren Credentials suchen, die er missbrauchen kann. Melden sich privilegierte Accounts an allen möglichen IT-Systemen an, so erhält der Angreifer eine Vielzahl von Chancen, die Credentials abzugreifen und sich zusätzliche Berechtigungen zu verschaffen, insbesondere wenn die Credentials dort gecached werden.

2.9 Fehlende Überwachung der Mitgliedschaft in privilegierten Gruppen

In den meisten Institutionen wächst die Anzahl der Konten mit administrativen Rechten stetig an und wird selten oder nie bereinigt. Dies verletzt das Prinzip der minimalen Rechte (Least Privilege) und führt dazu, dass Angreifer immer mehr Möglichkeiten haben, sich zusätzliche Berechtigungen zu verschaffen und zu missbrauchen.

2.10 Zu mächtige oder schwach gesicherte Dienstkonten

Anbieter von Anwendungssoftware setzen manchmal DA-Rechte für Dienstkonten voraus, um das Testen und Ausbringen ihrer Produkte zu vereinfachen, obwohl für den Betrieb deutlich weniger Rechte notwendig wären. Die zusätzlichen Rechte des Dienstkontos können von Angreifern missbraucht werden, um sich in der Domäne weiterzubewegen. Da die Credentials eines Dienstes, der im Kontext eines Dienstkontos ausgeführt wird, im geschützten Speicher des LSASS vorgehalten werden, kann der Angreifer diese dort extrahieren. So kann ein einzelner schwach gesicherter Serviceaccount zur Kompromittierung der gesamten Domäne führen.

Insbesondere gilt dies, wenn das Dienstkonto mit einem schwachen Passwort gesichert ist. Denn ein Angreifer kann beim Einsatz von Kerberos-Authentisierung ohne weiteres ein TGS-(Ticket Granting Service)-Ticket anfordern, in welchem das Passwort des Dienstaccounts verarbeitet ist, und letzteres offline per Brute-Force brechen.

2.11 Nutzung desselben lokalen Administratorpasswords auf mehreren Systemen

Lokale Konten können sich auf einem System anmelden, auch wenn es nicht mit der Domäne verbunden ist. Werden dieselben Credentials auf mehreren Systemen verwendet, kann der Administrator sich auf den anderen Systemen ebenfalls anmelden. Damit steigt die Gefahr, dass ein Angreifer auf einem der Systeme Domänencredentials mit höheren Rechten findet und diese missbrauchen kann, um die Domäne zu kompromittieren.

2.12 Fehlende Entfernung nicht mehr verwendeter Konten aus dem AD

Angreifer können nicht mehr verwendete Accounts, die im AD aber noch vorhanden sind, bevorzugt für Angriffe zu nutzen versuchen, da ein Missbrauch mangels Eigentümer möglicherweise länger nicht bemerkt wird.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz von Active Directory aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der ISB ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Fachverantwortliche

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

APP.2.2.A1 Planung des Active Directory [Fachverantwortliche]

Es MUSS ein geeignetes, möglichst hohes Domain Functional Level gewählt. Die Begründung SOLLTE geeignet dokumentiert werden. Ein bedarfsgerechtes Active Directory-Berechtigungskonzept MUSS entworfen werden. Administrative Delegationen MÜSSEN mit restriktiven und bedarfsgerechten Berechtigungen ausgestattet sein. Die geplante Active Directory-Struktur einschließlich etwaiger Schema-Änderungen SOLLTE nachvollziehbar dokumentiert sein.

APP.2.2.A2 Planung der Active Directory-Administration [Fachverantwortliche]

Es MUSS ein rollenbasiertes Berechtigungskonzept erstellt werden. Alle administrativen Aufgabenbereiche und Berechtigungen SOLLTEN geeignet dokumentiert sein.

In großen Domänen MUSS eine Aufteilung der administrativen Benutzer bezüglich Diensteverwaltung und Datenverwaltung des Active Directory existieren. Zusätzlich MÜSSEN hier die administrativen Aufgaben im Active Directory nach einem Delegationsmodell überschneidungsfrei verteilt sein.

APP.2.2.A3 Planung der Gruppenrichtlinien unter Windows

Es MUSS ein Konzept zur Einrichtung von Gruppenrichtlinien vorliegen. Mehrfachüberdeckungen MÜSSEN beim Gruppenrichtlinienkonzept möglichst vermieden werden. Durch die Dokumentation des Gruppenrichtlinienkonzepts MÜSSEN Ausnahmeregelungen erkannt werden können. Alle Gruppenrichtlinienobjekte MÜSSEN durch restriktive Zugriffsrechte geschützt sein. Für die Parameter in allen Gruppenrichtlinienobjekten MÜSSEN sichere Vorgaben festgelegt sein.

APP.2.2.A4 Schulung zur Active Directory-Verwaltung

Die Administratoren MÜSSEN mit allen Sicherheitsmechanismen und -aspekten von Active Directory in ihrem Tätigkeitsbereich vertraut sein. Sie SOLLTEN für die Arbeit mit Active Directory vor der Einrichtung sowie regelmäßig geschult sein.

APP.2.2.A5 Härtung des Active Directory

Built-in-Accounts MÜSSEN mit komplexen Passwörtern versehen werden und ausschließlich als Notfallkonten dienen. Privilegierte Accounts MÜSSEN Mitglieder der Gruppe Protected Users sein. Für Dienstkonten MÜSSEN (Group) Managed Service Accounts verwendet werden.

Für alle Domänen-Controller MÜSSEN restriktive Zugriffsrechte auf Betriebssystemebene vergeben sein. Der Active Directory-Restore-Modus MUSS durch ein geeignetes Passwort geschützt sein. Arbeiten in diesem Modus SOLLTEN nur unter Einhaltung des Vier-Augen-Prinzips erfolgen.

Es SOLLTE regelmäßig ein Abbild des Domänencontrollers erstellt werden. Die Berechtigungen für die Gruppe "Jeder" MUSS beschränkt werden. Die Domänencontroller MUSS gegen unautorisierte Neustarts geschützt sein.

Die Richtlinien für Domänen und Domänencontroller MÜSSEN sichere Einstellungen für Kennworte, Kontensperrung, Kerberos-Authentisierung, Benutzerrechte und Überwachung umfassen. Eine ausreichende Größe für das Sicherheitsprotokoll des Domänen-Controllers MUSS eingestellt sein. Bei externen Vertrauensstellungen zu anderen Domänen MÜSSEN Autorisierungsdaten der Benutzer gefiltert und anonymisiert werden.

APP.2.2.A6 Aufrechterhaltung der Betriebssicherheit von Active Directory

Alle Vertrauensbeziehungen im AD MÜSSEN regelmäßig evaluiert werden.

Die Dienste-Administratoren auf dem Domänencontroller DÜRFEN nur die notwendigen Rechte besitzen. Diese Rechte MÜSSEN in regelmäßigen Abständen überprüft werden. Die Gruppe der Domänenadministratoren MUSS leer oder möglichst klein sein. Nicht mehr verwendete Konten MÜSSEN im AD deaktiviert oder gelöscht werden.

Alle notwendigen Parameter des Active Directory SOLLTEN als Basisinformationen aktuell und nachvollziehbar festgehalten werden.

APP.2.2.A7 Umsetzung sicherer Verwaltungsmethoden für Active Directory [Fachverantwortliche]

Administratorkonten DÜRFEN NICHT für die gewöhnliche tägliche Arbeit verwendet werden. Serveradministrator-Konten DÜRFEN NICHT auf Workstations verwendet werden. Domänenadministrator-Konten DÜRFEN NICHT auf Workstations oder Servern genutzt werden.

Jeder Account MUSS sich eindeutig einem Mitarbeiter zuordnen lassen.

Die Anzahl der Dienste-Administratoren und der Datenadministratoren des Active Directory MUSS auf das notwendige Minimum vertrauenswürdiger Personen reduziert sein. Ihre Konten MÜSSEN angemessen abgesichert sein.

Das Standardkonto "Administrator" SOLLTE umbenannt und ein unprivilegiertes Konto mit dem Namen "Administrator" SOLLTE erstellt sein. Alltägliche, nichtadministrative Aufgaben MÜSSEN mit unprivilegierten Benutzerkonten durchgeführt werden.

Es MUSS sichergestellt sein, dass die Verwaltung von Dienste-Administratorkonten ausschließlich von Mitgliedern der Dienste-Administratorgruppe erfolgt. Die Gruppe "Kontenoperatoren" SOLLTE leer sein.

Administratoren SOLLTEN der Gruppe "Schema-Admins" nur temporär für den Zeitraum der Schema-Änderungen zugewiesen werden. Für die Gruppen "Organisations-Admins" und "Domänen-Admins" zur Administration der Stammdomäne SOLLTE ein Vier-Augen-Prinzip etabliert sein.

Die Arbeitsplätze zur Administration des Active Directory MÜSSEN ausreichend abgesichert sein. Bei Remoteadministration der Domänen-Controller MUSS der Datenverkehr geeignet verschlüsselt sein.

Es MUSS sichergestellt sein, dass die Gruppen "Administratoren" bzw. "Domänenadministratoren" Besitzer des Domänenstammobjektes der jeweiligen Domäne sind.

Der Einsatz von domänenlokalen Gruppen für die Steuerung der Leseberechtigung für Objektattribute SOLLTE vermieden werden.

Der Papierkorb des AD SOLLTE aktiviert werden.

In großen Institutionen SOLLTE mit einer Enterprise Identity Management-Lösung sichergestellt werden, dass die Rechte aller Anwender definierten Vorgaben entsprechen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Active Directory. Sie SOLLTEN grundsätzlich umgesetzt werden.

APP.2.2.A8 Konfiguration des sicheren Kanals unter Windows

Der Sichere Kanal unter Windows SOLLTE entsprechend den Sicherheitsanforderungen und den lokalen Gegebenheiten konfiguriert sein. Dabei SOLLTEN alle relevanten Gruppenrichtlinienparameter berücksichtigt werden.

APP.2.2.A9 Schutz der Authentisierung beim Einsatz von Active Directory

In der Umgebung des Active Directory SOLLTE konsequent das Authentisierungsprotokoll Kerberos eingesetzt werden. Wenn aus Kompatibilitätsgründen übergangsweise NTLMv2 eingesetzt wird, SOLLTE die Migration auf Kerberos geplant und terminiert werden. Die LM-Authentisierung SOLLTE deaktiviert sein. Der SMB-Datenverkehr SOLLTE signiert sein. Anonyme Zugriffe auf Domänencontroller SOLLTEN unterbunden sein.

APP.2.2.A10 Sicherer Einsatz von DNS für Active Directory

Es SOLLTEN integrierte DNS-Zonen bzw. die sichere dynamische Aktualisierung der DNS-Daten verwendet werden, um DNS-Clientabfragen durch unautorisierte Systeme zu vermeiden. Der Zugriff auf die Konfigurationsdaten des DNS-Servers SOLLTE nur von administrativen Konten erlaubt sein. Der DNS-Cache auf den DNS-Servern SOLLTE vor unberechtigten Änderungen geschützt sein. Der Zugriff auf den DNS-Dienst der Domänen-Controller SOLLTE auf das notwendige Maß beschränkt sein. Die Netzaktivitäten in Bezug auf DNS-Anfragen SOLLTEN überwacht werden. Der Zugriff auf die DNS-Daten im Active Directory SOLLTE mittels ACLs auf Administratoren beschränkt sein.

Sekundäre DNS-Zonen SOLLTEN vermieden werden. Zumindest SOLLTE die Zonen-Datei vor unbefugtem Zugriff geschützt werden.

Wird IPsec eingesetzt, um die DNS-Kommunikation abzusichern, SOLLTE ein ausreichender Datendurchsatz im Netz gewährleistet sein.

APP.2.2.A11 Überwachung der Active Directory-Infrastruktur

Die Active Directory-Infrastruktur SOLLTE anhand der systemeigenen Ereignisse überwacht und protokolliert werden. Die Ergebnisse der Sicherheitsüberwachung des Active Directory SOLLTEN regelmäßig ausgewertet werden. Verfügbarkeit und Systemressourcen der Domänen-Controller SOLLTEN überwacht werden. Änderungen auf Domänen-Ebene und an der Gesamtstruktur des Active Directory SOLLTEN überwacht, protokolliert und ausgewertet werden.

APP.2.2.A12 Datensicherung für Domänen-Controller

Es SOLLTE eine Datensicherungs- und Wiederherstellungsrichtlinie für Domänen-Controller existieren. Die eingesetzte Sicherungssoftware SOLLTE explizit vom Hersteller für die Datensicherung von Domänen-Controllern freigegeben sein. Für die Domänen-Controller SOLLTE ein separates Datensicherungskonto mit Dienste-Administratorenrechten eingerichtet sein. Die Anzahl der Mitglieder der Gruppe "Sicherungs-Operatoren" SOLLTE auf das notwendige Maß begrenzt sein. Der Zugriff auf das AdminSD-Holder-Objekt SOLLTE zum Schutz der Berechtigungen besonders geschützt sein.

Die Daten der Domänen-Controller SOLLTEN in regelmäßigen Abständen gesichert werden. Dabei SOLLTE ein Verfahren eingesetzt werden, das veraltete Objekte weitgehend vermeidet.

Die Sicherungsmedien SOLLTEN an einem geeigneten Standort aufbewahrt werden. Der korrekte Ablauf und das Wiedereinspielen von Datensicherungen der Domänen-Controller SOLLTEN in regelmäßigen Abständen überprüft werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

APP.2.2.A13 Zwei-Faktor-Authentifizierung (CIA)

Privilegierte Konten im Bereich des AD SOLLTEN mittels Zwei-Faktor-Authentifizierung geschützt werden.

APP.2.2.A14 Dedizierte privilegierte Administrationssysteme (CIA)

Die Administration des Active Directory SOLLTE auf dedizierte Administrationssysteme eingeschränkt werden. Diese SOLLTEN durch die eingeschränkte Aufgabenstellung besonders stark gehärtet sein.

APP.2.2.A15 Trennung von Administrations- und Produktionsumgebung (CIA)

Besonders kritische Systeme, wie Domaincontroller und Systeme zur Administration der Domain, SOLLTEN in einen eigenen Forest ausgegliedert werden, der einen einseitigen Trust in Richtung des Produktions-Forests besitzt.

4 Weiterführende Informationen

4.1 Literatur

- [ADRL] AD Reading Library
  Mit weiterführender Literatur des AD Security Blogs, (zuletzt abgerufen am 28.09.2017)
  https://adsecurity.org/page_id=41

- [ADSB] Active Directory Security Blog
  Sean Metcalf, (zuletzt abgerufen am 28.09.2017)
  https://adsecurity.org

- [ADSR] Liste von Security Resourcen
  AD Security Blog (zuletzt abgerufen am 28.09.2017)
  https://adsecurity.org/page_id=399

- [ESAE] Enhanced Security Administrative Environment
  Microsoft TechNet (zuletzt abgerufen am 28.09.2017)
  https://docs.microsoft.com/de-de/
  windows-server/identity/securing-privileged-access/securing-privileged-access

- [PAW] Privileged Access Workstations
  Microsoft TechNet, 04.2016
  http://download.microsoft.com/download/9/3/9/9392A4D2-D530-4344-8447-4A7CF1C01AEE/
  Privileged%20Access%20Workstation_Datasheet.pdf

- [TN283324] Einstiegspunkt Active Directory für Windwos Server 2012 (R2)
  Microsoft TechNet, (zuletzt abgerufen am 28.09.2017)
  https://technet.microsoft.com/en-us/library/dn283324.aspx

- [TN378801] Einstiegspunkt Active Directory für Windows Server 2008 R2
  Microsoft TechNet, 05.2009
  https://technet.microsoft.com/en-us/library/dd378801.aspx

- [TNAD] Einstiegspunkt für Active Directoy für Windows Server aktuell
  Microsoft TechNet
  https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/active-directory-domain-services

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Active Directory" von Bedeutung.

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.33 Personalausfall

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.38 Missbrauch personenbezogener Daten

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.42 Social Engineering

G 0.43 Einspielen von Nachrichten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen Anforderungen	G 0.11	G 0.14	G 0.15	G 0.18	G 0.19	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.29	G 0.30	G 0.31	G 0.32	G 0.33	G 0.36	G 0.37	G 0.38	G 0.39	G 0.40	G 0.42	G 0.43	G 0.45	G 0.46
APP.2.2.A1	x	x	x	x	x	x		x		x	x					x		x				x			x	x
APP.2.2.A2	x	x	x	x	x	x	x	x						x	x	x		x		x				x		x
APP.2.2.A3		x	x	x	x	x		x								x		x						x		x
APP.2.2.A4	x			x	x			x		x	x	x	x	x	x	x	x			x			x		x	x
APP.2.2.A5		x	x		x	x	x	x				x	x	x		x		x	x	x	x	x		x	x	x
APP.2.2.A6		x	x		x	x	x	x				x	x	x		x		x	x	x	x	x		x	x	x
APP.2.2.A7	x	x	x	x	x	x	x	x						x	x	x		x		x				x		x
APP.2.2.A8		x	x		x	x	x	x						x				x						x		x
APP.2.2.A9		x	x		x	x	x	x						x				x						x		x
APP.2.2.A10								x						x								x	x	x	x	x
APP.2.2.A11				x				x	x	x	x			x	x	x			x		x	x	x			
APP.2.2.A12									x										x		x	x			x	
APP.2.2.A13					x	x	x	x						x					x							
APP.2.2.A14		x	x		x	x	x	x						x	x	x			x							
APP.2.2.A15		x	x		x	x	x	x						x	x	x			x							

APP.3: Netzbasierte Dienste

APP.3.1 Webanwendungen

1 Beschreibung

1.1 Einleitung

Webanwendungen stellen Funktionen und dynamische Inhalte über das Internetprotokoll HTTP (Hypertext Transfer Protocol) bzw. HTTPS (HTTP über SSL bzw. TLS, d. h. geschützt durch eine verschlüsselte Verbindung) zur Verfügung. Dazu werden auf einem Server Dokumente und Benutzeroberflächen (z. B. Eingabemasken) erzeugt und an entsprechende Clientprogramme (Webbrowser) ausgeliefert. Webanwendungen werden gewöhnlich auf der Grundlage von Frameworks entwickelt. Diese stellen ein Rahmenwerk für häufig wiederkehrende Aufgaben zur Verfügung (z. B. für Sicherheitskomponenten).

Um eine Webanwendung zu betreiben, sind in der Regel mehrere IT-Systemkomponenten notwendig. Hierzu gehören üblicherweise ein Webserver, um Daten auszuliefern, ein Applikationsserver, um die eigentliche Anwendung zu betreiben und zusätzliche Hintergrundsysteme, die als Datenquellen über unterschiedliche Schnittstellen angebunden sind (z. B. Datenbank oder Verzeichnisdienst).

Webanwendungen werden sowohl in öffentlichen IT-Netzen als auch in Firmennetzen (Intranet) eingesetzt, um Daten und Anwendungen bereitzustellen. Abhängig von dem Zweck der Webanwendungen werden diese in der Regel von Anwendern genutzt, die sich im Vorfeld authentisieren müssen. Dabei müssen Webanwendungen Sicherheitsmechanismen umsetzen, die den Schutz der Daten gewährleisten und deren Missbrauch verhindern. Typische Sicherheitskomponenten bzw. -mechanismen sind: Authentisierung, Autorisierung, Ein- und Ausgabevalidierung, Session-Management, Fehlerbehandlung und Protokollierung.

1.2 Zielsetzung

Ziel des Bausteins ist der sichere Betrieb von Webanwendungen sowie der Schutz von Informationen, die durch eine Webanwendung verarbeitet werden.

1.3 Abgrenzung

In diesem Baustein werden die für Webanwendungen spezifischen Gefährdungen und Anforderungen betrachtet. Während Webserver die Webseiten ausliefern (siehe auch APP.3.2 *Webserver*), stellen Webanwendungen Funktionen zur Verfügung und bereiten dynamische Inhalte vor, die durch den Webserver ausgeliefert werden. Der Baustein APP.3.2 *Webserver* beinhaltet auch die redaktionelle Planung des Webauftritts sowie das Notfallmanagement, diese Aspekte werden daher in diesem Baustein nicht nochmals behandelt. Auch die sicherheitsrelevanten Aspekte einer serviceorientierte Architektur (SOA) (siehe APP.3.7 *Serviceorientierte Architekturen*) werden im vorliegenden Baustein nicht betrachtet.

2 Gefährdungslage

Die folgenden spezifischen Bedrohungen und Schwachstellen sind im Bereich Webanwendungen von besonderer Bedeutung:

2.1 Mängel bei der Entwicklung und der Erweiterung von Webanwendungen

Wird eine Webanwendung mit fehlenden oder unzureichenden Vorgaben und Standards entwickelt bzw. erweitert, so kann dies zu Fehlern, Qualitätseinbußen oder einer unvollständig umgesetzten Funktionalität führen. Fehler, die in frühen Entwicklungsphasen gemacht werden, werden häufig erst in einem fortgeschrittenen Entwicklungsstadium entdeckt. Um diese Fehler nachträglich zu beheben, muss oft der Quellcode der Webanwendung aufwendig geprüft und wieder korrigiert werden. Dadurch können die Entwicklungskosten deutlich zunehmen. Im Fall von grundlegenden, architektonischen Fehlern muss die Webanwendung eventuell sogar komplett neu entwickelt werden. Gibt es darüber hinaus keine Vorgaben, um Sicherheitsmechanismen umzusetzen, kann der erforderliche Schutzbedarf der zu verarbeitenden Daten möglicherweise verletzt werden.

2.2 Umgehung der Autorisierung bei Webanwendungen

Angreifer versuchen häufig, auf Funktionen oder Daten von Webanwendungen zuzugreifen, die nur für eine eingeschränkte Benutzergruppe verfügbar sind. Ist die Autorisierung fehlerhaft umgesetzt, kann ein Angreifer die Berechtigungen eines anderen Benutzers mit umfangreicheren Rechten erlangen und auf geschützte Bereiche und Daten zugreifen. Das geschieht üblicherweise, indem ein Angreifer seine Eingaben gezielt manipuliert, indem er (nicht vorgesehene) Befehle oder Anweisungen in die Textfelder eingibt.

2.3 Unzureichende Validierung von Ein- und Ausgabedaten

Verarbeitet eine Webanwendung Eingangsdaten, die von einem Angreifer manipuliert wurden, können Schutzmechanismen umgangen werden. Auch die Ausgabedaten der Webanwendung werden entweder direkt an den Browser des Benutzers, die aufrufende Anwendung oder an nachgelagerte Systeme übermittelt. Werden die Daten vor der Ausgabe nicht ausreichend validiert, könnten sie Schadcode enthalten, der auf den Zielsystemen interpretiert oder ausgeführt wird.

2.4 Fehlende oder mangelhafte Fehlerbehandlung durch Webanwendungen

Treten Fehler während des Betriebs einer Webanwendung auf, kann das z. B. die Verfügbarkeit der Webanwendung bis zur Unerreichbarkeit einschränken. So werden eventuell Aktionen unvollständig durchgeführt, zwischengespeicherte Zustände und Daten gehen verloren oder Sicherheitsmechanismen fallen aus. Werden Fehler nicht korrekt behandelt, kann sowohl der Betrieb als auch der Schutz der Funktionen und Daten nicht mehr gewährleistet werden.

2.5 Unzureichende Protokollierung von sicherheitsrelevanten Ereignissen

Werden sicherheitsrelevante Ereignisse von der Webanwendung unzureichend protokolliert, können diese zu einem späteren Zeitpunkt nicht nachvollzogen und die Ursache nicht mehr ermittelt werden. Kritische Fehler und Angriffe, wie beispielsweise unbefugte Konfigurationsänderungen an der Webanwendung, bleiben unbemerkt und eine Schwachstelle kann dann nur noch schwer behoben werden.

2.6 Offenlegung sicherheitsrelevanter Informationen bei Webanwendungen

Webseiten und Daten, die von einer Webanwendung generiert und ausgeliefert werden, können Informationen zu den Hintergrundsystemen enthalten, z. B. Angaben zu IT-Komponenten und Versionsständen von Frameworks. Diese Informationen können einem Angreifer Hinweise für einen gezielten Angriff auf die Webanwendung geben.

2.7 Missbrauch einer Webanwendung durch automatisierte Nutzung

Wenn ein Angreifer Funktionen einer Webanwendung automatisiert nutzt, kann er zahlreiche Vorgänge in kurzer Zeit ausführen und so auf Wiederholung basierende Angriffe gegen die Webanwendung effizient durchführen. Mithilfe eines wiederholt durchgeführten Login-Prozesses können z. B. gültige Kombinationen aus Benutzernamen und Passwort systematisch ermittelt (Brute-Force) oder Listen mit gültigen Benutzernamen erzeugt werden (Enumeration). Darüber hinaus kann das wiederholte Aufrufen von ressourcenintensiven Funktionen (z. B. komplexe Datenbankabfragen) für Denial-of-Service-Angriffe auf Anwendungsebene missbraucht werden.

2.8 Unzureichendes Session-Management von Webanwendungen

Wenn eine unbefugte Person aufgrund eines unzureichenden Session-Managements die Session-ID eines Benutzers ermittelt, lässt sich damit die Webanwendung im Kontext dieser Sitzung verwenden. Hierdurch kann z. B. ein Angreifer mit der Webanwendung als legitimer authentisierter Benutzer interagieren, ohne die eigentlichen Zugangsdaten zu kennen. Bei einem Session-Fixation-Angriff lässt sich zum Beispiel ein Angreifer zunächst eine Session-ID von der Webanwendung zuweisen und übermittelt diese dem Opfer (zum Beispiel über einen Link in einer E-Mail). Folgt das Opfer diesem Link und authentisiert sich anschließend gegenüber der Webanwendung mit der vom Angreifer übermittelten Session-ID, so kann der Angreifer die Anwendung anschließend mit der ihm bekannten Session-ID verwenden. Auf diese Weise ist es ihm möglich, im Sicherheitskontext des angegriffenen Benutzers auf die Webanwendung zuzugreifen und so Funktionen zu nutzen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz von Webanwendungen aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Beschaffer, Entwickler, Leiter Entwicklung, Leiter IT, Tester

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

APP.3.1.A1 Authentisierung bei Webanwendungen [Entwickler]

Um auf geschützte Ressourcen einer Webanwendung zugreifen zu können, MÜSSEN sich Benutzer gegenüber der Anwendung authentisieren. Dafür MUSS eine geeignete Authentisierungsmethode ausgewählt und der Auswahlprozess dokumentiert werden. Wird die sogenannte Digest-Authentisierungsmethode verwendet, MÜSSEN die Passwortdateien auf dem Webserver ausreichend geschützt werden.

Es MUSS eine zentrale Authentisierungskomponente verwendet werden, die möglichst mit etablierten Standardkomponenten umgesetzt wurde. Die Komponente MUSS die Benutzer dazu zwingen, sichere Passwörter gemäß einer Passwort-Richtlinie zu benutzen. Speichert eine Webanwendung Authentisierungsdaten auf einem Client, MUSS der Benutzer explizit zustimmen ("Opt-In") und auf die Risiken der Funktion hingewiesen werden.

Um sicherzugehen, dass eine gültige Sitzung (Session-ID) nicht von einem Angreifer übernommen wurde, MÜSSEN sich bei kritischen Funktionen die Benutzer erneut authentisieren. Auch MÜSSEN in der Webanwendung Grenzwerte für fehlgeschlagene Anmeldeversuche definiert sein. Alle angebotenen Authentisierungsverfahren der Webanwendung MÜSSEN das gleiche Sicherheitsniveau aufweisen. Zudem MÜSSEN Benutzer sofort informiert werden, wenn das Passwort zurückgesetzt wurde.

APP.3.1.A2 Zugriffskontrolle bei Webanwendungen [Entwickler]

Darf nur ein beschränkter Benutzerkreis die Webanwendung nutzen, MUSS mittels einer Autorisierungskomponente sichergestellt werden, dass Benutzer nur solche Aktionen durchführen können, für die sie auch berechtigt sind. Jeder Zugriff auf geschützte Inhalte und Funktionen MUSS kontrolliert werden, bevor er ausgeführt wird.

Allen Benutzern MÜSSEN restriktive Zugriffsrechte ordnungsgemäß zugewiesen werden. Wenn Mitarbeiter für eine Webanwendung Zugriffsrechte erhalten oder sich diese verändern, MÜSSEN die Verantwortlichen dies prüfen, bestätigen und nachvollziehbar dokumentieren. Die Dokumentation der vergebenen Zugriffsrechte MUSS immer auf dem aktuellen Stand sein. Auch MUSS es ein geregeltes Verfahren geben, um Benutzern Zugriffsrechte wieder zu entziehen. Sollte es nicht möglich sein, Zugriffsrechte zuzuweisen, MUSS dafür ein zusätzliches Sicherheitsprodukt eingesetzt werden.

Es MÜSSEN alle von der Webanwendung verwalteten Ressourcen von der Autorisierungskomponente berücksichtigt werden. Die Benutzer MÜSSEN serverseitig und zentral auf einem vertrauenswürdigen IT-System autorisiert werden. Ist die Zugriffskontrolle fehlerhaft, MÜSSEN Zugriffe abgelehnt werden. Auch MUSS es eine Zugriffskontrolle bei URL-Aufrufen und Objekt-Referenzen geben. Ebenso MUSS der Zugriff auf Dateien durch die Benutzer mit restriktiven Dateisystemberechtigungen beschränkt werden und es MUSS ein sicherer Umgang mit temporären Dateien vorgesehen werden.

APP.3.1.A3 Sicheres Session-Management [Entwickler]

Session-IDs MÜSSEN geeignet geschützt werden. Sie MÜSSEN zufällig erzeugt werden (mit ausreichender Entropie) . Wenn das der Webanwendung zugrunde liegende Framework Session-IDs generieren kann, MUSS die Funktion des Frameworks verwendet werden. Werden Session-IDs mithilfe eines Frameworks verwaltet und erzeugt, so MUSS das Framework sicher konfiguriert werden. Auch MUSS die Session-ID ausreichend geschützt werden, wenn sie übertragen und clientseitig gespeichert wird.

Eine Webanwendung MUSS den Benutzern die Möglichkeit geben, eine bestehende Sitzung explizit zu beenden. Nachdem der Benutzer sich angemeldet hat, MUSS eine bereits bestehende Session-ID durch eine neue ersetzt werden. Die Sitzungsdauer MUSS beschränkt werden, z. B. indem inaktive Sitzungen automatisch nach einer bestimmten Zeit ungültig werden und eine maximale Gültigkeitsdauer vergeben wird (Timeout). Nachdem die Sitzung ungültig ist, MÜSSEN alle Sitzungsdaten (sowohl server- als auch clientseitig) ungültig und gelöscht sein.

APP.3.1.A4 Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen [Entwickler]

Es MUSS sichergestellt werden, dass eine Webanwendung ausschließlich vorgesehene Daten und Inhalte einbindet und an den Benutzer ausliefert. Wenn eine Webanwendung eine Upload-Funktion für Dateien anbietet, MUSS diese Funktion eingeschränkt werden (z. B. auf notwendige Dateitypen). Auch Zugriffs- und Ausführungsrechte MÜSSEN in diesem Fall restriktiv gesetzt werden. Zudem MUSS sichergestellt werden, dass ein Benutzer Dateien nur im vorgegebenen Pfad speichern kann.

Die Ziele der Weiterleitungsfunktion einer Webanwendung MÜSSEN ausreichend eingeschränkt werden, sodass Benutzer ausschließlich auf vertrauenswürdige Webseiten weitergeleitet werden. Verlässt ein Benutzer die Vertrauensdomäne, MUSS er informiert werden.

APP.3.1.A5 Protokollierung sicherheitsrelevanter Ereignisse von Webanwendungen [Entwickler]

Eine Webanwendung MUSS sicherheitsrelevante Ereignisse mit den erforderlichen Merkmalen nachvollziehbar protokollieren. Der Zugriff auf die Protokolldaten MUSS auf wenige befugte Personen eingeschränkt werden. Bei der Auswertung der Protokolldaten MUSS sichergestellt werden, dass Schadcode in Protokoll-Einträgen vom Auswertungsprogramm nicht interpretiert wird. Vertiefende Informationen sind in OPS.1.1.5 Protokollierung zu finden.

APP.3.1.A6 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates

Systemadministratoren MÜSSEN sich regelmäßig über aktuelle Schwachstellen informieren und sicherheitsrelevante Updates zeitnah einspielen. Software-Updates und Patches für Webanwendungen DÜRFEN nur aus vertrauenswürdigen Quellen bezogen werden. Sie MÜSSEN vor dem Roll-Out ausreichend getestet werden. Bevor Updates oder Patches installiert werden, MUSS stets sichergestellt sein, dass der ursprüngliche Zustand der Webanwendung wiederhergestellt werden kann. Der aktuelle Patchlevel MUSS dokumentiert werden.

APP.3.1.A7 Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen [Entwickler]

Webanwendungen MÜSSEN durch geeignete Schutzmechanismen vor automatisierten Zugriffen geschützt werden, z. B. indem Grenzwerte für die Anzahl der Zugriffsversuche in einer bestimmten Zeitspanne definiert werden. Dabei MUSS jedoch berücksichtigt werden, wie sich die Grenzwerte auf die Webanwendung auswirken, z. B. könnte es zu Funktionseinschränkungen für berechtigte Benutzer kommen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Webanwendungen. Sie SOLLTEN grundsätzlich umgesetzt werden.

APP.3.1.A8 Systemarchitektur einer Webanwendung

Bereits in der Entwurfsphase einer Webanwendung SOLLTEN Sicherheitsaspekte beachtet werden. Auch SOLLTE darauf geachtet werden, dass die Architektur der Webanwendung die Geschäftslogik der Institution exakt erfasst und korrekt umsetzt.

In der Systemarchitektur SOLLTE vorgesehen werden, die Serverdienste durch jeweils separate IT-Systeme voneinander zu trennen. Auch SOLLTEN jeweils eigene Benutzerkonten für die unterschiedlichen Serverprozesse der Systemkomponenten verwendet werden,. Dabei SOLLTEN die Rechte dieser Dienstekonten auf Betriebssystemebene soweit eingeschränkt werden, dass nur auf die erforderlichen Ressourcen und Dateien des Betriebssystems zugegriffen werden kann.

Die Netzarchitektur SOLLTE einen mehrschichtigen Ansatz verfolgen (Multi-Tier-Architektur). Dabei SOLLTEN mindestens die Sicherheitszonen Webschicht, Anwendungsschicht und Datenschicht berücksichtigt werden. Aus diesen Zonen SOLLTE NICHT auf Systeme im Intranet zugegriffen werden können.

Die Softwarearchitektur der Webanwendung SOLLTE mit allen Bestandteilen und Abhängigkeiten dokumentiert werden. Die Dokumentation SOLLTE bereits während des Projektverlaufs aktualisiert und angepasst werden, sodass sie schon in der Entwicklungsphase benutzt werden kann und Entscheidungsfindungen nachvollziehbar sind. Es SOLLTEN in der Dokumentation alle für den Betrieb notwendigen Komponenten, die nicht Bestandteil der Webanwendung sind, als solche gekennzeichnet werden. Ebenso SOLLTE daraus hervorgehen, welche Komponenten welche Sicherheitsmechanismen umsetzen, wie die Webanwendung in eine bestehende Infrastruktur integriert wird und welche kryptografischen Funktionen und Verfahren eingesetzt werden.

APP.3.1.A9 Beschaffung, Entwicklung und Erweiterung von Webanwendungen [Tester, Leiter Entwicklung, Beschaffer, Entwickler]

Wenn Produkte für Webanwendungen beschafft werden, SOLLTE ein Anforderungskatalog erstellt werden. Um verschiedene Produkte miteinander vergleichen zu können, SOLLTE eine Bewertungsskala entwickelt werden.

Wird die eigentliche Webanwendung oder eine Erweiterung hierzu eigenentwickelt, SOLLTE nach einem geeigneten Vorgehensmodell vorgegangen werden. Dabei SOLLTEN vor der Inbetriebnahme alle Phasen des Modells durchlaufen werden. Für die Entwicklung SOLLTEN zudem Programmierrichtlinien vorgegeben werden, die dabei helfen, ein einheitliches Sicherheitsniveau zu etablieren.

Wenn die Sicherheitsmechanismen einer Webanwendung entworfen und entwickelt werden, SOLLTEN diese möglichst zukünftige Standards und Angriffstechniken berücksichtigen. Bei der Anwendungsentwicklung SOLLTEN die Entwicklungs-, Test- und Produktivsysteme voneinander getrennt sein.

Falls die Webanwendung von einem Dienstleister entwickelt wird, SOLLTE sichergestellt werden, dass dieser Dienstleister die nötigen Sicherheitsanforderungen bei der Entwicklung umsetzt und der Auftraggeber jederzeit auf den Quelltext zugreifen kann.

APP.3.1.A10 Abnahme und Freigabe von Webanwendungen [Leiter IT]

Bevor Webanwendungen oder Erweiterungen, die entweder selbst oder im Auftrag entwickelt wurden, in den Echtbetrieb übernommen werden, SOLLTEN sie abgenommen werden. Dies gilt auch für Standardsoftware, die für den speziellen Einsatzzweck angepasst wird. Die Ergebnisse des Software-Abnahme-Verfahrens SOLLTEN dokumentiert werden. Nach der Abnahme SOLLTE die Webanwendung formal freigegeben werden. Falls im laufenden Betrieb Fehler festgestellt werden, SOLLTE es ein Verfahren zur Fehlerbehebung geben.

APP.3.1.A11 Sichere Anbindung von Hintergrundsystemen

Hintergrundsysteme von Webanwendungen, auf denen Funktionalitäten und Daten ausgelagert werden, SOLLTEN ausreichend geschützt werden. Der Zugriff auf Hintergrundsysteme SOLLTE ausschließlich über definierte Schnittstellen und von definierten Systemen aus möglich sein. Der Datenverkehr zwischen den Benutzern und der Webanwendung bzw. den Anwendungen und weiteren Diensten sowie den Hintergrundsystemen SOLLTE durch Sicherheitsgateways (Firewalls) reglementiert werden. Außerdem SOLLTE der Datenverkehr verschlüsselt werden. Zugriffe der Webanwendung auf Hintergrundsysteme SOLLTEN zudem mit minimalen Rechten erfolgen.

Beim Einsatz eines Enterprise Service Bus (ESB) muss sichergestellt werden, dass sich alle Dienste gegenüber dem ESB authentisieren, bevor ihnen ein Zugriff erlaubt wird. Es SOLLTE ein eigenes logisches Netzsegment für den ESB vorhanden sein. Der Zugriff auf den ESB SOLLTE ausschließlich durch die angeschlossenen Anwendungen und Dienste möglich sein. Alle Zugriffe auf den ESB SOLLTEN authentisiert und bei der Kommunikation über Standort- und Netzgrenzen hinweg verschlüsselt sein.

APP.3.1.A12 Sichere Konfiguration von Webanwendungen [Entwickler]

Eine Webanwendung SOLLTE so konfiguriert sein, dass auf ihre Ressourcen und Funktionen ausschließlich über die vorgesehenen, abgesicherten Kommunikationspfade zugegriffen werden kann. Der Zugriff auf nicht benötigte Ressourcen und Funktionen SOLLTE daher eingeschränkt werden. Folgendes SOLLTE bei der Konfiguration von Webanwendungen berücksichtigt werden:

- Deaktivierung nicht benötigter HTTP-Methoden
- Zeichenkodierungskonfiguration
- Festlegung von Grenzwerten
- Restriktive Dateisystemberechtigungen
- Administration einer Webanwendung

APP.3.1.A13 Restriktive Herausgabe sicherheitsrelevanter Informationen [Entwickler]

Webseiten und Rückantworten von Webanwendungen SOLLTEN keine Informationen beinhalten, die einem Angreifer Hinweise geben, mit denen er Sicherheitsmechanismen umgehen kann. Dazu SOLLTE mindestens gehören:

- neutrale Fehlermeldungen
- keine sicherheitsrelevanten Kommentare oder Produkt- und Versionsangaben
- eingeschränkter Zugriff auf sicherheitsrelevante Dokumentation
- regelmäßiges Löschen nicht benötigter Dateien
- sichere Erfassung durch externe Suchmaschinen sowie der Verzicht auf absolute Pfadangaben

Die Webanwendung SOLLTE NICHT aus unsicheren Netzen administriert werden. Administrationszugänge hierauf SOLLTEN auf vertrauenswürdige Netzsegmente und IT-Systeme, wie z. B. aus dem Administrationsnetz, beschränkt werden. Konfigurationsdateien der Webanwendung SOLLTEN außerhalb des Web-Root-Verzeichnisses gespeichert werden.

APP.3.1.A14 Schutz vertraulicher Daten [Entwickler]

Vertrauliche Daten einer Webanwendung SOLLTEN durch sichere, kryptographische Algorithmen geschützt werden. Werden solche Daten übertragen, SOLLTE zum Beispiel eine SSL/TLS-Verschlüsselung eingesetzt werden. Zudem SOLLTE die HTTP-Post-Methode verwendet werden. Im Fall von Verbindungsfehlern SOLLTE bei einem verschlüsselten Kanal NICHT auf einen unverschlüsselten gewechselt werden.

Auch SOLLTE die Webanwendung durch Direktiven gewährleisten, dass clientseitig keine schützenswerten Daten zwischengespeichert werden. Weiterhin SOLLTEN in Formularen keine vertraulichen Formulardaten im Klartext angezeigt und auch nicht vom Browser gespeichert werden. Zugangsdaten der Webanwendung SOLLTEN serverseitig mithilfe von kryptographischen Algorithmen vor unbefugtem Zugriff geschützt werden (Salted Hash). Ebenso SOLLTEN Dateien mit Quelltexten der Webanwendung nicht abgerufen werden können. Auch SOLLTEN Konfigurationsdateien von Webanwendungen ausschließlich außerhalb des Web-Root-Verzeichnisses gespeichert werden.

APP.3.1.A15 Verifikation essentieller Änderungen

Sollen wichtige Einträge geändert werden, wie beispielsweise Passwörter und Konfigurationen, SOLLTE die Eingabe durch ein Passwort erneut verifiziert werden. Die Benutzer SOLLTEN über Änderungen mittels Kommunikationswege außerhalb der Web-Anwendung informiert werden, beispielsweise per E-Mail.

APP.3.1.A16 Umfassende Ein- und Ausgabevalidierung [Entwickler]

Alle an eine Webanwendung übergebenen Daten SOLLTEN als potenziell gefährlich behandelt und entsprechend gefiltert werden. Dabei SOLLTEN alle Ein- und Ausgabedaten sowie Datenströme und Sekundärdaten (z. B. Session-IDs) validiert werden. Serverseitig SOLLTEN die Daten auf einem vertrauenswürdigen IT-System geprüft werden. Fehleingaben SOLLTEN möglichst nicht automatisch behandelt werden (engl. *Sanitizing*). Lässt es sich jedoch nicht vermeiden, SOLLTE *Sanitizing* sicher umgesetzt werden, damit ein Missbrauch ausgeschlossen ist.

APP.3.1.A17 Fehlerbehandlung [Entwickler]

Treten während des Betriebs einer Webanwendung Fehler auf, SOLLTEN diese so behandelt werden, dass die Webanwendung weiter in einem konsistenten Zustand verbleibt. Folgende Punkte SOLLTEN bei der Fehlerbehandlung berücksichtigt werden:

- vertrauliche Informationen in Fehlermeldungen sind zu vermeiden,
- Fehlermeldungen müssen protokolliert werden,
- eine veranlasste Aktion muss im Fehlerfall abgebrochen und
- in der Folge der Zugriff auf die angeforderte Ressource oder Funktion abgewiesen werden.

Zuvor reservierte Ressourcen SOLLTEN im Rahmen der Fehlerbehandlung wieder freigegeben werden. Auch SOLLTE der Fehler möglichst von der Webanwendung selbst behandelt werden.

APP.3.1.A18 Kontrolle der Protokolldateien

Es SOLLTE für jede Webanwendung ein Konzept erstellt werden, das festlegt, wie umfangreich die Protokollierung sein soll und wie die Daten auszuwerten sind. Zudem SOLLTE ein Verantwortlicher benannt werden, der die Protokolle auswertet. Die Ergebnisse SOLLTEN dem ISB oder einem anderen hierfür bestimmten Mitarbeiter vorgelegt werden. Weiterhin SOLLTEN bestehende gesetzliche Vorgaben in Bezug auf die Protokolldaten eingehalten werden, wie zum Beispiel datenschutzrechtliche Aspekte.

APP.3.1.A19 Schutz vor SQL-Injection

Webanwendungen SOLLTEN alle Eingaben und Parameter sorgfältig überprüfen und filtern, bevor diese an das Datenbanksystem weitergeleitet werden. Zudem SOLLTEN Stored Procedures bzw. Prepared SQL-Statements eingesetzt werden. Können Prepared SQL-Statements nicht eingesetzt werden, SOLLTEN die SQL-Queries separat abgesichert werden.Um potenziellen Angreifern keine Anhaltspunkte für Angriffe zu liefern, SOLLTEN Webanwendungen neutrale Fehlermeldungen nach außen ausgeben.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

APP.3.1.A20 Einsatz von Web Application Firewalls (CIA)

Damit Daten auf höheren Protokollebenen gefiltert werden können, SOLLTEN Institutionen auf Web Application Firewalls (WAF) zurückgreifen. Wird eine WAF eingesetzt, SOLLTE die Konfiguration auf die zu schützende Webanwendung angepasst werden. Die Konfiguration der WAF SOLLTE nach jedem Update der Webanwendung geprüft werden.

APP.3.1.A21 Verhinderung von Clickjacking [Entwickler] (CI)

Um Clickjacking-Angriffe zu vermeiden, SOLLTE sichergestellt sein, dass die Inhalte auf allen Webseiten der Webanwendung ausschließlich auf der obersten Ebene des Browser-Fensters angezeigt werden. Zudem SOLLTE in den HTTP-Response-Headern der Webanwendung die Direktive *X-FRAME-OPTIONS* gesetzt werden.

APP.3.1.A22 Durchführung von Penetrationstests (CIA)

Webanwendungen SOLLTEN regelmäßig Penetrationstest unterzogen werden. Penetrationstests SOLLTEN dabei ausschließlich von zuverlässigen, vertrauenswürdigen und qualifizierten Personal oder Dienstleistern durchgeführt werden. Im Vorfeld SOLLTEN mit allen Auftragnehmern für Penetrationstests detaillierte Vereinbarungen zur Durchführung und Auswertung der Tests getroffen werden. Auch SOLLTE das Einverständnis aller zuständigen Stellen eingeholt werden. Für den Testzeitraum SOLLTEN die jeweiligen Ansprechpartner verbindlich feststehen und auch erreichbar sein. Nach dem Penetrationstest SOLLTEN die Ergebnisse ausreichend geschützt und vertraulich behandelt werden. Der Abschlussbericht SOLLTE dem ISB und den verantwortlichen Führungskräften vorgelegt werden.

APP.3.1.A23 Verhinderung von Cross-Site Request Forgery [Entwickler] (CI)

Um Cross-Site-Request-Forgery-(CSFR)-Angriffe zu erschweren, SOLLTE die Webanwendung Sicherheitsmechanismen unterstützen, die es ermöglichen, beabsichtigte Seitenaufrufe des Benutzers von unbeabsichtigt weitergeleiteten Befehlen Dritter zu unterscheiden. Mindestens SOLLTE dabei geprüft werden, ob neben der Session-ID ein geheimes Token für den Zugriff auf geschützte Ressourcen und Funk-

tionen benötigt wird. Auch SOLLTE bei Webanwendungen das Referrer-Feld im HTTP-Request als zusätzliches Merkmal geprüft werden, um so einen beabsichtigten Aufruf durch einen Benutzer zu erkennen.

APP.3.1.A24 Verhinderung der Blockade von Ressourcen [Entwickler] (A)

Zum Schutz vor Denial-of-Service-(DoS)-Angriffen SOLLTEN ressourcenintensive Operationen vermieden und besonders abgesichert werden. Ebenso SOLLTE ein möglicher Überlauf von Protokolldaten bei Webanwendungen überwacht und verhindert werden. SOAP-Nachrichten SOLLTEN anhand eines entsprechenden XML-Schemas validiert werden. Bei kritischen Diensten und Anwendungen SOLLTE geprüft werden, mit Anti-DoS-Dienstleistern zusammenzuarbeiten.

4 Weiterführende Informationen

4.1 Literatur

- [HILWEB] Hilfmittel zur Nutzung des Bausteins Webanwendung
  BSI, (zuletzt abgerufen am 29.09.2017)
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Vorabversionen/Baustein_Webanwendungen_Hilfsmittel.pdf

- [OWASP] Open Web Application Security Project
  OWASP, (zuletzt abgerufen am 28.09.2017)
  https://www.owasp.org

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Webanwendungen" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.36 Identitätsdiebstahl

G 0.38 Missbrauch personenbezogener Daten

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.43 Einspielen von Nachrichten

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen Anforderungen	G 0.14	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.28	G 0.30	G 0.32	G 0.36	G 0.38	G 0.39	G 0.40	G 0.43	G 0.46
APP.3.1.A1	x		x			x	x		x	x	x	x				x
APP.3.1.A2	x		x			x	x		x	x	x	x				x
APP.3.1.A3	x		x			x	x		x	x	x	x			x	x
APP.3.1.A4	x		x		x	x	x		x	x	x	x			x	x
APP.3.1.A5		x					x		x		x					
APP.3.1.A6	x		x	x	x	x	x	x	x			x	x			x
APP.3.1.A7	x		x			x	x		x	x	x	x		x	x	x
APP.3.1.A8		x					x	x								
APP.3.1.A9		x		x	x			x								
APP.3.1.A10		x		x	x			x								
APP.3.1.A11	x		x		x		x		x	x	x	x			x	x
APP.3.1.A12	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x
APP.3.1.A13	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x
APP.3.1.A14	x		x			x	x		x	x	x	x			x	x
APP.3.1.A15						x	x		x	x	x					x
APP.3.1.A16	x					x	x						x		x	x
APP.3.1.A17			x		x									x		
APP.3.1.A18		x					x		x		x					
APP.3.1.A19	x		x		x	x	x		x	x	x	x			x	x
APP.3.1.A20	x		x		x	x	x		x	x	x	x	x	x	x	x
APP.3.1.A21			x							x	x					x
APP.3.1.A22	x		x		x	x	x	x	x	x	x	x	x	x	x	x
APP.3.1.A23	x		x			x	x		x	x	x	x	x			x
APP.3.1.A24														x		

APP.3: Netzbasierte Dienste

APP.3.2 Webserver

1 Beschreibung

1.1 Einleitung

Ein Webserver ist die Kernkomponente jedes Webangebotes: Er nimmt Anfragen der Clients (Browser) entgegen und liefert, sofern möglich, die entsprechenden Inhalte zurück. Der Transport der Daten erfolgt in der Regel über das Hypertext Transfer Protocol (HTTP) oder dessen mit Transport Layer Security (TLS) verschlüsselte Variante HTTP Secure (HTTPS). Da Webserver eine einfache Schnittstelle zwischen Serveranwendungen und Benutzern bieten, werden sie auch häufig für interne Informationen und Anwendungen in Institutionsnetzen (Intranet) eingesetzt.

Webserver sind (meistens) direkt im Internet verfügbar und bieten somit eine exponierte Angriffsfläche. Deswegen müssen sie durch geeignete Schutzmaßnahmen abgesichert werden.

1.2 Zielsetzung

Ziel des Bausteins ist der Schutz des Webservers und der Informationen, die durch den Webserver bereitgestellt werden.

1.3 Abgrenzung

Die Bezeichnung Webserver wird sowohl für die Software verwendet, die die HTTP-Anfragen beantwortet, als auch für die IT-Systeme, auf denen diese Software ausgeführt wird. In diesem Baustein wird vorrangig die Webserver-Software betrachtet. Sicherheitsaspekte des IT-Systems, auf dem die Webserver-Software installiert ist, werden in den entsprechenden Bausteinen der Schicht IT-Systeme behandelt (siehe SYS.1.1 *Allgemeiner Server* sowie beispielsweise SYS.1.3 *Server unter Linux oder* SYS.1.2.2 *Windows Server 2012*).

Empfehlungen, wie Webserver in die Netzarchitektur zu integrieren und mit Firewalls abzusichern sind, finden sich in den Bausteinen NET.1.1 *Netz-Architektur und Design* bzw. NET.3.2 *Firewall*.

Dynamische Inhalte und über HTML hinausgehende Funktionen werden durch Webanwendungen bzw. Webservices bereitgestellt. Diese sind nicht Gegenstand des vorliegenden Bausteins, sondern werden in den Bausteinen APP.3.1 *Webanwendungen* und APP.3.5 *Webservices* behandelt.

Der Baustein CON.1 *Kryptokonzept* beschreibt, wie kryptografische Schlüssel sicher verwaltet werden können.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Webserver von besonderer Bedeutung:

2.1 Reputationsverlust

Schaffen es Angreifer, eine Webseite zu manipulieren bzw. umzugestalten (Defacement), so kann der Ruf der Institution geschädigt werden. Ebenso kann die Veröffentlichung falscher Informationen (etwa fehlerhafter Produktbeschreibungen) dazu führen, dass die Reputation der Institution in der Öffentlichkeit verloren geht oder dass die Institution abgemahnt wird. Ein Schaden kann auch entstehen, wenn die Webseite nicht verfügbar ist und potenzielle Kunden deshalb zu Mitbewerbern wechseln.

2.2 Manipulation des Webservers

Ein Angreifer kann sich Zugang zu einem Webserver verschaffen, um dort Dateien zu manipulieren. Er könnte beispielsweise die Konfiguration ändern, zusätzliche Dienste starten, Schadsoftware installieren oder Webinhalte modifizieren. Er könnte auch Dateien, die zum Download angeboten werden, durch Dateien mit Schadprogrammen ersetzen. Auch kann ein Angreifer den manipulierten Server beispielsweise nutzen, um DDoS-Angriffe (DDoS, Distributed Denial of Service) auszuführen. Wird der eigene Server dazu benutzt, Schadsoftware zu verteilen, kann es passieren, dass der Webserver auf Blacklists geführt wird und für Besucher nicht mehr erreichbar ist.

2.3 Distributed Denial of Service (DDoS)

Durch DDoS-Angriffe kann ein Webserver teilweise oder auch ganz ausfallen. Für Benutzer ist das Webangebot dann nur noch sehr langsam oder gar nicht mehr verfügbar. Für viele Institutionen ist ein solcher Ausfall schnell geschäftskritisch, z. B. für einen Online-Shop.

Neben DDoS lässt sich auch mit anderen Arten von Denial-of-Service-Angriffen die Verfügbarkeit eines Webangebotes gezielt für einzelne Nutzer beeinträchtigen, indem beispielsweise einzelne Accounts durch fehlerhafte Anmeldungen gesperrt werden. Ein Angreifer könnte z. B. durch ungültige Anmeldeversuche eine Benutzerkontensperre auslösen.

2.4 Verlust vertraulicher Daten

Viele Webserver verwenden noch veraltete kryptografische Verfahren, wie RC4 oder SSL. Eine unzureichende Authentisierung bzw. eine ungeeignete Verschlüsselung kann dazu führen, dass Angreifer die Kommunikation zwischen den Clients und den Servern oder zwischen den Servern mitlesen oder ändern können.

2.5 Verstoß gegen Gesetze oder Regelungen

Verstöße gegen gesetzliche Regelungen, insbesondere gegen Telemedien- und Datenschutzgesetze, können rechtliche Konsequenzen nach sich ziehen. Ferner können die Webserverinhalte gegen das Urheberrecht verstoßen, etwa wenn Bilder verwendet werden, für die keine Rechte erworben worden sind.

2.6 Software-Schwachstellen oder -Fehler

Werden Updates und Patches für Webserver oder benutzte Erweiterungen nicht oder zu spät eingespielt, kann der Webserver erfolgreich angegriffen werden. Dadurch können Angreifer Dateien oder Dienste manipulieren oder den Webserver für weitere Angriffe missbrauchen.

2.7 Fehlende oder mangelhafte Fehlerbehebung

Treten Fehler während des Betriebs eines Webservers auf, kann sich das zum Beispiel auf die Verfügbarkeit des Webservers auswirken. Auch werden eventuell Inhalte unvollständig dargestellt oder Sicherheitsmechanismen fallen aus. Werden Fehler nicht korrekt behandelt, ist sowohl der Betrieb als auch der Schutz der Funktionen und Daten eines Webservers nicht mehr gewährleistet.

2.8 Unzureichende Protokollierung von sicherheitsrelevanten Ereignissen

Werden sicherheitsrelevante Ereignisse vom Webserver unzureichend protokolliert, können diese zu einem späteren Zeitpunkt nicht nachvollzogen und die Ursache nicht mehr ermittelt werden. Kritische Fehler und Angriffe, wie beispielsweise unbefugte Konfigurationsänderungen, bleiben so lange Zeit unbemerkt.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Webserver aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Fachverantwortliche, Informationssicherheitsbeauftragter (ISB), Leiter IT

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

APP.3.2.A1 Sichere Konfiguration eines Webservers

Nachdem ein Webserver installiert wurde, MUSS eine sichere Grundkonfiguration vorgenommen werden. Dazu MUSS beispielsweise der Webserver-Prozess einem Benutzerkonto mit minimalen Rechten zugewiesen werden. Auch MUSS der Webserver in einer gekapselten Umgebung ausgeführt werden, sofern dies vom Betriebssystem unterstützt wird. Der Webserver-Dienst DARF NICHT über unnötige Schreibberechtigungen verfügen. Nicht benötigte Module und Funktionen des Webservers MÜSSEN deaktiviert werden.

APP.3.2.A2 Schutz der Webserver-Dateien

Alle Dateien auf dem Webserver, insbesondere Skripte und Konfigurationsdateien, MÜSSEN so geschützt werden, dass sie nicht unbefugt gelesen und geändert werden können.

Es MUSS sichergestellt sein, dass die Webserver-Anwendung nur auf Dateien zugreifen kann, die sich innerhalb eines definierten Verzeichnisbaums (WWW-Wurzelverzeichnis) befinden. Ressourcen außerhalb des WWW-Verzeichnisses DÜRFEN NICHT aus diesem heraus verlinkt oder verknüpft werden.

Weiterhin MÜSSEN Funktionen, die Verzeichnisse auflisten, deaktiviert werden. Dateien, die nicht verändert werden sollen, MÜSSEN schreibgeschützt sein. Vertrauliche Daten MÜSSEN verschlüsselt übertragen und gespeichert werden.

APP.3.2.A3 Absicherung von Datei-Uploads und -Downloads

Alle mithilfe des Webservers veröffentlichten Dateien MÜSSEN vorher auf Schadprogramme geprüft werden. Zudem MÜSSEN Dokumente von Restinformationen bereinigt werden. Abrufbare Dateien MÜSSEN auf einer separaten Partition der Festplatte gespeichert sein.

Es MUSS eine Maximalgröße für Datei-Uploads spezifiziert sein. Für Uploads MUSS genügend Speicherplatz reserviert werden. Der Ablageort der Uploads MUSS zufällig erzeugt werden und DARF NICHT durch den Benutzer beeinflussbar sein.

APP.3.2.A4 Protokollierung von Ereignissen

Der Webserver MUSS mindestens folgende Ereignisse protokollieren:

- erfolgreiche Zugriffe auf Ressourcen,
- fehlgeschlagene Zugriffe auf Ressourcen aufgrund von mangelnder Berechtigung, nicht vorhandenen Ressourcen und Server-Fehlern sowie
- allgemeine Fehlermeldungen.

Die Protokollierungsdaten SOLLTEN regelmäßig ausgewertet werden.

APP.3.2.A5 Authentisierung

Wenn sich Clients am Webserver authentisieren, MUSS hierfür eine verschlüsselte Verbindung genutzt werden (siehe APP.3.2.A11 *Verschlüsselung über TLS*). Die Passwortdateien auf dem Webserver MÜSSEN kryptografisch gesichert und vor unbefugtem Zugriff geschützt gespeichert werden.

APP.3.2.A6 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates

Die verantwortlichen Mitarbeiter MÜSSEN sich regelmäßig bei verschiedenen Quellen über aktuelle Schwachstellen in der eingesetzten Webserver-Software informieren und sicherheitsrelevante Updates zeitnah einspielen. Software-Updates und Patches für Webserver sowie benutzte zusätzliche Anwendungen und Erweiterungen MÜSSEN ausschließlich aus vertrauenswürdigen Quellen bezogen werden und ausreichend getestet werden, bevor sie eingespielt bzw. eingesetzt werden. Bevor Updates oder Patches installiert werden, MUSS stets sichergestellt sein, dass der ursprüngliche Zustand des Webservers wiederhergestellt werden kann.

APP.3.2.A7 Rechtliche Rahmenbedingungen für Webangebote [Informationssicherheitsbeauftragter (ISB)]

Werden über den Webserver für Dritte Inhalte publiziert oder Dienste angeboten, MÜSSEN dabei verschiedene rechtliche Rahmenbedingungen beachtet werden. So MÜSSEN die jeweiligen Telemedien- und Datenschutzgesetze sowie das Urheberrecht eingehalten werden. Auch SOLLTEN die Anforderungen an die Barrierefreiheit gemäß Behindertengleichstellungsgesetz beachtet werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Webserver. Sie SOLLTEN grundsätzlich umgesetzt werden.

APP.3.2.A8 Planung des Einsatzes eines Webservers

Um geeignete Sicherheitsmaßnahmen für den Webserver auszuwählen, SOLLTE geplant und dokumentiert werden, für welchen Zweck er eingesetzt und wie der Webserver in die vorhandene IT-Infrastruktur integriert werden soll. In der Dokumentation SOLLTEN auch die Informationen oder Dienstleistungen des Webangebots und die jeweiligen Zielgruppen beschrieben werden. Für den technischen Betrieb und die Webinhalte SOLLTEN Verantwortliche festgelegt werden.

APP.3.2.A9 Festlegung einer Sicherheitsrichtlinie für den Webserver [Informationssicherheitsbeauftragter (ISB)]

Es SOLLTE eine Sicherheitsrichtlinie erstellt werden, in der die erforderlichen Maßnahmen und Verantwortlichkeiten benannt sind. Weiterhin SOLLTE geregelt werden, wie Informationen zu aktuellen Sicherheitslücken besorgt werden, wie Sicherheitsmaßnahmen umgesetzt werden und wie vorgegangen werden soll, wenn Sicherheitsvorfälle eintreten.

APP.3.2.A10 Auswahl eines geeigneten Webhosters [Informationssicherheitsbeauftragter (ISB), Leiter IT]

Wird der Webserver nicht von der Institutionen selbst betrieben, sondern werden Angebote externer Dienstleister genutzt (Webhosting), SOLLTE die Institution bei der Auswahl eines geeigneten Webhosters auf folgende Punkte achten:

- Es SOLLTE vertraglich geregelt werden, wie die Dienste zu erbringen sind. Dabei SOLLTEN Sicherheitsaspekte schriftlich im Vertrag in einem Service Level Agreement (SLA) festgehalten werden.
- Bei allen angebotenen Produkten SOLLTE die Basisinstallation sicher gestaltet werden. Der Dienstleister SOLLTE seine Kunden über die Risiken von zusätzlichen Anwendungen und Erweiterungen (Plug-ins) informieren. Darüber hinaus SOLLTE er sich dazu verpflichten, regelmäßig auf vorhandene Updates der genutzten Programme hinzuweisen.
- Die für die Diensterbringung eingesetzten IT-Systeme SOLLTEN vom Dienstleister regelmäßig kontrolliert und gewartet werden. Er SOLLTE dazu verpflichtet werden, bei technischen Problemen oder einer Kompromittierung von Kundensystemen zeitnah zu reagieren.
- Der Dienstleister SOLLTE grundlegende technische und organisatorische Maßnahmen umsetzen, um seinen Informationsverbund zu schützen.

APP.3.2.A11 Verschlüsselung über TLS

Der Webserver SOLLTE für alle Verbindungen eine Verschlüsselung über TLS anbieten (HTTPS). Wenn eine HTTPS-Verbindung angeboten wird, dann SOLLTEN alle Inhalte über HTTPS verfügbar sein. Sogenannter Mixed Content SOLLTE NICHT verwendet werden. Kritische Aktionen, wie die Anmeldung an einer Webanwendung (Login), SOLLTEN über HTTPS erfolgen.

APP.3.2.A12 Geeigneter Umgang mit Fehlern und Fehlermeldungen

Aus den HTTP-Informationen und den angezeigten Fehlermeldungen SOLLTEN NICHT der Name und die Version der Webserver-Software ersichtlich sein. Auch SOLLTE sichergestellt werden, dass der Webserver ausschließlich anwendungsspezifische Fehlermeldungen ausgibt, die der Information des Benutzers dienen. Bei unerwarteten Fehlern SOLLTE der Webserver in einen sicheren Zustand übergehen.

APP.3.2.A13 Zugriffskontrolle für Webcrawler

Der Zugriff von Webcrawlern SOLLTE nach dem Robots-Exclusion-Standard geregelt werden. Inhalte SOLLTEN mit einem Zugriffsschutz versehen werden (siehe APP.3.2.A5 *Authentisierung*), um sie vor Webcrawlern zu schützen, die sich nicht an diesen Standard halten.

APP.3.2.A14 Integritätsprüfungen und Schutz vor Schadsoftware

Es SOLLTE regelmäßig geprüft werden, ob die Dateien und Webinhalte noch integer sind und nicht durch Angreifer verändert wurden. Auch SOLLTEN die Dateien regelmäßig auf Schadsoftware geprüft werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

APP.3.2.A15 Redundanz (A)

Webserver SOLLTEN redundant ausgelegt werden. Auch die Internetanbindung des Webservers und weitere IT-Systeme, wie etwa der Webanwendungsserver, SOLLTEN redundant ausgelegt sein.

APP.3.2.A16 Penetetrationstest und Revision [Informationssicherheitsbeauftragter (ISB), Leiter IT] (CIA)

Es SOLLTEN regelmäßig Penetrationstests durchgeführt werden. Die Tests SOLLTEN dabei ausschließlich von zuverlässigen, vertrauenswürdigen und qualifizierten Mitarbeitern oder Dienstleistern durchgeführt werden. Im Vorfeld SOLLTEN mit allen Auftragnehmern für Penetrationstests detaillierte Vereinbarungen zur Durchführung und Auswertung der Tests getroffen werden. Auch SOLLTE das Einverständnis aller zuständigen Stellen eingeholt werden. Für den Testzeitraum SOLLTEN die jeweiligen Ansprechpartner verbindlich feststehen und auch erreichbar sein. Nach dem Penetrationstest SOLLTEN die Ergebnisse ausreichend geschützt und vertraulich behandelt werden. Der Abschlussbericht SOLLTE dem ISB vorgelegt werden.

APP.3.2.A17 Erweiterte Authentisierungsmethoden für Webserver (CI)

Es SOLLTEN erweiterte Authentisierungsmethoden eingesetzt werden, z. B. Client-Zertifikate oder Mehr-Faktor-Authentisierung.

APP.3.2.A18 Schutz vor Denial-of-Service-Angriffen (A)

Um Denial-of-Service-Angriffe frühzeitig erkennen zu können, SOLLTE der Webserver ständig überwacht werden. Des Weiteren SOLLTEN Maßnahmen definiert und umgesetzt werden, die solche Angriffe verhindern oder zumindest abschwächen.

APP.3.2.A19 Einrichtung eines Internet-Redaktionsteams [Fachverantwortliche, Leiter IT] (CIA)

Um Webangebote zu pflegen, SOLLTE eine eigenständige Internetredaktion eingerichtet werden. Die Internetredaktion SOLLTE alle Rollen enthalten, die im Konzept für Webangebote als Verantwortliche genannt wurden. Bei umfangreichen Webangeboten SOLLTE zusätzlich ein Ansprechpartner für Webanwendungen bestimmt werden. Ebenso SOLLTEN Prozesse, Vorgehensweisen und Verantwortliche benannt werden für den Fall von Problemen oder Sicherheitsvorfällen.

4 Weiterführende Informationen

4.1 Literatur

- [CS068] BSI-Veröffentlichung zur Cyber-Sicherheit und sicheres Webhosting
  Bundesamt für Sicherheit in der Informationstechnik (BSI), 08.2013
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_068.pdf

- [HVK] Hochverfügbarkeitskompendium
  BSI, (zuletzt abgerufen am 28.09.2017)
  https://www.bsi.bund.de/DE/
  Themen/Sicherheitsberatung/Hochverfuegbarkeit/HVKompendi-
  um/hvkompendium_node.html

- [ISIWEB] BSI-Standards zur Internetsicherheit, Sicheres Bereitstellen von Webangeboten
  Bundesamt für Sicherheit in der Informationstechnik (BSI), (zuletzt abgerufen am 29.08.2017)
  https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Web-
  Server/web_server_node.html

- [MLFTLS] BSI-Handlungsleitfaden, Migration auf TLS 1.2
  Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.2, 06.2016
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/
  Mindeststandards/Migrationsleitfaden_Mindeststandard_BSI_TLS_1_2_Version_1_2.pdf

- [NIST80044] NIST Special Publication (SP) 800-44
  Guideline on Securing Public Web Servers, NIST,09.2017
  https://csrc.nist.gov/publications/detail/sp/800-44/version-2/final

- [TR21022] BSI Technische Richtlinie, Kryptografische Verfahren
  Verwendung von Transport Layer Security (TLS), Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017
  https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an **grundschutz@bsi.bund.de** gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Webserver" von Bedeutung.

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen Anforderungen	G 0.11	G 0.15	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.29	G 0.30	G 0.31	G 0.39	G 0.40	G 0.46
APP.3.2.A1				X		X	X	X										X
APP.3.2.A2				X		X	X	X										X
APP.3.2.A3				X												X	X	
APP.3.2.A4										X				X				
APP.3.2.A5		X					X	X						X				
APP.3.2.A6					X	X						X						X
APP.3.2.A7													X					
APP.3.2.A8			X								X				X			
APP.3.2.A9			X								X				X			
APP.3.2.A10	X		X										X					
APP.3.2.A11		X																
APP.3.2.A12				X					X	X								
APP.3.2.A13														X				
APP.3.2.A14																X		X
APP.3.2.A15									X							X		
APP.3.2.A16							X	X				X						
APP.3.2.A17							X	X						X				
APP.3.2.A18									X	X							X	
APP.3.2.A19			X							X								

APP.3: Netzbasierte Dienste

APP.3.3 Fileserver

1 Beschreibung

1.1 Einleitung

Ein Fileserver (oder auch Dateiserver) ist ein Server in einem Netz, der Dateien für alle zugriffsberechtigten Benutzer bzw. Clients zentral bereitstellt. Die Datenbestände können von zugriffsberechtigten Benutzern gleichzeitig genutzt werden, ohne diese z. B. auf Wechseldatenträger zu transportieren oder per E-Mail zu verteilen. Dadurch, dass die Daten zentral vorgehalten werden, können die Daten strukturiert und in verschiedenen Dateiversionen bereitgestellt werden. Bei Fileservern können Rechte zentral vergeben werden und die Datensicherung kann an zentraler Stelle erfolgen.

Ein Fileserver verwaltet meistens Massenspeicher, die mit ihm über Schnittstellen wie SCSI (Small Computer System Interface) oder SAS (Serial Attached SCSI) verbunden sind. Die Speicher befinden sich entweder direkt im Gehäuse des Fileservers oder sind extern angeschlossen. Letzteres wird oft als Directly Attached Storage (DAS) bezeichnet. Ein Fileserver kann auf herkömmlicher Server-Hardware oder einer dedizierten Appliance, z. B. einem Network Attached Storage (NAS), betrieben werden. Oft können bei großen Datenmengen auch zentrale SAN-Speicher (Storage Area Network) über HBA (Host-Bus-Addapter) im Server und SAN Switche angebunden werden.

1.2 Zielsetzung

In diesem Baustein werden die für einen Fileserver spezifischen Gefährdungen und die sich daraus ergebenden Anforderungen für einen sicheren Betrieb beschrieben.

1.3 Abgrenzung

Der vorliegende Baustein enthält grundsätzliche Anforderungen, die beim Betrieb von Fileservern zu beachten und zu erfüllen sind. Allgemeine und betriebssystemspezifische Aspekte eines Servers sind nicht Gegenstand des vorliegenden Bausteins, sondern werden im Baustein SYS1.1 Allgemeiner Server und in den entsprechenden betriebssystemspezifischen Bausteinen der Schicht IT-Systeme behandelt, z. B. SYS.1.3 Unix Server oder SYS.1.2.2 Windows Server 2012. Des Weiteren werden keine Anforderungen an Speichersysteme bzw. Speichernetze beschrieben, diese sind im Baustein SYS.1.8 Speichersysteme zu finden. Auch wird nicht auf dedizierte Dienste eingegangen, mit denen ein Fileserver betrieben werden kann, z. B. Samba.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind bei Fileservern von besonderer Bedeutung:

2.1 Ausfall eines Fileservers

Fällt ein Fileserver aus, kann der gesamte Informationsverbund davon betroffen sein und damit auch wichtige Geschäftsprozesse der Institution. Neben den Benutzern können auch Anwendungen auf Daten vom Fileserver angewiesen sein, um ordnungsgemäß zu funktionieren. Ist die Verfügbar-

keit von Daten und Diensten nicht gegeben, können z. B. Fristen nicht eingehalten werden oder essenzielle Geschäftsprozesse fallen aus. Ist zudem kein Notfallmanagementkonzept umgesetzt, können sich Wiederanlaufzeiten weiter erhöhen. In vielen Fällen führt dies zu finanziellen Einbußen der Institution oder es wirkt sich auf andere Institutionen aus.

2.2 Unzureichende Dimensionierung des Fileservers

Wird die Leitungsanbindung oder Speicherkapazität des Fileservers unzureichend dimensioniert, können sich die Zugriffszeiten erhöhen oder es kommt zu Speicherengpässen. Dadurch besteht beispielsweise die Gefahr, dass Mitarbeiter aufgrund der längeren Wartezeiten frustriert sind und damit beginnen, Daten lokal zu speichern. So kann nicht mehr nachvollzogen werden, wo Daten gespeichert sind und wer in Besitz der Daten ist.

2.3 Unzureichende Überprüfung von abgelegten Dateien

Ist ein Fileserver unzureichend in das Konzept zum Schutz vor Schadprogrammen der Institution einbezogen, besteht die Gefahr, dass Angreifer unbemerkt Schadsoftware auf dem Fileserver platzieren. Dadurch können die Daten auf dem Fileserver unberechtigt eingesehen oder manipuliert werden. Es bestehen aber auch Sicherheitsrisiken für alle Geräte und Anwendungen, die auf die Daten des Fileservers zugreifen. So kann sich zum Beispiel Schadsoftware sehr schnell in der gesamten Institution ausbreiten.

2.4 Fehlendes oder unzureichendes Zugriffsberechtigungskonzept

Werden Zugriffsberechtigungen und Freigaben nicht ordnungsgemäß konzipiert und vergeben, können eventuell Dritte unbefugt auf Daten zugreifen. Dadurch können Angreifer Daten verändern, löschen oder kopieren.

2.5 Unstrukturierte Datenhaltung

Wird die Speicherstruktur nicht vorgegeben bzw. halten sich die Mitarbeiter nicht daran, können Daten unübersichtlich und unkoordiniert auf dem Fileserver gespeichert werden. Das führt zu verschiedenen Problemen, wie zum Beispiel Speicherplatzverschwendung durch Redundanz, unbefugte Zugriffe, wenn sich z. B. Dateien in Verzeichnissen oder Dateisystemen befinden, die Dritten zugänglich gemacht werden oder nicht konsistente Versionsstände.

2.6 Ungeeignete Aufstellung des Fileserver

Werden Fileserver an leicht zugänglichen Orten aufgestellt, können Angreifer direkt auf deren Komponenten und damit auf die gespeicherten Daten zugreifen, z. B. indem sie Laufwerke abziehen oder ausbauen und mitnehmen. Kleinere NAS-Systeme können zudem leicht komplett gestohlen werden. Ebenso ist es möglich, dass ein Angreifer die Zugriffsbeschränkungen am Fileserver direkt aushebelt und so schützenswerte Daten einsehen kann. Hat er erst einmal Zugriff, kann er auch Schadprogramme einspielen und so die Sicherheit des gesamten Netzes gefährden.

2.7 Fehlendes oder unzureichendes Datensicherungskonzept

Fällt ein Fileserver komplett aus, sind einzelne Komponenten defekt oder löscht ein Mitarbeiter Dateien unbeabsichtigt, können ohne ein funktionierendes Backup wichtige Daten verloren gehen. Sollte zudem kein RAID (Redundant Array of Independent Disks) eingesetzt werden, wirkt sich der Ausfall eines einzelnen Datenträgers direkt auf den laufenden Betrieb aus, da die Dateien nicht mehr verfügbar sind.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Fileserver aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Benutzer, Haustechnik

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

APP.3.3.A1 Geeignete Aufstellung [Haustechnik]

Fileserver DÜRFEN NICHT in Büroräumen oder als Arbeitsplatzrechner betrieben werden. Sie MÜSSEN an Orten aufgestellt werden, zu denen nur berechtigte Personen Zutritt haben. Zudem MUSS auf eine schwingungsfreie bzw. erschütterungsfreie Umgebung des Fileservers geachtet werden. Auch Fileserver mit weiteren Funktionen, wie NAS-Systeme kombiniert mit einem WLAN-Access-Point oder mit Direktanschlüssen für Speicherkarten, MÜSSEN geeignet aufgestellt werden. Des Weiteren MUSS eine sichere Stromversorgung und entsprechend den Herstellervorgaben empfohlene Umgebungstemperatur und Luftfeuchte sichergestellt sein.

APP.3.3.A2 Einsatz von RAID-Systemen

Es MUSS geplant werden, ob im Fileserver ein RAID-System eingesetzt wird. Eine Entscheidung gegen ein solches System MUSS nachvollziehbar dokumentiert werden. Wenn ein RAID-System eingesetzt werden soll, MUSS entschieden werden:

- welches RAID-Level benutzt werden soll, um die Datenträger logisch zusammenzufassen,
- wie lang die Zeitspanne für einen RAID-Rebuild-Prozess sein darf und
- ob ein Software- oder ein Hardware-RAID eingesetzt werden soll.

Die RAID-Level MÜSSEN dem Stand der Technik entsprechen. Bei einem Hardware-RAID SOLLTE der RAID-Controller redundant ausgelegt sein. In einem RAID SOLLTEN Hotspare-Festplatten vorgehalten werden.

APP.3.3.A3 Einsatz von Antiviren-Programmen

Je nach Betriebssystem und anderen vorhandenen Schutzmechanismen MUSS der Fileserver in das Konzept zum Schutz vor Schadprogrammen der Institution einbezogen werden. Das eingesetzte Antiviren-Programm MUSS die über den Fileserver freigegebenen Dateien regelmäßig überprüfen. Neben Echtzeit- und On-Demand-Scans MUSS die eingesetzte Lösung auch komprimierte Dateien nach Schadprogrammen durchsuchen können. Darüber hinaus SOLLTE sie auch verschlüsselte Dateien prüfen können.

Alle Daten MÜSSEN durch die Antiviren-Lösung auf Schadsoftware untersucht werden, bevor sie auf dem Speichermedium abgelegt werden. Sowohl die Virensignaturen als auch die Antiviren-Software selbst MÜSSEN laufend aktualisiert werden. Es MUSS sichergestellt sein, dass Benutzer keine sicherheitsrelevanten Änderungen an den Einstellungen der Antiviren-Lösung vornehmen können.

APP.3.3.A4 Regelmäßige Datensicherung

Es MÜSSEN regelmäßig alle auf dem Fileserver befindlichen Daten gesichert werden. Dazu MUSS ein Datensicherungskonzept erstellt werden, das unter anderem definiert, in welchen Intervallen das Backup durchgeführt werden soll. Außerdem MUSS eine Datensicherung durchgeführt werden, wenn auf dem Fileserver etwas installiert oder neu konfiguriert wird. Alle gesicherten Daten MÜSSEN sich jederzeit wiederherstellen lassen. Dabei SOLLTE die maximale Wiederanlaufzeit erhoben und im Datensicherungskonzept berücksichtigt werden.

APP.3.3.A5 Restriktive Rechtevergabe

Zugriffsrechte auf die vom Fileserver verwalteten Dateien MÜSSEN restriktiv vergeben werden. Es MUSS sichergestellt sein, dass jeder Benutzer nur auf die Daten zugreifen kann, die er benötigt, um seine Aufgaben zu erfüllen. Systemverzeichnisse und -dateien DÜRFEN NICHT für unbefugte Benutzer freigegeben werden.

Es MUSS regelmäßig überprüft werden, ob die Zugriffsberechtigungen noch aktuell sind und der Sicherheitsrichtlinie entsprechen. Zudem MUSS es einen definierten Prozess geben, um Berechtigungen neu einzurichten, zu ändern oder zu entziehen. Alle Zugriffsrechte MÜSSEN nachvollziehbar dokumentiert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Fileserver. Sie SOLLTEN grundsätzlich umgesetzt werden.

APP.3.3.A6 Beschaffung eines Fileservers

Bevor ein Fileserver beschafft wird, SOLLTE eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Die Leistung, die Speicherkapazität, die Bandbreite sowie die Anzahl der Benutzer, die den Fileserver nutzen sollen, SOLLTE bei der Beschaffung des Fileservers berücksichtigt werden.

APP.3.3.A7 Auswahl eines Dateisystems

Es SOLLTE eine Anforderungsliste erstellt werden, anhand derer die Dateisysteme bewertet werden. Um Transaktionssicherheit zu gewährleisten, SOLLTE das Dateisystem eine Journaling-Funktion bieten. Auch SOLLTE es über einen Schutzmechanismus verfügen, der verhindert, dass zwei Benutzer oder Anwendungen zur gleichen Zeit schreibend auf eine Datei zugreifen. Es SOLLTE ein Dateisystem ausgewählt werden, das eine festgelegte Overhead-Grenze nicht überschreitet. Für Hochverfügbarkeitslösungen SOLLTEN verteilte Dateisysteme verwendet werden.

APP.3.3.A8 Strukturierte Datenhaltung [Benutzer]

Es SOLLTE eine Struktur festgelegt werden, nach der Daten abzulegen sind. Benutzer SOLLTEN regelmäßig über die geforderte strukturierte Datenhaltung informiert werden. Es SOLLTE schriftlich festgelegt werden, welche Daten lokal und welche auf dem Fileserver gespeichert werden dürfen. Programm- und Arbeitsdaten SOLLTEN getrennt gespeichert werden. Es SOLLTE regelmäßig überprüft werden, ob die Vorgaben zur strukturierten Datenhaltung eingehalten werden.

APP.3.3.A9 Sicheres Speichermanagement

Es SOLLTEN alle Speicherressourcen des Fileservers katalogisiert werden, z. B. Festplatten, Flash-Speicher, Bandlaufwerke. Zudem SOLLTE regelmäßig überprüft werden, ob die Speicher noch wie vorgesehen funktionieren. Um bei Engpässen schnell reagieren zu können, SOLLTEN Ersatzspeicher vorgehalten werden.

Wurde eine Speicherhierarchie (Primär-, Sekundär- bzw. Tertiärspeicher) aufgebaut, SOLLTE ein (teil-)automatisiertes Speichermanagement verwendet werden. Werden Daten automatisiert verteilt, SOLLTE regelmäßig manuell überprüft werden, ob das korrekt funktioniert.

Weiterhin SOLLTEN die eingesetzten Speicher in das Protokollierungskonzept des Informationsverbunds einbezogen werden. Folgende Ereignisse SOLLTEN mindestens protokolliert werden:

- Aktivitäten (Modifizieren, Hinzufügen bzw. Löschen von Daten),
- nicht autorisierte Zugriffe auf Daten und
- Änderungen von Zugriffsrechten.

APP.3.3.A10 Regelmäßige Tests des Datensicherungs- bzw. Wiederherstellungskonzepts

Es SOLLTE regelmäßig getestet werden, ob die Datensicherung und -wiederherstellung korrekt funktioniert. Dafür SOLLTE ein Zeitplan ausgearbeitet werden. Es SOLLTEN genügend Ressourcen bereitgestellt werden, um die Tests planen, konzipieren und durchführen zu können.

Die Ergebnisse SOLLTEN ausreichend dokumentiert werden. Aufgedeckte Mängel SOLLTEN dazu führen, dass das Datensicherungskonzept überarbeitet wird.

APP.3.3.A11 Einsatz von Quotas

Es SOLLTE überlegt werden, Quotas einzurichten. Alternativ SOLLTEN Mechanismen des verwendeten Datei- oder Betriebssystemsystems genutzt werden, die die Benutzer bei einem bestimmten Füllstand der Festplatte warnen oder nur noch dem Systemadministrator Schreibrechte einräumen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

APP.3.3.A12 Verschlüsselung des Datenbestandes (CI)

Alle Daten auf dem Fileserver SOLLTEN verschlüsselt werden. Dazu SOLLTEN die Datenträger vollständig verschlüsselt werden. Es SOLLTE sichergestellt werden, dass der Virenschutz die verschlüsselte Dateien auf Schadsoftware prüfen kann.Kryptografische Schüssel SOLLTEN sicher erzeugt und von den Daten getrennt aufbewahrt werden (siehe auch CON.1 Kryptokonzept).

APP.3.3.A13 Replizieren zwischen Standorten (A)

Für hochverfügbare Systeme SOLLTE eine angemessene Replikation der Daten auf mehreren Datenträgern stattfinden. Daten SOLLTEN zudem zwischen unabhängigen Geräten oder unabhängigen Standorten repliziert werden. Dafür SOLLTE ein geeigneter Replikationsmechanismus ausgewählt werden. Damit die Replikation wie vorgesehen funktionieren kann, SOLLTEN hinreichend genaue Zeitdienste genutzt und betrieben werden.

APP.3.3.A14 Einsatz von Error-Correction-Codes (I)

Es SOLLTEN grundsätzlich fehlererkennende bzw. fehlerkorrigierende Codes eingesetzt werden, um Daten zu speichern. Die notwendigen redundanten Bits SOLLTEN bei der Planung miteinbezogen werden. Es SOLLTE beachtet werden, dass je nach eingesetztem Verfahren Fehler nur mit einer gewissen Wahrscheinlichkeit erkannt und auch nur in begrenzter Größenordnung behoben werden können.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [HVK] Hochverfügbarkeitskompendium
  BSI, (zuletzt abgerufen am 28.09.2017)
  https://www.bsi.bund.de/DE/
  Themen/Sicherheitsberatung/Hochverfuegbarkeit/HVKompendium/hvkompendium_node.html

- [NISTSP800123] NIST Special Publication 800-123
  Guide to General Server Security, NIST, 07.2008
  https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Fileserver" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.43 Einspielen von Nachrichten

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen Anforderungen	G 0.14	G 0.16	G 0.18	G 0.19	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.30	G 0.31	G 0.32	G 0.39	G 0.40	G 0.43	G 0.44	G 0.45	G 0.46
APP.3.3.A1		x						x	x								x		
APP.3.3.A2								x	x									x	
APP.3.3.A3	x	x		x	x	x	x							x	x	x		x	x
APP.3.3.A4								x	x									x	x
APP.3.3.A5				x	x	x	x				x	x	x						x
APP.3.3.A6			x					x	x	x									
APP.3.3.A7																		x	x
APP.3.3.A8				x						x								x	
APP.3.3.A9			x	x	x		x	x	x	x	x	x	x		x			x	x
APP.3.3.A10			x											x				x	
APP.3.3.A11								x		x									
APP.3.3.A12	x			x		x					x	x				x			
APP.3.3.A13								x	x									x	x
APP.3.3.A14								x	x									x	x

APP.3: Netzbasierte Dienste

APP.3.4 Samba

1 Beschreibung

1.1 Einleitung

Samba ist ein frei verfügbarer und vollwertiger Active Directory Domain Controller (AD DC), der Authentisierungs-, Datei- und Druckdienste bereitstellen kann und dadurch die Interoperabilität zwischen der Windows- und Unix-Welt ermöglicht. *Samba* führt viele unterschiedliche Protokolle und Techniken zusammen. Dazu gehört beispielsweise das *Server-Message-Block-(SMB)*-Protokoll, auch bekannt unter dem neueren Namen *Common Internet File System* (CIFS). Als *Samba*-Server werden Server bezeichnet, auf denen *Samba* betrieben wird. In der Regel sind das Linux-Server.

Wurde *Samba* korrekt konzipiert und ordentlich konfiguriert, interagiert die Anwendung mit einem Windows-Client oder -Server, als ob er selbst ein Windows-System wäre.

1.2 Zielsetzung

Ziel des Bausteins ist es darzustellen, wie *Samba* in Institutionen sicher eingesetzt werden kann und wie sich die durch Samba bereitgestellten Informationen schützen lassen.

1.3 Abgrenzung

Dieser Baustein betrachtet *Samba* als Authentisierungs-, Datei- und Druckdienst. Da *Samba* in der Regel auf Linux-Servern eingesetzt wird und dort aus der Windows-Server-Welt bekannte Dienste darstellt, sind die Sicherheitsaspekte der Bausteine SYS.1.1 *Allgemeiner Server* und SYS.2.1 *Server unter Linux* zu berücksichtigen. Sicherheitsanforderungen für Drucker, Fileserver oder Verzeichnisdienste sind dagegen nicht Bestandteil dieses Bausteins, sondern werden in den Bausteinen SYS.4.1 *Drucker, Kopierer und Multifunktionsgeräte*, APP.2.1 *Allgemeiner Verzeichnisdienst* und APP.3.6 *DNS-Server* sowie APP.2.3 *OpenLDAP*, auch wenn die *Samba*-internen DNS- und LDAP-Dienste verwendet werden, beschrieben. Des Weiteren sind aufgrund der *Samba*-Funktionen, die Bausteine APP.3.3 *Fileserver* und APP.2.2 *Active Directory* zu berücksichtigen.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich *Samba* von besonderer Bedeutung:

2.1 Abhören ungeschützter Kommunikationsverbindungen von Samba

Wenn Angreifer ungeschützte Kommunikationsverbindungen von *Samba* abhören, können Informationen abgefangen und missbraucht werden. Beim Dateitransfer zwischen Linux-Servern, Windows-Servern und Clients werden oftmals Protokolle ohne umfangreiche Sicherheitseigenschaften eingesetzt, sodass sowohl Authentifizierungs- als auch Nutzdaten für Dritte zugänglich sind und von Unberechtigten missbraucht werden könnten. Das kann dazu führen, dass schützenswerte Informationen aus der Institution fließen.

2.2 Fehlerhafte Protokollierung in Samba

Nicht sachgerecht gestaltete oder fehlende Protokollierung in *Samba* kann zu Sicherheitsproblemen führen. Ohne eine angemessene Protokollierung bleiben Fehler oder Angriffe unerkannt und es können keine Präventivmaßnahmen und Indikatoren für Frühwarnsysteme definiert werden.

2.3 Fehlerhafte Notfallvorsorge in Samba

Auch Defizite bei der Notfallvorsorge können zu längeren Ausfallzeiten von *Samba* führen. So kann sich etwa nach einen erfolgten Angriff eine notwendige Neuinstallation verzögern, wenn Installationspakete nicht verfügbar sind. Vorhandene Installationspakete können wiederum zu unerwünschten Ergebnissen führen, wenn keine Versionsverwaltung für die Konfigurationsdateien verwendet wurde oder Kompilierungs- sowie Installationsoptionen der *Samba*-Server nicht vorgehalten werden.

2.4 Fehlende Anpassung von Samba

Um einige Fähigkeiten des *Samba*-Servers zu zeigen und um den Administratoren einen schnellen Einstieg zu ermöglichen, wird während der Installation des *Samba*-Servers die Konfigurationsdatei *smb.conf* mit Standardeinstellungen erzeugt. Mit den in dieser Datei voreingestellten Optionen kann der *Samba*-Server im Anschluss gestartet werden. Wird diese Datei unbedacht ohne weitere Einstellungen benutzt, kann das zu erheblichen Sicherheitslücken führen. Doch auch wenn die Datei geändert wird, können Fehler auftreten, die dazu führen, dass vertrauliche Informationen eingesehen werden können oder dass die Sicherheit, die Verfügbarkeit und die Leistung der Dienste eines *Samba*-Servers beeinträchtigt werden.

2.5 Software-Schwachstellen oder -Fehler in Samba

Samba ist eine freie Software, die innerhalb einer Community erstellt und weiterentwickelt wird. Eine gleichmäßige Qualität des Quellcodes kann daher nicht gewährleistet werden. Das kann zu Software-Schwachstellen oder -Fehlern und damit zu schwerwiegenden Sicherheitslücken in der Anwendung oder allen damit vernetzten IT-Systemen führen. Angreifer können solche Sicherheitslücken für unterschiedliche Angriffe nutzen. So beispielsweise, um Schadsoftware einzuschleusen und damit möglicherweise unbefugt an schützenswerte Informationen, wie vertrauliche Daten oder Dokumente und Zugangsdaten, zu gelangen. Ferner können Angreifer über Sicherheitslücken IT-Systeme manipulieren, was dazu führen kann, dass sich diese nicht mehr benutzen lassen oder nur noch fehlerhaft funktionieren.

2.6 Unberechtigte Nutzung oder Administration von Samba

Unbefugte können durch die Nutzung von Anwendungen oder Systemen an vertrauliche Informationen gelangen, diese manipulieren oder Störungen verursachen, sodass sie *Samba* unberechtigt administrieren können. Besonders kritisch ist es, wenn Konfigurationswerkzeuge wie z. B. das *Samba Web Administration Tool* (SWAT) eingesetzt werden. SWAT war bis vor Version 4 ein fester Bestandteil von *Samba*, wurde aber von den *Samba*-Entwicklern gering priorisiert. Daher wurden auch schwächere oder gar keine Sicherheitsmechanismen implementiert, beispielsweise wurde HTTPS nicht unterstützt.

2.7 Fehlerhafte Administration von Samba

Sind die Administratoren mit den umfangreichen Funktionen, Komponenten, Optionen und Konfigurationseinstellungen von *Samba* zu wenig vertraut, kann dies zu weitreichenden Komplikationen führen. So können Fehlkonfigurationen des DNS oder des Benutzer- und Rechtemanagements dazu führen, dass Unbefugte auf Ressourcen zugreifen können. Des Weiteren kann dies zu Betriebsunterbrechungen führen oder es können schützenswerte Informationen offengelegt werden.

2.8 Schadprogramme im Umfeld von Samba-Diensten

Wird *Samba* auf Linux-Systemen als Dateiserver eingesetzt, dann ist der Server selbst nicht direkt anfällig für Windows-Schadprogramme. Diese können aber in infizierten Dateien enthalten sein, die darauf abgelegt sind. Durch das *Samba*-System werden dann diese infizierten Dateien allen angebundenen Windows-Clients bereitgestellt und somit aktiv verbreitet.

2.9 Datenverlust bei Samba

Ein Datenverlust wirkt sich erheblich auf den IT-Einsatz aus. Wenn geschäftsrelevante Informationen zerstört oder verfälscht werden, können dadurch Geschäftsprozesse und Fachaufgaben verzögert oder gar nicht mehr ausgeführt werden. Bei *Samba* ist beispielsweise zu beachten, dass sich die Eigenschaften der Dateisysteme unter Windows und Unix erheblich voneinander unterscheiden. Deswegen ist nicht immer sichergestellt, dass die Zugriffsrechte unter Windows aufrechterhalten bleiben. Auch können dadurch Informationen zu *Alternate Data Streams* (ADS) und DOS-Attributen verloren gehen.

2.10 Integritätsverlust schützenswerter Informationen bei Samba

Wenn Informationen nicht mehr integer sind, kann es dadurch zu vielen Problemen kommen. Informationen können dann im einfachsten Fall nicht mehr gelesen, also auch nicht mehr weiterverarbeitet werden. *Samba* selbst legt wichtige Betriebsdaten in Datenbanken im *Trivial-Database*-(TDB)-Format ab. Sollten diese Datenbanken vom Betriebssystems nicht ausreichend leistungsfähig und konsistent behandelt werden, können sie Probleme verursachen, wenn *Samba*-Dienste benutzt werden.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich *Samba* aufgeführt. Grundsätzlich ist der IT-Betrieb dafür zuständig, die Anforderungen zu erfüllen. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Leiter IT

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

APP.3.4.A1 Planung des Einsatzes eines Samba-Servers [Leiter IT]

Die Einführung eines *Samba*-Servers MUSS sorgfältig geplant und geregelt werden. Dabei MUSS abhängig vom Einsatzszenario definiert werden, welche Aufgaben der *Samba*-Server zukünftig erfüllen soll, in welcher Betriebsart er daher betrieben wird und welche Komponenten von *Samba* und welche weiteren Komponenten dafür erforderlich sind.

Soll die Cluster-Lösung CTDB (Cluster Trivia Data Base) eingesetzt werden, MUSS die Einführung von Samba sorgfältig konzeptioniert werden. Wenn *Samba* die Active-Directory-(AD)-Dienste auch für Linux- und Unix-Systeme bereitstellen soll, MUSS die Einführung sorgfältig geplant und die Installation getestet werden. Des Weiteren MUSS das Authentisierungsverfahren für das AD sorgfältig konzipiert und implementiert werden. Die Einführung und die Reihenfolge, in der die *Stackable-Virtual-File-System*-(VFS)-Module ausgeführt werden, MUSS sorgfältig konzipiert und die Umsetzung dokumentiert werden.

Wird IPv6 unter Samba benutzt, MUSS auch das sorgfältig geplant und zudem in einer betriebsnahen Testumgebung auf eine fehlerfreie Integration hin überprüft werden.

APP.3.4.A2 Sichere Grundkonfiguration eines Samba-Servers

Nachdem der *Samba*-Server installiert wurde, MUSS der Dienst sicher konfiguriert werden. Hierfür MÜSSEN unter anderem Einstellungen für die Zugriffskontrollen, aber auch Einstellungen, welche die Leistungsfähigkeit des Servers beeinflussen, angepasst werden. Es MUSS sichergestellt werden, dass die Zugriffsberechtigungen für jeden Benutzer individuell bestimmt werden.

Generell MUSS sichergestellt werden, dass nur ausgewählten Benutzern und Benutzergruppen erlaubt wird, sich mit dem *Samba*-Dienst zu verbinden und dass Benutzer nur auf die Informationen innerhalb ihrer Freigaben zugreifen können.

Samba MUSS so konfiguriert werden, dass Verbindungen nur von sicheren Hosts und Netzen entgegengenommen werden und dass es sich nur mit sicheren Netzadressen verbindet. Änderungen an der Konfiguration SOLLTEN sorgfältig dokumentiert werden, sodass zu jeder Zeit nachvollzogen werden kann, wer aus welchem Grund was geändert hat. Dabei MUSS nach jeder Änderung überprüft werden, ob die Syntax noch korrekt ist.

Zusätzliche Softwaremodule, wie SWAT, DÜRFEN NICHT installiert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Samba. Sie SOLLTEN grundsätzlich umgesetzt werden.

APP.3.4.A3 Sichere Konfiguration des Betriebssystems für einen Samba-Server

Datenbanken im Trivial-Database-(TDB)-Format SOLLTEN NICHT auf einer Partition gespeichert werden, die ReiserFS als Dateisystem benutzt. Wird eine *netlogon*-Freigabe konfiguriert, SOLLTEN unberechtigte Benutzer NICHT Dateien in dieser Freigabe modifizieren können.

Das Betriebssystem des *Samba*-Servers SOLLTE Access Control Lists (ACLs) in Verbindung mit dem eingesetzten Dateisystem unterstützen. Zusätzlich SOLLTE sichergestellt werden, dass das Dateisystem mit den passenden Parametern eingebunden wird.

Die Voreinstellungen von *SMB Message Signing* SOLLTEN beibehalten werden, sofern sie nicht im Widerspruch zu den existierenden Sicherheitsrichtlinien im Informationsverbund stehen. Mit einem lokalen Paketfilter SOLLTEN Ports, über die der *Samba*-Server nicht erreichbar sein soll, geblockt werden.

Es SOLLTE *Kerberos* eingesetzt werden, um die Schwachstellen von NT LAN-Manager (NTLM) oder NTLMv2 sowie eine zu hohe Netzlast zu vermeiden. Wird mit *Kerberos* authentisiert, SOLLTE der zentrale Zeitserver lokal auf dem Domain Controller installiert werden. Der NTP-Dienst SOLLTE so gehärtet werden, dass nur autorisierte Clients die Zeit abfragen können.

APP.3.4.A4 Sicherstellung der NTFS-Eigenschaften auf einem Samba-Server

Wird eine Version von *Samba* eingesetzt, die im *New Technology File System* (NTFS) sogenannte *Alternate Data Streams* (ADS) nicht abbilden kann, SOLLTE sichergestellt werden, dass Dateisystemobjekte keine ADS mit wichtigen Informationen enthalten, bevor diese über Systemgrenzen hinweg kopiert oder verschoben werden.

APP.3.4.A5 Sichere Konfiguration der Zugriffssteuerung bei einem Samba-Server

Die von *Samba* standardmäßig verwendeten Parameter, mit denen DOS-Attribute auf das Linux-Dateisystem abgebildet werden, SOLLTEN NICHT verwendet werden. Stattdessen SOLLTE *Samba* so konfiguriert werden, dass es DOS-Attribute und die Statusindikatoren zur Vererbung (Flag) in *Extended Attributes* speichert. Die Freigaben SOLLTEN ausschließlich über die Registry verwaltet werden.

Ferner SOLLTEN die effektiven Zugriffsberechtigungen auf die Freigaben des *Samba*-Servers ebenso wie die Protokolldateien regelmäßig überprüft werden.

APP.3.4.A6 Sichere Konfiguration von Winbind unter Samba

Der Einsatz von *Winbind* SOLLTE sorgfältig geplant und geregelt werden. Für jeden Windows-Domänenbenutzer SOLLTE im Betriebssystem des Servers ein Benutzerkonto mit allen Gruppenmitgliedschaften vorhanden sein. Falls das nicht möglich ist, SOLLTE *Winbind* eingesetzt werden. Dabei SOLLTE *Winbind* Domänen-Benutzernamen in eindeutige Linux-Benutzernamen umsetzen. Hierbei SOLLTE beachtet werden, dass Kollisionen zwischen lokalen Linux-Benutzern und Domänen-Benutzern verhindert werden.

Des Weiteren SOLLTEN die PAM (*Pluggable Authentication Modules*) eingebunden werden.

APP.3.4.A7 Sichere Konfiguration von DNS unter Samba

Wenn *Samba* als DNS-Server eingesetzt wird, SOLLTE die Einführung sorgfältig geplant und die Umsetzung vorab getestet werden.

Da *Samba* verschiedene AD-Integrationsmodi unterstützt, SOLLTEN die DNS-Einstellungen entsprechend dem Verwendungsszenario von *Samba* vorgenommen werden. Wird *Samba* als primärer AD DC verwendet, SOLLTE der DNS-Dienst auf dem *Samba*-Server installiert und sorgfältig konfiguriert werden.

APP.3.4.A8 Sichere Konfiguration von LDAP unter Samba

Werden die Benutzer unter *Samba* mit LDAP verwaltet, SOLLTE das sorgfältig geplant und dokumentiert werden. Die Zugriffsberechtigungen auf das LDAP SOLLTEN mittels ACLs geregelt werden.

APP.3.4.A9 Sichere Konfiguration von Kerberos unter Samba

Zur Authentisierung SOLLTE das von *Samba* implementierte *Heimdal Kerberos Key Distribution Center* (KDC) verwendet werden. Es SOLLTE darauf geachtet werden, dass die von *Samba* vorgegebene Kerberos-Konfigurationsdatei verwendet wird. Es SOLLTEN nur ausreichend sichere Verschlüsselungsverfahren für Kerberos-Tickets benutzt werden.

APP.3.4.A10 Sicherer Einsatz externer Programme auf einem Samba-Server

Da externe Programme Einfallstore für Angreifer bieten, SOLLTE sichergestellt werden, dass *Samba* nur überprüfte und vertrauenswürdige externe Programme aufruft.

APP.3.4.A11 Sicherer Einsatz von Kommunikationsprotokollen beim Einsatz eines Samba-Servers

Für ein zuverlässig funktionierendes Netz SOLLTEN auf den Windows-Clients nur wirklich benötigte Protokolle genutzt werden. Falls *Netware*-Systeme auf den *Samba*-Server zugreifen müssen, SOLLTE berücksichtigt werden, dass *Internetwork Packet Exchange* (IPX) benötigt wird. Sofern IPv6 eingesetzt wird, SOLLTEN erforderliche Besonderheiten berücksichtigt werden.

APP.3.4.A12 Schulung der Administratoren eines Samba-Servers

Administratoren SOLLTEN zu den genutzten spezifischen Bereichen von *Samba*, wie z. B. Benutzerauthentisierung, Windows- und Unix-Rechtemodelle, aber auch zu NTFS ACLs und NTFS ADS ausgebildet werden.

APP.3.4.A13 Regelmäßige Sicherung wichtiger Systemkomponenten eines Samba-Servers

Es SOLLTEN alle Systemkomponenten in das institutionsweite Datensicherungskonzept eingebunden werden, die erforderlich sind, um einen *Samba*-Server wiederherzustellen. Auch die Kontoinformationen aus allen eingesetzten Backends SOLLTEN berücksichtigt werden. Ebenso SOLLTEN alle TDB-Dateien gesichert werden. Des Weiteren SOLLTE die Registry mitgesichert werden, falls sie für Freigaben eingesetzt wurde.

Die Konfigurationsdaten, Statusinformationen und Systemdateien SOLLTEN kompatibel zueinander sein.

APP.3.4.A14 Erstellen eines Notfallplans für den Ausfall von Samba-Servern

Um den *Samba*-Server im Notfall schnell neu installieren zu können, SOLLTEN die notwendigen Installationspakete und Informationen an einem festgelegten Ort hinterlegt werden. Es SOLLTE gewährleistet sein, dass sie jederzeit verfügbar sind. Die Dokumentation der *Samba*-Konfiguration SOLLTE dabei stets aktuell und nachvollziehbar sein.

Für den *Samba*-Server SOLLTE abhängig von der Serverrolle und den Verfügbarkeitsanforderungen getestet werden, ob er sich wiederherstellen lässt und wie lange das dauert. Anhand der Ergebnisse SOLLTE der Notfallplan verbessert werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

APP.3.4.A15 Verschlüsselung der Datenpakete unter Samba (CI)

Um die Integrität und Vertraulichkeit der Datenpakete auf dem Transportweg zu gewährleisten, SOLLTEN die Datenpakete mit den in SBM3 integrierten Verschlüsselungsverfahren verschlüsselt werden.

4 Weiterführende Informationen

4.1 Literatur

- [SAMBA] Samba
  Opening Windows to a Wider World, SAMBA, (zuletzt abgerufen am 29.09.2017)
  https://www.samba.org/

- [UBUNTU] ubuntuuser
  Wiki Samba, (zuletzt abgerufen am 29.09.2017)
  https://wiki.ubuntuusers.de/Samba

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Samba" von Bedeutung.

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.15	G 0.18	G 0.19	G 0.28	G 0.30	G 0.31	G 0.39	G 0.40	G 0.45	G 0.46
APP.3.4.A1		x				x		x		
APP.3.4.A2		x				x	x	x		
APP.3.4.A3		x				x		x		
APP.3.4.A4		x				x			x	
APP.3.4.A5		x	x			x				x
APP.3.4.A6		x				x				
APP.3.4.A7	x				x					
APP.3.4.A8		x		x		x				
APP.3.4.A9	x	x	x			x				
APP.3.4.A10		x				x	x	x	x	
APP.3.4.A11		x							x	
APP.3.4.A12		x								x
APP.3.4.A13	x		x							
APP.3.4.A14								x		
APP.3.4.A15	x		x							x

APP.3: Netzbasierte Dienste

APP.3.6 DNS-Server

1 Beschreibung

1.1 Einleitung

In diesem Baustein werden die grundsätzlichen Sicherheitseigenschaften des Domain Name System (DNS) und der hierfür benötigten Server betrachtet. DNS ist ein Netzdienst, der dazu eingesetzt wird, Hostnamen von IT-Systemen in IP-Adressen umzuwandeln. Üblicherweise wird zu einem Hostnamen die entsprechende IP-Adresse gesucht (Vorwärtsauflösung). Ist hingegen die IP-Adresse bekannt und der Hostname wird gesucht, wird dies als Rückwärtsauflösung bezeichnet. DNS kann mit einem Telefonbuch verglichen werden, das Namen nicht in Telefonnummern, sondern in IP-Adressen auflöst. Welche Namen zu welchen IP-Adressen gehören, wird im Domain-Namensraum verwaltet. Dieser ist hierarchisch aufgebaut und wird von DNS-Servern zur Verfügung gestellt. DNS-Server verwalten den Domain-Namensraum im Internet, werden aber auch häufig im internen Netz der Institution eingesetzt. Auf den Rechnern der Benutzer sind standardmäßig sogenannte Resolver installiert, über die Anfragen an DNS-Server gestellt werden und die als Antwort Informationen über den Domain-Namensraum zurückliefern. Die Bezeichnung DNS-Server steht im eigentlichen Sinne für die verwendete Software, wird jedoch meist auch als Synonym für den Rechner benutzt, auf dem diese Software betrieben wird.

DNS-Server können nach ihren Aufgaben unterschieden werden, dabei gibt es grundsätzlich zwei verschiedenen Typen: Advertising DNS-Server und Resolving DNS-Server. Advertising DNS-Server sind üblicherweise dafür zuständig, Anfragen aus dem Internet zu verarbeiten. Resolving DNS-Server hingegen verarbeiten Anfragen aus dem internen Netz.

Ein Ausfall eines DNS-Servers kann sich gravierend auf den Betrieb einer IT-Infrastruktur auswirken. Dabei ist nicht direkt das ausgefallene DNS-System problematisch, sondern die daraus resultierende Einschränkung DNS-basierter Dienste. Unter Umständen sind Webserver, E-Mail-Server nicht mehr erreichbar und die Fernwartung funktioniert nicht mehr. Da DNS von sehr vielen Netzanwendungen benötigt wird, müssen laut Spezifikation (RFC 1034) mindestens zwei autoritative DNS-Server (Advertising DNS-Server) für jede Zone betrieben werden.

1.2 Zielsetzung

In diesem Baustein werden die für einen DNS-Server spezifischen Gefährdungen und die sich daraus ergebenden Anforderungen für einen sicheren Betrieb beschrieben.

1.3 Abgrenzung

Der vorliegende Baustein enthält grundsätzliche Anforderungen, die zu beachten und zu erfüllen sind, wenn eine Institution DNS-Server betreibt. Der Fokus liegt dabei auf der Verfügbarkeit von DNS-Servern, der Integrität der übertragenen Informationen sowie auf Problemen, die auftreten können, wenn DNS-Server betrieben werden. Allgemeine und betriebssystemspezifische Aspekte eines Servers sind jedoch nicht Gegenstand des vorliegenden Bausteins, sondern werden im Baustein SYS1.1. *Allgemeiner Server* und in den entsprechenden betriebssystemspezifischen Bausteinen der Schicht IT-Systeme behandelt, z. B. SYS.1.3 *Unix-Server* oder SYS.1.2.2 *Windows Server 2012*.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für DNS-Server von besonderer Bedeutung:

2.1 Ausfall des DNS-Servers

Fällt ein DNS-Server aus, kann der gesamte IT-Betrieb hiervon betroffen sein. Da Clients und andere Server der Institution dann nicht mehr in der Lage sind interne und externe Adressen aufzulösen, können keine Datenverbindungen mehr aufgebaut werden. Auch externe IT-Systeme, z. B. von mobilen Mitarbeitern, Kunden und Geschäftspartnern, können nicht auf die Server der Institution zugreifen, wodurch in der Regel essenzielle Geschäftsprozesse gestört sind.

2.2 Unzureichende Leitungskapazitäten

Reichen die Leitungskapazitäten für einen DNS-Server nicht aus, können sich die Zugriffszeiten auf interne und externe Dienste erhöhen. Dadurch sind diese eventuell nur eingeschränkt oder gar nicht mehr nutzbar. Auch können Angreifer den DNS-Server dann leichter durch einen Denial-of-Service-(DoS)-Angriff überlasten.

2.3 Fehlende oder unzureichende Planung des DNS-Einsatzes

Planungsfehler stellen sich oft als besonders schwerwiegend heraus, da leicht flächendeckende Sicherheitslücken geschaffen werden können. Wird der DNS-Einsatz nicht oder nur unzureichend geplant, kann dies zu Problemen und Sicherheitslücken im laufenden Betrieb führen. Sind beispielsweise die Firewall-Regeln, um DNS-Verkehr im Netz zu ermöglichen, zu freizügig definiert, kann dies unter Umständen einen Angriff ermöglichen. Sind die Regeln jedoch zu restriktiv formuliert, können legitime Clients keine Anfragen an die DNS-Server stellen und werden beeinträchtigt, wenn sie Dienste wie E-Mail, FTP oder Ähnlichem benutzen.

2.4 Fehlerhafte Domain-Informationen

Selbst wenn der DNS-Einsatz sorgfältig geplant und somit alle sicherheitsrelevanten Punkte berücksichtigt wurden, ist das nicht ausreichend, wenn semantisch und/oder syntaktisch fehlerhafte Domain-Informationen erstellt werden. Beispielsweise, wenn einem Hostnamen eine falsche IP-Adresse zugeordnet wird, Daten fehlen oder nicht erlaubte Zeichen verwendet werden oder die Vorwärts- und Rückwärtsauflösung inkonsistent ist. Enthalten Domain-Informationen Fehler, funktionieren Dienste, die diese Informationen benutzen, aufgrund der Falschinformationen nur eingeschränkt.

2.5 Fehlerhafte Konfiguration eines DNS-Servers

Sicherheitskritische Standardeinstellungen, selbst konfigurierte sicherheitskritische Einstellungen oder fehlerhafte Konfigurationen können dazu führen, dass ein DNS-Server nicht ordnungsgemäß funktioniert. Ist beispielsweise ein Resolving DNS-Server so konfiguriert, dass er rekursive Anfragen uneingeschränkt, also sowohl aus dem internen LAN als auch aus dem Internet, entgegennimmt, kann aufgrund der erhöhten Last die Verfügbarkeit des Servers stark beeinträchtigt sein. Zusätzlich könnte er dadurch anfällig für DNS-Reflection-Angriffe werden.

Ebenso besteht bei fehlerhaft konfigurierten DNS-Servern die Gefahr, dass die Zonentransfers nicht auf berechtigte DNS-Server beschränkt sind. Damit kann jeder Host, der die Möglichkeit hat, eine Anfrage an die DNS-Server zu stellen, die gesamten Domain-Informationen dieser Server auslesen. Die so gewonnenen Daten können spätere Angriffe erleichtern.

2.6 DNS-Manipulation

Mit einem DNS-Cache-Poisoning-Angriff wird das Ziel verfolgt, dass der angegriffene Rechner falsche Zuordnungen von IP-Adressen und Namen speichert. Dabei wird ausgenutzt, dass DNS-Server erhaltene Domain-Informationen für einen gewissen Zeitraum im Cache zwischenspeichern. Gefälschte Daten können sich so weit verbreiten. Werden entsprechende Anfragen an den manipulierten DNS-Server gestellt, liefert dieser als Antwort die gefälschten Daten. Der Empfänger der Antwort speichert diese zwi-

schen und sein Cache ist somit ebenfalls "vergiftet". Die gespeicherten Daten haben eine definierte Haltbarkeit (Time-To-Live, TTL). Wird der Resolving DNS-Server nach einer manipulierten Adresse gefragt, so wird er erst dann wieder einen anderen DNS-Server anfragen, wenn die Haltbarkeit abgelaufen ist. So ist es möglich, dass sich manipulierte DNS-Informationen lange halten, obwohl sie auf dem ursprünglich angegriffenen DNS-Server bereits wieder korrigiert sind. Gelingt es einem Angreifer beispielsweise die Namensauflösung für eine Domain zu übernehmen, indem er die Einträge so manipuliert, dass seine DNS-Server befragt werden, sind alle Subdomains automatisch mitbetroffen. DNS-Cache-Poisoning-Angriffe werden oft mit dem Ziel geführt, Anfragen auf maliziöse Server umzuleiten.

2.7 DNS-Hijacking

DNS-Hijacking ist eine Angriffsmethode, die verwendet wird, um die Kommunikation zwischen Advertising DNS-Servern und Resolvern über das IT-System eines Angreifers zu leiten. Dem Angreifer ist es mit dieser Man-in-the-Middle-Attacke möglich, die Kommunikation zwischen den Servern abzuhören und aufzuzeichnen. Die weitaus größere Gefahr besteht jedoch darin, dass ein erfolgreicher Angreifer jeglichen Verkehr der beiden Kommunikationspartner beliebig verändern kann. Wird nach einem erfolgreichen DNS-Hijacking-Angriff vom Resolver eines Client-IT-Systems eine Anfrage an einen DNS-Server gesendet, kann der Angreifer beispielsweise die Zuordnung von Namen und IP-Adresse abändern. DNS-Hijacking lässt sich auch mit anderen Angriffen kombinieren, besonders Phishing bietet sich in diesem Fall an.

2.8 DNS-DoS

Bei einem DoS-Angriff auf einen DNS-Server werden so viele Anfragen an diesen gesendet, dass die Netzverbindung zum DNS-Server bzw. der DNS-Server selbst überlastet wird. In der Regel werden die Anfragen über Botnetze versendet, um die notwendige Datenrate zu erreichen. Ein auf diese Weise überlasteter DNS-Server kann keine legitimen Anfragen mehr beantworten.

2.9 DNS-Reflection

Bei einem DNS-Reflection-Angriff handelt es sich um einen DoS-Angriff, bei dem nicht der DNS-Server, an den die Anfragen gestellt werden, das Ziel ist, sondern der Empfänger der Antworten. Es wird ausgenutzt, dass bestimmte Anfragen eine verhältnismäßig große Antwortdatenmenge erzeugen. Es ist dabei möglich, einen Verstärkungsfaktor von 100 und mehr zu erreichen. Das bedeutet, dass die Antwort, gemessen in Bytes, mindestens 100-mal größer ist als die Anfrage. Durch die Anzahl und Größe der Antworten wird die Netzbandbreite bzw. der Rechner selbst über die Leistungskapazität hinaus überlastet. Somit kann jede beliebige technische IT-Komponente das Angriffsziel sein (siehe 2.8 *DNS-DoS*). DNS-Reflection-Angriffe werden durch Open-Resolver begünstigt.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen an DNS-Server aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Leiter IT, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

APP.3.6.A1 Planung des DNS-Einsatzes

Da eine funktionierende Namensauflösung eine Grundvoraussetzung für viele Anwendungen und damit für einen reibungslosen Betrieb ist, MÜSSEN DNS-Server sorgfältig geplant werden. Dabei MUSS zunächst festgelegt werden, wie der Netzdienst DNS aufgebaut werden soll und welche Domain-Informationen schützenswert sind. Es MUSS auch geplant werden, wie DNS-Server in das Netz des Informationsverbundes eingebunden werden sollen. Die getroffenen Entscheidungen MÜSSEN dokumentiert werden.

APP.3.6.A2 Einsatz redundanter DNS-Server

Advertising DNS-Server (externe Anfragen) MÜSSEN redundant ausgelegt werden. Deshalb MUSS es für jeden Advertising DNS-Server mindestens einen zusätzlichen Secondary DNS-Server geben.

APP.3.6.A3 Verwendung von separaten DNS-Servern für interne und externe Anfragen

Advertising DNS-Server (externe Anfragen) und Resolving DNS-Server (interne Anfragen) MÜSSEN serverseitig getrennt sein. Die Resolver der internen IT-Systeme DÜRFEN NUR die internen Resolving DNS-Server verwenden, um Namen aufzulösen.

APP.3.6.A4 Sichere Grundkonfiguration eines DNS-Servers

Ein Resolving DNS-Server MUSS so konfiguriert werden, dass er ausschließlich Anfragen aus dem internen Netz akzeptiert. Wenn er Anfragen versendet, MUSS er zufällige Source Ports benutzen. Sind DNS-Server bekannt, die falsche Domain-Informationen liefern, MUSS der Resolving DNS-Server daran gehindert werden, Anfragen dorthin zu senden. Ein Advertising DNS-Server MUSS so konfiguriert werden, dass er Anfragen aus dem Internet immer iterativ behandelt.

Es MUSS sichergestellt werden, dass DNS-Zonentransfers zwischen Primary und Secondary DNS-Servern funktionieren. Zudem MÜSSEN Zonentransfers so konfiguriert werden, dass diese nur zwischen Primary und Secondary DNS-Servern möglich sind. Um Zonentransfers abzusichern, MÜSSEN diese auf bestimmte IP-Adressen beschränkt werden. Die Version des verwendeten DNS-Server-Produktes MUSS verborgen werden.

APP.3.6.A5 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates

Die verantwortlichen Mitarbeiter MÜSSEN sich regelmäßig bei verschiedenen Quellen über neu bekannt gewordene Schwachstellen im eingesetzten DNS-Server-Produkt informieren und sicherheitsrelevante Updates zeitnah einspielen. Vorab MUSS jedoch auf einem Testsystem überprüft werden, ob die Sicherheitsupdates kompatibel sind und keine Fehler verursachen. Solange keine Patches bei bekannten Schwachstellen verfügbar sind, MÜSSEN andere geeignete Maßnahmen getroffen werden, um die DNS-Server zu schützen. Bevor ein Patch eingespielt wird, MÜSSEN die Zonen- und Konfigurationsdateien gesichert werden.

APP.3.6.A6 Absicherung von dynamischen DNS-Updates

Um dynamische Updates sicher nutzen zu können, DÜRFEN NUR legitimierte IT-Systeme Domain-Informationen ändern. Auch MUSS festgelegt werden, welche Domain-Informationen die IT-Systeme ändern dürfen.

APP.3.6.A7 Überwachung von DNS-Servern

Um DNS-Server reibungslos zu betreiben und eventuelle Störungen oder Anomalien festzustellen, MÜSSEN diese laufend überwacht werden. Auch MUSS überwacht werden, wie ausgelastet die DNS-Server sind, um rechtzeitig die Leistungskapazität der Hardware anpassen zu können. Darüber hinaus MÜSSEN alle sicherheitsrelevanten Ereignisse an DNS-Servern geeignet protokolliert werden.

APP.3.6.A8 Verwaltung von Domainnamen [Leiter IT]

Es MUSS sichergestellt sein, dass die Registrierungen für alle Domains, die von einer Institution benutzt werden, regelmäßig und rechtzeitig verlängert werden. Es MUSS ein Mitarbeiter bestimmt werden, der dafür verantwortlich ist, die Internet-Domainnamen zu verwalten. Sofern ein Internetdienstleister mit der Domainverwaltung beauftragt wird, MUSS darauf geachtet werden, dass die Institution die Kontrolle über die Domains behält.

APP.3.6.A9 Erstellen eines Notfallplans für DNS-Server

Es MUSS ein Notfallplan für DNS-Server erstellt werden. Er MUSS in die bereits vorhandenen Notfallpläne der Institution integriert werden. Auch MUSS darin ein Datensicherungskonzept für die Zonen- und Konfigurationsdateien beschrieben sein, das in das existierende Datensicherungskonzept der Institution integriert werden MUSS. Der Notfallplan MUSS auch einen Wiederanlaufplan für DNS-Server enthalten.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich DNS-Server. Sie SOLLTEN grundsätzlich umgesetzt werden.

APP.3.6.A10 Auswahl eines geeigneten DNS-Server-Produktes

Wird ein DNS-Server-Produkt beschafft, SOLLTE darauf geachtet werden, dass sich damit alle Sicherheitsanforderungen der Institution geeignet umsetzen lassen. Das Produkt SOLLTE sich in der Praxis ausreichend bewährt haben und die aktuellen RFC-Standards unterstützen. Es SOLLTE den Verantwortlichen dabei unterstützen, syntaktisch korrekte Master Files zu erstellen. Außerdem SOLLTE für das ausgewählte DNS-Server-Produkt genügend geschultes Personal vorhanden sein.

APP.3.6.A11 Ausreichende Dimensionierung der DNS-Server

Da die Hardware eines DNS-Servers die Leistung des gesamten Systems beeinflusst, SOLLTE sie ausreichend dimensioniert sein. Auch SOLLTE die Hardware ausschließlich für den Betrieb eines DNS-Servers benutzt werden. Ebenso SOLLTE die Netzanbindung der DNS-Server ausreichend bemessen sein.

APP.3.6.A12 Schulung der Verantwortlichen [Vorgesetzte, Leiter IT]

Es SOLLTE durch Schulungen sichergestellt werden, dass die Verantwortlichen mit den einzelnen Konfigurationsmöglichkeiten und sicherheitsrelevanten Aspekten der DNS-Server vertraut sind.

APP.3.6.A13 Einschränkung der Sichtbarkeit von Domain-Informationen

Der Namensraum eines Informationsverbundes SOLLTE in einen öffentlichen und einen institutionsinternen Bereich aufgeteilt werden. Im öffentlichen Teil SOLLTEN nur solche Domain-Informationen enthalten sein, die von Diensten benötigt werden, die von extern erreichbar sein sollen. IT-Systeme im internen Netz SOLLTEN selbst dann keinen von außen auflösbaren DNS-Namen erhalten, wenn sie eine öffentliche IP-Adresse besitzen.

APP.3.6.A14 Platzierung der Nameserver

Primary und Secondary Advertising DNS-Server SOLLTEN in verschiedenen Netzsegmenten platziert werden.

APP.3.6.A15 Auswertung der Logdaten

Die Logdateien des DNS-Servers sowie des unterliegenden Betriebssystems SOLLTEN regelmäßig überprüft und ausgewertet werden.

APP.3.6.A16 Integration eines DNS-Servers in eine "P-A-P"-Struktur

Die DNS-Server SOLLTEN in eine "Paketfilter – Application-Level-Gateway – Paketfilter"-(P-A-P)-Struktur (siehe auch NET.3.2 *Firewall*) integriert werden: Der Advertising DNS-Server SOLLTE in diesem Fall in einer demilitarisierten Zone (DMZ) des äußeren Paketfilters angesiedelt sein. Der Resolving DNS-Server SOLLTE in einer DMZ des inneren Paketfilters aufgestellt sein.

APP.3.6.A17 Einsatz von DNSSEC

Die DNS-Protokollerweiterung DNSSEC SOLLTE sowohl auf Resolving DNS-Servern als auch auf Advertising DNS-Servern aktiviert werden. Die dabei verwendeten Schlüssel Key-Signing-Keys (KSK) und Zone-Signing-Key (ZSK) SOLLTEN regelmäßig gewechselt werden.

APP.3.6.A18 Erweiterte Absicherung von Zonentransfers

Um Zonentransfers stärker abzusichern, SOLLTEN zusätzlich Transaction Signatures (TSIG) eingesetzt werden.

APP.3.6.A19 Aussonderung von DNS-Servern

Wird ein DNS-Server ausgesondert, SOLLTEN alle Speichermedien des Servers sicher gelöscht werden. Außerdem SOLLTE der DNS-Server sowohl aus dem Domain-Namensraum als auch aus dem Netzverbund gelöscht werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

APP.3.6.A20 Prüfung des Notfallplans auf Durchführbarkeit (A)

Es SOLLTE regelmäßig überprüft werden, ob der Notfallplan durchführbar ist.

APP.3.6.A21 Hidden-Master (CIA)

Um Angriffe auf den primären Advertising DNS-Server zu erschweren, SOLLTE eine sogenannte Hidden-Master-Anordnung vorgenommen werden.

APP.3.6.A22 Anbindung der DNS-Server über unterschiedliche Provider [Leiter IT] (IA)

Extern erreichbare DNS-Server SOLLTEN über unterschiedliche Provider angebunden werden.

4 Weiterführende Informationen

4.1 Literatur

- [BSICS055] Sichere Bereitstellung von DNS-Diensten:
  Handlungsempfehlungen für Internet-Service-Provider (ISP) und große Unternehmen, BSI, 2013
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_055.pdf

- [BSIDNSSEC] Umsetzung von DNSSEC
  Handlungsempfehlungen zur Einrichtung und zum Betrieb der Domain Name Security Extensions, BSI, 2015
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/
  Cyber-Sicherheit/Themen/Umsetzung_von_DNSSEC.pdf

- [ISILANA] BSI-Standard zur Internet-Sicherheit (Isi-Reihe):
  Sichere Anbindung von lokalen Netzen an das Internet (Isi-LANA), Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014
  https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-LANA/lana_node.html

- [NIST800-81-2] NIST Special Publication 800-81-2:
  Secure Domain Name System (DNS) – Deployment Guide, NIST, 09.2013
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "DNS-Server" von Bedeutung.

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.43 Einspielen von Nachrichten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.09	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.30	G 0.31	G 0.32	G 0.40	G 0.43	G 0.45	G 0.46
APP.3.6.A1	x	x																
APP.3.6.A2								x	x	x					x			
APP.3.6.A3						x	x				x				x			
APP.3.6.A4			x			x	x								x	x	x	x
APP.3.6.A5				x	x		x				x							
APP.3.6.A6						x	x					x						x
APP.3.6.A7								x	x	x					x			
APP.3.6.A8		x																
APP.3.6.A9							x								x		x	
APP.3.6.A10				x	x						x							
APP.3.6.A11								x	x	x					x			
APP.3.6.A12		x											x	x				
APP.3.6.A13		x	x															
APP.3.6.A14		x	x			x	x	x	x	x					x			
APP.3.6.A15						x	x		x	x				x				
APP.3.6.A16						x	x					x				x		
APP.3.6.A17						x	x					x			x	x		x
APP.3.6.A18						x	x					x						x
APP.3.6.A19			x															
APP.3.6.A20							x	x	x	x					x		x	
APP.3.6.A21			x			x	x					x						
APP.3.6.A22	x																	

APP.4: Business-Anwendungen

APP.4.3 Relationale Datenbank-systeme

1 Beschreibung

1.1 Einleitung

Datenbanksysteme (DBS) sind ein weithin genutztes Hilfsmittel, um rechnergestützt große Datensammlungen zu organisieren, zu erzeugen, zu verändern und zu verwalten. Ein DBS besteht aus dem so genannten Datenbankmanagement-System (DBMS) und einer oder mehrerer Datenbanken. Eine Datenbank ist eine Zusammenstellung von Daten samt ihrer Beschreibung (Metadaten), die persistent im Datenbanksystem abgelegt werden. Da Datenbanksysteme einer zentralen Bedeutung in einer IT-Infrastruktur zukommt, ergeben sich wesentliche Sicherheitsanforderungen an sie. Meist sind Kernprozesse einer Institution von den Informationen aus den Datenbanken abhängig, wodurch sich entsprechende Verfügbarkeitsanforderungen ergeben. Zusätzlich bestehen oft hohe Anforderungen an Vertraulichkeit und Integrität der in den Datenbanken gespeicherten Informationen.

1.2 Zielsetzung

Ziel des Bausteins ist es, relationale Datenbanksysteme sicher betreiben zu können sowie die Informationen, die in Datenbanken verarbeitet und gespeichert werden, angemessen zu schützen. Dazu werden Anforderungen beschrieben, mit denen sich Datenbanksysteme sicher planen, umsetzen und betreiben lassen und durch die spezifische Gefährdungen reduziert werden können.

1.3 Abgrenzung

In diesem Baustein werden Anforderungen an relationale Datenbanksysteme beschrieben. Sicherheitsanforderungen an nicht-relationale Datenbanksysteme sind nicht Gegenstand des vorliegenden Bausteins, sondern werden im Baustein APP.4.5 *Nicht-Relationale Datenbanksysteme* aufgeführt.

Um die Informationen in den Datenbanken durchgängig zu schützen, sollten bereits in der Anwendungsentwicklung Sicherheitsanforderungen an den Aufbau der Datenbanktabellen und den Zugriff auf die Datenbank beachtet werden. Anforderungen hierzu werden jedoch nicht in diesem Baustein aufgeführt, sondern finden sich z. B. in CON.3 *Softwareentwicklung*, APP.3.1 *Web-Anwendungen* sowie APP.3.5 *Webservices*.

Ebenso geht der Baustein nicht auf Gefährdungen und Anforderungen ein, die das dem Datenbanksystem zugrunde liegende Betriebssystem und die Hardware betreffen. Aspekte hierzu finden sich in den entsprechenden betriebssystemspezifischen Bausteinen der Schicht IT-Systeme, z. B. SYS.1.3 *Unix-Server* oder SYS.1.2.2 *Windows Server 2012*.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich relationale Datenbanksysteme von besonderer Bedeutung:

2.1 Unzureichende Dimensionierung der Systemressourcen

Verfügt die Hardware eines Datenbanksystems nicht über genügend Systemressourcen, besteht die Gefahr, dass die Datenbank ganz ausfällt oder fehlerhaft arbeitet. Dadurch können beispielsweise Daten nicht gespeichert werden. Auch können in Stoßzeiten die Ressourcen stark ausgelastet werden und sich dadurch die Performance verschlechtern. Dies wiederum kann dazu führen, dass Anwendungen nicht oder nicht fehlerfrei ausgeführt werden.

2.2 Aktivierte Standard-Benutzerkonten

Bei der Erstinstallation bzw. im Auslieferungszustand eines Datenbankmanagementsystems sind Benutzer- und Administrationskonten häufig nicht oder nur mit Passwörtern gesichert, die öffentlich bekannt sind. Dadurch besteht die Gefahr, dass diese Konten missbräuchlich genutzt werden. Beispielsweise kann sich ein Angreifer mit den öffentlich bekannten Anmeldedaten am Datenbankmanagementsystem als Benutzer oder sogar als Administrator anmelden. Danach kann er die Konfiguration oder die gespeicherten Daten auslesen, manipulieren oder löschen.

2.3 Unzureichende Vergabe von Berechtigungen

Werden Berechtigungen fehlerhaft vergeben oder verwaltet, können Verantwortliche oder Benutzer des Datenbankmanagementsystems Berechtigungen erhalten, die über das zwingend notwendige Maß hinausgehen. So ist es möglich, dass die zu umfassend berechtigten Verantwortlichen oder Benutzer unerlaubte Aktionen auf dem Datenbankmanagementsystem ausführen, die weitreichende Folgen nach sich ziehen, wie das folgende Beispiel zeigt:

Durch ein fehlerhaftes SQL-Statement (beispielsweise in einem Installationsskript) löscht ein Benutzer unbeabsichtigt sehr viele Datensätze in der Datenbank. Nachher wird festgestellt, dass der Benutzer für diese Datensätze eigentlich nur Leserechte benötigt hätte, aber unnötigerweise auch über Löschrechte verfügte.

2.4 Unverschlüsselte Datenbankanbindung

In der Standardkonfiguration verbinden sich viele Datenbankmanagementsysteme unverschlüsselt mit den Anwendungen. Wird zwischen Anwendungen und Datenbankmanagementsystem unverschlüsselt kommuniziert, können übertragene Daten und Zugangsinformationen mitgelesen oder auf dem Transportweg manipuliert werden.

2.5 Datenverlust in der Datenbank

Durch Hardware- oder Softwarefehler sowie durch menschliches Versagen können Daten in der Datenbank verloren gehen. Da in Datenbanken meist wichtige Informationen für Anwendungen gespeichert sind, können Dienste ausfallen oder ganze Produktionsprozesse still stehen.

2.6 Integritätsverlust der gespeicherten Daten

Durch falsch konfigurierte Datenbanken, Softwarefehler oder manipulierte Daten kann die Integrität der Informationen in der Datenbank verletzt werden. Wird dies nicht oder erst spät bemerkt, können Kernprozesse der Institution stark beeinträchtigt werden. Werden beispielsweise die Integritätsbeziehungen (referenzielle Integrität) zwischen den Tabellen nicht korrekt definiert, kann dies dazu führen, dass sich die Daten in der Datenbank in einem fehlerhaften Zustand befinden. Wird dieser Fehler erst im Produktivbetrieb oder gar nicht bemerkt, müssen nicht nur die inkonsistenten Daten aufwendig bereinigt und rekonstruiert werden. Es kann mit der Zeit auch ein weitreichendes Schadensausmaß eingetreten sein, beispielsweise wenn es sich um kritische Daten (steuerrelevante Daten, Rechnungsdaten oder gar um Steuerungsdaten für ganze Produktionssysteme) handelt.

2.7 SQL-Injections

Eine häufige Angriffsmethode auf Datenbanksysteme sind SQL-Injections. Greift eine Anwendung auf die Daten einer SQL-Datenbank zu, so werden Befehle in Form von SQL-Anweisungen an das DBMS übermittelt. Werden Eingabedaten innerhalb der Anwendung unzureichend validiert, kann ein Angreifer eigene SQL-Befehle in die Anwendung einschleusen, die dann mit der Berechtigung des Dienstkontos der Anwendung bearbeitet werden. Ein Angreifer kann so Daten lesen, manipulieren, löschen, neue Daten hinzufügen oder auch Systembefehle aufrufen. Obwohl SQL-Injections primär die Anwendungen im Frontend betreffen, wirken sie sich erheblich auf das Datenbanksystem selbst und die damit verbundene Infrastruktur aus.

2.8 Unzureichendes Patchmanagement

Durch den umfangreichen Funktionsumfang der Datenbankmanagementsysteme treten relativ häufig Fehler oder Schwachstellen auf, die über Patches und Aktualisierungen vom Hersteller behoben werden. Werden diese jedoch nicht oder zu spät eingespielt, können Schwachstellen ausgenutzt und das Datenbankmanagementsystem erfolgreich angegriffen werden. Dadurch ist es möglich, dass Angreifer die Systeme manipulieren und so geschäftskritische Daten abfließen, Dienste ausfallen oder ganze Produktionsprozesse still stehen.

2.9 Unsichere Konfiguration des Datenbankmanagementsystems

Häufig sind in der Standardkonfiguration des Datenbankmanagementsystems nicht benötigte Funktionen aktiviert, die es einem potenziellen Angreifer erleichtern, Informationen aus der Datenbank auszulesen oder zu manipulieren. Beispielsweise kann sich ein Angreifer aufgrund einer unveränderten Standardinstallation mit einer von der Institution nicht benutzten Programmierschnittstelle verbinden, um das DBMS zu administrieren, ohne sich dafür authentifizieren zu müssen. Dadurch kann er unerlaubt auf die Datenbanken der Institution zugreifen.

2.10 Malware und unsichere Datenbank-Skripte

Bei vielen Datenbankmanagementsystemen ist es möglich, bestimmte Aktionen über Skripte zu automatisieren, die im Kontext der Datenbank ausgeführt werden, z. B. mithilfe der Procedural Language/Structured Query Language (PL/SQL). Dazu gehören unter anderem auch sogenannte Datenbanktrigger. Werden diese jedoch von den Verantwortlichen ungeprüft benutzt, besteht die Gefahr, dass die Datenbank-Skripte nicht den Anforderungen an die Softwareentwicklung der Institution genügen.

Ebenfalls kann ein Angreifer Kernfunktionen (z. B. Data Dictionary Tables) einer Datenbank manipulieren, beispielsweise mithilfe von Schadprogrammen oder Datenbank-Skripten. Diese Art von Angriffen ist nur schwer zu entdecken. Qualitätsmängel in diesen Skripten und Malware können sowohl die Vertraulichkeit als auch die Integrität und die Verfügbarkeit der in den Datenbanken abgelegten Daten gefährden.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Datenbanksysteme aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Entwickler, Fachverantwortliche, Informationssicherheitsbeauftragter (ISB), Leiter IT, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

APP.4.3.A1 Erstellung einer Sicherheitsrichtlinie für Datenbanksysteme [Informationssicherheitsbeauftragter (ISB)]

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie für Datenbanksysteme erstellt werden, in der nachvollziehbar Anforderungen und Vorgaben beschrieben sind, wie Datenbanksysteme sicher betrieben werden können. Die Richtlinie MUSS allen im Bereich Datenbanksysteme verantwortlichen Mitarbeitern bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies mit dem ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse MÜSSEN sinnvoll dokumentiert werden.

APP.4.3.A2 Installation des Datenbankmanagementsystems

Es MUSS sichergestellt sein, dass die Installationspakete des Datenbankmanagementsystems aus sicheren Quellen stammen. Bereits veröffentlichte Patches MÜSSEN eingespielt werden, bevor das DBMS betrieben wird.

APP.4.3.A3 Basishärtung des Datenbankmanagementsystems

Das Datenbankmanagementsystem MUSS gehärtet werden. Hierfür MUSS eine Checkliste mit den durchzuführenden Schritten zusammengestellt und abgearbeitet werden. Auch MÜSSEN alle Passwörter entsprechend den internen Anforderungen der Institution geändert werden. Alle Passwörter MÜSSEN verschlüsselt gespeichert werden. Die Basishärtung MUSS regelmäßig überprüft und falls erforderlich angepasst werden.

APP.4.3.A4 Geregeltes Anlegen neuer Datenbanken

Neue Datenbanken MÜSSEN nach einem definierten Prozess angelegt werden. Wenn eine neue Datenbank angelegt wird, MÜSSEN Grundinformationen zur Datenbank nachvollziehbar dokumentiert werden.

APP.4.3.A5 Benutzer- und Berechtigungskonzept

Das Benutzer- und Berechtigungskonzept (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*) der Institution MUSS um die für Datenbankmanagementsysteme notwendigen Berechtigungen für Rollen, Profile und Benutzergruppen erweitert werden.

Es MUSS ein Prozess etabliert werden, der regelt, wie Datenbankbenutzer und deren Berechtigungen angelegt, genehmigt, eingerichtet, modifiziert und wieder entzogen bzw. gelöscht werden. Dabei DÜRFEN immer NUR so viele Zugriffsrechte vergeben werden, wie für die jeweiligen Aufgaben erforderlich sind (Need-to-know-Prinzip). Alle Änderungen SOLLTEN dokumentiert werden. Die eingerichteten Benutzer und die ihnen zugeordneten Berechtigungen MÜSSEN regelmäßig überprüft und falls erforderlich angepasst werden.

APP.4.3.A6 Passwortänderung [Fachverantwortliche]

Alle Passwörter der Datenbankbenutzer MÜSSEN der Passwortrichtlinie der Institution entsprechen (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*). Es MUSS gewährleistet sein, dass die Passwörter beim geringsten Verdacht eines Sicherheitsvorfalles geändert werden. Insbesondere bei privilegierten Datenbankaccounts und Dienstkonten SOLLTE ein Passwortwechsel sorgfältig geplant und gegebenenfalls mit den Anwendungsverantwortlichen abgestimmt werden.

APP.4.3.A7 Zeitnahes Einspielen von Sicherheitsupdates

Vorhandene Sicherheitsupdates für das Datenbankmanagementsystem und das Betriebssystem MÜSSEN zeitnah installiert werden. Vorab MUSS auf einem Testsystem überprüft werden, ob die Sicherheitsupdates kompatibel sind und keine Fehler verursachen. Bevor ein Patch eingespielt wird, MUSS das Datenbanksystem gesichert werden (siehe APP.4.3.A9 *Datensicherung eines Datenbanksystems*).

Zusätzlich MUSS eine verantwortliche Rolle definiert werden, die dafür zuständig ist, sich regelmäßig über bekannte Sicherheitslücken des Datenbankmanagementsystems sowie über verfügbare Sicherheitsupdates zu informieren. Des Weiteren MUSS geprüft werden, ob die Update-Intervalle des Datenbankmanagementsystems auf die Update-Zyklen des Herstellers abgestimmt werden können. Das Ergebnis SOLLTE nachvollziehbar dokumentiert werden.

APP.4.3.A8 Datenbank-Protokollierung

Sicherheitsrelevante Ereignisse des Datenbanksystems MÜSSEN mit einem eindeutigen Zeitstempel protokolliert werden. Dabei MÜSSEN sich Art und Umfang der Protokollierung am Schutzbedarf der zu verarbeiteten Informationen orientieren. Zusätzlich MUSS geprüft werden, ob die Protokollierung der Fachanwendungen zusammen mit der Protokollierung der Datenbank alle erforderlichen Informationen abdeckt, um betriebs- und sicherheitsrelevante Veränderungen an der Datenbank-Infrastruktur und den Anwendungen zu erkennen. Es SOLLTE so protokolliert werden, dass die Protokolldateien nicht nachträglich veränderbar sind. Vertiefende Informationen sind in OPS.1.1.57 *Protokollierung* zu finden.

APP.4.3.A9 Datensicherung eines Datenbanksystems

Es MÜSSEN regelmäßig Systemsicherungen des DBMS und der Daten durchgeführt werden. Auch bevor eine Datenbank neu erzeugt wird, MUSS das Datenbanksystem gesichert werden. Hierfür SOLLTEN die dafür zulässigen Dienstprogramme benutzt werden.

Alle Transaktionen SOLLTEN so gesichert werden, dass sie jederzeit wiederherstellbar sind. Sofern die Datensicherung die verfügbaren Kapazitäten übersteigt, SOLLTE ein erweitertes Konzept (z. B. inkrementelle Sicherung) erstellt werden, um die Datenbank zu sichern. Abhängig vom Schutzbedarf der Daten SOLLTEN die Wiederherstellungsparameter vorgegeben werden (siehe OPS.1.1.5 *Datensicherung).*

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Relationale Datenbanksysteme. Sie SOLLTEN grundsätzlich umgesetzt werden.

APP.4.3.A10 Auswahl geeigneter Datenbankmanagementsysteme

Bevor Datenbankmanagementsysteme beschafft werden, SOLLTEN Anforderungen an die DBMS definiert und in einem Anforderungskatalog dokumentiert werden. Danach SOLLTEN alle infrage kommenden Datenbankmanagementsysteme anhand des Katalogs bewertet werden. Die Ergebnisse SOLLTEN dokumentiert werden.

APP.4.3.A11 Ausreichende Dimensionierung der Hardware [Leiter IT, Fachverantwortliche]

Datenbankmanagementsysteme SOLLTEN auf ausreichend dimensionierter Hardware installiert werden. Die Hardware SOLLTE über genügend Reserven verfügen, um auch eventuell steigenden Anforderungen gerecht zu werden. Zeichnen sich trotzdem während des Betriebs Ressourcenengpässe ab, SOLLTEN diese frühzeitig behoben werden. Wenn die Hardware dimensioniert wird, SOLLTE das erwartete Wachstum für den geplanten Einsatzzeitraum berücksichtigt werden.

APP.4.3.A12 Einheitlicher Konfigurationsstandard von Datenbankmanagementsystemen [Leiter IT, Informationssicherheitsbeauftragter (ISB)]

Für alle eingesetzten Datenbankmanagementsysteme SOLLTE ein einheitlicher Konfigurationsstandard definiert werden. Alle Datenbankmanagementsysteme SOLLTEN nach diesem Standard konfiguriert und einheitlich betrieben werden. Falls es bei einer Installation notwendig ist vom Konfigurationsstandard abzuweichen, SOLLTEN alle Schritte vom ISB freigegeben und nachvollziehbar dokumentiert werden. Der Konfigurationsstandard SOLLTE regelmäßig überprüft und falls erforderlich angepasst werden.

APP.4.3.A13 Restriktive Handhabung von Datenbank-Links

Es SOLLTE sichergestellt sein, dass nur Verantwortliche dazu berechtigt sind, Datenbank-Links (DB-Links) anzulegen. Werden solche Links angelegt, MÜSSEN sogenannte Private DB-Links vor Public DB-Links bevorzugt angelegt werden. Alle von den Verantwortlichen angelegten DB-Links SOLLTEN dokumentiert und regelmäßig überprüft werden. Zudem SOLLTEN DB-Links mitberücksichtigt werden, wenn das Datenbanksystem gesichert wird (siehe APP.4.3.A9 *Datensicherung eines Datenbanksystems*).

APP.4.3.A14 Überprüfung der Datensicherung eines Datenbanksystems

Die vorgenommenen Datensicherungen SOLLTEN regelmäßig daraufhin überprüft werden, ob die Integrität der Sicherungsdateien noch gewährleistet ist. Die verantwortlichen Mitarbeiter SOLLTEN zudem regelmäßig üben, wie sich Datenbanken im Notfall schnell wiederherstellen lassen.

APP.4.3.A15 Schulung der Datenbankadministratoren [Vorgesetzte, Leiter IT]

Es SOLLTE gewährleistet sein, dass nur ausreichend geschulte Mitarbeiter das Datenbankmanagementsystem administrieren. Es SOLLTE ein Schulungsplan erstellt werden, mit dem sichergestellt wird, dass Datenbankverantwortliche rechtzeitig zu Themen der Informationssicherheit (siehe ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*)und Performance sowie zu den Funktionen neuer Versionen des Datenbankmanagementsystems geschult werden.

APP.4.3.A16 Verschlüsselung der Datenbankanbindung

Das Datenbankmanagementsystem SOLLTE so konfiguriert werden, dass Datenbankverbindungen immer verschlüsselt werden. Die dazu eingesetzten kryptografischen Verfahren und Protokolle SOLLTEN den internen Vorgaben der Institution entsprechen (siehe CON.1 *Kryptokonzept*).

APP.4.3.A17 Datenübernahme oder Migration [Fachverantwortliche]

Falls initial oder regelmäßig Daten in eine Datenbank übernommen werden, SOLLTE vorab definiert werden, wie diese Datenübernahme erfolgen soll. Nachdem Daten übernommen wurden, SOLLTE geprüft werden, ob sie vollständig und unverändert sind.

APP.4.3.A18 Überwachung des Datenbankmanagementsystems

Es SOLLTEN Parameter, Ereignisse und Betriebszustände des Datenbankmanagementsystems definiert werden, die für den sicheren Betrieb kritisch sind. Diese SOLLTEN mithilfe eines Monitoring-Systems überwacht werden. Für alle kritischen Parameter und Ereignisse SOLLTEN Schwellwerte festgelegt werden. Wenn diese Werte überschritten werden, MUSS geeignet reagiert werden (z. B. müssen die zustän-

digen Mitarbeiter alarmiert werden). Anwendungsspezifische Parameter, Ereignisse und deren Schwellwerte SOLLTEN mit den Verantwortlichen für die Fachanwendungen abgestimmt werden (siehe auch APP.4.3.A11 *Ausreichende Dimensionierung der Hardware*).

APP.4.3.A19 Schutz vor schädlichen Datenbank-Skripten [Entwickler]

Werden Datenbank-Skripte entwickelt, SOLLTEN hierfür verpflichtende Qualitätskriterien definiert werden (siehe CON.3 *Softwareentwicklung*). Datenbank-Skripte SOLLTEN auf gesonderten Testsystemen ausführlichen Funktionstests unterzogen werden, bevor sie produktiv eingesetzt werden. Die Ergebnisse SOLLTEN dokumentiert werden.

APP.4.3.A20 Regelmäßige Audits

Bei allen Komponenten des Datenbanksystems SOLLTE regelmäßig überprüft werden, ob alle festgelegten Sicherheitsmaßnahmen umgesetzt und diese korrekt konfiguriert sind. Dabei SOLLTE geprüft werden, ob der dokumentierte Stand dem Ist-Zustand entspricht, ob die Konfiguration des Datenbankmanagementsystems der dokumentierten Standardkonfiguration entspricht, ob alle Datenbank-Skripte benötigt werden und ob sie dem Qualitätsstandard der Institution genügen. Zusätzlich SOLLTEN die Protokolldateien des Datenbanksystems und des Betriebssystems nach Auffälligkeiten untersucht werden (siehe DER.1 *Detektion von sicherheitsrelevanten Ereignissen*). Die Auditergebnisse SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTE nachgegangen werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

APP.4.3.A21 Einsatz einer Datenbank-Firewall (CI)

Es SOLLTE eine Datenbank-Firewall eingesetzt werden, wenn auf Anwendungsseite nicht sichergestellt werden kann, dass die Datenbank ausreichend geschützt ist, z. B. vor SQL-Injections. Ebenso SOLLTE durch die Datenbank-Firewall unterbunden werden, dass unberechtigt auf eine Datenbank zugegriffen werden kann. Bevor eine Datenbank-Firewall eingesetzt wird, SOLLTEN mögliche Nebeneffekte evaluiert werden. Wenn Datenbank-Anwendungen aktualisiert werden, SOLLTE darauf geachtet werden, dass auch die Firewall angepasst wird.

APP.4.3.A22 Notfallvorsorge (CIA)

Für das Datenbankmanagementsystem SOLLTE ein Notfallplan erstellt werden, der festlegt, wie ein Notbetrieb realisiert werden kann und welche Ressourcen dafür nötig sind (siehe DER.4 *Notfallmanagement*). Zusätzlich SOLLTE der Notfallplan definieren, wie aus dem Notbetrieb der Regelbetrieb wiederhergestellt werden kann. Der Notfallplan SOLLTE die nötigen Meldewege, Reaktionswege, Ressourcen und Reaktionszeiten der Fachverantwortlichen festlegen, durch sich ein möglicher Notfall schnell eskalieren lässt. Auf Basis eines Wiederanlaufkoordinationsplanes SOLLTEN alle von der Datenbank abhängigen IT-Systeme vorab ermittelt und berücksichtigt werden.

APP.4.3.A23 Archivierung (CIA)

Ist es erforderlich, Daten eines Datenbanksystems zu archivieren, SOLLTE ein entsprechendes Archivierungskonzept erstellt werden. Es SOLLTE sichergestellt sein, dass die Datenbestände zu einem späteren Zeitpunkt wieder vollständig und konsistent verfügbar sind.

Im Archivierungskonzept SOLLTEN sowohl die Intervalle der Archivierung als auch die Vorhaltefristen der archivierten Daten festgelegt werden. Zusätzlich SOLLTE dokumentiert werden, mit welcher Technik die Datenbanken archiviert wurden. Mit den archivierten Daten SOLLTEN regelmäßig Wiederherstellungstests durchgeführt werden. Die Ergebnisse SOLLTEN dokumentiert werden.

APP.4.3.A24 Datenverschlüsselung in der Datenbank (C)

Die Daten in den Datenbanken SOLLTEN verschlüsselt werden. Dabei SOLLTEN vorher unter anderem folgende Faktoren betrachtet werden:

- Einfluss auf die Performance,
- Schlüsselverwaltungsprozesse und -verfahren, einschließlich separater Schlüsselaufbewahrung und -sicherung,
- Einfluss auf Backup-Recovery-Konzepte,
- funktionale Auswirkungen auf die Datenbank, beispielsweise Sortiermöglichkeiten.

APP.4.3.A25 Sicherheitsüberprüfungen von Datenbanksystemen (CIA)

Datenbanksysteme SOLLTEN regelmäßig mithilfe von Sicherheitsüberprüfungen überprüft werden. Bei den Sicherheitsüberprüfungen SOLLTEN die systemischen und herstellerspezifischen Aspekte der eingesetzten Datenbank-Infrastruktur (z. B. Verzeichnisdienste) sowie des eingesetzten Datenbankmanagementsystems betrachtet werden.

4 Weiterführende Informationen

4.1 Literatur

- [ISF] The Standard of Good Practice
  Information Security Forum (ISF), 06.2016

- [NISTSP800123] NIST Special Publication 800-123
  Guide to General Server Security, NIST, 07.2008
  https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

- [TELEKOM_DB] Sicherheitsanforderungen Datenbanksysteme
  Privacy and Security Assessment Verfahren: Sicherheitsanforderungen Datenbanksysteme, Deutsche Telekom, 06.2014
  https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/sicherheit/sicherheit/privacy-and-security-assessment-verfahren-342724

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Relationale Datenbanksysteme" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.43 Einspielen von Nachrichten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.14	G 0.15	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.30	G 0.31	G 0.32	G 0.36	G 0.37	G 0.39	G 0.40	G 0.43	G 0.45	G 0.46
APP.4.3.A1			x								x		x									
APP.4.3.A2					x			x				x										
APP.4.3.A3	x	x		x		x	x	x					x					x				x
APP.4.3.A4	x	x		x		x	x	x					x									x
APP.4.3.A5								x					x		x	x	x					
APP.4.3.A6				x		x	x	x					x			x						
APP.4.3.A7	x			x		x	x	x				x	x					x				x
APP.4.3.A8										x	x						x					
APP.4.3.A9						x	x														x	x
APP.4.3.A10			x		x																	
APP.4.3.A11									x	x	x								x			
APP.4.3.A12	x	x		x		x	x	x					x					x				x
APP.4.3.A13							x	x					x									
APP.4.3.A14						x	x														x	x
APP.4.3.A15	x			x										x		x						
APP.4.3.A16		x																		x		
APP.4.3.A17						x	x			x												
APP.4.3.A18									x	x	x								x			
APP.4.3.A19				x		x	x	x				x		x				x				x
APP.4.3.A20				x	x		x	x		x		x	x			x						x
APP.4.3.A21				x		x		x				x	x									x
APP.4.3.A22									x										x		x	
APP.4.3.A23						x	x														x	x
APP.4.3.A24	x	x		x	x		x	x										x				x
APP.4.3.A25		x	x	x		x	x	x		x		x	x		x			x				x

APP.5: E-Mail / Groupware / Kommunikation

APP.5.1 Allgemeine Groupware

1 Beschreibung

1.1 Einleitung

Als Groupware (auch kollaborative Software genannt) werden Anwendungen und Systeme bezeichnet, mit denen mehrere Personen (Gruppen) über räumliche und/oder zeitliche Distanzen hinweg zusammenarbeiten können. Mithilfe von Groupware-Systemen können Gruppen untereinander und miteinander kooperieren und Termine abstimmen. Dokumente und Daten lassen sich durch Groupware von mehreren Benutzern gleichzeitig verwenden und bearbeiten, wodurch der Informationsfluss effizienter gestaltet wird.

Unter dem Begriff Groupware-Systeme werden unter anderem der Groupware-Server, die zugehörigen Groupware-Clients und die erforderlichen Groupware-Dienste zusammengefasst. Neben den Basisfunktionen, wie z. B. Projektmanagement, E-Mail, Kalender oder Notizbuch, bieten neuere Applikationen sogenannte Social-Media-Erweiterungen an, durch die Mitarbeiter noch besser kommunizieren und kooperieren können.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, Informationen zu schützen, die in und mit Groupware abgelegt, verarbeitet oder übertragen werden. Dazu müssen die für Groupware eingesetzten IT-Komponenten und deren Schnittstellen angemessen abgesichert und geeignete Verfahrensweisen etabliert werden.

1.3 Abgrenzung

Der Baustein enthält lediglich spezifische Gefährdungen und Anforderungen für Groupware-Systeme. Gefährdungen und Anforderungen für die spezifischen Bausteine von Serverplattform, Betriebssystem und Clients sind nicht Bestandteil des Bausteins. Diese sind in den Bausteinen SYS.1.1 Allgemeiner Server sowie SYS.1.2 Allgemeiner Client und in den jeweiligen betriebssystemspezifischen Bausteinen zu finden.

Der Baustein APP.5.1 Groupware wird in einem Informationsverbund meist in Verbindung mit einem weiteren spezifischen Baustein der Schicht APP.1 E-Mail/Groupware/Kommunikation genutzt, diese müssen ebenfalls separat umgesetzt werden. Zu diesen Bausteinen zählen unter anderem APP.1.2 Microsoft Exchange/Outlook, APP.1.3 Kontact, APP.1.4 Lotus Notes/Domino und APP.1.5 Instant Messaging.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Groupware von besonderer Bedeutung:

2.1 Unzureichende Planung der Groupware

Der Groupware-Prozess kann ohne entsprechend dokumentierte Regelungen und einem definierten Sicherheitsverfahren nicht geeignet in der Institution eingehalten werden. Potenzielle Sicherheitsrisiken können insbesondere dann auftreten, wenn die Groupware fehlerhaft in die Verzeichnisdienste eingebunden wird, Datenbanken dedupliziert werden und die spezifischen Aspekte von Groupware nicht in einer Sicherheitsrichtlinie dokumentiert sind.

Falls in der Planung der Groupware-Systeme die prozessualen, organisatorischen und technischen Regelungen vernachlässigt werden, könnten die daraus entstehenden Freiheiten, fehlerhafte Einstellungen, Programmierungen und Angriffe (intern/extern) hervorrufen. Dies würde die Groupware-Systeme, den Groupware-Prozess und prozessübergreifende Schnittstellen in ihren Aufgabenerfüllungen behindern.

2.2 Fehlerhafte Einstellung der Groupware

Da Groupware-Systeme komplex sind, können durch die vielen möglichen Einstellungen und durch die sich gegenseitig beeinflussenden Parameter zahlreiche Sicherheitsprobleme entstehen. So könnten beispielsweise Serverkomponenten auf ungeeigneten Systemen betrieben werden. Zusätzlich wäre es möglich, das essentielle Einstellungen (zum Beispiel Verschlüsselung einzelner Groupware-Dienste oder Beschränkungen der Rechte entsprechend dem Berechtigungsmanagement) ignoriert oder missachtet werden. Diese Sicherheitslücken können zu einem signifikanten Verlust der Verfügbarkeit, Authentizität und Vertraulichkeit von Informationen führen und somit die Funktionen der Groupware-Systeme behindern und verarbeitete Daten verfälschen.

Werden Rechte bei einer Groupware-Datenbank fehlerhaft vergeben, kann dies im Berechtigungsmanagement der Institution schädigende Daten-Leak-Szenarien oder unberechtigte Manipulation verursachen. Die Manipulationen können dabei zum Beispiel in fehlerhaften Einstellungen resultieren, die das gesamte Groupware-System stören oder einzelne Dienste.

2.3 Missbrauch selbst entwickelter Makros und Programmierschnittstellen bei Groupware-Diensten

In vielen Tools und Anwendungen gibt es Programmierschnittstellen (z. B. als Application Programming Interface – API), die es erlauben, bestimmte Funktionen anderen Anwendungen bereitzustellen oder den Funktionsumfang der Anwendung zu erweitern. Groupware kann jedoch dazu missbraucht werden, um Schadsoftware zu verbreiten. Dazu zählen beispielsweise Schadprogramme, die direkt die Groupware-Systeme infizieren, um Informationen abzugreifen, zu verändern oder zu löschen.

Auch können Makros dazu genutzt werden, Nachrichten, Termine oder Aufgaben weiterzuleiten bzw. zu verschieben. Sind Makros fehlerhaft oder werden in ihnen falsche Werte berechnet, können z. B. Indexfehler zu falschen Ergebnissen und möglicherweise unwirtschaftlichen Entscheidungen in der Institution führen.

2.4 Fehlerhafte Vergabe von Zugangs- und Zugriffsrechten auf Groupware-Dienste

Wenn Zugangsrechte zu einem Groupware-Client oder Zugriffsrechte auf gespeicherte Daten in Groupware-Diensten nicht genügend beschränkt werden, können Sicherheitslücken entstehen. Werden diese Rechte fehlerhaft angelegt und administriert, kann zudem der Betrieb gestört werden, beispielsweise wenn ein Mitarbeiter nicht auf für ihn wichtige Informationen zugreifen kann. Ebenso ist es möglich, dass dadurch Angreifer auf vertrauliche Informationen zugreifen und so schützenswerte Daten einsehen können.

2.5 Unzureichendes Wissen der Administratoren von Groupware-Systemen

Schon kleine Konfigurationsfehler können die Sicherheit eines Groupware-Systems beeinträchtigen. Personal, das zu wenig über Groupware-Anwendungen und -Dienste weiß, kann aufgrund der komplexen Systemarchitekturen und der spezifischen Schutzmechanismen der eingesetzten Groupware unab-

sichtlich Sicherheitslücken verursachen. Ein unzureichender geschulter Administrator kann auch in einem Notfall oft nicht effektiv reagieren (z. B. bei Funktionsfehlern und Kompromittierungen). Durch unzureichend geschulte und sensibilisierte Administratoren können unerwünschte Zustände innerhalb der Groupware-Dienste und -Prozesse entstehen. Hierzu kann gehören, dass zwischen den Endgeräten und den Groupware-Systemen nicht vollständig synchronisiert wird oder aber auch, dass im Kalender die Zeitzonen zu fehlerhaften Startzeiten beiden vorhandenen Terminen führt.

2.6 Datenverlust bei Groupware-Anwendungen

Der Verlust gespeicherter Daten in Groupware-Anwendungen kann erhebliche Auswirkungen auf Geschäftsprozesse und damit auf die gesamte Institution haben. Werden Daten in Verbindung mit Groupware-Anwendungen verfälscht oder gehen verloren, können privatwirtschaftliche Institutionen in ihrer Existenz bedroht sein. In Behörden kann der Verlust oder die Verfälschung jener Daten die internen Verwaltungs- und Fachaufgaben verzögern oder sogar ausschließen.

Insgesamt kann der Verlust gespeicherter Daten in Groupware-Anwendungen, neben einem Arbeitsausfall und den Kosten für eine Wiederbeschaffung, auch zu langfristigen Konsequenzen, wie beispielsweise Vertrauenseinbußen bei Kunden und Partnern, sowie einem negativen Eindruck in der Öffentlichkeit, führen.

2.7 Angriffe auf Groupware-Systeme und -Anwendungen

Groupware-Systeme und einzelne Groupware-Anwendungen können durch Dritte kompromittiert werden. Bei Groupware-Systemen können z. B. die Benutzer, das interne Netz, genutzte Groupware-Server sowie der Nachrichtenempfänger vorsätzlich angegriffen werden. Eventuelle Sicherheitslücken können durch Angreifer benutzt werden, um Informationen in geschlossenen Groupware-Systemen auszulesen, zu verändern oder zu löschen. Auch bei einem nicht ausreichend geschützten Zugang zu den Groupware-Anwendungen könnten Angreifer beispielsweise auf vertrauliche Daten zugreifen.

2.8 Unzuverlässigkeit von Groupware

Über Groupware-Dienste lassen sich schnell und komfortabel Daten austauschen. Das ist jedoch nicht immer zuverlässig: So können durch fehlerhafte IT-Systeme oder gestörte Übertragungswege Nachrichten verlorengehen. Ursachen dafür sind beispielsweise beschädigte Leitungen, ausgefallene Netzkopplungselemente oder falsch konfigurierte Kommunikationssoftware. E-Mails können auch abhandenkommen, weil die Empfängeradresse nicht korrekt angegeben wurde. Ebenso ist möglich, dass Nachrichten durch Dritte abgefangen werden oder dass diese gezielt Konversationen mitlesen.

Groupware-Dienste sind in der Grundeinstellung meistens nicht kryptografisch abgesichert. Dadurch können über Kalenderdienste eventuell auch Unbefugte die Terminplanung von Gruppen oder einzelnen Personen einsehen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Groupware aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Benutzer, Datenschutzbeauftragter, Informationssicherheitsbeauftragter (ISB), Leiter IT, Leiter Organisation, Notfallbeauftragter, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

APP.5.1.A1 Sichere Installation von Groupware-Systemen [Leiter IT]

Alle für ein Groupware-System benötigten Komponenten (z. B. auch die Sicherheitsgateways) MÜSSEN entsprechend der geplanten Systemlandschaft sicher installiert und konfiguriert werden. Während das System installiert wird, MÜSSEN alle Passwörter sicher gewählt sein. Nicht genutzte Komponenten MÜSSEN deaktiviert werden. Auch MÜSSEN die Installationsquellen vor unbefugtem Zugriff geschützt werden.

APP.5.1.A2 Sichere Konfiguration der Groupware-Clients [Leiter IT, Benutzer]

Die Groupware-Clients der Benutzer MÜSSEN durch den Administrator so vorkonfiguriert sein, dass sie, ohne das der Benutzer etwas tun muss, maximal sicher sind. Die Benutzer MÜSSEN darauf hingewiesen werden, dass die Konfiguration nicht selbstständig geändert werden darf. Es MUSS zudem verhindert und untersagt sein, dass Passwörter im Klartext gespeichert werden. Werden Nachrichten auf einem Mailserver gespeichert und wird z. B. über Internet Message Access Protocol (IMAP) darauf zugegriffen, MUSS eine Größenbeschränkung für das serverseitige Postfach eingerichtet werden. Bevor Dateianhänge ausgeführt werden, MÜSSEN sie mit einem Svchutzprogramm vor Schadsoftware überprüft werden. Es MÜSSEN sichere Einstellungen für E-Mails im HTML-Format, die Vorschaufunktionen und die E-Mail-Filterregeln sowie für die sichere automatische Weiterleitung von E-Mails gewählt werden.

APP.5.1.A3 Sicherer Betrieb von Groupware-Systemen [Leiter IT, Informationssicherheitsbeauftragter (ISB)]

Es MÜSSEN alle sicherheitsrelevanten Servicepacks, Updates und Patches für das jeweilige Softwareprodukt eingespielt werden. Administratoren MÜSSEN sich daher regelmäßig über neu bekanntgewordene Schwachstellen, der eingesetzten Groupware-Systeme und der genutzten Betriebssysteme informieren und sie zeitnah schließen. Um Groupware-Systeme in der Institution abzusichern, MÜSSEN Schutzmechanismen gegen Denial-of-Service-(DoS)-Attacken ergriffen werden. Die lokale Kommunikation MUSS angemessen geschützt sein. Die Kommunikation über öffentliche Netze MUSS verschlüsselt sein. Außerdem MÜSSEN die Zugriffsrechte auf die lokal angeschlossenen Benutzer beschränkt werden. Es SOLLTE eine Richtlinie erstellt werden, die über die in der jeweiligen Groupware erlaubten Protokolle und Dienste informiert. Insbesondere der Mailserver MUSS so eingestellt werden, dass er nicht als Spam Relay missbraucht werden kann.

APP.5.1.A4 Datensicherung Archivierung bei Groupware [Informationssicherheitsbeauftragter (ISB), Datenschutzbeauftragter, Benutzer]

Bei einem Groupware-System MÜSSEN die Daten regelmäßig gesichert werden. Dafür MUSS geregelt werden, wie die gesendeten und empfangenen E-Mails der E-Mail-Clients und auf E-Mail-Servern gesichert werden. Auch SOLLTE eine dokumentierte Vorgehensweise erstellt werden, wie E-Mails zu archivieren sind. Dabei SOLLTE grundsätzlich geregelt sein, wie, wann und wo gesendete und empfangene E-Mails archiviert werden, beispielsweise ob zentral oder dezentral ggf. von den Benutzern selbst. Bei der Archivierung von E-Mails SOLLTEN z. B. zeitliche und organisatorische Sicherheitsaspekte beachtet werden. Der erforderliche Zeitraum SOLLTE überprüft, die Archivierung geplant und zudem überlegt werden, wie sich die E-Mails wieder einspielen lassen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Allgemeine Groupware. Sie SOLLTEN grundsätzlich umgesetzt werden.

APP.5.1.A5 Festlegung der Kommunikationspartner [Leiter Organisation, Leiter IT, Informationssicherheitsbeauftragter (ISB), Datenschutzbeauftragter]

Es SOLLTE festgelegt werden, welche Kommunikationspartner welche Informationen erhalten dürfen. Sollen Informationen an einen Kommunikationspartner außerhalb der eigenen Institution übertragen werden, SOLLTE sichergestellt werden, dass der Empfänger berechtigt ist, diese Informationen weiterzuverarbeiten. Alle Informationen SOLLTEN entsprechend ihrer strategischen Bedeutung für die Institution klassifiziert werden. Die Kommunikationspartner SOLLTEN darauf hingewiesen werden, dass die übermittelten Daten nur zu dem Zweck benutzt werden dürfen, zu dem sie weitergegeben wurden. Auch aus Datenschutzgründen (Bundesdatenschutzgesetz (BDSG), Weitergabekontrolle) SOLLTE eine Übersicht erstellt werden, welche Empfänger berechtigt sind, Informationen, insbesondere personenbezogene Daten zu erhalten. Bei zu übermittelnden Daten SOLLTE ersichtlich sein, welche Kommunikationspartner Informationen erhalten haben bzw. erhalten werden.

APP.5.1.A6 Vertretungsregelungen bei E-Mail-Nutzung [Vorgesetzte, Informationssicherheitsbeauftragter (ISB), Benutzer]

Für die E-Mail-Bearbeitung SOLLTE für jeden Mitarbeiter jederzeit ein geeigneter Vertreter benannt sein. Vertreter SOLLTEN auf das Postfach des Vertretenden zugreifen können. Alternativ SOLLTEN die E-Mails an den Vertreter weitergeleitet werden. Werden E-Mails weitergeleitet, SOLLTEN die vertretenden Benutzer mindestens darüber informiert werden. Um die Vertreterregelungsprozesse zu unterstützen, SOLLTEN für Autoreply-Funktionen in E-Mail-Programmen spezielle Regelungen etabliert werden, mit denen diese Funktionen sicher gesteuert werden können. Wenn Mitarbeiter die Autoreply-Funktionen benutzen, SOLLTEN KEINE interne Informationen weitergegeben werden.

APP.5.1.A7 Planung des sicheren Einsatzes von Groupware-Systemen [Leiter IT, Informationssicherheitsbeauftragter (ISB)]

Bevor eine Institution ein Groupware-System einführt, SOLLTE entschieden werden, wofür es genutzt wird und welche Informationscluster zukünftig auf dem Groupware-System verarbeitet werden sollen. Es SOLLTE entschieden werden, ob ein eigener Groupware-Server in der Institution eingesetzt oder ein Provider genutzt werden soll. Auch SOLLTE ermittelt werden, wie die Groupware-Clients auf die Server zugreifen. Für jede benutzte Funktion einer Groupware SOLLTE eine eigene Planung durchgeführt werden, bei der auch deren Sicherheitsaspekte berücksichtigt werden.

Bei der Planung SOLLTE auch festgelegt werden, welche Daten,. unter welchen Rahmenbedingungen über Groupware-Dienste übermittelt werden dürfen und wie sich dies auf den Schutzbedarf auswirkt. Es SOLLTE ebenso beschrieben werden, wie ein ordnungsgemäßer Dateitransfer gewährleistet werden kann, z. B. durch organisatorische Regelungen oder technische Maßnahmen. Darüber hinaus SOLLTE auch geregelt werden, ob und wie Groupware-Dienste privat benutzt werden dürfen. Auch SOLLTEN Institutionen regeln, wie Mitarbeiter mit Webmail umgehen sollen.

APP.5.1.A8 Festlegung einer Sicherheitsrichtlinie für Groupware [Leiter IT, Informationssicherheitsbeauftragter (ISB), Benutzer]

Es SOLLTE eine Sicherheitsrichtlinie für Groupware-Systeme und -Anwendungen erstellt und regelmäßig aktualisiert werden. Alle Benutzer und Administratoren SOLLTEN über neue oder veränderte Sicherheitsvorgaben für Groupware-Systeme informiert werden. Die Groupware-Sicherheitsrichtlinie SOLLTE konform zu den geltenden übergeordneten Sicherheitsrichtlinien der Institution sein. Es SOLLTE geprüft werden, ob die Sicherheitsrichtlinien korrekt angewendet werden.

Es SOLLTE eine Sicherheitsrichtlinie für Benutzer und eine für Administratoren erstellt werden. Für die Benutzer SOLLTE darin angegeben werden, wie sich die Kommunikation absichern lässt (z. B. für die Netz- oder E-Mail-Kommunikation), welche Benutzerzugriffsrechte es gibt (z. B. auf Groupware-Server oder -Datenbanken), wie Informationen an Kommunikationspartner weitergegeben werden sollen und wie sich übermittelte Informationen absichern lassen (z. B. Signaturen/Verschlüsselungen). Die zu regelnden Inhalte für Administratoren SOLLTEN darüber hinaus die Einstellungsoptionen der Groupwa-

re-Komponenten beinhalten, außerdem die Vorgaben für mögliche Zugriffe von anderen Servern auf einen Groupware-Server und Angaben zum berechtigten Zugriffspunkt, von dem aus auf einen Groupware-Server zugegriffen werden darf.

APP.5.1.A9 Sichere Administration von Groupware-Systemen [Leiter IT]

Administrative Zugänge sowie die dazugehörigen Aufgaben SOLLTEN abhängig ihrer Zuständigkeit getrennt werden. Um ein Groupware-System reibungslos zu betreiben, SOLLTEN Administratoren ernannt und geschult werden. Alle Administrationsaufgaben im Bereich Groupware und die vergebenen Berechtigungen SOLLTEN ausreichend dokumentiert werden. An Administratoren SOLLTEN nur die für die jeweiligen Aufgaben notwendigen Berechtigungen vergeben werden. Nachdem alle Groupware-Komponenten installiert wurden, SOLLTEN sie sicher konfiguriert werden. Es SOLLTE darauf geachtet werden, dass die genutzten Groupware-Systeme ausreichend dimensioniert sind. Auch SOLLTEN vertrauenswürdige Groupware-Dokumentationen bei der Administration berücksichtigt werden. Es SOLLTE regelmäßig überprüft werden, ob die vorhandenen Dokumentationen aktuell sind.

APP.5.1.A10 Schulung zur Systemarchitektur und Sicherheit von Groupware-Systemen für Administratoren [Leiter IT, Informationssicherheitsbeauftragter (ISB)]

Um ein Groupware-System korrekt und sicher administrieren zu können, SOLLTEN die verantwortlichen Administratoren geschult werden. Für die Schulungen SOLLTE überlegt werden, einen Schulungsplan festzulegen. Die Administratoren SOLLTEN in allen sicherheitsrelevanten Bereichen des Groupware-Systems ausgebildet werden. Weitere Schulungsschwerpunkte SOLLTEN sein:

- Überblick über Lösungen für Kommunikationssicherheit (z. B. Verschlüsselung, VPN),
- Protokollierung,
- Sichern und Verwalten von Konfigurationsdaten,
- Datensicherung,
- Incident Handling sowie
- Disaster-Recovery-Maßnahmen.

APP.5.1.A11 Berechtigungsverwaltung für Groupware-Systeme [Leiter IT, Informationssicherheitsbeauftragter (ISB)]

Die vergebenen Berechtigungen, vor allem die privilegierten, SOLLTEN regelmäßig mit dem Berechtigungskonzept abgeglichen und zeitnah angepasst werden, wenn sich die Aufgaben der Benutzer und der Administratoren ändern. Es SOLLTE ein Berechtigungskonzept erstellt werden, das alle Groupware-Komponenten umfasst. Berechtigungen SOLLTEN möglichst restriktiv vergeben werden. Administrative Tätigkeiten auf Betriebssystemebene und Groupware-Anwendungsebene SOLLTEN soweit wie möglich voneinander getrennt werden. Auch innerhalb der Administration SOLLTEN Rollen und Verantwortlichkeiten getrennt werden.

APP.5.1.A12 Schulung zu Sicherheitsmechanismen von Groupware-Clients für Beutzer [Leiter IT, Informationssicherheitsbeauftragter (ISB)]

Es SOLLTEN alle Benutzer für die Arbeit mit dem Groupware-Client geschult und eingewiesen werden. Dabei SOLLTE den Benutzern gezeigt werden, welche Sicherheitsmechanismen verfügbar sind und wie sie eingesetzt werden können. Wer Groupware nutzt, SOLLTE für Gefährdungen und einzuhaltende Sicherheitsmaßnahmen sensibilisiert werden. Die Benutzer SOLLTEN über potenzielles Fehlverhalten belehrt werden. Sie SOLLTEN auch davor gewarnt werden, an E-Mail-Kettenbriefen teilzunehmen und viele Mailinglisten zu abonnieren.

APP.5.1.A13 Verifizierung der zu übertragenden Daten vor Weitergabe und Beseitigung von Restinformationen [Leiter IT, Benutzer]

Bevor eine Datei per E-Mail über einen Groupware-Dienst verschickt wird, SOLLTE überprüft werden, ob diese Restinformationen enthält, die nicht veröffentlicht werden dürfen. Alle Benutzer SOLLTEN über die Gefahren von Rest- und Zusatzinformationen in Dateien sensibilisiert werden. Um diese Gefahren zu minimieren, SOLLTEN Dateien stichprobenhaft auf enthaltene Restinformationen überprüft wer-

den. Alle Zusatzinformationen (Dateieigenschaften) von Dateien in Standardsoftwareformaten SOLLTEN ermittelt, überprüft und falls erforderlich angepasst werden, bevor sie weitergegeben werden. Ebenso SOLLTE darauf geachtet werden, dass die Dateien keine sogenannten Slack Bytes enthalten.

APP.5.1.A14 Vermeidung problematischer Dateiformate [Benutzer]

Es SOLLTE vorgegeben werden, wie mit E-Mails im HTML-Format, mit anderen Dateiformaten und Dateianhängen umzugehen ist. Für HTML-formatierten E-Mails SOLLTE eine Richtlinie erstellt werden, die auf entsprechende Inhalte von Benutzerschulungen, Weiterleitungseinstellungen, Umwandlungsoptionen (z. B. in Textformate), Benutzerhinweise sowie auf mögliche sichere und gesonderte Arbeitsplätze eingeht.

APP.5.1.A15 Protokollierung von Groupware-Systemen [Leiter IT]

Es SOLLTEN alle sicherheitsrelevanten Ereignisse von Groupware-Systemen protokolliert werden. Dafür SOLLTE ein geeignetes Protokollierungskonzept erstellt werden. Der Zugriff auf die Protokolldaten SOLLTE eingeschränkt werden. Wichtige Systemereignisse, wie Änderungen, Fehler und Störungen an Hardware, Betriebssystem, Treibern, Diensten und sonstiger Software, SOLLTEN protokolliert und regelmäßig ausgewertet werden.

APP.5.1.A16 Umgang mit SPAM [Leiter IT, Informationssicherheitsbeauftragter (ISB), Benutzer]

Grundsätzlich SOLLTEN alle Benutzer unerwünschte E-Mails ignorieren und löschen. Es SOLLTE auf unerwünschte E-Mails NICHT geantwortet, Links in der E-Mail gefolgt oder ein Anhang ausgeführt werden. Falls die Institution E-Mail-Filterprogramme einführen möchte, SOLLTE das mit dem Datenschutzbeauftragten, der Personalvertretung und den Benutzern abgesprochen werden. Für Newsgroups und Mailinglisten SOLLTEN Regelungen erstellt werden.

APP.5.1.A17 Auswahl eines Groupware- oder Mail-Providers [Vorgesetzte, Datenschutzbeauftragter]

Soll kein eigener Groupware-Server betrieben werden, sondern ein Dienstleister für den Betrieb des Groupware-Server beauftragt werden, SOLLTEN die funktionalen Aspekte identifiziert und mit dem möglichen Provider abgestimmt werden. Auch SOLLTE sichergestellt werden, dass der Groupware- oder Mail-Provider alle erforderlichen Sicherheitsmechanismen umsetzt und dass seine Server sicher betrieben werden. Benötigte interne Anforderungen SOLLTEN unter der Betrachtung von juristischen Aspekten schriftlich fixiert werden. Es SOLLTEN alle Mitarbeiter darüber informiert werden, was dabei zu beachten ist, wenn sie externe Groupware-Dienste benutzen.

APP.5.1.A18 Spam- und Virenschutz durch Einsatz eines E-Mail-Scanners auf dem Mailserver [Informationssicherheitsbeauftragter (ISB)]

Auf dem zentralen Mailserver SOLLTE ein E-Mail-Scanner mit integriertem speicher resistenten Virenschutzprogramm installiert werden, der eingehende und ausgehende E-Mails, insbesondere deren Anhänge, auf Spam-Merkmale und schädliche Inhalte überprüft. Da verschlüsselte E-Mails nicht automatisch überprüft werden können, SOLLTE auch festgelegt werden, wie mit solchen E-Mails zu verfahren ist. Wenn ein E-Mail-Scanner genutzt wird, SOLLTEN darüber alle Mitarbeiter, der Datenschutzbeauftragte und der Personalvertretung informiert werden.

APP.5.1.A19 Verschlüsselung von Groupware [Leiter IT, Informationssicherheitsbeauftragter (ISB), Benutzer]

Daten, die durch Groupware-Systeme übermittelt werden, SOLLTEN mithilfe geeigneter Schutzmechanismen abgesichert werden. So SOLLTE mit Verschlüsselungsverfahren und digitalen Signaturen die Integrität und Vertraulichkeit elektronisch übermittelter Informationen sichergestellt werden, beispielsweise durch eine TLS-Verbindungsverschlüsselung.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

APP.5.1.A20 Erstellen eines Notfallplans für den Ausfall von Groupware-Systemen [Notfallbeauftragter, Leiter IT, Informationssicherheitsbeauftragter (ISB)] (A)

Es SOLLTE ein Konzept entworfen werden, wie die Folgen eines Ausfalls minimiert werden können und was bei einem Ausfall zu tun ist. Die Notfallplanung für das eingesetzte Groupware-System SOLLTE den existierenden Notfallplan der Institution berücksichtigen. Wichtige Aufgaben, um das Groupware-System aufrechtzuerhalten bzw. wieder in Betrieb nehmen zu können, SOLLTEN so beschrieben sein, dass sie von entsprechend geschultem Personal durchgeführt werden können. Es SOLLTE ein Wiederanlaufplan für das Groupware-System erstellt werden, der beschreibt, wie die Systeme nach einem Ausfall wieder geregelt hochzufahren sind. Notfallübungen zur Systemwiederherstellung SOLLTEN regelmäßig, auch alle Aspekte eines Systemausfalls bzw. einer Kompromittierung berücksichtigt, durchgeführt werden.

APP.5.1.A21 Ende-zu-Ende Verschlüsselung (CI)

Um schutzbedürftige Informationen über alle Kommunikationspartner hinweg vertraulich zu halten, SOLLTE eine Ende-zu-Ende-Verschlüsselung eingesetzt werden. Es SOLLTEN nur Protokolle zur Verschlüsselung genutzt werden, die dem heutigen Stand der Technik entsprechen (siehe CON.1 Kryptokonzept).

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [ISF] The Standard of Good Practice
  Information Security Forum (ISF), 06.2016

- [KOLAB] Kolab Groupware
  Dokumentation, (zuletzt abgerufen am 29.09.2017)
  https://docs.kolab.org/

- [TN170645] Exchange Server 2016
  Microsoft Technet, (zuletzt abgerufen 29.09.2017)
  https://technet.microsoft.com/de-de/library/mt170645(v=exchg.160).asp

- [ZIMBRA] Zimbra Groupware
  Dokumentation, (zuletzt abgerufen am 29.09.2017)
  https://www.zimbra.com/documentation/

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Allgemeine Groupware" von Bedeutung.

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.33 Personalausfall

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.11	G 0.14	G 0.15	G 0.16	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.25	G 0.26	G 0.27	G 0.28	G 0.30	G 0.31	G 0.32	G 0.33	G 0.36	G 0.37	G 0.40	G 0.41	G 0.42	G 0.45	G 0.46
APP.5.1.A1			x				x		x				x	x	x									
APP.5.1.A2			x				x	x				x		x	x									
APP.5.1.A3					x															x			x	x
APP.5.1.A4				x					x	x													x	
APP.5.1.A5						x													x					x
APP.5.1.A6		x			x	x											x							x
APP.5.1.A7	x				x																			
APP.5.1.A8					x																			
APP.5.1.A9			x	x								x		x	x	x		x	x					
APP.5.1.A10					x		x												x					
APP.5.1.A11		x		x		x										x		x	x					
APP.5.1.A12					x		x												x					
APP.5.1.A13					x	x	x												x					
APP.5.1.A14					x		x												x					x
APP.5.1.A15								x	x												x		x	x
APP.5.1.A16							x															x	x	x
APP.5.1.A17	x				x																			
APP.5.1.A18							x	x	x														x	x
APP.5.1.A19		x		x		x			x										x					x
APP.5.1.A20	x					x				x	x									x	x			
APP.5.1.A21		x		x		x			x										x					x

APP.5: E-Mail / Groupware / Kommunikation

APP.5.2 Microsoft Exchange und Outlook

1 Beschreibung

1.1 Einleitung

Microsoft Exchange ist eine Groupware-Lösung für mittlere bis große Institutionen. Mit ihr können elektronisch Nachrichten übermittelt werden und sie verfügt über weitere Dienste, um Workflows zu unterstützen und um mobile Geräten mittels Microsoft Exchange ActiveSync zu verwalten. Nachrichten, wie E-Mails, können mit Microsoft Exchange zentral verwaltet, zugestellt, gefiltert und versendet werden. Ebenso können typische Groupware-Anwendungen, wie Newsgroups, Kalender und Aufgabenlisten sowie Unified Messaging von Microsoft Exchange angeboten und verwaltet werden. Um die Funktionen von Microsoft Exchange nutzen zu können, ist neben dem Server-Dienst eine zusätzliche Client-Software nötig. Die Kombination aus Microsoft Exchange-Servern und Outlook-Clients wird hier als Microsoft Exchange-System bezeichnet.

Microsoft Outlook ist ein Client, der durch die Installation des Office-Pakets von Microsoft oder durch Integration in die Betriebssysteme von mobilen Geräten direkt zur Verfügung gestellt wird. Darüber hinaus ermöglicht es die Webanwendung "Outlook Web App" über den Browser z. B. auf E-Mails, Kontakte und den Kalender zuzugreifen. Diese Dienstleistung ist im Microsoft Exchange-Paket bereits enthalten.

1.2 Zielsetzung

Das Ziel dieses Bausteins über typische Gefährdungen für Microsoft Exchange und Outlook zu informieren sowie aufzuzeigen, wie Microsoft Exchange und Outlook sicher in Institutionen eingesetzt werden.

1.3 Abgrenzung

Der Baustein enthält spezifische Gefährdungen und Anforderungen für Microsoft Exchange-Systeme. Gefährdungen und Anforderungen für die spezifischen Bausteine von Serverplattform, Betriebssystem und Clients sind nicht Bestandteil des Bausteins. Diese sind in den Bausteinen SYS.1.1 Allgemeiner Server sowie SYS.1.2 Allgemeiner Client und in den jeweiligen betriebssystemspezifischen Bausteinen zu finden.

Die Anforderungen aus dem Baustein APP.5.1. Groupware sind in jedem Fall zu erfüllen. Der vorliegende Baustein präzisiert und ergänzt Anforderungen, die für Microsoft Exchange-Systeme spezifisch sind.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Microsoft Exchange und Outlook von besonderer Bedeutung:

2.1 Fehlende oder unzureichende Regelungen für Microsoft Exchange und Outlook

Übergreifende Regelungen und Vorgaben für Microsoft Exchange und Outlook sind notwendig, damit die Sicherheit der Informationen, die mit Microsoft Exchange und Outlook verarbeitet werden, gewährleistet wird. Beispielsweise können Daten verloren gehen, ungewollt verändert oder gelöscht werden, wenn Microsoft Exchange fehlerhaft und ungeregelt in das Active Directory eingebunden wird. Ähnliches gilt, wenn Postfachdatenbanken ungeregelt depubliziert und Microsoft Exchange unzureichend in der Sicherheitsrichtlinie berücksichtigt wird. Gleiches gilt, wenn die Microsoft Outlook-Clients ungeregelt auf die Microsoft Exchange-Server zugreifen können.

2.2 Fehlerhafte Migration von Microsoft Exchange

Microsoft Exchange-Systeme werden in der Praxis häufiger migriert als neu installiert. Um auf eine neue Version des Microsoft Exchange-Servers zu migrieren, muss in einigen Fällen das Betriebssystem auf eine neuere Version aktualisiert werden. Neue Betriebssysteme stellen ihrerseits oft Anforderungen an das bestehende Domänenkonzept und die existierenden Verzeichnisdienste.

Wenn die Migration nicht sorgfältig geplant und durchgeführt wird, kann die interne Kommunikation über Microsoft Exchange in der Institution massiv gestört werden, was einen Rückgang der Produktivität zur Folge haben könnte. Während der Migration können Probleme bei der Konfiguration auftreten, indem sich z. B. die Konfigurationseinstellungen für die unterschiedlichen Versionen geändert haben oder bei der Anbindung an Verzeichnisdienste. Des Weiteren können fehlerhafte Protokolleinstellungen zu Unregelmäßigkeiten bei der Informationsübermittlung, Authentisierung und Verschlüsselung führen.

2.3 Unzulässiger Browserzugriff auf Microsoft Exchange

Mit Microsoft Exchange können die Anwender über einen Browser auf das eigene E-Mail-Konto zugreifen. Hierzu werden die Internet Information Services (IIS) verwendet, die fester Bestandteil des Microsoft Exchange-Servers sind. Wenn diese Funktion unsachgemäß geplant und fehlerhaft konfiguriert wird, kann unter Umständen unkontrolliert von außen auf das interne Netz zugegriffen werden.

Wenn über einer Browser, der aus dem Internet genutzt wird, auf die E-Mails zugegriffen werden soll, birgt dies ein großes Gefahrenpotenzial. Ohne direkten Zugriff auf das Netz der Institution könnten Angreifer auf die E-Mails zugreifen und so unter anderem E-Mail-Adressen und -Inhalte ausspähen, E-Mail-Funktionen missbrauchen, Spam-Mails verschicken sowie Zugang zu firmeninternen Informationen erhalten.

2.4 Unerlaubte Anbindung anderer Systeme an Microsoft Exchange

Microsoft Exchange-Systeme sind eng mit dem Betriebssystem Microsoft Windows verzahnt und arbeiten durch sogenannte Konnektoren mit Fremdsystemen zusammen. Mithilfe der Konnektoren (auch Connectors genannt) ist es anderen Systemen möglich, über bestimmte Protokolle (z. B. POP3) E-Mails von Microsoft Exchange-Servern abzurufen.

Wenn bei einer Migration von Microsoft Exchange die Konnektoren nicht mit berücksichtigt werden, können die vorhandenen Konnektoren inkompatibel zu der migrierten Microsoft Exchange-Version sein. Hierdurch können E-Mails verloren gehen oder ungewollt verändert werden.

Außerhalb des homogenen Microsoft-Umfelds sind Sicherheitsstellungen, die sich nicht auf das Microsoft Exchange-System beziehen, ungültig. Ebenso verhält es sich mit festgelegten Sicherheitsparametern in Microsoft Exchange, die sich auf den Windows Server beziehen. Wenn verschiedene Teilsysteme separat administriert werden, können stets Inkonsistenzen auftreten. Unsachgemäß angebundene Fremdsysteme können zudem zur Folge haben, dass Daten verloren gehen oder das System blockiert wird.

2.5 Fehlerhafte Administration von Zugangs- und Zugriffsrechten unter Microsoft Exchange und Outlook

Werden Zugangsrechte zu einem Microsoft Outlook-Client bzw. auf innerhalb von Microsoft Exchange und Outlook gespeicherte Daten fehlerhaft angelegt und administriert, können Sicherheitslücken entstehen. Dies ist beispielsweise der Fall, wenn über die notwendigen Rechte hinaus zusätzliche Rechte vergeben werden und dadurch unberechtigte Personen auf vertrauliche Informationen zugreifen können.

2.6 Fehlerhafte Konfiguration von Microsoft Exchange

Eine häufige Ursache für erfolgreiche Angriffe auf Dienste wie Microsoft Exchange sind fehlerhaft konfigurierte Systeme. Da ein Microsoft Exchange-System sehr komplex ist, können durch diverse Konfigurationseinstellungen und durch die sich gegenseitig beeinflussenden Parameter zahlreiche Sicherheitsprobleme entstehen. Die möglichen Fehlkonfigurationen erstrecken sich von der Installation und dem Betrieb der Microsoft Exchange-Komponenten auf ungeeigneten Systemen über nicht getätigte Verschlüsselungen und unzureichende Zugriffsbeschränkungen auf Microsoft Exchange-Servern bis hin zur fehlerhaften Rechtevergabe bei der Erzeugung oder Initialisierung einer Microsoft Exchange-Datenbank.

2.7 Fehlerhafte Konfiguration von Outlook

Der E-Mail-Client Microsoft Outlook ist ein wichtiger Teil des Microsoft Exchange-Systems. Für die Gesamtsicherheit des Systems ist es wichtig, dass der Client korrekt konfiguriert ist. Schon das ausgewählte Kommunikationsprotokoll kann spezielle Sicherheitsprobleme nach sich ziehen. Ebenso könnten private Schlüssel kompromittiert werden, mit denen E-Mails verschlüsselt und signiert werden. Wird auf Netzebene verschlüsselt, zum Beispiel durch IPSec oder TLS, kann dieser Verschlüsselungsmechanismus bei einem fehlerhaft konfigurierten Client unwirksam werden. Durch Fehlkonfiguration können Sicherheitsprobleme entstehen, zum Beispiel der Verlust der Vertraulichkeit durch unbefugten Zugriff.

2.8 Fehlfunktionen und Missbrauch selbst entwickelter Makros sowie Programmierschnittstellen unter Microsoft Outlook

Viele Softwarehersteller sehen in ihren Tools und Anwendungen Programmierschnittstellen vor, zum Beispiel als Application Programming Interface (API). Diese erlauben es, bestimmte Funktionen auch aus anderen Programmen heraus zu nutzen oder den Funktionsumfang der Anwendung zu erweitern. Microsoft Outlook kann missbraucht werden, um Schadsoftware zu verbreiten. Zu den Schadsoftwarevarianten zählen zum Beispiel bösartige Tools und Makros, die direkt Microsoft Outlook und die damit verbundenen E-Mail-Funktionen ausnutzen, um Informationen abzugreifen, zu verändern oder zu löschen. Makros wiederum können dazu genutzt werden, Nachrichten, Termine oder Aufgaben weiterzuleiten oder zu verschieben. Dabei können Fehler in Makros ein erhöhtes Risiko darstellen. Indexfehler innerhalb von Makros können zu falschen Ergebnissen und zu möglicherweise unwirtschaftlichen Entscheidungen in der Institution führen. Spezifische Folgen können unnötige Kosten oder ein automatisierter Datenabfluss sein.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Microsoft Exchange und Outlook aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Informationssicherheitsbeauftragter (ISB), Leiter IT, Notfallbeauftragter

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

APP.5.2.A1 Planung des Einsatzes von Microsoft Exchange und Outlook [Leiter IT, Informationssicherheitsbeauftragter (ISB)]

Bevor Microsoft Exchange und Outlook eingesetzt werden können, MUSS der Einsatz von Microsoft Exchange und Outlook sorgfältig geplant werden. Dabei MÜSSEN mindestens folgende Punkte beachtet werden:

- Aufbau der E-Mail-Infrastruktur,
- anzubindende Clients beziehungsweise Server-Systeme,
- Nutzung von funktionalen Erweiterungen,
- Absicherung der Zugangsports der Server- /Client-Komponenten,
- Vertraulichkeit, Integrität und Verfügbarkeit,
- zu verwendende Protokolle und
- Integration der Server- und Client-Systeme in die hierfür vorgesehenen Netzsegmente.

APP.5.2.A2 Auswahl einer geeigneten Microsoft Exchange-Infrastruktur [Leiter IT]

Es MUSS entschieden werden, mit welchen Systemen und Anwendungskomponenten, sowie in welcher hierarchischen Abstufung die Microsoft Exchange-Infrastruktur realisiert werden sollte. Im Rahmen der Auswahl MUSS auch entschieden werden, ob die Systeme als Cloud- oder lokaler Dienst betrieben werden sollen.

APP.5.2.A3 Berechtigungsmanagement

Für die Systeme der Microsoft Exchange-Infrastruktur MUSS ein Berichtigungskonzept erstellt, geeignet dokumentiert und angewendet werden. Es MÜSSEN den privilegierten Anwendern, sowie den Administratoren nur so viele Berechtigungen eingeräumt, wie für die Aufgabenerfüllung notwendig ist (Minimalprinzip). Es MUSS regelmäßig überprüft werden, ob die zugeteilten Rechte noch angemessen sind.

APP.5.2.A4 Zugriffsrechte auf Microsoft Exchange-Objekte

Die Zugriffsberechtigungen auf Microsoft Exchange-Objekte MÜSSEN auf Grundlage der das Prinzip des geringsten Privilegs (least privilege) festgelegt werden. Es MÜSSEN serverseitige Benutzerprofile für einen rechnerunabhängigen Zugriff auf Microsoft Exchange-Daten verwendet werden. Die Standard-NTFS-Berechtigungen auf das Microsoft Exchange-Verzeichnis MÜSSEN angepasst werden, sodass nur autorisierte Administratoren und Systemkonten auf die Daten in diesem Verzeichnis zugreifen können.

APP.5.2.A5 Datensicherung von Microsoft Exchange [Notfallbeauftragter]

Das bestehende Microsoft Exchange-System MUSS vor Installationen und Konfigurationsänderungen sowie in zyklischen Abständen gesichert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Microsoft Exchange und Outlook. Sie SOLLTEN grundsätzlich umgesetzt werden.

APP.5.2.A6 Sichere Installation eines Microsoft Exchange-Systems

Die Installation SOLLTE auf Basis der Einsatzplanung von Microsoft Exchange und Outlook und der festgelegten Sicherheitsrichtlinie erfolgen (siehe APP.1.2.A1 Planung des Einsatzes von Microsoft Exchange und Outlook). Da sich Microsoft Exchange-Systeme sehr stark in die Windows Umgebung integrieren, speziell in das Active Directory, SOLLTEN die entsprechenden spezifischen Sicherheitsrichtlinien berücksichtigt werden. Die Systeme, auf denen Microsoft Exchange und Outlook installiert werden soll, SOLLTEN geeignet abgesichert sein.

APP.5.2.A7 Migration von Microsoft Exchange-Systemen

Alle Migrationsschritte SOLLTEN gründlich geplant und dokumentiert werden. Es SOLLTEN die Microsoft Windows-Systemadministratoren an der Planung beteiligt werden. Es SOLLTEN bei der Planung der Migration Postfächer, Objekte, Sicherheitsrichtlinien, Active-Directory-Konzepte, E-Mail-Systeme und Funktionsunterschiede bei Microsoft Exchange und Outlook in den verschiedenen Versionen berücksichtigt werden. Das neue System SOLLTE, bevor es installiert wird, in einem separaten Testnetz geprüft werden, um Softwarefehlern und Kompatibilätsproblemen entgegenzuwirken.

APP.5.2.A8 Sicherer Betrieb von Microsoft Exchange

Alle Systeme und Anwendungen der Infrastruktur SOLLTEN so konfiguriert sein, dass sie den Schutzbedarf angemessen erfüllen. Dafür SOLLTE eine passende Basiskonfiguration zusammengestellt und dokumentiert werden. Die Einstellungen der einzelnen Konnektoren SOLLTEN ebenfalls angepasst werden.

Die Verantwortlichen SOLLTEN bekannt gewordene Schwachstellen zeitnah in Abhängigkeit vom Schutzbedarf und der Kritikalität beheben. Generell SOLLTE darauf geachtet werden, dass Patches und Updates nur aus vertrauenswürdigen Quellen bezogen werden.

APP.5.2.A9 Sichere Konfiguration von Microsoft Exchange-Servern

Microsoft Exchange-Server SOLLTEN aufbauend auf den Vorgaben aus dem Sicherheitskonzept konfiguriert werden. Es SOLLTE eine maximal zulässige Größe sowohl für eingehende als auch für ausgehende Nachrichten eingestellt werden. Vorhandene Konnektoren SOLLTEN geeignet konfiguriert werden. Die Protokollierung des Microsoft Exchange-Systems SOLLTE aktiviert werden. Für vorhandenes Customizing SOLLTE ein entsprechendes Konzept erstellt werden.

Bei der Verwendung von funktionalen Erweiterungen (zum Beispiel Microsoft Exchange Access Sync, Spiegelport, Spamfilter, Outlook Web-App oder Data Loss Prevention) SOLLTE sichergestellt sein, dass die definierten Anforderungen an die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit weiterhin erfüllt sind.

APP.5.2.A10 Einstellungen von Outlook

Nur Administratoren SOLLTEN die Outlook-Umgebung ändern können. Dazu SOLLTE für jeden Anwender ein eigenes Outlook-Profil mit den benutzerspezifischen Einstellungen angelegt werden. Die Anwender SOLLTEN nur ausgewählte Einstellungen (z. B. Signatur einrichten, Abwesenheitsagent aktivieren) benutzerdefiniert verändern können. . Dateianhänge SOLLTEN prinzipiell nicht automatisch aus E-Mails heraus geöffnet werden können. Vorschaufenster und die Autovorschau SOLLTE deaktiviert werden. E-Mails SOLLTEN NICHT automatisiert weitergeleitet werden.

APP.5.2.A11 Absicherung der Kommunikation von und zu Microsoft Exchange-Systemen

Es SOLLTE nachvollziehbar entschieden werden, mit welchen Schutzmechanismen die Kommunikation von und zu Microsoft Exchange-Systemen abgesichert wird. Es SOLLTE entschieden und nachvollziehbar dokumentiert werden, welches der verschiedenen möglichen Verfahren Internet Protocol Security (IPSec) oder Transport Layer Security (TLS) eingesetzt werden soll.

Es SOLLTEN die

- Administrationsschnittstellen,
- Client-Server-Kommunikation,
- vorhandene Web-based-Distributed-Authoring-and-Versioning-(WebDAV)-Schnittstellen,
- die Server-Server-Kommunikation, die Nachrichten-Kommunikation und
- die Public-Key-Infrastruktur, die auf der E-Mail-Verschlüsselung von Microsoft Outlook (S/MIME) basieren,

verschlüsselt werden.

APP.5.2.A12 Einsatz von Microsoft Exchange für Outlook Anywhere

Outlook Anywhere SOLLTE entsprechend der Sicherheitsanforderungen der Institution konfiguriert werden. Der Zugriff auf Microsoft Exchange über das Internet SOLLTE auf die notwendigen Anwender beschränkt werden. Die Kommunikation zu Outlook Anywhere SOLLTE verschlüsselt werden (siehe APP.1.2.A11 Absicherung der Kommunikation von und zu Microsoft Exchange-Systemen).

APP.5.2.A13 Schulung von Administratoren [Leiter IT]

Für den Betrieb der Komponenten der Microsoft Exchange-Infrastruktur SOLLTE nur geeignetes und geschultes Personal eingesetzt werden.

APP.5.2.A14 Schulung zu Sicherheitsmechanismen von Outlook für Anwender [Informationssicherheitsbeauftragter (ISB)]

Outlook-Anwender SOLLTEN regelmäßig über bestehende und neue Gefahren beim Arbeiten mit Microsoft Outlook sensibilisiert und geschult werden. Allen Anwendern SOLLTEN relevante Sicherheitsmechanismen und die entsprechenden Vorgehensweisen innerhalb von Outlook vermittelt werden. Hierbei SOLLTEN Regelungen z. B. für Zugriffsmechanismen, Authentisierungsformen und kryptografische Vorgaben für die E-Mail-Verschlüsselung berücksichtigt werden.

APP.5.2.A15 Anwendungsdokumentation für Microsoft Exchange

Die Inhalte des Betriebshandbuches für Microsoft Exchange SOLLTEN nachvollziehbar dokumentiert sein. Das Betriebshandbuch SOLLTE angelehnt an den Lebenszyklus die Phasen Inbetriebnahme, Betrieb, Aussonderung und Wiederanlauf aufgebaut sein. Die Dokumentation SOLLTE gegen unbefugten Zugriff geschützt werden. Änderungen SOLLTEN nachvollziehbar dokumentiert bzw. referenziert sein.

APP.5.2.A16 Erstellung eines Notfallplans für den Ausfall von Microsoft Exchange und Outlook [Notfallbeauftragter]

Im Rahmen der Notfallvorsorge SOLLTE ein Konzept entworfen werden, mit dem sich die Folgen eines Ausfalls der Microsoft Exchange und Outlook-Komponenten minimieren lassen. Im Notfallplan SOLLTE definiert werden, was bei einem Ausfall zu tun ist, um eine zeitnahe Wiederherstellung des Normalbetriebs zu gewährleisten.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

APP.5.2.A17 Verschlüsselung von Microsoft Exchange-Systemdatenbanken (CIA)

Es SOLLTE ein Konzept für die Verschlüsselung von pst-Dateien und Informationsspeicher-Dateien erstellt werden. Die Anwender SOLLTEN über die Funktionsweise und die Schutzmechanismen bei der Verschlüsselung von pst-Dateien informiert werden. Weitere Aspekte für lokale pst-Dateien, die berücksichtigt werden SOLLTEN, wenn Microsoft Exchange-Systemdatenbanken verschlüsselt werden, sind:

- eigene Verschlüsselungsfunktionen,
- Verschlüsselungsgrade sowie
- Mechanismen zur Absicherung der Daten in einer pst-Datei.

Mechanismen wie z. B. Encrypting File System oder Windows BitLocker Laufwerkverschlüsselung SOLLTEN zur Absicherung der Daten in einer pst-Datei genutzt werden.

APP.5.2.A18 Regelmäßige Sicherheitsprüfungen für Microsoft Exchange-Systeme (CIA)

Das Microsoft Exchange-System SOLLTE regelmäßig auf Fehlkonfigurationen und Schwachstellen geprüft wird. Dafür SOLLTE es regelmäßig einer Sicherheitsprüfung durch unterschiedliche Personen unterzogen werden. Es empfiehlt sich, dafür eine Prüfliste aufzubauen, um einen definierten Prüfumfang zu gewährleisten. Folgende Aspekte SOLLTEN bei einer Prüfung berücksichtigt werden:

- regelmäßige Recherchen sicherheitsrelevanter Informationen,
- Berechtigungen für Revisionsbenutzer,
- regelmäßige Prüfung der Berechtigungen,
- Prüfung der Aktualität der Updates und
- Prüfung der Sicherheit der Kommunikationsschnittstellen.

Die Microsoft Exchange-Berechtigungen SOLLTEN regelmäßig mindestens stichprobenartig geprüft werden.

4 Weiterführende Informationen

4.1 Literatur

- [TecNet] Microsoft Technet
  Microsoft Technet, (zuletzt abgerufen am 29.09.2017)
  https://technet.microsoft.com/de-de

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Microsoft Exchange und Outlook" von Bedeutung.

G 0.15 Abhören

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.36 Identitätsdiebstahl

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.45 Datenverlust

Elementare Gefährdungen / Anforderungen	G 0.15	G 0.16	G 0.18	G 0.19	G 0.21	G 0.22	G 0.25	G 0.26	G 0.28	G 0.30	G 0.31	G 0.32	G 0.36	G 0.40	G 0.45
APP.5.2.A1			x	x		x								x	
APP.5.2.A2			x		x		x	x							
APP.5.2.A3										x	x	x	x		
APP.5.2.A4						x				x		x			
APP.5.2.A5				x											x
APP.5.2.A6					x					x					
APP.5.2.A7			x				x	x							
APP.5.2.A8								x	x						
APP.5.2.A9						x			x						
APP.5.2.A10					x				x	x	x	x			
APP.5.2.A11	x			x		x									
APP.5.2.A12	x			x		x							x		
APP.5.2.A13										x	x				
APP.5.2.A14										x	x				
APP.5.2.A15			x				x	x							
APP.5.2.A16							x	x						x	
APP.5.2.A17				x						x					
APP.5.2.A18					x			x							

Bundesamt
für Sicherheit in der
Informationstechnik

SYS: IT-Systeme

SYS.1.1	Allgemeiner Server	459
SYS.1.2.2	Windows Server 2012	470
SYS.1.3	Server unter Unix	478
SYS.1.5	Virtualisierung	484
SYS.1.8	Speicherlösungen	493
SYS.2.1	Allgemeiner Client	503
SYS.2.2.2	Clients unter Windows 8.1	515
SYS.2.2.3	Clients unter Windows 10	524
SYS.2.3	Clients unter Unix	533
SYS.3.1	Laptops	540
SYS.3.2.1	Allgemeine Smartphones und Tablets	547
SYS.3.2.2	Mobile Device Management (MDM)	556
SYS.3.2.3	iOS (for Enterprise)	565
SYS.3.2.4	Android	577
SYS.3.4	Mobile Datenträger	582
SYS.4.1	Drucker, Kopierer und Multifunktionsgeräte	589
SYS.4.4	Allgemeines IoT-Gerät	597

SYS.1: Server

SYS.1.1 Allgemeiner Server

1 Beschreibung

1.1 Einleitung

Dieser Baustein deckt allgemeine Sicherheitsanforderungen für alle IT-Systeme ab, die anderen IT-Systemen Dienste bereitstellen, wie Clients oder anderen Servern. Diese Dienste können Basisdienste für das lokale oder externe Netz sein, aber auch den E-Mail-Austausch ermöglichen oder Datenbanken und Druckerdienste anbieten. Server haben eine zentrale Bedeutung für die Informationstechnik und damit für funktionierende Arbeitsabläufe einer Institution. Oft erfüllen Server Aufgaben, ohne dass eine direkte interaktive Nutzung durch einen Benutzer erfolgt. Ergänzend gibt es Serverdienste, die direkt mit den Anwendern interagieren und nicht auf den ersten Blick als Server-Dienst wahrgenommen werden, beispielsweise X-Server unter Unix.

1.2 Zielsetzung

Ziel dieses Bausteins ist der Schutz von Informationen, die auf Servern verarbeitet, angeboten oder darüber übertragen werden, sowie der damit zusammenhängenden Dienste.

1.3 Abgrenzung

In der Regel werden Serversysteme unter Betriebssystemen betrieben, bei denen jeweils spezifische Sicherheitsanforderungen zu berücksichtigen sind. Für verbreitete Server-Betriebssysteme sind im IT-Grundschutz-Kompendium eigene Bausteine vorhanden, die diesen Baustein präzisieren. Der Baustein "Allgemeiner Server" bildet die Grundlage für die konkreten Bausteine, auf der diese aufbauen. Sofern für ein betrachtetes System ein konkreter Baustein existiert, ist dieser zusätzlich zum Baustein Allgemeiner Server anzuwenden. Falls für eingesetzte Serversysteme kein spezifischer Baustein existiert, müssen die Anforderungen dieses Bausteins geeignet konkretisiert werden.

Die jeweils spezifischen Dienste, die vom Server angeboten werden, sind nicht Bestandteil dieses Bausteins. Für diese Server-Dienste müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz. Soweit für ein Serversystem im Einzelfall auch eine interaktive Nutzung durch Benutzer vorgesehen ist (z. B. Terminalserver), sind die damit verbundenen Sicherheitsaspekte ebenfalls gesondert zu betrachten, beispielsweise indem die entsprechenden konkretisierten Bausteine angewendet werden.

2 Gefährdungslage

Die folgenden spezifischen Bedrohungen und Schwachstellen sind für Allgemeine Server von besonderer Bedeutung.

2.1 Software-Schwachstellen oder -Fehler

Je komplexer Software ist, desto häufiger treten Programmier- oder Designfehler auf. Unter Software-Schwachstellen werden unbeabsichtigte Programmfehler verstanden, die dem Anwender nicht oder noch nicht bekannt sind und ein Sicherheitsrisiko für das IT-System darstellen. Es werden ständig neue Sicherheitslücken in vorhandener, auch in weitverbreiteter oder ganz neuer Software gefunden.

Werden Softwarefehler nicht erkannt und zeitnah behoben, können die bei der Anwendung entstehenden Fehler weitreichende Folgen haben. Bei weitverbreiteter Standardsoftware können Software-Schwachstellen schnell dazu führen, dass schwerwiegende Sicherheitsprobleme für alle Arten von Institutionen entstehen können.

Insbesondere Fehler in Serverdiensten können gravierende Auswirkungen haben. Bei einer Schwachstelle oder einem Fehler in einem Netzdienst sind keine lokalen Zugriffsrechte notwendig, um diese auszunutzen, oft reicht es, dass der Angreifer über das Netz zugreifen kann. Bietet der Server den Serverdienst mit der Schwachstelle oder dem Fehler im Internet an, könnte unter Umständen von jedem IT-System weltweit dieser Fehler oder diese Schwachstelle ausgenutzt werden.

2.2 Datenverlust

Der Verlust von Daten kann besonders bei Servern erhebliche Auswirkungen auf Geschäftsprozesse und damit auf die gesamte Institution haben. Sehr viele IT-Systeme, wie Clients oder andere Server, sind oft darauf angewiesen, dass die dort zentral gespeicherten Daten verfügbar sind.

Wenn geschäftsrelevante Informationen, egal welcher Art, zerstört oder verfälscht werden, können dadurch Geschäftsprozesse und Fachaufgaben verzögert oder sogar deren Ausführung verhindert werden. Insgesamt kann der Verlust gespeicherter Daten, neben dem Ausfall und den Kosten für die Wiederbeschaffung der Daten, vor allem zu langfristigen Konsequenzen, wie Vertrauenseinbußen bei Kunden und Partnern, juristischen Auswirkungen sowie einem negativen Eindruck in der Öffentlichkeit, führen. In vielen Institutionen existieren Regelungen, dass keine Daten auf den lokalen Clients gespeichert werden dürfen, sondern hierfür zentrale Ablagen auf den Servern genutzt werden müssen. Ein Datenverlust dieser Daten hat dann gravierende Auswirkungen, von den verursachten direkten und indirekten Schäden können Institutionen sogar in ihrer Existenz bedroht sein.

2.3 Verhinderung von Diensten

Eine Art eines Angriffs auf die Verfügbarkeit, der "Denial of Service" genannt wird, zielt darauf ab, die Benutzer daran zu hindern, Funktionen oder Geräte zu verwenden, die ihnen normalerweise zur Verfügung stehen. Dieser Angriff steht häufig im Zusammenhang mit verteilten Ressourcen, indem ein Angreifer diese Ressourcen so stark in Anspruch nimmt, dass andere Benutzer an der Arbeit gehindert werden und nicht mehr auf Ressourcen, von denen sie abhängig sind, zugreifen können. In der Regel sind IT-Systeme auch stark voneinander abhängig, von der Verknappung der Ressourcen eines Servers sind schnell weitere Server betroffen. Es können zum Beispiel CPU-Zeit, Speicherplatz oder Bandbreite künstlich verknappt werden, dies kann dazu führen, dass der Dienst oder eine Ressource überhaupt nicht mehr genutzt werden kann.

2.4 Bereitstellung unbenötigter Betriebssystemkomponenten und Applikationen

Schon bei der Installation des Server-Betriebssystems besteht die Möglichkeit, alle mitgelieferten Applikationen und Dienste zu installieren. Auch im Betrieb wird oft Software installiert, die kurz getestet, aber danach nicht mehr benötigt wird. Oft ist gar nicht bekannt, dass diese nicht genutzten Anwendungen und Dienste auf den Servern vorhanden sind. Auf diese Weise befinden sich zahlreiche Applikationen und Dienste auf dem Server, die nicht eingesetzt werden und so den Server unnötig belasten.

Solche nicht genutzten Anwendungen und Dienste können Schwachstellen enthalten. Wenn die Anwendungen dann nicht mehr aktualisiert werden, können sie ein Einfallstor für Angreifer sein. Sind die installierten Anwendungen und Dienste unbekannt, ist dem IT-Betrieb nicht bewusst, dass diese ebenfalls aktualisiert werden müssen.

2.5 Überlastung von Servern

Wenn Server nicht ausreichend dimensioniert sind, ist irgendwann der Punkt erreicht, an dem sie den Anforderungen der Benutzer nicht mehr gerecht werden. Je nach Art der betroffenen Systeme kann dies eine Vielzahl von negativen Auswirkungen haben, beispielsweise dass die Server oder Dienste vorübergehend nicht verfügbar sind oder dass Datenverluste auftreten. Die Überlastung eines einzelnen Servers kann bei komplexen IT-Landschaften dazu führen, das bei weiteren Servern Probleme oder Ausfälle auftreten können.

Auslöser für die Überlastung von Informationssystemen können sein, dass

- installierte Dienste oder Anwendungen falsch konfiguriert sind und so unnötig Speicher beanspruchen,
- vorhandene Speicherplatzkapazitäten überschritten werden,
- zahlreiche Anfragen zur gleichen Zeit ein System überbeanspruchen und dadurch die Prozessoren überlastet werden,
- zu viel Rechenleistung von den Diensten beansprucht wird oder
- eine große Anzahl Nachrichten zur gleichen Zeit versendet werden.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz von allgemeinen Servern aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Haustechnik

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.1.1.A1 Geeignete Aufstellung [Haustechnik]

Server MÜSSEN an Orten betrieben werden, zu denen nur berechtigte Personen Zutritt haben. Server MÜSSEN daher in Rechenzentren, Rechnerräumen oder abschließbaren Serverschränken aufgestellt beziehungsweise eingebaut werden, siehe hierzu die entsprechenden Bausteine. Es MUSS geregelt werden, wer Zutritt zu den Räumen beziehungsweise physischen Zugang auf die Server selbst erhält. Server DÜRFEN NICHT als Arbeitsplatzrechner genutzt werden.

Es MUSS auf eine geeignete räumliche Trennung der Systeme, die gesichert werden sollen, von den sichernden Systemen, etwa Backup-Servern in unterschiedlichen Brandabschnitten, geachtet werden, um die Auswirkungen bei einem physischen Schaden zu begrenzen.

SYS.1.1.A2 Benutzerauthentisierung

Um den Server zu nutzen, MÜSSEN sich die Benutzer gegenüber dem IT-System authentisieren. Sollen hierfür die Benutzer und Administratoren Passwörter verwenden, MÜSSEN sichere Passwörter benutzt werden. Hierfür SOLLTE es eine Passwort-Richtlinie geben. Diese Passwörter MÜSSEN komplex genug sein, geheim gehalten und regelmäßig gewechselt werden.

SYS.1.1.A3 Restriktive Rechtevergabe

Zugriffsrechte auf Dateien, die auf Servern gespeichert sind, MÜSSEN restriktiv vergeben werden. Jeder Benutzer DARF nur auf die Dateien Zugriffsrechte erhalten, die er für seine Aufgabenerfüllung benötigt. Das Zugriffsrecht selbst wiederum MUSS auf die notwendige Zugriffsart beschränkt sein, so ist es zum Beispiel in den seltensten Fällen notwendig, ein Schreibrecht auf Programmdateien zu vergeben.

Es SOLLTE regelmäßig überprüft werden, ob die Berechtigungen, insbesondere für Systemverzeichnisse und -dateien, den Vorgaben der Sicherheitsrichtlinie entsprechen. Auf Systemdateien SOLLTEN möglichst nur die Systemadministratoren Zugriff haben. Der Kreis der zugriffsberechtigten Administratoren SOLLTE möglichst klein gehalten werden. Auch System-Verzeichnisse SOLLTEN nur die notwendigen Privilegien für die Benutzer zur Verfügung stellen.

SYS.1.1.A4 Rollentrennung

Es MUSS sichergestellt werden, dass Kennungen mit Administratorrechten nur für Administrationsaufgaben verwendet werden. Für alle Administratoren MÜSSEN zusätzliche Benutzer-Kennungen eingerichtet werden, die nur über die eingeschränkten Rechte verfügen, die die Administratoren zur Aufgabenerfüllung außerhalb der Administration benötigen. Für Arbeiten, die nicht der Administration dienen, MÜSSEN die Administratoren ausschließlich diese Benutzer-Kennungen verwenden. Über die notwendigen Benutzer-Kennungen hinaus SOLLTEN keine weiteren Benutzer auf dem Server angelegt werden.

SYS.1.1.A5 Schutz der Administrationsschnittstellen

Abhängig von der genutzten Zugangsart (lokal, remote oder zentrales Systemmanagement) MÜSSEN geeignete Sicherheitsvorkehrungen getroffen werden. Die zur Administration verwendeten Methoden MÜSSEN in der Sicherheitsrichtlinie festgelegt werden. Die Administration MUSS entsprechend der Sicherheitsrichtlinie durchgeführt werden.

Für die Anmeldung von Benutzern und Diensten am System MÜSSEN Authentisierungsverfahren eingesetzt werden, die dem Schutzbedarf der Server angemessen sind. Dies SOLLTE in besonderem Maße für administrative Zugänge berücksichtigt werden. Soweit möglich, SOLLTE dabei auf zentrale, netzbasierte Authentisierungsdienste zurückgegriffen werden.

Die Administration MUSS über sichere Protokolle erfolgen. Es SOLLTE überlegt werden, alternativ ein eigenes Administrationsnetz einzurichten.

SYS.1.1.A6 Deaktivierung nicht benötigter Dienste und Kennungen

Alle nicht benötigten Dienste MÜSSEN von Servern deaktiviert oder deinstalliert werden, vor allem Netzdienste. Nicht benötigte Benutzerkennungen MÜSSEN entweder gelöscht oder zumindest so deaktiviert werden, dass unter diesen Kennungen keine Anmeldungen am System möglich sind. Vorhandene Standard-Kennungen MÜSSEN soweit wie möglich geändert oder deaktiviert werden. Voreingestellte Passwörter von Standard-Kennungen MÜSSEN geändert werden. Auf Servern SOLLTE der Speicherplatz für die einzelnen Benutzer, aber auch für Anwendungen, geeignet beschränkt werden.

Die getroffenen Entscheidungen SOLLTEN so dokumentiert werden, dass nachvollzogen werden kann, welche Konfiguration und Softwareausstattung für die Server gewählt wurden.

SYS.1.1.A7 Updates und Patches für Firmware, Betriebssystem und Anwendungen

Administratoren MÜSSEN sich regelmäßig über bekannt gewordene Schwachstellen der Betriebssysteme, eingesetzter Anwendungen und Dienste informieren. Die identifizierten Schwachstellen MÜSSEN so schnell wie möglich behoben werden, damit sie nicht durch Angreifer ausgenutzt werden können. Generell MUSS darauf geachtet werden, dass Patches und Updates nur aus vertrauenswürdigen Quellen bezogen werden.

Solange keine entsprechenden Patches zur Verfügung stehen, MÜSSEN abhängig von der Schwere der Schwachstellen und Bedrohungen andere geeignete Maßnahmen zum Schutz des Systems getroffen werden.

SYS.1.1.A8 Regelmäßige Datensicherung

Datensicherungen MÜSSEN vor Installationen und umfangreichen Konfigurationsänderungen sowie außerdem in festgelegten Intervallen vorgenommen werden. Diese MÜSSEN es ermöglichen, die auf dem Server gespeicherten Daten wieder herzustellen. In virtuellen Umgebungen SOLLTE geprüft werden, ob die Systemsicherung unter Umständen durch Snapshot-Mechanismen der Virtualisierungsumgebung realisiert werden kann.

SYS.1.1.A9 Einsatz von Viren-Schutzprogrammen

In Abhängigkeit des installierten Betriebssystems, des bereitgestellten Dienstes und anderer vorhandener Schutzmechanismen des Servers MUSS geprüft werden, ob Viren-Schutzprogramme eingesetzt werden sollen und können. Konkrete Aussagen, ob Viren-Schutz notwendig ist, sind in der Regel in den betriebssystemspezifschen Bausteinen des IT-Grundschutzes zu finden. Die entsprechenden Signaturen eines Viren-Schutzprogramms MÜSSEN regelmäßig aktualisiert werden. Neben Echtzeit- und On-Demand-Scans MUSS eine eingesetzte Lösung die Möglichkeit bieten, auch komprimierte und verschlüsselte Daten nach Schadprogrammen zu durchsuchen.

SYS.1.1.A10 Protokollierung

Es MUSS entschieden werden, welche Informationen durch die Server mindestens protokolliert werden sollen, wie lange die Protokolldaten aufbewahrt werden und wer unter welchen Voraussetzungen die Protokolldaten einsehen darf. Es MÜSSEN datenschutzrechtliche Vorgaben berücksichtigt werden. Generell MÜSSEN alle sicherheitsrelevanten Systemereignisse protokolliert werden. Diese umfassen mindestens:

- Systemstarts und Reboots,
- erfolgreiche und erfolglose Anmeldungen am System (Betriebssystem und Anwendungssoftware),
- fehlgeschlagene Berechtigungsprüfungen,
- blockierte Datenströme (Verstöße gegen ACLs oder Firewallregeln),
- Einrichtung oder Änderungen von Benutzern, Gruppen und Berechtigungen,
- sicherheitsrelevante Fehlermeldungen (z. B. Hardwaredefekte, Überschreitung von Kapazitätsgrenzen),
- Warnmeldungen von Sicherheitssystemen (z. B. Virenschutz).

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Allgemeiner Server. Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.1.1.A11 Festlegung einer Sicherheitsrichtlinie für Server

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die Anforderungen an Server konkretisiert werden. Die Richtlinie SOLLTE allen Administratoren und anderen Personen, die an der Beschaffung und dem Betrieb der Server beteiligt sind, bekannt sein und Grundlage für deren Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft und die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

SYS.1.1.A12 Planung des Server-Einsatzes

Jedes Serversystem SOLLTE geeignet geplant werden, dabei sind mindestens folgende Punkte zu berücksichtigen:

- Auswahl der Hardwareplattform, des Betriebssystems und der Anwendungssoftware
- Dimensionierung der Hardware (Leistung, Speicher, Bandbreite, ...)
- Art und Anzahl der Kommunikationsschnittstellen

- Leistungsaufnahme und Wärmelast, Platzbedarf und Bauform
- Realisierung administrativer Zugänge (siehe SYS.1.1.A3 Schutz der Administrationsschnittstellen)
- Zugriffe von Benutzern
- Realisierung der Protokollierung (siehe SYS.1.1.A7 Protokollierung)
- Realisierung der Systemaktualisierung (siehe SYS.1.1.A5 Updates und Patches für Betriebssystem und Anwendungen)
- Einbindung ins System- und Netzmanagement, die Datensicherung und Schutzsysteme (Virenschutz, IDS u. a.)

Alle Entscheidungen, die in der Planungsphase getroffen wurden, SOLLTEN so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

SYS.1.1.A13 Beschaffung von Servern

Bevor ein oder mehrere Server beschafft werden, SOLLTE eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden.

SYS.1.1.A14 Erstellung eines Benutzer- und Administrationskonzepts

Ablauf, Rahmenbedingungen und Anforderungen an administrative Aufgaben, sowie die Aufgabentrennungen zwischen den verschiedenen Rollen der Benutzer des IT-Systems SOLLTEN in einem Benutzer- und Administrationskonzept festgeschrieben werden.

SYS.1.1.A15 Unterbrechungsfreie und stabile Stromversorgung [Haustechnik]

Jeder Server SOLLTE an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen werden. Die USV SOLLTE hinsichtlich Leistung und Stützzeit ausreichend dimensioniert sein. Wenn Änderungen an den Verbrauchern durchgeführt wurden, SOLLTE erneut geprüft werden, ob die Stützzeit ausreichend ist. Sowohl für die USV-Geräte als auch die Server SOLLTE ein Überspannungsschutz vorhanden sein.

Die tatsächliche Kapazität der Batterie und damit die Stützzeit der USV SOLLTE regelmäßig getestet werden. Die USV SOLLTE regelmäßig gewartet werden. Die USV SOLLTE in ein vorhandenes System- und Netzmanagement eingebunden werden.

SYS.1.1.A16 Sichere Installation und Grundkonfiguration von Servern

Server SOLLTEN so aufgesetzt werden, dass bei der Installation ausschließlich die benötigten Dienste ausgewählt werden. Installationen auf einem Server SOLLTEN nur von autorisierten Personen (Administratoren oder vertraglich gebundene Dienstleister) nach einem definierten Installationsprozess durchgeführt werden. System- und Anwendungssoftware SOLLTE aus vertrauenswürdigen Installationsquellen bezogen werden. Für sich wiederholende Installationen SOLLTEN geeignete Installations-Templates erstellt und angewendet werden.

Alle Installationsschritte SOLLTEN so dokumentiert werden, dass die Installation durch einen sachkundigen Dritten anhand der Dokumentation nachvollzogen und wiederholt werden kann.

Die Grundeinstellungen von Servern SOLLTEN überprüft und nötigenfalls entsprechend den Vorgaben der Sicherheitsrichtlinie angepasst werden. Erst nachdem die Installation und die Konfiguration abgeschlossen ist, SOLLTE der Server mit dem Internet verbunden werden.

SYS.1.1.A17 Einsatzfreigabe

Bevor das Serversystem im produktiven Betrieb eingesetzt und bevor es an ein produktives Netz angeschlossen wird, SOLLTE eine Einsatzfreigabe erfolgen. Diese SOLLTE geeignet dokumentiert werden. Für die Einsatzfreigabe SOLLTEN die Installations- und Konfigurationsdokumentation und die Funktionsfähigkeit des Systems in einem Test geprüft werden. Sie SOLLTE durch eine in der Institution dafür autorisierte Stelle erfolgen.

SYS.1.1.A18 Verschlüsselung der Kommunikationsverbindungen

Für alle vom Server angebotenen und genutzten Netzdienste SOLLTE geprüft werden, ob mit vertretbarem Aufwand eine Verschlüsselung der Kommunikationsverbindungen möglich und praktikabel ist. Ist dies mit vertretbarem Aufwand möglich, SOLLTE die Verschlüsselung aktiviert werden.

SYS.1.1.A19 Einrichtung lokaler Paketfilter

Vorhandene lokale Paketfilter SOLLTEN über ein Regelwerk so ausgestaltet werden, dass die eingehende und ausgehende Kommunikation auf die erforderlichen Kommunikationspartner, Kommunikationsprotokolle bzw. Ports und Schnittstellen beschränkt werden.

SYS.1.1.A20 Beschränkung des Zugangs über Netze

Generell SOLLTE das gesamte Netz einer Institution durch ein entsprechendes Sicherheitsgateway gegen unbefugte Zugänge geschützt sein. Server, die Dienste nach außen hin anbieten, SOLLTEN in einer Demilitarisierten Zone (DMZ) aufgestellt werden.

Server SOLLTEN möglichst nicht im selben IP-Subnetz wie die Clients platziert werden. Server SOLLTEN zumindest durch einen Router von den Clients getrennt sein.

SYS.1.1.A21 Betriebsdokumentation

Betriebliche Aufgaben, die an einem Server durchgeführt werden, SOLLTEN nachvollziehbar dokumentiert werden (wer?, wann?, was?). Aus der Dokumentation SOLLTEN insbesondere Konfigurationsänderungen nachvollziehbar sein. Sicherheitsrelevante Aufgaben (wer ist z. B. befugt, neue Festplatten einzubauen) SOLLTEN dokumentiert werden. Alles, was automatisch dokumentiert werden kann, SOLLTE auch automatisch dokumentiert werden. Die Dokumentation SOLLTE gegen unbefugten Zugriff und Verlust geschützt werden.

SYS.1.1.A22 Einbindung in die Notfallplanung

Der Server SOLLTE im Notfallmanagementprozess berücksichtigt werden. Dazu SOLLTEN die Notfallanforderungen an das System ermittelt und geeignete Notfallmaßnahmen umgesetzt werden, z. B. indem Wiederanlaufpläne erstellt oder Passwörter und kryptographische Schlüssel sicher hinterlegt werden.

SYS.1.1.A23 Systemüberwachung

Das Serversystem SOLLTE in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept eingebunden werden, das den Systemzustand und die Funktionsfähigkeit des Systems und der darauf betriebenen Dienste laufend überwacht und Fehlerzustände sowie die Überschreitung definierter Grenzwerte an das Betriebspersonal meldet.

SYS.1.1.A24 Sicherheitsprüfungen

Serversysteme SOLLTEN regelmäßigen Sicherheitstests unterzogen werden, die die Einhaltung der Sicherheitsvorgaben überprüfen und ggf. vorhandene Schwachstellen identifizieren. Dies SOLLTE in besonderem Maße für Systeme mit externen Schnittstellen gelten. Angesichts mittelbarer Angriffe über infizierte Systeme im eigenen Netz SOLLTEN jedoch auch interne Serversysteme in festgelegten Zyklen entsprechend überprüft werden. Es SOLLTE geprüft werden, ob die Sicherheitsprüfungen dabei auch automatisiert, z. B. mittels geeigneter Skripte, realisiert werden können.

SYS.1.1.A25 Geregelte Außerbetriebnahme eines Servers

Bei der Außerbetriebnahme eines Servers SOLLTE sichergestellt werden, dass keine wichtigen Daten, die eventuell auf den verbauten Datenträgern gespeichert sind, verloren gehen, und dass keine sensitiven Daten zurück bleiben. Es SOLLTE einen Überblick darüber geben, welche Daten wo auf dem Server gespeichert sind. Es SOLLTE außerdem sichergestellt sein, dass vom Server angebotene Dienste durch einen anderen Server übernommen wurden, wenn dies erforderlich ist.

Es SOLLTE eine Checkliste erstellt werden, die bei der Außerbetriebnahme eines Servers abgearbeitet werden kann. Diese Checkliste SOLLTE mindestens Aspekte zur Datensicherung, Migration von Diensten und dem anschließenden sicheren Löschen aller Daten umfassen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.1.1.A26 Mehr-Faktor-Authentisierung (C)

Bei höherem Schutzbedarf SOLLTE eine sichere Zwei- oder Mehr-Faktor-Authentisierung für den Zugang zum Server eingerichtet werden, z. B. mit kryptographischen Zertifikaten, Chipkarten oder Token. Vordringlich SOLLTEN alle administrativen Zugänge zum Server mit Mehr-Faktor-Authentisierung abgesichert werden.

SYS.1.1.A27 Hostbasierte Angriffserkennung (IA)

Mit dem Einsatz von hostbasierten Angriffserkennungssystemen (Host-based Intrusion Detection Systems, IDS bzw. Intrusion Prevention Systems, IPS) SOLLTE das Systemverhalten auf Anomalien und Missbrauch hin überwacht werden. Die eingesetzten IDS/IPS-Mechanismen SOLLTEN geeignet ausgewählt, konfiguriert und ausführlich getestet werden. Im Falle einer Angriffserkennung SOLLTE das Betriebspersonal geeignet alarmiert werden.

Über Betriebssystem-Mechanismen oder geeignete Zusatzprodukte SOLLTEN Veränderungen an Systemdateien und Konfigurationseinstellungen überprüft, eingeschränkt und gemeldet werden.

SYS.1.1.A28 Redundanz (A)

Serversysteme mit hohen Verfügbarkeitsanforderungen SOLLTEN gegen Ausfälle geeignet geschützt sein. Hierzu SOLLTEN mindestens geeignete Redundanzen verfügbar sein und/oder Wartungsverträge mit den Lieferanten abgeschlossen werden. Es SOLLTE geprüft werden, ob bei sehr hohen Anforderungen Hochverfügbarkeitsarchitekturen mit automatischem Failover, gegebenenfalls über verschiedene Standorte hinweg, erforderlich sind.

SYS.1.1.A29 Einrichtung einer Testumgebung (CIA)

Um Veränderungen am System oder der Konfiguration testen zu können, ohne den Produktivbetrieb zu gefährden, SOLLTEN entsprechende Testsysteme vorgehalten oder bei Bedarf bereitgestellt werden (z. B. als virtuelle Images). Die Testsysteme SOLLTEN den Produktivsystemen weitestmöglich entsprechen (Softwareversionen, Konfiguration). Für Anwendungssysteme SOLLTEN geeignete Testdaten generiert werden, die keine vertraulichen oder personenbezogenen Inhalte der produktiven Daten umfassen.

SYS.1.1.A30 Ein Dienst pro Server (CIA)

Abhängig von der Bedrohungslage und dem Schutzbedarf der Dienste SOLLTE auf einem Server nur jeweils ein Dienst betrieben werden.

SYS.1.1.A31 Application Whitelisting (CI)

Es SOLLTE bei erhöhtem Schutzbedarf über Application Whitelisting sichergestellt werden, dass nur erlaubte Programme ausgeführt werden. Zum einen SOLLTEN vollständige Pfade bzw. Verzeichnisse festgelegt werden, aus denen dies möglich sein darf. Zum anderen SOLLTE alternativ einzelnen Anwendungen explizit die Ausführung gestattet werden.

4 Weiterführende Informationen

4.1 Literatur

- [ISi-Server] Absicherung eines Servers (ISi-Server), BSI, 09.2013
  Bundesamt für Sicherheit in der Informatiostechnik, 02.2017
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf

- [NISTSP800123] NIST Special Publication 800-123
  Guide to General Server Security, NIST, 07.2008
  https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an **grundschutz@bsi.bund.de** gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Allgemeiner Server" von Bedeutung.

G 0.08 Ausfall oder Störung der Stromversorgung

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.43 Einspielen von Nachrichten

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.08	G 0.09	G 0.14	G 0.16	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.30	G 0.31	G 0.32	G 0.39	G 0.40	G 0.43	G 0.44	G 0.45	G 0.46
SYS.1.1.A1	x	x		x							x	x									x		
SYS.1.1.A2			x			x			x						x								
SYS.1.1.A3			x			x			x						x		x						x
SYS.1.1.A4			x			x									x		x						x
SYS.1.1.A5			x			x		x	x	x					x		x						x
SYS.1.1.A6			x			x				x					x								
SYS.1.1.A7							x			x		x		x					x				
SYS.1.1.A8																						x	
SYS.1.1.A9								x	x									x	x				
SYS.1.1.A10										x	x	x			x								
SYS.1.1.A11	x	x		x	x		x				x		x	x	x	x					x	x	
SYS.1.1.A12	x	x		x	x						x		x	x	x			x			x		
SYS.1.1.A13					x					x		x		x			x						
SYS.1.1.A14					x	x		x	x						x	x							
SYS.1.1.A15	x										x	x											
SYS.1.1.A16							x				x	x		x	x								x
SYS.1.1.A17											x	x		x									
SYS.1.1.A18			x			x			x						x		x			x			x
SYS.1.1.A19			x			x				x	x								x	x			
SYS.1.1.A20			x							x					x				x				
SYS.1.1.A21	x	x	x	x				x			x												
SYS.1.1.A22			x			x																	
SYS.1.1.A23								x	x	x	x	x	x				x		x				
SYS.1.1.A24					x						x	x	x										
SYS.1.1.A25		x																					
SYS.1.1.A26			x							x					x								
SYS.1.1.A27								x	x	x	x	x	x				x		x				
SYS.1.1.A28	x	x		x							x												
SYS.1.1.A29					x		x				x	x											
SYS.1.1.A30										x	x			x			x		x				
SYS.1.1.A31							x	x	x	x								x	x				

SYS.1.2: Windows Server

SYS.1.2.2 Windows Server 2012

1 Beschreibung

1.1 Einleitung

Mit Windows Server 2012 hat Microsoft im September 2012 ein Serverbetriebssystem auf den Markt gebracht, das in Bezug auf die Sicherheit diverse Verbesserungen gegenüber bisherigen Windows-Versionen (insbesondere auch Windows Server 2008 R2) mitbringt. Technisch wird dabei nicht auf dem Vorgänger aufgebaut, sondern auf der Codebasis des Client-Betriebssystems Windows 8. Mit dem Release Windows Server 2012 R2 von Oktober 2013 wurde das Betriebssystem weiter verbessert und erweitert, um Windows 2012 R2 zum Server-Pendant zu Windows 8.1 auf der Clientseite machen.

Dieser Baustein beschäftigt sich mit der Absicherung von Windows Server 2012 und Windows Server 2012 R2 gleichermaßen, auf relevante Unterschiede und Besonderheiten wird jeweils geeignet hingewiesen. Dabei wird die Schreibweise "Windows Server 2012 (R2)" verwendet, wenn beide Versionen gemeint sind. Das Ablaufdatum für den Mainstream Support bzw. den Extended Support ("End-of-Life", EOL) ist in beiden Fällen der 09.01.2018 bzw. der 10.01.2023.

1.2 Zielsetzung

Zielsetzung dieses Bausteins ist der Schutz von Informationen und Prozessen, die durch Serversysteme auf Basis von Windows Server 2012 (R2) im Regelbetrieb verarbeitet bzw. gesteuert werden.

1.3 Abgrenzung

Der Baustein Windows Server 2012 (R2) ist auf alle Zielobjekte anzuwenden, die unter dem Betriebssystem Microsoft Windows Server 2012 (R2) betrieben werden. Er konkretisiert und ergänzt die Aspekte, die im Bausteinen SYS.1.1 Allgemeiner Server behandelt werden, um Spezifika von Windows Server 2012 (R2), ohne dabei die Anforderungen des Bausteins APP.2.2 Active Directory zu wiederholen.

Im Rahmen dieses Bausteins wird von einer Standardeinbindung in eine Active Directory-Domäne ausgegangen, wie sie in Unternehmen und Behörden üblich ist. Besonderheiten von Stand-alone-Systemen werden nur punktuell erwähnt, wo die Unterschiede besonders relevant erschienen.

Sicherheitsanforderungen möglicher Serverrollen und -Funktionen wie Fileserver (APP.3.3 Fileserver), Webserver (APP.3.2 Webserver) oder Exchange (APP.5.2 Exchange/Outlook) sind Gegenstand eigener Bausteine, genauso wie das Thema Virtualisierung (SYS.1.5 Server-Virtualisierung). In diesem Baustein geht es um die grundlegende Absicherung auf Betriebssystemebene mit bordeigenen Mitteln unabhängig vom Einsatzzweck des Servers.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Windows Server 2012 (R2) von besonderer Bedeutung:

2.1 Unzureichende Planung von Windows Server 2012 (R2)

Windows Server 2012 (R2) ist ein komplexes modernes Betriebssystem, das über eine große Zahl von Funktionen und Konfigurationsoptionen verfügt. Ein Beispiel sind die verschiedenen mächtigen installierbaren Serverrollen. Mit jeder weiteren Funktion vergrößert sich die Angriffsfläche, zudem steigt die Wahrscheinlichkeit von Schwachstellen und Fehlkonfigurationen. Bei der Einbindung in die Domäne und der Vernetzung mit anderen Systemen und Diensten gibt es ebenfalls sehr viele Freiheitsgrade. Auch wenn moderne Windows-Versionen in vielen Bereichen gute Standardeinstellungen mitbringen, ist die Grundkonfiguration immer noch nicht in jedem Fall die sicherste. Dies kann bei unzureichender Planung zu einer Vielzahl von Angriffsvektoren führen, die Angreifer leicht ausnutzen können. Werden außerdem nicht schon vor der Installation zentrale Entscheidungen getroffen, wird mit einem unsicheren und undefinierten Zustand begonnen, der sich kaum beheben lässt.

2.2 Unbedachte Cloud-Nutzung

Windows Server 2012 (R2) bietet an verschiedenen Stellen die Möglichkeit, Cloud-Dienste zu nutzen, ohne dass Drittsoftware installiert werden muss. Hierzu gehören beispielsweise Microsoft Azure Online Backup oder die Online-Speicherung von BitLocker-Wiederherstellungsschlüsseln. Während Cloud-Dienste grundsätzlich Vorteile insbesondere auf die Verfügbarkeit bieten können, bestehen bei unbedachtem Einsatz Risiken für die Vertraulichkeit sowie eine Abhängigkeit von Dienstleistern. So können Daten über Cloud-Dienste in die Hände unberechtigter Dritter gelangen, seien es Angreifer oder aber auch staatliche Akteure. Wird ein Cloud-Dienst durch den Anbieter eingestellt, kann dies erhebliche Auswirkungen auf die eigenen Geschäftsprozesse haben.

2.3 Fehlerhafte Administration von Windows-Servern

Windows Server 2012 und Windows Server 2012 R2 haben im Vergleich zu den Vorgängerversionen viele neue sicherheitsrelevante Funktionen hinzubekommen. Bei anderen Features haben sich Teilfunktionen, Parameter oder Standardkonfigurationen verändert. Sind die Administratoren nicht ausreichend in den Besonderheiten der Systeme geschult, so drohen Konfigurationsfehler und Fehlhandlungen, die neben der Funktionalität auch die Sicherheit beeinträchtigen können.

Eine besondere Gefahr stellen uneinheitliche Windows-Server-Sicherheitseinstellungen dar (z. B. bei (SMB, RPC oder LDAP). Wenn die Konfiguration nicht systematisch und zentral geplant, dokumentiert, überprüft und nachgehalten wird, droht ein sogenannter Konfigurationsdrift: Je mehr sich die konkreten Konfigurationen funktional ähnlicher Systeme unbegründet und undokumentiert auseinander bewegen, desto schwieriger wird es, einen Überblick über den Status Quo zu behalten und die Sicherheit ganzheitlich und konsequent aufrechtzuerhalten.

2.4 Unsachgemäßer Einsatz von Gruppenrichtlinien (GPOs)

Gruppenrichtlinien (GPOs) sind eine nützliche und mächtige Art, viele (Sicherheits-)Aspekte von Windows Server 2012 (R2) zu konfigurieren, insbesondere in einer Domäne. Bei der großen Zahl möglicher Einstellungen ist es leicht möglich, versehentlich widersprüchliche oder inkompatible Einstellungen zu setzen oder Themenbereiche zu vergessen. Dies führt bei unsystematischer Vorgehensweise mindestens zu Betriebsstörungen, die teilweise schwer zu beheben sind, wenn nicht gar zu schwerwiegenden Schwachstellen auf dem Server oder auf verbundenen Clientsystemen. Insbesondere falsch verstandene Vererbungsregeln und Filter können dazu führen, dass GPOs gar nicht auf ein System angewendet werden.

2.5 Verlust verschlüsselter Daten

Wenn Daten verschlüsselt sind, wie etwa beim Einsatz von BitLocker oder der Geräteverschlüsselung auf Windows Server 2012 (R2), kann es zum kompletten Datenverlust kommen, wenn der Schlüssel verloren geht und es keinen Wiederherstellungsschlüssel gibt. Auch ein Backup verschlüsselter Daten hilft hier nicht weiter.

2.6 Integritätsverlust schützenswerter Informationen oder Prozesse

Windows Server 2012 (R2) verfügt über eine Vielzahl von Funktionen, um die Integrität von durch das Betriebssystem verarbeiteten Informationen zu schützen. Jede einzelne davon kann mit Schwachstellen behaftet sein. Zudem mangelt es häufig an einer konsequenten Konfiguration, nicht zuletzt aus Gründen der vermuteten Benutzerfreundlichkeit oder Bequemlichkeit. Informationen und Prozesse können so durch unbefugte Mitarbeiter oder externe Angreifer verfälscht und oftmals sogar die Spuren verwischt werden. Häufig werden auch Schadprogramme eingesetzt, um Informationen aus der Ferne zu manipulieren.

2.7 Software-Schwachstellen oder -Fehler

Jede Software enthält Schwachstellen, umso mehr gilt dies für komplexe Systeme wie Windows Server 2012 (R2). Sicherheitslücken in Komponenten können es einem Angreifer ermöglichen, Schadprogramme einzuschleusen, auszuführen oder Funktionen des Systems zu missbrauchen bzw. Sicherheitsmechanismen zu umgehen. Das kann z. B. dazu führen, dass Informationen manipuliert werden oder in falsche Hände geraten. Jede weitere installierte Rolle oder Funktion erhöht die Chance, dass Schwachstellen auftreten und durch Angreifer entdeckt werden. Nicht alle Schwachstellen sind sofort öffentlich bekannt und nicht für alle bekannten Schwachstellen sind sofort Patches verfügbar. Zudem müssen diese auch erst eingespielt werden.

2.8 Unberechtigtes Erlangen oder Missbrauch von Administratorrechten

Die reguläre Arbeit unter Standardbenutzerrechten für Administratoren ist inzwischen gute Praxis. Da der Administrator jedoch an bestimmten Stellen trotzdem seine Rechte erhöhen muss, kann ein Angreifer dort potentiell eingreifen und privilegierte Rechte erlangen. Auch ein Missbrauch von Rechten durch legitime Administratoren ist ein relevantes Schadensszenario. Da die Rollen oft sehr mächtig sind, sind hier die Auswirkungen in der Regel beträchtlich, insbesondere bei Domänenadministratoren. Auch ohne Passwörter zu erraten oder zu brechen, können Angreifer z. B. durch sogenannte Pass-the-Hash-Verfahren geeignete Credentials auslesen und missbrauchen, um sich lateral im Netz weiterzubewegen.

2.9 Kompromittierung von Fernzugängen

Da Windows Server 2012 (R2) über eine Vielzahl von Möglichkeiten verfügt, aus der Ferne verwaltet zu werden, können diese grundsätzlich auch missbraucht werden. Fernzugänge, wie z. B. RDP-Benutzersitzungen, können durch unsichere bzw. unsicher verwendete Protokolle, schwache Authentifizierung (z. B. schwache Passwörter) oder fehlerhafte Konfiguration für Dritte erreichbar sein. Hierdurch können der Server und die dort gespeicherten Informationen weitgehend kompromittiert werden. Oft können so auch weitere, mit dem Server verbundene IT-Systeme kompromittiert werden.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz von Windows Server 2012 (R2) aufgeführt. Grundsätzlich ist der *IT-Betrieb* für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	-

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.1.2.2.A1 Planung von Windows Server 2012

Der Einsatz von Windows Server 2012 (R2) MUSS vor der Installation sorgfältig geplant werden. Die Anforderungen an die Hardware MÜSSEN vor der Beschaffung geprüft werden. Es MUSS eine begründete und dokumentierte Entscheidung für eine geeignete Windows Server 2012 (R2)-Edition getroffen werden. Der Einsatzzweck des Servers MUSS dabei spezifiziert werden, inkl. einer geplanten Einbindung ins Active Directory. Die Nutzung von ins Betriebssystem integrierten Cloud-Diensten MUSS grundsätzlich abgewogen und geplant werden. Wenn nicht benötigt, MUSS die Einrichtung von Microsoft-Konten auf dem Server blockiert werden.

SYS.1.2.2.A2 Sichere Installation von Windows Server 2012

Das Installationsmedium MUSS aus einer nachweislich integren Quelle bezogen werden. Es DÜRFEN KEINE anderen als die benötigten Serverrollen und Features bzw. Funktionen installiert werden. Wenn vom Funktionsumfang her ausreichend, MUSS die Server-Core-Variante installiert werden. Andernfalls MUSS begründet werden, warum die Server-Core-Variante nicht genügt. Der Server MUSS im Rahmen der Installation zunächst auf einen aktuellen Patch-Stand gebracht werden.

SYS.1.2.2.A3 Sichere Administration von Windows Server 2012

Lokale Administrationskonten MÜSSEN einzigartige, sichere Passwörter besitzen. Alle Administratoren, die für das Serversystem zuständig sind, MÜSSEN in den sicherheitsrelevanten Aspekten der Administration von Windows Server 2012 bzw. R2 geschult sein. Sie DÜRFEN administrative Rechte NICHT einsetzen, wo diese nicht zwingend erforderlich sind. Browser auf dem Server DÜRFEN NICHT zum Surfen im Web verwendet werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Windows Server 2012. Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.1.2.2.A4 Sichere Konfiguration von Windows Server 2012

Es SOLLTEN NICHT mehrere wesentliche Funktionen bzw. Rollen durch einen einzigen Server erfüllt werden. Vor Inbetriebnahme SOLLTE das System grundlegend gehärtet werden. Dafür SOLLTEN funktionsspezifische institutionsweite Sicherheitsvorlagen erstellt und gepflegt werden, die auf die Serversysteme ausgerollt werden. Die Einstellungen SOLLTEN anfangs und bei Änderungen vor Produktivnahme getestet werden. Der Internet Explorer SOLLTE auf dem Server nur in der Enhanced Security Configuration und im Enhanced Protected Mode genutzt werden.

SYS.1.2.2.A5 Schutz vor Schadsoftware

Außer bei IT-Systemen mit Windows Server 2012, die stand-alone ohne Netzanschluss und Wechselmedien betrieben werden, SOLLTE vor dem ersten Verbinden mit dem Netz oder Wechselmedien ein Virenschutzprogramm installiert werden. Die Signaturen SOLLTEN regelmäßig aktualisiert werden. Zudem SOLLTEN regelmäßig alle Festplatten vollständig gescannt werden. Es SOLLTEN Alarme für die zuständigen Administratoren bei Virenfunden konfiguriert sein.

SYS.1.2.2.A6 Sichere Authentisierung und Autorisierung in Windows Server 2012

In Windows Server 2012 R2 SOLLTEN alle Benutzer Mitglieder der Sicherheitsgruppe "Geschützte Nutzer" sein. Konten für Dienste und Computer SOLLTEN NICHT Mitglied von "Geschützte Nutzer" sein. Service-Accounts in Windows Server 2012 (R2) SOLLTEN Mitglieder der Gruppe "Managed Service Account" sein. Der Local Credential Store LSA SOLLTE geschützt sein. Der Einsatz dynamischer Zugriffsregeln auf Ressourcen SOLLTE bevorzugt werden.

Die Administratoren von Windows Server 2012 (R2) SOLLTEN auf ihren eigenen Clients mit beschränkten Rechten arbeiten.

SYS.1.2.2.A7 Sicherheitsprüfung von Windows Server 2012

Die Sicherheitskonfiguration von Windows Server 2012 (R2) SOLLTE mittels geeigneter Tools regelmäßig überprüft, dokumentiert und verbessert werden.

SYS.1.2.2.A8 Schutz der Systemintegrität

Secure Boot SOLLTE aktiv sein. AppLocker SOLLTE aktiviert und möglichst strikt konfiguriert sein. Die Auswirkungen von Änderungen SOLLTEN vorab getestet werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.1.2.2.A9 Lokale Kommunikationsfilterung (CI)

Die lokale Firewall SOLLTE für eingehenden und ausgehenden Netzverkehr aktiviert und möglichst strikt eingestellt sein. Die Identität von Remote-Systemen und die Integrität der Verbindungen mit diesen SOLLTE kryptographisch abgesichert sein.

SYS.1.2.2.A10 Festplattenverschlüsselung bei Windows Server 2012 (C)

Bei Systemen mit Windows Server 2012 (R2) SOLLTEN die Datenträger mit BitLocker oder einem anderen Produkt verschlüsselt werden. Dies SOLLTE auch für virtuelle Maschinen mit produktiven Daten gelten. Bei höherem Schutzbedarf SOLLTE nicht nur das TPM allein als Schlüsselschutz dienen. Das Wiederherstellungspasswort SOLLTE im Active Directory oder einem anderen geeigneten sicheren Ort gespeichert werden. Bei sehr hohen Vertraulichkeits- oder Abstreitbarkeitsanforderungen SOLLTE eine Full Volume Encryption erfolgen.

SYS.1.2.2.A11 Angriffserkennung bei Windows Server 2012 (CIA)

Sicherheitsrelevante Ereignisse in Windows Server 2012 (R2) SOLLTEN an einem zentralen Punkt gesammelt und ausgewertet werden. Verschlüsselte Partitionen SOLLTEN nach einer definierten Anzahl von Entschlüsselungsversuchen gesperrt werden.

SYS.1.2.2.A12 Redundanz und Hochverfügbarkeit (A)

Es SOLLTE geprüft werden, welche Verfügbarkeitsanforderungen durch Betriebssystemfunktionen wie Failover Cluster und Network Load Balancing bzw. NIC-Teaming (LBFO) umgesetzt oder unterstützt werden kann. Für Außenstellen SOLLTE BranchCache aktiviert werden.

SYS.1.2.2.A13 Starke Authentifizierung bei Windows Server 2012 (CI)

Es SOLLTE ein rollenbasiertes Administrations-Modell für die Administration unterschiedlicher Serverfunktionen entworfen und umgesetzt werden. Für kritische Dienste SOLLTE eine Zwei-Faktor-Authentifizierung implementiert sein.

SYS.1.2.2.A14 Herunterfahren verschlüsselter Server und virtueller Maschinen (CI)

Um die verschlüsselten Daten auch im Betrieb zu schützen, SOLLTEN nicht benötigte Server (inkl. virtuelle Maschinen) immer heruntergefahren oder in den Ruhezustand versetzt werden. Dies SOLLTE möglichst automatisiert erfolgen. Die Entschlüsselung der Daten SOLLTE einen interaktiven Schritt erfordern, oder sie SOLLTE zumindest im Sicherheitsprotokoll festgehalten werden.

4 Weiterführende Informationen

4.1 Literatur

- [ISFSY12] The Standard of Good Practice - Area SY1.2 Server Configuration
  Information Security Forum (ISF), June 2016, insbesondere Area SY1.2 - Server Configuration

- [NISTSP800123] NIST Special Publication 800-123
  Guide to General Server Security, NIST, 07.2008
  https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

- [PAYNE] Windows Event Forwarding for everyone
  Microsoft Technet, Blog, Jessica Payne, 11.2015
  https://blogs.technet.microsoft.com/jepayne/2015/11/23/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem/

- [TN831360] Secure Windows Server 2012 R2 and Windows Server 2012, Microsoft
  Micorosoft Technet, 11.2013
  https://technet.microsoft.com/en-us/library/hh831360.aspx

- [TN831778] Security and Protection, Micorosoft
  Microsoft Technet, 02.2014
  https://technet.microsoft.com/en-us/library/hh831778.aspx

- [TN832031] Secure Windows
  Für Windows 8/8.1, gilt größtenteils auch für Windows Server 2012 / 2012 R2, 03.2014
  https://technet.microsoft.com/en-us/library/hh832031.aspx

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Windows Server 2012" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.33 Personalausfall

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.38 Missbrauch personenbezogener Daten

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.43 Einspielen von Nachrichten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.14	G 0.15	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.29	G 0.30	G 0.31	G 0.32	G 0.33	G 0.36	G 0.37	G 0.38	G 0.39	G 0.40	G 0.41	G 0.42	G 0.43	G 0.45	G 0.46
SYS.1.2.2.A1			x								x		x														
SYS.1.2.2.A2	x	x		x	x	x	x	x	x	x		x		x	x	x		x	x	x	x	x		x	x	x	x
SYS.1.2.2.A3	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
SYS.1.2.2.A4	x	x		x	x	x	x	x	x	x		x	x	x	x	x		x	x	x	x	x		x	x	x	x
SYS.1.2.2.A5	x	x		x		x	x	x	x	x	x			x		x		x	x	x	x	x		x	x	x	x
SYS.1.2.2.A6	x	x		x		x	x	x			x			x	x	x		x	x	x	x	x	x	x	x		x
SYS.1.2.2.A7	x	x	x	x		x	x	x			x	x		x	x	x		x	x	x	x	x	x		x	x	x
SYS.1.2.2.A8						x	x	x	x	x									x		x						x
SYS.1.2.2.A9	x	x		x		x	x	x						x	x	x					x	x					x
SYS.1.2.2.A10	x			x		x	x											x	x	x							x
SYS.1.2.2.A11	x			x		x	x	x				x		x		x					x	x	x	x	x	x	x
SYS.1.2.2.A12											x															x	
SYS.1.2.2.A13	x	x		x		x	x	x			x			x	x	x		x	x	x	x	x	x	x	x		x
SYS.1.2.2.A14	x			x		x	x											x	x	x							x

SYS.1: Server

SYS.1.3 Server unter Unix

1 Beschreibung

1.1 Einleitung

Auf Server-Systemen werden häufig die Betriebssysteme Linux oder Unix eingesetzt. Beispiele für klassische Unix-Systeme sind die BSD-Reihe (FreeBSD, OpenBSD und NetBSD), Solaris und AIX. Linux ist kein klassisches Unix (der Kernel basiert nicht auf dem ursprünglichen Quelltext, aus dem sich die verschiedenen Unix-Derivate entwickelt haben), sondern ein funktionelles Unix-System. In diesem Baustein werden alle Betriebssysteme der Unix-Familie betrachtet, also auch Linux als funktionelles Unix-System.

Linux ist freie Software und wird von der Open-Source-Gemeinschaft entwickelt. Daneben gibt es Anbieter, die die verschiedenen Software-Komponenten zu einer Distribution zusammenfassen und pflegen, sowie weitere Dienstleistungen anbieten. Für Linux-Server werden häufig die Distributionen

- Debian
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server
- Ubuntu Server

eingesetzt. Darüber hinaus gibt es für spezielle Einsatzzwecke und Geräte zugeschnittene Linux-Distributionen wie Endian für Firewall-Systeme, OpenMediaVault für NAS-Systeme oder OpenWRT für Router.

Die auf einem Server angebotenen Dienste sind oft zentral und daher in besonderem Maße exponiert. Hierdurch sind Unix-Server nicht nur für Geschäftsprozesse kritisch, sondern geraten deswegen nicht selten in den Fokus von Angreifern. Deswegen kommt der Verfügbarkeit und Absicherung von Unix-Servern eine besondere Bedeutung zu.

1.2 Zielsetzung

Zielsetzung des Bausteins ist der Schutz von Informationen, die von Unix-Servern verarbeitet werden. Die Anforderungen des Bausteins adressieren vorrangig Linux-Server, können aber generell für Unix-Server adaptiert werden. Es werden Anforderungen formuliert, wie das Betriebssystem konfiguriert und betrieben werden soll.

1.3 Abgrenzung

Der Baustein enthält grundsätzliche Anforderungen zur Einrichtung und zum Betrieb von Unix-Servern. Er konkretisiert und ergänzt die Aspekte, die im Bausteinen SYS.1.1 Allgemeiner Server behandelt werden, um Spezifika von Unix-Systemen.

Soll der Server nicht selber verwaltet werden, sondern wird dieser durch Dritte gehostet, sind zusätzlich die Anforderungen des Bausteins OPS.3.1 Outsourcing-Nutzung zu berücksichtigen. Sicherheitsanforderungen möglicher Server-Funktionen wie Webserver (APP.3.2 Webserver) oder Server

für Groupware (siehe APP.5.1 Groupware) sind Gegenstand eigener Bausteine, eine Ausnahme sind die Unix-spezifischen Server-Dienste NIS, NFS und SSH, die ebenfalls in diesem Baustein behandelt werden. Das Thema Virtualisierung wird im Baustein SYS.1.5 Server-Virtualisierung beleuchtet. In diesem Baustein geht es um die grundlegende Absicherung auf Betriebssystemebene mit bordeigenen Mitteln unabhängig vom Einsatzzweck des Servers.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Server unter Unix von besonderer Bedeutung:

2.1 Ausspähen von System- und Benutzerinformationen

Durch verschiedene Unix-Programme ist es möglich, Daten abzufragen, die das IT -System über die Benutzer speichert. Hiervon sind auch solche Daten betroffen, die Auskunft über das Leistungsprofil eines Benutzers geben können. Zu diesen Informationen zählen sowohl Informationen über weitere angemeldete Benutzer wie auch technische Informationen zur Betriebssysteminstallation und -konfiguration.

Beispielsweise kann mit einem einfachen Programm, das in einem bestimmten Zeitintervall die Informationen auswertet, die der Befehl "who" liefert, jeder Benutzer ein genaues Nutzungsprofil für einen Account erstellen. Zum Beispiel lassen sich auf diese Weise die Abwesenheitszeiten des oder der Systemadministratoren feststellen, um diese Zeiten für unberechtigte Handlungen zu nutzen. Des Weiteren lässt sich feststellen, welche Terminals für einen privilegierten Zugang zugelassen sind. Weitere Programme mit ähnlichen Missbrauchsmöglichkeiten sind "finger" oder "ruser".

2.2 Ausnutzbarkeit der Skriptumgebung

In Unix-Betriebssystemen ist die Nutzung von Skriptsprachen weit verbreitet. Skripte sind eine Auflistung von einzelnen Kommandos, die in einer Textdatei gespeichert und aufgerufen werden. Durch den großen Funktionsumfang der Skriptumgebung können Angreifer Skripte umfangreich für ihre Zwecke nutzen. Darüber hinaus ist die Eindämmung von aktivierten Skriptsprachen sehr schwierig.

2.3 Dynamisches Laden von gemeinsam genutzten Bibliotheken

Mit der Kommandozeilenoption "LD_PRELOAD" wird die angegebene Bibliothek vor allen anderen in einer Anwendung benötigten Bibliotheken geladen und deren Funktionen werden von der Anwendung genutzt. Ein Angreifer könnte das Betriebssystem so manipulieren, dass Schadfunktionen bei der Nutzung von bestimmten Anwendungen mit ausgeführt werden.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Server unter Unix aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	-

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.1.3.A1 Benutzerauthentisierung unter Unix

Um den Unix-Server zu nutzen, MÜSSEN sich die Benutzer gegenüber dem IT-System authentisieren. Die Authentisierung über ein Netz MUSS verschlüsselt werden. Wenn mit einem Benutzerkonto nur bestimmte Dienste genutzt werden dürfen, DARF das Benutzerkonto nicht für andere Dienste genutzt werden können.

SYS.1.3.A2 Sorgfältige Vergabe von IDs

Jeder Login-Name, jede Benutzer-ID (UID) und jede Gruppen-ID (GID) DARF nur einmal vorkommen. Jeder Benutzer MUSS Mitglied mindestens einer Gruppe sein. Jede in der Datei "/etc/passwd" vorkommende GID MUSS in der Datei "/etc/group" definiert sein. Jede Gruppe SOLLTE nur die Benutzer enthalten, die unbedingt notwendig sind. Bei vernetzten Systemen MUSS außerdem darauf geachtet werden, dass die Vergabe von Benutzer- und Gruppennamen, UID und GID im Systemverbund konsistent erfolgt.

SYS.1.3.A3 Automatisches Einbinden von Wechsellaufwerken

Wechsellaufwerke wie z. B. USB-Sticks oder CDs/DVDs DÜRFEN nicht automatisch eingebunden werden.

SYS.1.3.A4 Schutz von Anwendungen

Um die Ausnutzung von Schwachstellen in Anwendungen zu erschweren, MUSS "ASLR" und "DEP/NX" im Kernel aktiviert und von den Anwendungen genutzt werden. Sicherheitsfunktionen des Kernels und der Standardbibliotheken, wie z. B. Heap- und Stackschutz, DÜRFEN NICHT deaktiviert werden.

SYS.1.3.A5 Sichere Installation von Software-Paketen

Die Integrität und Authentizität der zu installierenden Softwarepakete MUSS immer geprüft werden. Die Software-Pakete MÜSSEN unter einem unprivilegierten Benutzeraccount entpackt, konfiguriert und übersetzt werden. Erst der letzte Schritt, die eigentliche Installation des übersetzten Programms, DARF mit höheren Privilegien erfolgen. Dabei DARF die zu installierende Software NICHT unkontrolliert in das Wurzeldateisystem des Servers installiert werden.

Wird die Software aus dem Quelltext übersetzt, dann SOLLTEN die gewählten Parameter geeignet dokumentiert werden. Anhand dieser Dokumentation SOLLTE der Quelltext jederzeit nachvollziehbar und reproduzierbar kompiliert werden können. Alle weiteren Installationsschritte SOLLTEN dabei ebenfalls dokumentiert werden, damit sich die Konfiguration im Notfall schnell reproduzieren lässt.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Server unter Unix. Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.1.3.A6 Verwaltung von Benutzern und Gruppen

Zur Verwaltung von Benutzern und Gruppen SOLLTEN die entsprechenden Verwaltungswerkzeuge genutzt werden. Von einer direkten Bearbeitung der Konfigurationsdateien "/etc/passwd" und "/etc/group" und "/etc/sudoers" SOLLTE abgesehen werden.

SYS.1.3.A7 Zusätzliche Absicherung des Zugangs zum Single-User- und Wiederherstellungsmodus

Der Unix-Server SOLLTE durch Vergabe eines Boot-Passworts in der Firmware des Servers abgesichert werden. Alternativ SOLLTE eine festgelegte Bootreihenfolge mit eingebauter Boot-Festplatte zuerst festlegt und der Bootloader abgesichert werden.

SYS.1.3.A8 Verschlüsselter Zugriff über Secure Shell

Um eine verschlüsselte und authentisierte interaktive Verbindung zwischen zwei IT-Systemen aufzubauen, SOLLTE ausschließlich SSH verwendet werden. Alle anderen Protokolle, deren Funktionalität durch Secure Shell abgedeckt wird, SOLLTEN vollständig abgeschaltet werden.

SYS.1.3.A9 Absicherung des Bootvorgangs

Beim Booten SOLLTE die Integrität vom (Pre-)Bootloader bis zum Kernel überprüft werden. Die hierfür genutzten Schlüssel SOLLTEN bei der Ersteinrichtung überprüft werden. Es SOLLTE geprüft werden, ob hierfür Secure Boot als Teil der UEFI-Spezifikation genutzt werden kann.

SYS.1.3.A10 Verhinderung der Ausbreitung bei der Ausnutzung von Schwachstellen

Dienste und Anwendungen SOLLTEN mit individuellen Sicherheitsrichtlinien abgesichert werden (z. B. mit AppArmor oder SELinux). Auch chroot-Umgebungen sowie LXC- oder Docker-Container SOLLTEN dabei berücksichtigt werden. Es SOLLTE sichergestellt sein, dass mitgelieferte Standardprofile bzw. -Regeln aktiviert sind.

SYS.1.3.A11 Einsatz der Sicherheitsmechanismen von NFS

Nur hierfür vorgesehene Server SOLLTEN Verzeichnisse für andere Clients freigeben (siehe auch APP.3.3 Fileserver). Es SOLLTEN über NFS (Network File System) nur Verzeichnisse exportiert werden, die unbedingt notwendig sind. In den Dateien "/etc/exports" beziehungsweise "/etc/dfs/fstab" SOLLTEN die mountbaren Verzeichnisse auf das notwendige Maß reduziert werden. Die mountbaren Verzeichnisse SOLLTEN nur für bestimmte IT -Systeme sowie Benutzer unter Berücksichtigung der festgelegten Berechtigungsstruktur freigegeben werden.

SYS.1.3.A12 Einsatz der Sicherheitsmechanismen von NIS

NIS (Network Information Service) SOLLTE nur in einer sicheren Umgebung eingesetzt werden. In /etc/passwd, /etc/group sowie allen anderen sicherheitsrelevanten Dateien SOLLTE der Eintrag "+::0:0:::" nicht enthalten sein. Der Server-Prozess "ypserv" SOLLTE nur Anfragen von vorher festgelegten Rechnern beantworten.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.1.3.A13 Zusätzlicher Schutz der priviligierten Anmeldeinformationen (CI)

Die Passwörter der administrativen Konten SOLLTEN in mehrere Teile geteilt und durch Anwendung des Vier-Augen-Prinzips zusätzlich geschützt werden. Alternativ SOLLTE die Authentisierung mit Smartcards erfolgen.

Auch administrative Konten SOLLTEN so eingerichtet werden, dass diese nach einer vorher festgelegten Anzahl fehlerhafter Anmeldeversuche gesperrt werden.

SYS.1.3.A14 Verhinderung des Ausspähens von System- und Benutzerinformationen (C)

Die Ausgabe von Informationen über das Betriebssystem und der Zugriff auf Protokoll- und Konfigurationsdateien SOLLTE für Benutzer auf das notwendige Maß beschränkt werden. Außerdem SOLLTEN bei Befehlsaufrufen keine sensitiven Informationen als Parameter übergeben werden.

SYS.1.3.A15 Zusätzliche Absicherung des Bootvorgangs (CIA)

Bootloader und Kernel SOLLTEN durch selbstkontrolliertes Schlüsselmaterial signiert und nicht benötigtes Schlüsselmaterial entfernt werden.

SYS.1.3.A16 Zusätzliche Verhinderung der Ausbreitung bei der Ausnutzung von Schwachstellen (CI)

Die Nutzung von Systemaufrufen SOLLTE insbesondere für exponierte Dienste und Anwendungen auf die unbedingt notwendigen Systemaufrufe beschränkt werden. Die Standardprofile bzw. -Regeln von z.B. SELinux, AppArmor SOLLTEN manuell überprüft und ggf. an die eigenen Sicherheitsrichtlinien angepasst werden. Falls erforderlich, SOLLTEN neue Regeln bzw. Profile erstellt werden.

SYS.1.3.A17 Zusätzlicher Schutz des Kernels (CI)

Es SOLLTEN mit speziell gehärteten Kernels geeignete Schutzmechanismen wie Speicherschutz, Dateisystemabsicherung und rollenbasierte Zugriffskontrolle, die die Ausnutzung von Schwachstellen und die Ausbreitung im Betriebssystem verhindern sollen, genutzt werden.

4 Weiterführende Informationen

4.1 Literatur

- [ISi-Server] Absicherung eines Servers (ISi-Server), BSI, 09.2013
  Bundesamt für Sicherheit in der Informatiostechnik, 02.2017
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf

- [NISTSP800123] NIST Special Publication 800-123
  Guide to General Server Security, NIST, 07.2008
  https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Server unter Unix" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.39 Schadprogramme

G 0.43 Einspielen von Nachrichten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.14	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.28	G 0.30	G 0.31	G 0.32	G 0.39	G 0.43	G 0.45	G 0.46
SYS.1.3.A1	x			x	x			x						
SYS.1.3.A2	x			x				x	x	x			x	x
SYS.1.3.A3			x		x			x						
SYS.1.3.A4				x	x		x				x			
SYS.1.3.A5		x					x							
SYS.1.3.A6			x					x	x					
SYS.1.3.A7			x		x			x						
SYS.1.3.A8	x				x							x		
SYS.1.3.A9			x		x			x						
SYS.1.3.A10						x	x				x			
SYS.1.3.A11	x			x						x			x	
SYS.1.3.A12			x					x		x				
SYS.1.3.A13								x		x				
SYS.1.3.A14	x							x						x
SYS.1.3.A15						x	x							
SYS.1.3.A16	x			x						x			x	
SYS.1.3.A17	x			x						x			x	

SYS.1: Server

SYS.1.5 Virtualisierung

1 Beschreibung

1.1 Einleitung

Bei der Virtualisierung von IT-Systemen werden ein oder mehrere virtuelle IT-Systeme auf einem physischen IT-System ausgeführt. Ein solches physisches IT-System wird als Virtualisierungsserver bezeichnet. Mehrere Virtualisierungsserver können zu einer virtuellen Infrastruktur zusammengefasst werden. Darin können die Virtualisierungsserver selbst und die auf ihnen betriebenen virtuellen IT-Systeme gemeinsam verwaltet werden.

Die Virtualisierung von IT-Systemen bietet viele Vorteile für den IT-Betrieb in einem Informationsverbund. Es können Kosten für Hardwarebeschaffung, Strom und Klimatisierung eingespart werden, wenn die Ressourcen der physischen IT-Systeme effizienter genutzt werden. Allerdings ist die Virtualisierung auch eine Herausforderung für den Betrieb des Informationsverbundes. Da durch die eingesetzte Virtualisierungstechnik unterschiedliche Bereiche und Arbeitsfelder im Informationsverbund berührt werden, müssen Wissen und Erfahrungen aus den unterschiedlichsten Bereichen zusammengeführt werden.

1.2 Zielsetzung

Der Baustein beschreibt, wie virtualisierte IT-Systeme im Informationsverbund sicher eingeführt und betrieben werden können.

1.3 Abgrenzung

In diesem Baustein wird nur die Virtualisierung vollständiger IT-Systeme behandelt, andere Techniken, die teilweise ebenfalls mit dem Wort Virtualisierung in Verbindung gebracht werden (Anwendungsvirtualisierung mittels Terminalservern, Storage-Virtualisierung, Container etc.), sind nicht Gegenstand dieses Bausteins.

Im Bereich der Software-Entwicklung werden die Begriffe *Virtuelle Maschine* und *Virtueller-Maschinen-Monitor* auch für Laufzeitumgebungen benutzt, z. B. Java, Microsoft .NET. Solche Laufzeitumgebungen werden in diesem Baustein ebenfalls nicht betrachtet.

Virtuelle Infrastrukturen werden in der Regel mit speziellen Management-Systemen verwaltet. Da mit diesen umfassend auf die Virtualisierungsinfrastruktur zugegriffen werden kann, ist es wichtig, diese ausreichend abzusichern. Das betrifft sowohl den Server (kann physisch oder virtuell sein), auf dem die Management-Software ausgeführt wird, als auch das Produkt selber. Details werden im Baustein NET.1.2 *Netzmanagement* beschrieben.

Virtualisierungsumgebungen werden meistens gemeinsam mit Massenspeichern (NAS oder SAN) eingesetzt. Anbindung und Absicherung dieser Systeme werden in diesem Baustein ebenfalls nicht betrachtet (siehe hierfür Baustein SYS.1.8 *Speicherlösungen*).

Durch die Virtualisierung müssen die Netze der Institution anders strukturiert werden. Dieses Thema wird in diesem Baustein nicht umfassend behandelt. Dafür muss der Baustein NET.1.1 *Netzarchitektur und -design* umgesetzt werden. Auch die Netzvirtualisierung wird im vorliegenden Baustein nur angerissen. Sicherheitsaspekte von virtuellen Netzkomponenten werden im Baustein NET.1.4 *Netzvirtualisierung* behandelt.

Um virtuelle IT-Systeme abzusichern, müssen die jeweils zutreffenden Bausteine der Schicht *SYS (IT-Systeme)* angewendet werden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Virtualisierung von besonderer Bedeutung:

2.1 Fehlerhafte Planung der Virtualisierung

Ein Virtualisierungsserver ermöglicht den Betrieb virtueller IT-Systeme, integriert die Systeme in das Rechenzentrum und steuert dabei deren Anbindung an weitere Infrastrukturelemente, z. B. Netze und Speichernetze. Wird nicht geplant, wie die Virtualisierungsserver technisch und organisatorisch in die bestehende Infrastruktur zu integrieren sind, kann dies dazu führen, dass die Verantwortlichkeiten für unterschiedliche Bereiche womöglich nicht klar definiert sind, z. B. für Anwendungen, Betriebssysteme und Netzkomponenten. Weiterhin können sich die Zuständigkeiten verschiedener Bereiche überschneiden oder es ist keine passende Rechtestruktur vorhanden, um administrative Zugriffe für die unterschiedlichen Bereiche zu trennen.

2.2 Fehlerhafte Konfiguration der Virtualisierung

Durch Virtualisierung ändert sich die Art und Weise, wie Server provisioniert werden. Ressourcen wie CPU, RAM, Netzanbindung und Speicher werden in der Regel zentral über ein Management-System konfiguriert und sind nicht mehr durch Hardware und Verkabelung vorgegeben. Dadurch kann es schneller zu Konfigurationsfehlern kommen. Wird beispielsweise ein hoch schutzbedürftiges virtuelles IT-System fälschlicherweise in einer externen DMZ platziert, ist dieses dadurch aus dem Internet erreichbar und somit einem erhöhten Risiko ausgesetzt.

2.3 Unzureichende Ressourcen für virtuelle IT-Systeme

Virtualisierungsserver benötigen für den Betrieb der virtuellen IT-Systeme Speicherplatz, der entweder lokal im Virtualisierungsserver selbst oder in einem Speichernetz bereitgestellt wird. Werden die hierfür benötigten Speicherkapazitäten nicht ausreichend groß geplant, bestehen weitreichende Risiken für die Verfügbarkeit der virtuellen IT-Systeme und die Integrität der in ihnen verarbeiteten Informationen. Das gilt insbesondere dann, wenn spezielle Virtualisierungsfunktionen, wie Snapshots oder die Überbuchung von Speicherplatz, benutzt werden.

Engpässe können nicht nur den Speicherplatz auf Festplatten oder in Speichernetzen betreffen, sondern auch den Arbeitsspeicher (RAM) oder die Netzanbindung. Außerdem könnten sich durch unzureichende Ressourcen auf dem Virtualisierungsserver die virtuellen Maschinen gegenseitig in ihrem Betrieb stören und letztlich nicht mehr korrekt arbeiten oder ganz ausfallen.

2.4 Informationsabfluss oder Ressourcen-Engpass durch Snapshots

Durch einen Snapshot kann der Zustand einer virtuellen Maschine eingefroren und gesichert werden. Wird ein solcher Snapshot zu einem späteren Zeitpunkt wiederhergestellt, gehen alle in der Zwischenzeit vorgenommenen Änderungen verloren. Dadurch können auch bereits gepatchte Sicherheitslücken wieder offen sein. Weiterhin können durch offene Dateien, Dateitransfers oder Datenbanktransaktionen zum Zeitpunkt des Snapshots inkonsistente Daten entstehen.

Außerdem können Angreifer Snapshots dazu missbrauchen, um unberechtigt auf die Daten eines virtuellen IT-Systems zuzugreifen. Denn wenn der Snapshot im laufenden Betrieb erstellt wurde, ist auch der Inhalt des Hauptspeichers auf die Festplatte gesichert worden und kann auf einer virtuellen Umgebung außerhalb der ursprünglichen IT-Infrastruktur wiederhergestellt und analysiert werden. Ebenso können Snapshots sehr groß werden und dadurch kann die Speicherkapazität knapp werden.

2.5 Ausfall des Verwaltungsservers für Virtualisierungssysteme

Da über den Verwaltungsserver sämtliche Funktionen einer virtuellen Infrastruktur gesteuert und administriert werden, führt ein Ausfall dieses Verwaltungssystems dazu, dass keine Konfigurationsänderungen an der virtuellen Infrastruktur durchgeführt werden können. Die Administratoren können in dieser Zeit weder auf auftretende Probleme wie Ressourcenengpässe oder den Ausfall einzelner Virtualisierungsserver reagieren noch neue Virtualisierungsserver in die Infrastruktur integrieren bzw. neue virtuelle IT-Systeme anlegen. Auch die *Live Migration* und damit die dynamische Zuteilung von Ressourcen für einzelne Gast-Systeme ist ohne Verwaltungsserver nicht möglich.

2.6 Missbräuchliche Nutzung von Gastwerkzeugen

Gastwerkzeuge werden häufig mit sehr hohen Berechtigungen ausgeführt. Dadurch lassen sie sich beispielsweise für Denial-of-Service-Angriffe missbrauchen oder Angreifer übernehmen mit ihnen gleich das ganze Host-System.

2.7 Kompromittierung der Virtualisierungssoftware

Die Virtualisierungssoftware (auch: Hypervisor) ist die zentrale Komponente eines Virtualisierungsservers, sie steuert alle auf diesem Server ausgeführten virtuellen Maschinen und teilt ihnen Prozessor- und Speicherressourcen zu. Wird diese Komponente erfolgreich angegriffen, führt dies auch dazu, dass alle virtuellen IT-Systeme des Servers kompromittiert sind.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Virtualisierung aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Leiter IT, Leiter Netze, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.1.5.A1 Einspielen von Aktualisierungen und Sicherheitsupdates

Host-Betriebssystem, Management-Software und Hardware-Firmware MÜSSEN regelmäßig aktualisiert werden. Vorhandene Sicherheitsupdates MÜSSEN zeitnah eingespielt werden. Vorab MUSS auf einem Testsystem überprüft werden, ob die Sicherheitsupdates kompatibel sind und keine Fehler verursachen.

SYS.1.5.A2 Sicherer Einsatz virtueller IT-Systeme

Jeder Administrator von virtuellen IT-Systemen MUSS wissen, wie sich eine Virtualisierung auf die betriebenen IT-Systeme und Anwendungen auswirkt. Die Zugriffsrechte für Administratoren auf virtuelle IT-Systeme MÜSSEN auf das tatsächlich notwendige Maß reduziert sein.

Es MUSS gewährleistet sein, dass die für die virtuellen IT-Systeme notwendigen Netzverbindungen in der virtuellen Infrastruktur verfügbar sind. Auch MUSS geprüft werden, ob die Anforderungen an die Isolation und Kapselung der virtuellen IT-Systeme sowie der darauf betriebenen Anwendungen hinreichend erfüllt sind. Weiterhin MÜSSEN die eingesetzten virtuellen IT-Systeme den Anforderungen an die Verfügbarkeit und den Datendurchsatz genügen. Im laufenden Betrieb MUSS die Performance der virtuellen IT-Systeme überwacht werden.

SYS.1.5.A3 Sichere Konfiguration virtueller IT-Systeme

Gast-Systeme DÜRFEN NICHT auf Geräte und Schnittstellen des Virtualisierungsservers zugreifen. Ist eine solche Verbindung jedoch notwendig, MUSS diese exklusiv und nur für die notwendige Dauer vom Administrator des Host-Systems hergestellt werden. Dafür MÜSSEN verbindliche Regelungen festgelegt werden.

Virtuelle IT-Systeme SOLLTEN nach den Sicherheitsrichtlinien der Institution konfiguriert und geschützt werden (siehe dazu die jeweils passenden Bausteine der Schicht *SYS*).

SYS.1.5.A4 Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen

Es MUSS sichergestellt werden, dass bestehende Sicherheitsmechanismen (z. B. Firewalls) und Monitoring-Systeme nicht durch virtuelle Netze umgangen werden können. Auch MUSS ausgeschlossen sein, dass über virtuelle IT-Systeme, die mit mehreren Netzen verbunden sind, unerwünschte Netzverbindungen aufgebaut werden können.

Netzverbindungen zwischen virtuellen IT-Systemen und physischen IT-Systemen sowie für virtuelle Sicherheitsgateways SOLLTEN gemäß den Sicherheitsrichtlinien der Institution konfiguriert werden.

SYS.1.5.A5 Schutz der Administrationsschnittstellen

Alle Administrations- und Management-Zugänge zum Mananagement-System und zu den Host-Systemen MÜSSEN eingeschränkt werden. Es MUSS sichergestellt sein, dass aus nicht-vertrauenswürdigen Netzen heraus nicht auf die Administrationsschnittstellen zugegriffen werden kann.

Um die Virtualisierungsserver oder die Management-Systeme zu administrieren bzw. zu überwachen, SOLLTEN ausreichend verschlüsselte Protokolle eingesetzt werden. Sollte dennoch auf unverschlüsselte und damit unsichere Protokolle zurückgegriffen werden, MUSS für die Administration ein eigenes Administrationsnetz genutzt werden.

SYS.1.5.A6 Protokollierung in der virtuellen Infrastruktur

Betriebszustand, Auslastung und Netzanbindungen der virtuellen Infrastruktur MÜSSEN laufend protokolliert werden. Werden Kapazitätsgrenzen erreicht, MÜSSEN virtuelle Maschinen verschoben und eventuell die Hardware erweitert werden. Die Protokollierungsdaten SOLLTEN regelmäßig ausgewertet werden.

SYS.1.5.A7 Zeitsynchronisation in virtuellen IT-Systemen

Die Systemzeit aller produktiv eingesetzten IT-Systeme MUSS immer synchron sein (siehe auch OPS.1.1.5 *Protokollierung*).

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Virtualisierung. Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.1.5.A8 Planung einer virtuellen Infrastruktur [Leiter IT, Leiter Netze]

Der Aufbau der virtuellen Infrastruktur SOLLTE detailliert geplant werden. Dabei SOLLTEN die geltenden Regelungen und Richtlinien für den Betrieb von IT-Systemen, Anwendungen, Netzen und Speichernetzen berücksichtigt werden. Wenn mehrere virtuelle IT-Systeme auf einem Virtualisierungsserver betrieben werden, SOLLTEN keine Konflikte hinsichtlich des Schutzbedarfs der IT-Systeme auftreten.

Weiterhin SOLLTEN die Aufgaben der einzelnen Administratorengruppen festgelegt und klar voneinander abgegrenzt werden. Es SOLLTE auch geregelt werden, welcher Mitarbeiter für den Betrieb welcher Komponente verantwortlich ist. Die Administratoren SOLLTEN ausreichend qualifiziert sein.

SYS.1.5.A9 Netzplanung für virtuelle Infrastrukturen [Leiter IT, Leiter Netze]

Der Aufbau des Netzes für virtuelle Infrastrukturen SOLLTE detailliert geplant werden. Dafür SOLLTE der Baustein NET.1.1 *Netzarchitektur und -design* berücksichtigt werden. Auch SOLLTE geprüft werden, ob für bestimmte Virtualisierungsfunktionen (wie z. B. die *Live Migration*) ein eigenes Netz aufgebaut und genutzt werden muss.

Es SOLLTE geplant werden, welche Netzsegmente aufgebaut werden müssen (z. B. Managementnetz, Speichernetz) und wie sie sich sicher voneinander trennen und schützen lassen. Dabei SOLLTE sichergestellt werden, dass das produktive Netz vom Managementnetz getrennt ist (siehe SYS.1.5.A11 *Administration der Virtualisierungsinfrastruktur über ein gesondertes Managementnetz*). Auch die Verfügbarkeitsanforderungen an das Netz SOLLTEN beachtet und erfüllt werden.

SYS.1.5.A10 Einführung von Verwaltungsprozessen für virtuelle IT-Systeme [Leiter IT]

Für Virtualisierungsserver und virtuelle IT-Systeme SOLLTEN Prozesse für die Inbetriebnahme, die Inventarisierung, den Betrieb und die Außerbetriebnahme definiert und etabliert werden. Die Prozesse SOLLTEN dokumentiert und regelmäßig aktualisiert werden.

Wenn der Einsatz geplant wird, SOLLTE festgelegt werden, welche Virtualisierungsfunktionen die virtuellen IT-Systeme benutzen dürfen.

Bevor ein virtuelles IT-System betrieben wird, SOLLTE in einer Test- und Entwicklungsumgebung geprüft werden, ob es für den Produktiveinsatz geeignet ist. Test- und Entwicklungsumgebungen SOLLTEN NICHT auf demselben Virtualisierungsserver betrieben werden wie produktive virtuelle IT-Systeme.

SYS.1.5.A11 Administration der Virtualisierungsinfrastruktur über ein gesondertes Managementnetz

Die Virtualisierungsinfrastruktur SOLLTE ausschließlich über ein separates Managementnetz administriert werden. Die verfügbaren Sicherheitsmechanismen der eingesetzten Managementprotokolle zur Authentisierung, Integritätssicherung und Verschlüsselung SOLLTEN aktiviert und alle unsicheren Managementprotokolle deaktiviert werden (siehe NET.1.2 *Netz-Management*).

SYS.1.5.A12 Rechte- und Rollenkonzept für die Administration einer virtuellen Infrastruktur

Anhand der in der Planung definierten Aufgaben und Rollen (siehe SYS.1.5.A8 *Planung einer virtuellen Infrastruktur*) SOLLTE für die Administration virtueller IT-Systeme und Netze, der Virtualisierungsserver sowie der Management-Umgebung ein Rechte- und Rollenkonzept erstellt und umgesetzt werden. Alle Komponenten der virtuellen Infrastruktur SOLLTEN in ein zentrales Identitäts- und Berechtigungsmanagement eingebunden werden.

Administratoren von virtuellen Maschinen und Administratoren der Virtualisierungsumgebung SOLLTEN unterschieden und mit unterschiedlichen Zugriffsrechten ausgestattet werden.

Weiterhin SOLLTE die Management-Umgebung virtuelle Maschinen gruppieren können, um eine geeignete Strukturierung verbunden mit einer entsprechenden Administratoren-Rollenzuteilung einzuführen.

SYS.1.5.A13 Auswahl geeigneter Hardware für Virtualisierungsumgebungen

Die verwendete Hardware SOLLTE kompatibel zur eingesetzten Virtualisierungslösung sein. Dabei SOLLTE darauf geachtet werden, dass der Hersteller der Virtualisierungslösung über den geplanten Einsatzzeitraum auch Support für die betriebene Hardware anbietet.

SYS.1.5.A14 Einheitliche Konfigurationsstandards für virtuelle IT-Systeme [Leiter IT]

Für die eingesetzten virtuellen IT-Systeme SOLLTEN einheitliche Konfigurationsstandards definiert werden. Die virtuellen IT-Systeme SOLLTEN nach diesen Standards konfiguriert werden. Die Konfigurationsstandards SOLLTEN regelmäßig überprüft und falls erforderlich angepasst werden.

SYS.1.5.A15 Betrieb von Gast-Betriebssystemen mit unterschiedlichem Schutzbedarf

Falls virtuelle IT-Systeme mit unterschiedlichem Schutzbedarf gemeinsam auf einem Virtualisierungsserver betriebenen werden, SOLLTE dabei sichergestellt sein, dass die virtuellen IT-Systeme ausreichend gekapselt und voneinander isoliert sind. Auch SOLLTE dann die Netztrennung in der eingesetzten Virtualisierungslösung ausreichend sicher sein. Ist das nicht der Fall, SOLLTEN weitergehende Sicherheitsmaßnahmen identifiziert und umgesetzt werden.

SYS.1.5.A16 Kapselung der virtuellen Maschinen

Die Funktionen *Kopieren* und *Einfügen* von Informationen zwischen virtuellen Maschinen SOLLTEN deaktiviert sein.

SYS.1.5.A17 Überwachung des Betriebszustands und der Konfiguration der virtuellen Infrastruktur

Der Betriebszustand der virtuellen Infrastruktur SOLLTE überwacht werden. Dabei SOLLTE z. B. geprüft werden, ob noch ausreichend Ressourcen verfügbar sind und ob es eventuell Konflikte bei gemeinsam benutzten Ressourcen eines Virtualisierungsservers gibt.

Weiterhin SOLLTEN die Konfigurationsdateien der virtuellen IT-Systeme regelmäßig auf unautorisierte Änderungen überprüft werden. Auch SOLLTE überwacht werden, ob die virtuellen Netze den jeweiligen virtuellen IT-Systemen korrekt zugeordnet sind.

Werden Konfigurationsänderungen an der Virtualisierungsinfrastruktur vorgenommen, SOLLTEN diese geprüft bzw. getestet werden, bevor sie umgesetzt werden.

SYS.1.5.A18 Schulung der Administratoren virtueller Umgebungen [Vorgesetzte, Leiter IT, Leiter Netze]

Alle Administratoren der virtuellen Umgebung SOLLTEN ausreichend geschult werden. In der Schulung SOLLTE vermittelt werden, wie virtuelle Infrastrukturen sicher aufgebaut und betrieben werden können.

SYS.1.5.A19 Regelmäßige Audits der Virtualisierungsinfrastruktur

Es SOLLTE regelmäßig auditiert werden, ob der Ist-Zustand der virtuellen Infrastruktur dem in der Planung festgelegtem Zustand entspricht und ob die Konfiguration der virtuellen Komponenten die vorgegebene Standardkonfiguration einhält. Die Auditergebnisse SOLLTEN nachvollziehbar dokumentiert werden. Abweichungen SOLLTEN behoben werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.1.5.A20 Verwendung von hochverfügbaren Architekturen [Leiter IT, Leiter Netze] (A)

Die virtuelle Infrastruktur SOLLTE hochverfügbar ausgelegt werden. Alle Virtualisierungsserver SOLLTEN in Clustern zusammengeschlossen werden.

SYS.1.5.A21 Sichere Konfiguration virtueller IT-Systeme bei erhöhtem Schutzbedarf (IA)

Für virtuelle IT-Systeme SOLLTEN Überbuchungsfunktionen für Ressourcen deaktiviert werden.

SYS.1.5.A22 Härtung des Virtualisierungsservers (CI)

Der Virtualisierungsserver SOLLTE gehärtet werden. Um virtuelle IT-Systeme voreinander und gegenüber dem Virtualsierungsserver zusätzlich zu isolieren und zu kapseln, SOLLTEN Mandatory Access Controls eingesetzt werden. Ebenso SOLLTE das IT-System gehärtet werden, auf dem die Management-Software installiert ist.

SYS.1.5.A23 Rechte-Einschränkung der virtuellen Maschinen (CI)

Alle Schnittstellen und Kommunikationskanäle, die es einem virtuellen IT-System erlauben, Informationen über das Host-System auszulesen und abzufragen, SOLLTEN deaktiviert sein oder unterbunden werden. Weiterhin SOLLTE ausschließlich der Virtualisierungsserver auf seine Ressourcen zugreifen können. Außerdem SOLLTE es NICHT möglich sein, dass sich virtuelle IT-Systeme sogenannte *Pages* des Arbeitsspeichers teilen.

SYS.1.5.A24 Deaktivierung von Snapshots virtueller IT-Systeme (CIA)

Für alle virtuellen IT-Systeme SOLLTE die Snapshot-Funktion deaktiviert werden.

SYS.1.5.A25 Minimale Nutzung von Konsolenzugriffen auf virtuelle IT-Systeme (A)

Direkte Zugriffe auf die emulierten Konsolen virtueller IT-Systeme SOLLTEN auf ein Mindestmaß reduziert werden. Die virtuellen Systeme SOLLTEN möglichst über das Netz gesteuert werden.

SYS.1.5.A26 Einsatz einer PKI [Leiter IT, Leiter Netze] (CIA)

Da die Kommunikation zwischen den Komponenten der IT-Infrastruktur häufig mithilfe von Zertifikaten abgesichert wird, SOLLTE eine Public-Key-Infrastruktur (PKI) eingesetzt werden.

SYS.1.5.A27 Einsatz zertifizierter Virtualisierungssoftware [Leiter IT] (CIA)

Es SOLLTE zertifizierte Virtualisierungssoftware der Stufe EAL 4 oder höher eingesetzt werden.

SYS.1.5.A28 Verschlüsselung von virtuellen IT-Systemen (CI)

Alle virtuellen IT-Systeme SOLLTEN verschlüsselt werden.

4 Weiterführende Informationen

4.1 Literatur

- [CSE113] CSE-113: Server-Virtualisierung
  CSE-113:Server-Virtualisierung, BSI-Veröffentlichung zur Cyber-Sicherheit, 03.2015
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_113.htm

- [ISFSY13] Information Security Forum (ISF)
  insbesondere Area SY1.3 - Virtual Servers, 06.2016

- [NIST800125] NIST Special Publication (SP) 800-125, Guide to Security for Full Virtualization Technologies, 01.2011
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Virtualisierung" von Bedeutung.

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.43 Einspielen von Nachrichten

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen Anforderungen	G 0.15	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.29	G 0.30	G 0.31	G 0.32	G 0.40	G 0.43	G 0.46
SYS.1.5.A1								x		x	x							
SYS.1.5.A2													x		x			
SYS.1.5.A3						x	x		x	x								
SYS.1.5.A4						x	x											
SYS.1.5.A5	x					x	x						x					
SYS.1.5.A6								x	x	x								
SYS.1.5.A7									x									
SYS.1.5.A8		x								x		x	x	x				
SYS.1.5.A9	x	x				x	x			x			x					
SYS.1.5.A10		x	x	x	x				x									
SYS.1.5.A11	x				x		x											
SYS.1.5.A12		x											x		x			
SYS.1.5.A13		x							x									
SYS.1.5.A14			x		x	x	x											
SYS.1.5.A15						x	x						x				x	
SYS.1.5.A16						x	x						x					
SYS.1.5.A17								x	x	x								
SYS.1.5.A18			x											x				
SYS.1.5.A19			x			x	x		x									
SYS.1.5.A20								x	x								x	
SYS.1.5.A21									x	x								
SYS.1.5.A22			x		x	x	x											
SYS.1.5.A23						x	x											
SYS.1.5.A24						x	x						x					
SYS.1.5.A25									x	x								
SYS.1.5.A26	x				x	x	x									x		
SYS.1.5.A27	x			x	x	x	x											
SYS.1.5.A28	x																	x

SYS.1: Server

SYS.1.8 Speicherlösungen

1 Beschreibung

1.1 Einleitung

Das stetige Wachstum digitaler Informationen und die zunehmende Menge unstrukturierter Informationen führen dazu, dass innerhalb von Institutionen zentrale Speicherlösungen eingesetzt werden. Dabei unterliegen die Anforderungen an solche Speicherlösungen einem stetigen Wandel, der sich beispielsweise an folgenden Aspekten beobachten lässt:

- Die Daten einer Institution sollen jederzeit, an jedem Ort und für unterschiedliche Anwendungsszenarien verfügbar sein. Dadurch gelten für moderne Speicherlösungen häufig gestiegene Verfügbarkeitsanforderungen.
- Die zunehmende Digitalisierung sämtlicher Informationen in einer Institution macht es notwendig, dass weitreichende rechtliche Vorgaben (Compliance-Anforderungen) beachtet und eingehalten werden.
- Speicherlösungen sollen dynamisch an die sich stetig ändernden Anforderungen anpassbar sein und Speicherplatz zentral bereitstellen können.

In der Vergangenheit wurden Speicherlösungen oft umgesetzt, indem Speichermedien direkt an einen Server angeschlossen wurden. Diese sogenannten Direct-Attached-Storage-(DAS)-Systeme können die aktuellen und zukünftigen Anforderungen jedoch oft nicht mehr abdecken. Daher sind die heute weit verbreiteten zentralen Speicherlösungen und deren Bestandteile notwendig, die sich wie Folgt unterscheiden lassen:

- Speicherlösungen: Eine Speicherlösung besteht aus einem oder mehreren Speichernetzen sowie mindestens einem Speichersystem.
- Speichernetze: Speichernetze ermöglichen einerseits den Zugriff auf die Speichersysteme, andererseits die Replikation von Daten zwischen Speichersystemen.
- Speichersysteme: Als Speichersystem wird die zentrale Instanz bezeichnet, die für andere IT-Systeme Speicherplatz zur Verfügung stellt. Ein Speichersystem erlaubt außerdem den zeitgleichen Zugriff mehrerer IT-Systeme auf den vorhandenen Speicherplatz.

1.2 Zielsetzung

Das Ziel dieses Bausteins ist es aufzuzeigen, wie zentrale Speicherlösungen sicher geplant, betrieben und ausgesondert werden.

1.3 Abgrenzung

In diesem Baustein werden Speichersysteme zusammen mit den dazugehörigen Speichernetzen betrachtet. Datensicherungsgeräte, die an das Speichersystem oder an das Speichernetz angeschlossen sind, werden hier nicht betrachtet, sondern im Baustein OPS.1.2.2 *Archivierung* behandelt. Konzeptionelle Aspekte der Datensicherung werden im Baustein CON.3 *Datensicherungskonzept* erläutert. Zudem werden keine Anforderungen an Fileserver beschrieben. Diese sind im Baustein APP.3.3 *Fileserver* zu finden.

Falls auf externe Dienstleister zurückgegriffen wird, um eine Speicherlösung zu betreiben, müssen die Anforderungen des Bausteins OPS.2.1 *Outsourcing für Kunden* gesondert berücksichtigt werden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Speicherlösungen von besonderer Bedeutung:

2.1 Fehlende oder unzureichende Abgrenzung von Verantwortlichkeiten bei Speicherlösungen

Zentrale Speicherlösungen erhöhen die Anforderungen an die Administration. Werden dabei die Verantwortlichkeiten für unterschiedliche Bereiche nicht klar definiert, kann das zu Fehlkonfigurationen führen. Administriert beispielsweise ein klassischer Netzadministrator FC-Switches (Fibre Channel, FC), so kann er möglicherweise auf Komponenten zugreifen, für die er nicht zuständig und nicht ausgebildet ist. Ein solcher Vorgang kann dazu führen, dass FC-Switches nicht richtig konfiguriert werden. Dadurch könnten wichtige Dienste ausfallen, weil alle an die FC-Switches angeschlossenen Server nicht mehr auf die Speichersysteme zugreifen können.

2.2 Unsichere Default-Einstellungen bei Speicherkomponenten

Häufig werden Speicherkomponenten mit einer Default-Konfiguration ausgeliefert, damit die Geräte schnell und mit möglichst umfassender Funktionalität in Betrieb genommen werden können. So sind in vielen Geräten nicht benötigte Funktionen aktiviert, wie z. B. HTTP, Telnet und unsichere SNMP-Versionen. Werden Speicherkomponenten mit unsicheren Werkseinstellungen produktiv eingesetzt, kann einfacher unberechtigt auf sie zugegriffen werden. Das kann dazu führen, dass z. B. Dienste nicht mehr verfügbar sind oder dass unerlaubt auf vertrauliche Informationen der Institution zugegriffen wird.

2.3 Manipulation von Daten über das Speichersystem

Über ein mangelhaft konfiguriertes Storage Area Network (SAN) können sich ungewollt Netze verbinden. Ist beispielsweise ein Server mit SAN-Anschluss aus dem Internet erreichbar und so von außen kompromittierbar, kann dieser als Einstiegspunkt für Angreifer genutzt werden, um unberechtigt auf schützenswerte Informationen zuzugreifen, die im SAN gespeichert sind. Da auf diese Weise alle Sicherheits- und Überwachungsmaßnahmen wie Firewalls oder IDS (Intrusion Detection Systeme) in den IT-Netzen einer Institution umgangen werden können, ist das Schadenspotential groß.

2.4 Verlust der Vertraulichkeit durch storagebasierte Replikationsmethoden

Storagebasierte Replikationsmethoden haben den Zweck, gespeicherte oder archivierte Daten in Echtzeit über ein Speichernetz zu duplizieren und diese damit zusätzlich redundant abzuspeichern. Hierdurch sollen Datenverluste vermieden werden. Die automatisierte Replikation unverschlüsselter Daten birgt allerdings sowohl im eigenen Netz als auch bei der Nutzung öffentlicher Netze Risiken: So kann unberechtigt auf legitimen Replikationsverkehr zugegriffen werden, beispielsweise mittels FC-Analysern (FC-Replikation) oder Sniffern (IP-Replikation).

2.5 Zugriff auf Informationen anderer Mandanten durch WWN-Spoofing

Geräte in einem FC-SAN werden intern über World Wide Names (WWNs) verwaltet und zugeordnet. Sie entsprechen in gewisser Weise den MAC-Adressen von Ethernet-Netzadaptern. Mittels Programmen, die durch den Hersteller der Host Bus Adapter (HBA) zur Verfügung gestellt werden, kann der WWN eines HBAs geändert werden. Dadurch kann ein Angreifer auf Daten zugreifen, für die er keine Berechtigung besitzt. Die Manipulation von WWNs, auch als WWN-Spoofing bezeichnet, birgt für eine Institution erhebliches Gefahrenpotenzial. Insbesondere im Zusammenhang mit mandantenfähigen Speichersystemen können Unberechtigte auf die Informationen anderer Mandanten zugreifen.

2.6 Überwindung der logischen Netzseparierung

Werden die Netzstrukturen unterschiedlicher Mandanten nicht durch physisch getrennte Netze, sondern durch virtuelle Storage Area Networks (VSANs) separiert, kann hierdurch die Informationssicherheit der Institution gefährdet werden. Gelingt es einem Angreifer in das Netz eines anderen Mandanten einzudringen, kann er sowohl auf das virtuelle SAN dieses Mandanten als auch auf die übertragenen Nutzdaten zugreifen.

2.7 Ausfall von Komponenten einer Speicherlösung

Komplexe, netzbasierte Speicherlösungen bestehen oft aus vielen Komponenten (z. B. FC-Switches, Storage Controller, Virtualisierungs-Appliance). Fallen Komponenten einer Speicherlösung aus, kann dies dazu führen, dass wichtige Anwendungen nicht mehr korrekt arbeiten und somit Datenverluste drohen.

2.8 Erlangung physischen Zugangs auf SAN-Switches

Existieren in einer Institution unzureichende Zutritts- und Zugangskontrollen zu den Komponenten eines Speichersystems oder fehlen diese gänzlich, kann es einem Angreifer gelingen, sich physischen Zugang zu vorhandenen Switches zu verschaffen bzw. zusätzliche FC-SAN-Switches an das Netz anzuschließen. Ziel des Angreifers könnte es sein, auf die verteilte Zoning-Datenbank zuzugreifen, um diese so zu verändern, dass er auf die Speichersysteme zugreifen kann.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen an Speicherlösungen aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist er dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Haustechnik, Informationssicherheitsbeauftragter (ISB), Leiter IT, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.1.8.A1 Geeignete Aufstellung von Speichersystemen [Haustechnik, Leiter IT]

Die IT-Komponenten MÜSSEN in gesicherten Räumen aufgestellt werden. Zu diesen Räumen DÜRFEN NUR Berechtigte Zutritt haben. Zudem MUSS eine sichere Stromversorgung und entsprechend den Herstellervorgaben empfohlene Umgebungstemperatur und Luftfeuchte sichergestellt sein.

SYS.1.8.A2 Sichere Grundkonfiguration von Speicherlösungen

Bevor eine Speicherlösung produktiv eingesetzt wird, MUSS sichergestellt sein, dass alle eingesetzten Software- und Firmwarekomponenten aktuell sind. Danach MUSS eine sichere Grundkonfiguration hergestellt werden.

Nicht benötigte Benutzerkonten MÜSSEN deaktiviert werden. Auch MÜSSEN Standard-Passwörter im Einklang mit der Passwortrichtlinie geändert bzw. neue Accounts angelegt werden.

Nicht genutzte Schnittstellen des Speichersystems MÜSSEN deaktiviert werden. Die Default-Konfiguration, die vorgenommene Grundkonfiguration und die aktuelle Konfiguration SOLLTEN redundant und geschützt aufbewahrt werden.

SYS.1.8.A3 Restriktive Rechtevergabe

Für Speicherlösungen MUSS ein Rechte- und Rollenkonzept erstellt werden. Alle auf der jeweiligen Lösung eingerichteten Benutzerkonten MÜSSEN diesem Konzept entsprechen. Alle Benutzerkonten MÜSSEN nach dem Prinzip der minimalen Berechtigungen eingerichtet werden.

SYS.1.8.A4 Schutz der Administrationsschnittstellen

Alle Administrations- und Management-Zugänge der Speichersysteme MÜSSEN eingeschränkt werden. Es MUSS sichergestellt sein, dass aus nicht-vertrauenswürdigen Netzen heraus nicht auf die Administrationsschnittstellen zugegriffen werden kann.

Es SOLLTEN ausreichend verschlüsselte Protokolle eingesetzt werden. Sollte dennoch auf unverschlüsselte und damit unsichere Protokolle zurückgegriffen werden, MUSS für die Administration ein eigenes Administrationsnetz genutzt werden.

SYS.1.8.A5 Protokollierung bei Speichersystemen

Die interne Protokollierung der Speichersysteme MUSS so konfiguriert werden, dass Informationen protokolliert werden, die dazu dienen, Probleme früh zu erkennen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Speicherlösungen. Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.1.8.A6 Erstellung einer Sicherheitsrichtlinie für Speicherlösungen [Informationssicherheitsbeauftragter (ISB)]

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTE eine spezifische Sicherheitsrichtlinie für Speicherlösungen erstellt werden. Darin SOLLTEN nachvollziehbar Anforderungen und Vorgaben beschrieben sein, wie Speicherlösungen sicher geplant, administriert, installiert, konfiguriert und betrieben werden können.

Die Richtlinie SOLLTE allen für Speicherlösungen verantwortlichen Administratoren bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, SOLLTE dies mit dem ISB abgestimmt und dokumentiert werden. Es SOLLTE regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

SYS.1.8.A7 Planung von Speicherlösungen [Informationssicherheitsbeauftragter (ISB), Leiter IT]

Es SOLLTE eine Anforderungsanalyse durchgeführt werden, in der unter anderem die Themen Performance und Kapazität betrachtet werden. Auf Basis der ermittelten Anforderungen, SOLLTE dann eine detaillierte Planung für Speicherlösungen erstellt werden. Darin SOLLTEN folgende Punkte berücksichtigt werden:

- Auswahl geeigneter Hardware,
- Auswahl von Herstellern und Lieferanten,
- Entscheidung für oder gegen zentrale Managementsysteme,
- Planung des Netzanschlusses,
- Planung der Infrastruktur sowie
- Integration in bestehende Prozesse.

SYS.1.8.A8 Auswahl einer geeigneten Speicherlösung [Informationssicherheitsbeauftragter (ISB), Leiter IT]

Es SOLLTEN die technischen Grundlagen unterschiedlicher Speicherlösungen detailliert beleuchtet und deren Auswirkungen auf den möglichen Einsatz in der Institution geprüft werden. Dabei SOLLTEN Möglichkeiten und Grenzen der verschiedenen Speichersystemarten für die Verantwortlichen der Institution transparent dargestellt werden. Die Entscheidungskriterien für eine Speicherlösung SOLLTEN nachvollziehbar dokumentiert werden. Ebenso SOLLTE die Entscheidung für die Auswahl einer Speicherlösung nachvollziehbar dokumentiert werden.

SYS.1.8.A9 Auswahl von Lieferanten für eine Speicherlösung [Informationssicherheitsbeauftragter (ISB), Leiter IT]

Anhand der spezifizierten Anforderungen an eine Speicherlösung SOLLTE ein geeigneter Lieferant ausgewählt werden. Die Auswahlkriterien und die Entscheidung für einen Lieferanten SOLLTEN nachvollziehbar dokumentiert werden. Außerdem SOLLTEN Aspekte der Wartung und Instandhaltung schriftlich in sogenannten Service-Level-Agreements (SLAs) festgehalten werden. Die SLAs SOLLTEN eindeutig und quantifizierbar sein. Es SOLLTE genau geregelt werden, wann der Vertrag mit dem Lieferanten endet.

SYS.1.8.A10 Erstellung und Pflege eines Betriebshandbuchs [Informationssicherheitsbeauftragter (ISB), Leiter IT]

Es SOLLTE ein Betriebshandbuch erstellt werden. Darin SOLLTEN alle erforderlichen Regelungen, Anforderungen und Einstellungen dokumentiert werden, die erforderlich sind, um Speicherlösungen zu betreiben. Das Betriebshandbuch SOLLTE regelmäßig aktualisiert werden.

SYS.1.8.A11 Sicherer Betrieb einer Speicherlösung

Das Speichersystem SOLLTE hinsichtlich der Verfügbarkeit der internen Anwendungen, der Systemauslastung sowie kritischer Ereignisse überwacht werden (siehe auch SYS.1.8.A13 *Überwachung und Verwaltung von Speicherlösungen*). Weiterhin SOLLTEN für Speicherlösungen feste Wartungsfenster definiert werden, in denen Änderungen durchgeführt werden können. Insbesondere Firmware- oder Betriebssystemupdates von Speichersystemen oder den Netzkomponenten einer Speicherlösung SOLLTEN ausschließlich innerhalb eines solchen Wartungsfensters durchgeführt werden. Alle Änderungen SOLLTEN zudem über das Änderungsmanagement aktiviert und mit allen beteiligten Fachverantwortlichen abgestimmt werden.

SYS.1.8.A12 Schulung der Administratoren [Vorgesetzte, Leiter IT]

Die für die Speicherlösungen zuständigen Administratoren SOLLTEN ausreichend geschult werden. In den Schulungen SOLLTEN Kenntnisse vermittelt werden, mit welchen Vorgehensweisen, Techniken und Werkzeugen sich Speichersysteme und die zugehörigen Komponenten einrichten und sicher betreiben lassen. Zudem SOLLTEN herstellerspezifische Aspekte zu einzelnen Produkten und Komponenten thematisiert werden. Setzt eine Institution neue Produkte ein, SOLLTEN die Administratoren speziell dazu nachgeschult werden.

SYS.1.8.A13 Überwachung und Verwaltung von Speicherlösungen

Um Fehlersituationen und Sicherheitsprobleme erkennen und beheben zu können, SOLLTEN Speicherlösungen überwacht werden. Dabei SOLLTEN alle erhobenen Daten vorrangig daraufhin geprüft werden, ob die Vorgaben des Betriebshandbuchs eingehalten werden (siehe auch SYS.1.8.A10 *Erstellung und Pflege eines Betriebshandbuchs*).

Einzelne Komponenten der Speicherlösung und des Gesamtsystems SOLLTEN zentral verwaltet werden. Zudem SOLLTEN die wesentlichen Nachrichten herausgefiltert werden, um diese besser darzustellen.

Sofern eine Speicherlösung durch einen externen Dienstleister betrieben wird, SOLLTE definiert und dokumentiert werden, wie die vertraglich vereinbarten SLAs überwacht werden.

SYS.1.8.A14 Absicherung eines SANs durch Segmentierung

Ein SAN SOLLTE segmentiert werden. Es SOLLTE ein Konzept erarbeitet werden, das die SAN-Ressourcen den jeweiligen Servern zuordnet. Hierfür SOLLTE anhand der Sicherheitsanforderungen und des Administrationsaufwands entschieden werden, welche Segmentierung in welchem Einsatzszenario eingesetzt werden soll. Die aktuelle Ressourcenzuordnung SOLLTE mithilfe von Verwaltungswerkzeugen einfach und übersichtlich erkennbar sein. Weiterhin SOLLTE die aktuelle Zoning-Konfiguration dokumentiert werden. Die Dokumentation SOLLTE auch in Notfällen verfügbar sein.

SYS.1.8.A15 Sichere Trennung von Mandanten in Speicherlösungen

Es SOLLTE definiert und nachvollziehbar dokumentiert werden, welche Anforderungen die Institution an die Mandantenfähigkeit einer Speicherlösung stellt. Die eingesetzten Speicherlösungen SOLLTEN diesen dokumentierten Anforderungen genügen.

Im Block-Storage-Umfeld SOLLTE *LUN Masking* eingesetzt werden, um Mandanten voneinander zu trennen. In Fileservice-Umgebungen SOLLTE es möglich sein, mit virtuellen Fileservern zu agieren. Dabei SOLLTE jedem Mandanten ein eigener Fileservice zugeordnet werden.

Beim Einsatz von IP oder iSCSI SOLLTEN die Mandanten über eine Segmentierung im Netz voneinander getrennt werden. Wird Fibre Channel eingesetzt, SOLLTE mithilfe von VSANs und Soft-Zoning separiert werden.

SYS.1.8.A16 Sicheres Löschen in SAN-Umgebungen

Für das Speichersystem SOLLTE festgelegt werden, welche Informationen mit welchen Verfahren zu löschen sind. In mandantenfähigen Speichersystemen SOLLTE sichergestellt werden, dass Logical Unit Numbers (LUNs), die einem bestimmten Mandanten zugeordnet sind, gelöscht werden.

SYS.1.8.A17 Dokumentation der Systemeinstellungen von Speichersystemen

Alle Systemeinstellungen von Speichersystemen SOLLTEN dokumentiert werden. Die Dokumentation SOLLTE die technischen und organisatorischen Vorgaben sowie alle spezifischen Konfigurationen der Speichersysteme der Institution enthalten.

Sofern die Dokumentation der Systemeinstellungen vertrauliche Informationen beinhaltet, SOLLTEN diese vor unberechtigtem Zugriff geschützt werden. Die Dokumentation SOLLTE regelmäßig überprüft werden und immer aktuell sein, insbesondere hinsichtlich der Rechtevergabe. Auch SOLLTE dafür gesorgt werden, dass sie in allen Notfallszenarien verfügbar ist.

SYS.1.8.A18 Sicherheits-Audits und Berichtswesen bei Speichersystemen [Informationssicherheitsbeauftragter (ISB)]

Alle eingesetzten Speichersysteme SOLLTEN regelmäßig auditiert werden. Dafür SOLLTE ein entsprechender Prozess eingerichtet werden. Es SOLLTE geregelt werden, welche Sicherheitsreports mit welchen Inhalten regelmäßig zu erstellen sind. Zudem SOLLTE auch geregelt werden, wie mit Abweichungen von Vorgaben umgegangen wird und wie oft und in welcher Tiefe Audits durchgeführt werden.

SYS.1.8.A19 Aussonderung von Speicherlösungen

Werden ganze Speicherlösungen oder einzelne Komponenten einer Speicherlösung nicht mehr benötigt, SOLLTEN alle darauf vorhandenen Daten auf andere Speicherlösungen übertragen werden. Hierfür SOLLTE eine Übergangsphase eingeplant werden. Anschließend SOLLTEN alle Nutzdaten und Konfigurationsdaten sicher gelöscht werden. Aus allen relevanten Dokumenten SOLLTEN alle Verweise auf die außer Betrieb genommene Speicherlösung entfernt werden.

SYS.1.8.A20 Notfallvorsorge und Notfallreaktion für Speicherlösungen [Leiter IT]

Es SOLLTE ein Notfallplan für die eingesetzte Speicherlösung erstellt werden. Der Plan SOLLTE genau beschreiben, wie in bestimmten Notfallsituationen vorzugehen ist. Auch SOLLTEN Handlungsanweisungen in Form von Maßnahmen und Kommandos enthalten sein, die die Fehleranalyse und Fehlerkorrektur unterstützen. Um Fehler zu beheben, SOLLTEN geeignete Werkzeuge eingesetzt werden.

Es SOLLTEN regelmäßige Übungen und Tests des Notfallplans durchgeführt werden. Nach den Übungen und Tests sowie nach einem Notfall SOLLTEN die dabei erzeugten Daten sicher gelöscht werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.1.8.A21 Einsatz von Speicher-Pools zur Mandantentrennung (CI)

Mandanten SOLLTEN Speicherressourcen aus unterschiedlichen sogenannten Speicher-Pools zugewiesen werden. Dabei SOLLTE ein Speichermedium immer nur einem einzigen Pool zugewiesen werden. Die logischen Festplatten (LUNs), die aus einem solchen Pool generiert werden, SOLLTEN nur einem einzigen Mandanten zugeordnet werden.

SYS.1.8.A22 Einsatz einer hochverfügbaren SAN-Lösung [Informationssicherheitsbeauftragter (ISB)] (A)

Es SOLLTE eine hochverfügbare SAN-Lösung eingesetzt werden. Die eingesetzten Replikationsmechanismen SOLLTEN den Verfügbarkeitsanforderungen der Institution an die Speicherlösung entsprechen. Auch die Konfiguration der Speicherlösung SOLLTE den Verfügbarkeitsanforderungen gerecht werden. Außerdem SOLLTE ein Test- und Konsolidierungssystem vorhanden sein.

SYS.1.8.A23 Einsatz von Verschlüsselung für Speicherlösungen [Informationssicherheitsbeauftragter (ISB)] (CI)

Alle in Speicherlösungen abgelegten Daten SOLLTEN verschlüsselt werden. Es SOLLTE festgelegt werden, auf welchen Ebenen (Data-in-Motion und Data-in-Rest) verschlüsselt wird. Dabei SOLLTE beachtet werden, dass die Verschlüsselung auf dem Transportweg auch bei Replikationen und Backup-Traffic relevant ist.

SYS.1.8.A24 Sicherstellung der Integrität der SAN-Fabric (I)

Um die Integrität der SAN-Fabric sicherzustellen, SOLLTEN Protokolle mit zusätzlichen Sicherheitsmerkmalen eingesetzt werden. Bei den folgenden Protokollen SOLLTEN deren Sicherheitseigenschaften berücksichtigt und entsprechende Konfigurationen verwendet werden:

- Diffie Hellman Challenge Handshake Authentication Protocol (DH-CHAP),
- Fibre Channel Authentication Protocol (FCAP) und
- Fibre Channel Password Authentication Protocol (FCPAP).

SYS.1.8.A25 Mehrfaches Überschreiben der Daten einer LUN (C)

In SAN-Umgebungen SOLLTEN Daten gelöscht werden, indem die zugehörigen Speichersegmente einer LUN mehrfach überschrieben werden.

SYS.1.8.A26 Absicherung eines SANs durch Hard-Zoning

Um SANs zu segmentieren, SOLLTE Hard-Zoning eingesetzt werden.

4 Weiterführende Informationen

4.1 Literatur

- [27040] ISO/IEC 27040:2015
  Information technology - Security techniques - Storage security, 01.2015
  https://www.iso.org/standard/44404.html

- [ISFSY14] Information Security Forum (ISF)
  The Standard of Good Practice - insbesonder Area SY1.4 Network Storage Systems, 06.2016

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Speicherlösungen" von Bedeutung.

G 0.08 Ausfall oder Störung der Stromversorgung

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.15 Abhören

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.08	G 0.11	G 0.15	G 0.16	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.24	G 0.25	G 0.26	G 0.27	G 0.28	G 0.29	G 0.30	G 0.31	G 0.32	G 0.40	G 0.44	G 0.45	G 0.46
SYS.1.8.A1	x			x							x										x		
SYS.1.8.A2			x			x	x			x					x							x	x
SYS.1.8.A3																	x		x				
SYS.1.8.A4			x						x	x							x						
SYS.1.8.A5													x	x									
SYS.1.8.A6					x									x	x	x							
SYS.1.8.A7					x									x	x	x							
SYS.1.8.A8					x		x																
SYS.1.8.A9		x			x																		
SYS.1.8.A10					x																		
SYS.1.8.A11												x	x	x									
SYS.1.8.A12						x												x					
SYS.1.8.A13													x	x									
SYS.1.8.A14			x						x	x													
SYS.1.8.A15			x						x	x													
SYS.1.8.A16						x																	
SYS.1.8.A17												x	x										
SYS.1.8.A18									x	x					x		x						
SYS.1.8.A19						x																	
SYS.1.8.A20													x									x	
SYS.1.8.A21			x						x	x													
SYS.1.8.A22												x								x			x
SYS.1.8.A23			x																				
SYS.1.8.A24																							x
SYS.1.8.A25						x																	
SYS.1.8.A26			x						x	x													

SYS.2: Desktop-Systeme

SYS.2.1 Allgemeiner Client

1 Beschreibung

1.1 Einleitung

Als "Allgemeiner Client" wird ein IT-System mit einem beliebigen Betriebssystem bezeichnet, das die Trennung von Benutzern zulässt. Es sollten mindestens eine Administrator- und eine Benutzer-Umgebung eingerichtet werden können. Typischerweise ist ein solches IT-System vernetzt und wird als Client in einem Client-Server-Netz genutzt. Das IT-System kann auf einer beliebigen Plattform betrieben werden. Dabei kann es sich beispielsweise um einen PC mit oder ohne Festplatte, um ein mobiles oder stationäres Gerät, aber auch um eine Linux-Workstation oder einen Apple Mac handeln. Das IT-System verfügt in der Regel über Laufwerke für auswechselbare Datenträger, weitere Schnittstellen für den Datenaustausch sowie andere Peripheriegeräte.

1.2 Zielsetzung

Zielsetzung dieses Bausteins ist der Schutz von Informationen, die auf Clients, unabhängig des auf ihnen betriebenen Betriebssystems, erstellt, gelesen, bearbeitet, gespeichert oder versendet werden.

1.3 Abgrenzung

In der Regel werden Client-Systeme unter einem Betriebssystem betrieben, das jeweils eigene Sicherheitsmaßnahmen erfordert. Für verbreitete Client-Betriebssysteme sind eigene Bausteine vorhanden, die diesen Baustein ergänzen. Der Baustein "Allgemeiner Client" bildet die Grundlage für die konkreten Bausteine, auf der diese aufbauen. Sofern für ein betrachtetes IT-System ein konkreter Baustein existiert, ist dieser zusätzlich zum Baustein Allgemeiner Client anzuwenden. Falls für eingesetzte Client-Systeme kein spezifischer Baustein existiert, müssen die Anforderungen dieses Bausteins geeignet angepasst werden. Sicherheitsempfehlungen für nicht frei konfigurierbare mobile Endgeräte, wie Smartphones oder Tablets, sind generell in der Schicht SYS.3 Mobile Devices zu finden.

Falls der Client weitere Schnittstellen zum Datenaustausch hat, wie z. B. USB, Bluetooth, LAN oder WLAN, müssen diese entsprechend den Sicherheitsvorgaben der Institution abgesichert werden, wie dies in den entsprechenden Bausteinen beschrieben ist. Hierzu sind Informationen in SYS.3.4 Mobile Datenträger, NET.2.3 Nahfunk und NET.2.2 WLAN-Nutzung zu finden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Allgemeiner Client von besonderer Bedeutung:

2.1 Schadprogramme

Schadprogramme werden mit dem Ziel entwickelt, unerwünschte und schädliche Funktionen auf Rechnern auszuführen. Sie werden meist heimlich aktiv, ohne dass die Benutzer dies wissen oder hierzu einwilligen. Je nach Ausprägung bieten sie einem Angreifer umfangreiche Kommunikations- und Steuerungsmöglichkeiten mit vielen Funktionen. Unter anderem könnten sie gezielt Passwörter ausforschen, IT-Systeme fernsteuern, Schutzsoftware deaktivieren oder Daten ausspionieren.

Clients sind besonders anfällig für Schadsoftware: Sie werden direkt von den Benutzern bedient und sind somit oft das Einfallstor für Schadsoftware. Besuchen die Benutzer infizierte Webseiten, öffnen E-Mails mit kompromittierendem Inhalt von privaten E-Mail-Konten oder kopieren Schadsoftware über lokale Datenträger auf den Client, verbreitet sich so die Schadsoftware über die Clients in das Netz der Institution. Zentrale Schutzmechanismen, wie z.B. ein Virenschutz auf dem Datei- oder E-Mail-Server, können so oft umgangen werden.

2.2 Unstrukturierte lokale Datenhaltung

Trotz regelmäßiger gegensätzlicher Empfehlung speichern viele Anwender auch wichtige Daten ausschließlich lokal ab. Beispielsweise werden Daten häufig statt auf einem zentralen Dateiserver in lokalen Benutzerverzeichnissen abgelegt. Auch E-Mails werden häufig nur lokal archiviert. Dieses Vorgehen kann zu folgenden Problemen führen:

- Datenverlust bei Hardwaredefekten und
- kein Zugriff auf relevante Daten im Vertretungsfall.

Aber auch wenn grundsätzliche Vorgaben zur zentralen Speicherung eingehalten werden, werden häufig zusätzlich lokale Kopien der zentral gespeicherten Daten angelegt. Dies kann zu folgenden Problemen führen:

- Verschwendung von lokalen Speicherplatz,
- vorschnelle oder nicht erfolgte Löschung von Daten und
- inkonsistente Versionsstände

2.3 Datenverlust

Auf Clients werden typischerweise verteilt über die gesamte Institution viele Daten gespeichert, deren Verlust erhebliche Auswirkungen auf Geschäftsprozesse und damit auf die gesamte Institution haben kann. Werden geschäftsrelevante Daten zerstört oder verfälscht, können dadurch Geschäftsprozesse und Fachaufgaben verzögert oder sogar deren Ausführung verhindert werden. Insgesamt kann der Verlust gespeicherter Daten, neben einem Arbeitsausfall und den Kosten für eine Wiederbeschaffung, auch zu langfristigen Konsequenzen, wie beispielsweise Vertrauenseinbußen bei Kunden und Partnern, sowie einem negativen Eindruck in der Öffentlichkeit führen. Von den durch Datenverluste verursachten direkten und indirekten Schäden können Institutionen im Extremfall in ihrer Existenz bedroht sein.

2.4 Hardware-Defekte durch Fehlbedienung

Anders als bei zentralen IT-Systemen wie Servern arbeiten Client-Benutzer direkt am Endgerät. Durch den physischen Zugriff können sie den Client gewollt oder ungewollt beschädigen. Beispielsweise können sie gegen auf dem Boden stehende IT-Systeme treten, Monitore umwerfen, über Kabel stolpern oder Getränke in Tastaturen gießen. Oft ist es nicht ausreichend, Hardware erst bei einem Defekt zu ersetzen. Bei einem Festplattendefekt zum Beispiel können gespeicherte Daten meist nicht wiederhergestellt werden. Außerdem kann das IT-System bis zum Abschluss der Reparatur nicht eingesetzt werden. Bei einem Ausfall eines mobilen Gerätes unterwegs kann die Arbeit erst nach der Rückkehr fortgesetzt werden.

2.5 Software-Schwachstellen oder -Fehler

Für jede Art von Software gilt: Je komplexer sie ist, desto häufiger können Programmier- oder Designfehler auftreten. Unter Software-Schwachstellen werden Programmfehler verstanden, die den Anwendern oft (noch) nicht bekannt sind und die ein Sicherheitsrisiko für das -System darstellen. Beinahe täglich werden neue Sicherheitslücken in lange genutzter, aber auch in neuer Software gefunden.

Auf Clients werden in der Regel eine Vielzahl verschiedener Applikationen installiert, hierdurch erhöht sich die Menge an Schwachstellen, von denen das System betroffen sein kann. Hinzu kommt, dass eine größere Anzahl von (mobilen) Clients viel schwerer mit reparierenden Patches aktualisiert werden kann, als beispielsweise wenige Server.

Werden Softwarefehler nicht erkannt oder nicht umgehend behoben, kann das zu schwerwiegenden Folgen führen. Eine Software-Schwachstelle in einer viel genutzten Standardsoftware kann schnell dazu führen, dass weltweit Sicherheitsprobleme für alle Arten von Institutionen entstehen.

2.6 Unberechtigte IT-Nutzung

Die Identifikation und Authentisierung von Benutzern soll verhindern, dass ein Client unberechtigt verwendet wird. Aber auch IT-Systeme, bei denen sich Benutzer über Benutzer-IDs und Passwörter identifizieren und authentisieren müssen, können unberechtigt genutzt werden, wenn es einem Angreifer gelingt, die Zugangsdaten auszuspähen oder zu erraten. Wird keine Bildschirmsperre aktiviert, kann der Client auch bei kurzzeitiger Abwesenheit unberechtigt genutzt werden.

2.7 Bereitstellung nicht benötigter Betriebssystemkomponenten und Applikationen

Bei der Installation eines Betriebssystems besteht in der Regel die Möglichkeit, optionale Software zu installieren. Auch im laufenden Betrieb wird regelmäßig Software installiert und getestet. Mit jeder weiteren Anwendung steigen nicht nur Rechen- und Speicherlast eines Clients stetig, sondern auch die Wahrscheinlichkeit, Schwachstellen darin zu finden. Nicht benötigte Software unterliegt außerdem häufig keinem regelmäßigen Patchmanagement, so dass auch bekannte Sicherheitslücken nicht zeitnah geschlossen werden. Dadurch können Angreifer schon lange bekannte Schwachstellen nutzen.

2.8 Abhören von Räumen mittels Mikrofon und Kamera

Viele Clients verfügen über ein Mikrofon und eine Kamera. Diese können von Jedem verwendet werden, der über entsprechende Zugriffsrechte verfügt, bei vernetzten Systemen auch von Externen. Werden diese Rechte nicht sorgfältig vergeben, können Unbefugte Mikrofon oder Kamera dazu missbrauchen, um über das Internet Räume abzuhören oder unbemerkt Besprechungen aufzuzeichnen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz von Clients aufgeführt. Grundsätzlich ist der *IT-Betrieb* für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Benutzer, Haustechnik

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.2.1.A1 Benutzerauthentisierung

Um den Client zu nutzen, MÜSSEN sich die Benutzer gegenüber dem IT-System authentisieren. Sollen die Benutzer hierfür Passwörter verwenden, MÜSSEN sichere Passwörter benutzt werden. Die Passwörter MÜSSEN der Passwort-Richtlinie der Institution entsprechen, siehe ORP.4 Identitäts- und Berechtigungsmanagement.

SYS.2.1.A2 Rollentrennung

Der Client MUSS so eingerichtet werden, dass normale Tätigkeiten nicht mit Administrationsrechten erfolgen. Nur Administratoren DÜRFEN Administrationsrechte erhalten. Es DÜRFEN nur Administratoren die Systemkonfiguration ändern, Anwendungen installieren bzw. entfernen oder Systemdateien modifizieren bzw. löschen können. Benutzer DÜRFEN ausschließlich lesenden Zugriff auf Systemdateien haben.

Ablauf, Rahmenbedingungen und Anforderungen an administrative Aufgaben sowie die Aufgabentrennungen zwischen den verschiedenen Rollen der Benutzer des IT-Systems SOLLTEN in einem Benutzer- und Administrationskonzept festgeschrieben werden.

SYS.2.1.A3 Aktivieren von Autoupdate-Mechanismen

Automatische Update-Mechanismen (Autoupdate) MÜSSEN aktiviert werden, sofern nicht andere Mechanismen, wie regelmäßige manuelle Wartung oder ein zentrales Softwareverteilungssystem für Updates eingesetzt werden. Wenn für Autoupdate-Mechanismen ein Zeitintervall vorgegeben werden kann, SOLLTE mindestens täglich automatisch nach Updates gesucht und diese installiert werden.

SYS.2.1.A4 Regelmäßige Datensicherung

Zur Vermeidung von Datenverlusten MÜSSEN regelmäßige Datensicherungen erstellt werden. In den meisten Rechnersystemen können diese weitgehend automatisiert erfolgen. Es MÜSSEN Regelungen getroffen werden, welche lokal abgespeicherten Daten von wem wann gesichert werden. Es MÜSSEN mindestens die Daten regelmäßig gesichert werden, die nicht aus anderen Informationen abgeleitet werden können. Auch Clients MÜSSEN in das Datensicherungskonzept der Institution einbezogen werden. Bei vertraulichen und ausgelagerten Backups SOLLTEN die gesicherten Daten verschlüsselt gespeichert werden. Für eingesetzte Software SOLLTE separat entschieden werden, ob sie von der regelmäßigen Datensicherung erfasst werden muss. Es MUSS regelmäßig getestet werden, ob die Datensicherung auch wie gewünscht funktioniert, vor allem, ob gesicherte Daten problemlos zurückgespielt werden können. Die Benutzer SOLLTEN über die Regelungen, von wem und wie Datensicherungen erstellt werden, informiert werden.

SYS.2.1.A5 Bildschirmsperre [Benutzer]

Eine Bildschirmsperre MUSS verwendet werden, damit keine Unbefugten auf den aktivierten Clients zugreifen können. Sie SOLLTE sich sowohl manuell vom Benutzer aktivieren lassen, als auch nach einem vorgegebenen Inaktivitäts-Zeitraum automatisch gestartet werden. Es MUSS sichergestellt sein, dass die Bildschirmsperre erst nach einer erfolgreichen Benutzerauthentikation deaktiviert werden kann.

SYS.2.1.A6 Einsatz von Viren-Schutzprogrammen

In Abhängigkeit des installierten Betriebssystems und anderer vorhandener Schutzmechanismen des Clients MUSS geprüft werden, ob Viren-Schutzprogramme eingesetzt werden sollen. Konkrete Aussagen, ob Viren-Schutz notwendig ist, sind in der Regel in den Betriebssystem-Bausteinen des IT-Grundschutzes zu finden. Die entsprechenden Signaturen eines Viren-Schutzprogrammes MÜSSEN regelmäßig aktualisiert werden. Neben Echtzeit- und On-Demand-Scans MUSS eine eingesetzte Lösung die Möglichkeit bieten, auch komprimierte und verschlüsselte Daten nach Schadprogrammen zu durchsuchen.

Viren-Schutzprogramme auf den Clients MÜSSEN so konfiguriert sein, dass die Benutzer weder sicherheitsrelevante Änderungen an den Einstellungen vornehmen können noch sie deaktivieren können.

SYS.2.1.A7 Protokollierung

Es MUSS entschieden werden, welche Informationen auf Clients mindestens protokolliert werden sollen, wie lange die Protokolldaten aufbewahrt werden und wer unter welchen Voraussetzungen die Protokolldaten einsehen darf. Generell MÜSSEN alle sicherheitsrelevanten Systemereignisse protokolliert werden.

SYS.2.1.A8 Absicherung des Boot-Vorgangs

Der Startvorgang des IT-Systems ("Booten") MUSS gegen Manipulation abgesichert werden. Es MUSS festgelegt werden, von welchen Medien gebootet werden darf. Es SOLLTE entschieden werden, ob und wie der Bootvorgang kryptographisch geschützt werden soll. Es MUSS sichergestellt werden, dass nur Administratoren die Clients von einem anderen als dem voreingestellten Laufwerken oder externen Speichermedien booten können. Nur Administratoren DÜRFEN von eingebauten optischen oder externen Speichermedien booten können. Die Konfigurationseinstellungen des Boot-Vorgangs Firmware MÜSSEN nur durch Benutzer mit administrativen Rechten verändert werden können.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Allgemeiner Client. Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.2.1.A9 Festlegung einer Sicherheitsrichtlinie für Clients

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die Anforderungen an allgemeine Clients konkretisiert werden. Die Richtlinie SOLLTE allen Benutzern sowie allen Personen, die an der Beschaffung und dem Betrieb der Clients beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft und die Ergebnisse sinnvoll dokumentiert werden.

SYS.2.1.A10 Planung des Einsatzes von Clients

Zum sicheren Betrieb von Clients SOLLTE im Vorfeld geplant werden, wo und wie die Clients eingesetzt werden sollen. Die Planung SOLLTE dabei nicht nur Aspekte betreffen, die klassischerweise mit dem Begriff Sicherheit verknüpft werden, sondern auch normale betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen. Neben Client-Typ-spezifischen Anforderungsprofilen SOLLTEN Vorgaben zur Authentisierung und Benutzerverwaltung definiert werden. Alle Entscheidungen, die in der Planungsphase getroffen wurden, SOLLTEN so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

SYS.2.1.A11 Beschaffung von Clients

Bevor Clients beschafft werden, SOLLTE eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Der jeweilige Hersteller SOLLTE für den gesamten geplanten Nutzungszeitraum Patches für Schwachstellen zeitnah zur Verfügung stellen können. Die zu beschaffenden Systeme SOLLTEN über eine Firmware-Konfigurationsoberfläche für UEFI SecureBoot und für das TPM (sofern vorhanden) verfügen, die eine Kontrolle durch den Eigentümer (Institution) gewährt und so den selbstverwalteten Betrieb von SecureBoot und des TPM ermöglicht.

SYS.2.1.A12 Kompatibilitätsprüfung von Software

Vor einer beabsichtigten Beschaffung von Software SOLLTE deren Kompatibilität zum eingesetzten Betriebssystem in der vorliegenden Konfiguration geprüft und die Kompatibilitätsprüfung in das Freigabeverfahren der Software aufgenommen werden. Ist vom Hersteller der Software oder aus anderen Fachkreisen keine verbindliche Information zur Kompatibilität vorhanden, so SOLLTE die Kompatibilität in

einer Testumgebung geprüft werden. Vor einer beabsichtigten Hardwareänderung oder bei einer Betriebssystemmigration SOLLTE auch die Treibersoftware für alle betreffenden Komponenten auf Kompatibilität zum Betriebssystem gewährleistet werden.

SYS.2.1.A13 Zugriff auf Ausführungsumgebungen mit unbeobachtbarer Codeausführung

Der Zugriff auf Ausführungsumgebungen mit unbeobachtbarer Codeausführung (z.B. durch das Betriebssystem speziell abgesicherte Speicherbereiche, Firmwarebereiche, etc.) SOLLTE nur durch Benutzer mit administrativen Berechtigungen möglich sein.

SYS.2.1.A14 Updates und Patches für Firmware, Betriebssystem und Anwendungen

Administratoren SOLLTEN sich regelmäßig über bekannt gewordene Schwachstellen informieren. Die identifizierten Schwachstellen SOLLTEN so schnell wie möglich behoben werden. Generell SOLLTE darauf achtet werden, dass Patches und Updates nur aus vertrauenswürdigen Quellen bezogen werden. Wenn notwendig, SOLLTEN die betreffenden Anwendungen beziehungsweise das Betriebssystem nach dem Update neu gestartet werden.

Solange keine entsprechenden Patches zur Verfügung stehen, SOLLTEN abhängig von der Schwere der Schwachstellen andere geeignete Maßnahmen zum Schutz des IT-Systems getroffen werden.

SYS.2.1.A15 Sichere Installation und Konfiguration von Clients

Es SOLLTE festgelegt werden, welche Komponenten des Betriebssystems, Fachanwendungen und weitere Tools installiert werden sollen. Die Installation und Konfiguration der IT-Systeme SOLLTE nur von autorisierten Personen (Administratoren oder vertraglich gebundene Dienstleister) nach einem definierten Prozess durchgeführt werden. Alle Installations- und Konfigurationsschritte SOLLTEN so dokumentiert werden, dass die Installation und Konfiguration durch einen sachkundigen Dritten anhand der Dokumentation nachvollzogen und wiederholt werden kann (siehe auch SYS.2.1.A36 Betriebsdokumentation).

Die Grundeinstellungen von Clients SOLLTEN überprüft und nötigenfalls entsprechend den Vorgaben der Sicherheitsrichtlinie angepasst werden. Erst nachdem die Installation und die Konfiguration abgeschlossen ist, SOLLTE der Client mit dem Internet verbunden werden.

SYS.2.1.A16 Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen

Nach der Installation SOLLTE überprüft werden, welche Komponenten der Firmware, des Betriebssystems, Anwendungen und weitere Tools auf den Clients installiert und aktiviert sind. Nicht benötigte Module, Programme, Dienste, Benutzerkennungen und Schnittstellen SOLLTEN deaktiviert oder ganz deinstalliert werden. Außerdem SOLLTEN nicht benötigte Laufzeitumgebungen, Interpretersprachen und Compiler deinstalliert werden. Entsprechende, nicht benötigte, jedoch fest mit dem IT-System verbundene Komponenten SOLLTEN deaktiviert werden. Auch in der Firmware vorhandene, nicht benötigte Komponenten (z.B. Diebstahlschutz, Fernwartung) SOLLTEN abgeschaltet werden. Es SOLLTE verhindert werden, dass diese Komponenten wieder reaktiviert werden können. Die getroffenen Entscheidungen SOLLTEN so dokumentiert werden, dass nachvollzogen werden kann, welche Konfiguration und Softwareausstattung für die IT-Systeme gewählt wurden.

SYS.2.1.A17 Einsatzfreigabe

Bevor der Client im produktiven Betrieb eingesetzt und bevor es an ein produktives Netz angeschlossen wird, SOLLTE eine Einsatzfreigabe erfolgen. Diese SOLLTE dokumentiert werden. Für die Einsatzfreigabe SOLLTE die Installations- und Konfigurationsdokumentation und die Funktionsfähigkeit der IT-Systeme in einem Test geprüft werden. Sie SOLLTE durch eine in der Institution dafür autorisierte Stelle erfolgen.

SYS.2.1.A18 Nutzung von TLS [Benutzer]

Kommunikationsverbindungen SOLLTEN durch Verschlüsselung geschützt werden, soweit möglich. Benutzer SOLLTEN darauf achten, dass bei Web-Seiten SSL/TLS verwendet wird.

Der IT-Betrieb SOLLTE dafür sorgen, dass die eingesetzten Client-Produkte eine sichere Version von TLS unterstützen. Die Clients SOLLTEN kryptographische Algorithmen und Schlüssellängen verwenden, die dem Stand der Technik und den Sicherheitsanforderungen der Institution entsprechen.

Neue Zertifikate SOLLTEN erst nach Überprüfung des "Fingerprints" aktiviert werden. Die Validierung von Zertifikaten SOLLTE in Anwendungsprogrammen wie Browsern und E-Mail-Clients aktiviert werden. Session Renegotiation und TLS-Kompression SOLLTEN deaktiviert werden.

SYS.2.1.A19 Restriktive Rechtevergabe

Der verfügbare Funktionsumfang des IT-Systems SOLLTE für einzelne Benutzer oder Benutzergruppen eingeschränkt werden, so dass sie genau die Rechte besitzen und auf die Funktionen zugreifen können, die sie für ihre Aufgabenwahrnehmung benötigen. Zugriffsberechtigungen SOLLTEN hierfür möglichst restriktiv vergeben werden. Es SOLLTE regelmäßig überprüft werden, ob die Berechtigungen, insbesondere für Systemverzeichnisse und -dateien, den Vorgaben der Sicherheitsrichtlinie entsprechen. Auf Systemdateien SOLLTEN möglichst nur die Systemadministratoren Zugriff haben. Der Kreis der zugriffsberechtigten Administratoren SOLLTE möglichst klein gehalten werden. Auch System-Verzeichnisse SOLLTEN nur die notwendigen Privilegien für die Benutzer zur Verfügung stellen.

SYS.2.1.A20 Schutz der Administrationsschnittstellen

Abhängig davon, ob Clients lokal, über das Netz oder über zentrale netzbasierte Tools administriert werden, SOLLTEN geeignete Sicherheitsvorkehrungen getroffen werden. Die zur Administration verwendeten Methoden SOLLTEN in der Sicherheitsrichtlinie festgelegt und die Administration SOLLTE entsprechend der Sicherheitsrichtlinie durchgeführt werden. Die Administration über das Netz SOLLTE über sichere Protokolle erfolgen.

SYS.2.1.A21 Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras

Der Zugriff auf Mikrofon und Kamera eines Clients SOLLTE nur durch den Benutzer selber möglich sein, solange er lokal am IT-System arbeitet. Wenn ein vorhandenes Mikrofon oder eine Kamera nicht genutzt und deren Missbrauch verhindert werden soll, SOLLTEN diese, wenn möglich, ausgeschaltet, abgedeckt (nur Kamera), deaktiviert oder physikalisch vom Gerät getrennt werden. Es SOLLTE geregelt werden, wie Kameras und Mikrofone in Clients genutzt und wie die Rechte vergeben werden.

SYS.2.1.A22 Abmelden nach Aufgabenerfüllung [Benutzer]

Es SOLLTEN alle Benutzer verpflichtet werden, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT-Anwendung abzumelden, vor allem bei Nutzung eines Systems durch mehrere Benutzer. Ist für einen Benutzer absehbar, dass nur eine kurze Unterbrechung der Arbeit erforderlich ist, SOLLTE er die Bildschirmsperre aktivieren statt sich abzumelden. Wenn technisch möglich, SOLLTE die Bildschirmsperre nach längerer Inaktivität automatisch aktiviert bzw. der Benutzer automatisch abgemeldet werden.

SYS.2.1.A23 Nutzung von Client-Server-Diensten

Wenn möglich, SOLLTEN zum Informationsaustausch dedizierte Serverdienste genutzt und direkte Verbindungen zwischen Clients vermieden werden. Falls dies nicht möglich ist, SOLLTE festgelegt werden, welche Client-zu-Client-Dienste (früher oft als "Peer-to-Peer" bezeichnet) genutzt und welche Informationen darüber ausgetauscht werden dürfen. Wenn erforderlich, SOLLTEN die Benutzer für die Nutzung solcher Dienste geschult werden. Direkte Verbindungen zwischen Clients SOLLTEN sich nur auf das LAN beschränken. Auto-Discovery-Protokolle SOLLTEN auf das notwendige Maß beschränkt werden.

SYS.2.1.A24 Umgang mit Wechseldatenträgern im laufenden System

Es SOLLTE verhindert werden, dass auf Clients von Laufwerken oder über Schnittstellen unkontrolliert Software installiert oder unberechtigt Daten kopiert werden können. Es SOLLTE generell verhindert werden, dass von den Clients auf Daten aus nicht vertrauenswürdigen Quellen zugegriffen wird. Vertiefende Informationen zu Wechseldatenträgern sind im Baustein SYS.3.4 Mobile Datenträger zu finden.

SYS.2.1.A25 Richtlinie zur sicheren IT-Nutzung [Benutzer]

Es SOLLTE eine Richtlinie erstellt werden, in der für alle Mitarbeiter transparent beschrieben wird, welche Rahmenbedingungen bei der IT-Nutzung eingehalten werden müssen und welche Sicherheitsmaßnahmen zu ergreifen sind. Die Richtlinie SOLLTE folgende Punkte abdecken:

- Sicherheitsziele der Institution
- Wichtige Begriffe
- Aufgaben und Rollen mit Bezug zur Informationssicherheit
- Ansprechpartner zu Fragen der Informationssicherheit
- Von den Mitarbeitern umzusetzende und einzuhaltende Sicherheitsmaßnahmen

Die Richtlinie SOLLTE allen Benutzern zur Kenntnis gegeben werden. Jeder neue Benutzer SOLLTE die Kenntnisnahme der Richtlinie bestätigen, bevor er die Informationstechnik nutzen darf. Nach größeren Änderungen an der Richtlinie oder nach spätestens zwei Jahren SOLLTE eine erneute Bestätigung erforderlich.

SYS.2.1.A26 Schutz von Anwendungen

Um die Ausnutzung von Schwachstellen in Anwendungen zu erschweren, SOLLTE ASLR und DEP/NX im Kernel aktiviert und von den Anwendungen genutzt werden. Sicherheitsfunktionen des Kernels und der Standardbibliotheken wie z. B. Heap- und Stackschutz SOLLTEN NICHT deaktiviert werden.

SYS.2.1.A27 Geregelte Außerbetriebnahme eines Clients

Bei der Außerbetriebnahme eines Clients SOLLTE sichergestellt werden, dass keine wichtigen Daten, die eventuell auf den verbauten Datenträgern gespeichert sind, verloren gehen, und dass keine sensitiven Daten zurück bleiben. Es SOLLTE einen Überblick darüber geben, welche Daten wo auf den IT-Systemen gespeichert sind. Es SOLLTE eine Checkliste erstellt werden, die bei der Außerbetriebnahme eines IT-Systems abgearbeitet werden kann. Diese Checkliste SOLLTE mindestens Aspekte zur Datensicherung weiterhin benötigter Daten und dem anschließenden sicheren Löschen aller Daten umfassen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.2.1.A28 Verschlüsselung der Clients (C)

Wenn vertrauliche Informationen auf den Clients gespeichert werden, SOLLTEN die schutzbedürftigen Dateien, ausgewählte Dateisystembereiche oder besser die gesamte Festplatte verschlüsselt werden. Hierfür SOLLTE ein eigenes Konzept erstellt und die Details der Konfiguration besonders sorgfältig dokumentiert werden, da im Fall von Problemen die Daten auf den verschlüsselten Dateisystemen sonst vollständig verloren sein können. In diesem Zusammenhang SOLLTEN folgende Inhalte geregelt werden: Authentifizierung (z. B. Passwort, PIN, Token), Ablage der Wiederherstellungsinformationen, zu verschlüsselnde Laufwerke, Schreibrechte auf unverschlüsselte Datenträger und wie sichergestellt wird, dass die Wiederherstellungsinformationen nur berechtigten Personen zugänglich sind. Auch verschlüsselte Dateien, Partitionen oder Datenträger SOLLTEN regelmäßig gesichert werden. Das verwendete Schlüsselmaterial DARF NICHT im Klartext auf den Clients gespeichert sein.

Benutzer SOLLTEN darüber aufgeklärt werden, wie sie sich bei Verlust eines Authentisierungsmittels zu verhalten haben.

SYS.2.1.A29 Systemüberwachung (A)

Die Clients SOLLTEN in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept eingebunden werden, das den Systemzustand und die Funktionsfähigkeit der Clients laufend überwacht und Fehlerzustände sowie die Überschreitung definierter Grenzwerte an das Betriebspersonal meldet.

SYS.2.1.A30 Einrichten einer Referenzinstallation für Clients (CIA)

Für Clients SOLLTE eine Referenzinstallation erstellt werden, in der die Grundkonfiguration und alle Konfigurationsänderungen, Updates und Patches vor dem Einspielen auf den Clients bei den Anwendern vorab getestet werden können. Darüber hinaus SOLLTE eine solche Referenzinstallation auch dazu genutzt werden, die Clients vereinfacht zu installieren und wieder aufzusetzen, indem eine entsprechend vorkonfigurierte Installation auf geeignete Art und Weise auf die zu installierenden Clients überspielt wird ("klonen"). Für verschiedene typische und häufiger wiederkehrende Testfälle SOLLTEN Checklisten erstellt werden, die beim Testen abgearbeitet werden können. Zusätzlich SOLLTEN alle Tests so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

SYS.2.1.A31 Einrichtung lokaler Paketfilter (CIA)

Auf jedem Rechner SOLLTEN, zusätzlich zu den eingesetzten zentralen Sicherheitsgateways, lokale Paketfilter eingesetzt werden. Als Strategie zur Paketfilter-Implementierung SOLLTE eine Whitelist-Strategie gewählt werden.

SYS.2.1.A32 Einsatz zusätzlicher Maßnahmen zum Schutz vor Exploits (CIA)

Auf dem IT-System SOLLTEN zusätzliche Maßnahmen zum expliziten Schutz vor Exploits (Schutz: Erschweren der erfolgreichen Ausführung) getroffen werden. Wenn notwendige Schutzmaßnahmen nicht mit Bordmitteln erfüllt werden können, SOLLTEN zusätzliche geeignete Sicherheitsprodukte eingesetzt werden. Sollte es nicht möglich sein, entsprechende Maßnahmen mit Bordmitteln oder einem geeigneten Sicherheitsprodukt umzusetzen, SOLLTEN andere geeignete (in der Regel organisatorische) Sicherheitsmaßnahmen ergriffen werden.

SYS.2.1.A33 Application Whitelisting (CIA)

Es SOLLTE über Application Whitelisting sichergestellt werden, dass nur erlaubte Programme und Skripte ausgeführt werden. Die Regeln SOLLTEN so eng wie möglich gefasst werden. Falls Pfade und Hashes nicht explizit angegeben werden können, SOLLTEN alternativ auch Zertifikats-basierte oder Pfad-Regeln genutzt werden.

SYS.2.1.A34 Einsatz von Anwendungsisolation (CIA)

Anwendungen, mit denen externe Daten bearbeitet werden, SOLLTEN ausschließlich in einer vom Betriebssystem isolierten Ablaufumgebung betrieben werden.

SYS.2.1.A35 Aktive Verwaltung der Wurzelzertifikate (CI)

Im Zuge der Beschaffung und Installation des Clients SOLLTE dokumentiert werden, welche Wurzelzertifikate für den Betrieb des Clients notwendig sind. Auf dem Client SOLLTEN lediglich die für den Betrieb notwendigen und vorab dokumentierten Wurzelzertifikate enthalten sein. Es SOLLTE regelmäßig überprüft werden, ob die vorhandenen Wurzelzertifikate noch den Vorgaben der Institution entsprechen. Es SOLLTEN alle auf dem IT-System vorhandenen Zertifikatsspeicher in die Prüfung einbezogen werden (z.B. UEFI-Zertifikatsspeicher, Zertifikatsspeicher von Web-Browsern, etc.).

SYS.2.1.A36 Selbstverwalteter Einsatz von SecureBoot und TPM

Auf UEFI-kompatiblen Systemen SOLLTEN Bootloader, Kernel sowie alle benötigten Firmware-Komponenten durch selbstkontrolliertes Schlüsselmaterial signiert und nicht benötigtes Schlüsselmaterial entfernt werden. Sofern das TPM nicht benötigt wird, SOLLTE es deaktiviert werden.

SYS.2.1.A37 Schutz vor unbefugten Anmeldungen (CIA)

Um einen Zugang zum System durch kompromittierte Anmeldeinformationen zu verhindern, SOLLTE eine Mehrfaktorauthentisierung verwendet werden.

SYS.2.1.A38 Einbindung in die Notfallplanung (A)

Die Clients SOLLTEN im Notfallmanagementprozess berücksichtigt werden. Die Clients sind anhand der Geschäftsprozesse, für die sie benötigt werden, für den Wiederanlauf zu priorisieren. Es SOLLTEN geeignete Notfallmaßnahmen vorgesehen werden, indem mindestens Wiederanlaufpläne erstellt, Bootmedien zur Systemwiederherstellung generiert sowie Passwörter und kryptographische Schlüssel sicher hinterlegt werden.

SYS.2.1.A39 Unterbrechungsfreie und stabile Stromversorgung [Haustechnik] (A)

Bei erhöhten Anforderungen an die Verfügbarkeit von stationären Clients SOLLTEN diese an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen werden. Die USV SOLLTE hinsichtlich Leistung und Stützzeit ausreichend dimensioniert sein. Wenn Änderungen an den Verbrauchern durchgeführt wurden, SOLLTE erneut geprüft werden, ob die Stützzeit ausreichend ist. Sowohl für die USV-Geräte als auch die Clients SOLLTE ein Überspannungsschutz vorhanden sein.

Die tatsächliche Kapazität der Batterie und damit die Stützzeit der USV SOLLTE regelmäßig getestet werden. Die USV SOLLTE regelmäßig gewartet werden.

SYS.2.1.A40 Betriebsdokumentation

Die Durchführung betrieblicher Aufgaben an Clients SOLLTE nachvollziehbar dokumentiert werden (wer?, wann?, was?), vor allem wenn dies Gruppen von Clients betrifft. Aus der Dokumentation SOLLTEN insbesondere Konfigurationsänderungen nachvollziehbar sein, auch sicherheitsrelevanten Aufgaben (wer ist z. B. befugt, neue Festplatten einzubauen) SOLLTEN dokumentiert werden. Alles, was automatisch dokumentiert werden kann, SOLLTE auch automatisch dokumentiert werden. Die Dokumentation SOLLTE gegen unbefugten Zugriff und Verlust geschützt werden.

SYS.2.1.A41 Verhinderung der Überlastung der lokalen Festplatte

Es SOLLTE überlegt werden, Quotas einzurichten. Alternativ SOLLTEN Mechanismen des verwendeten Datei- oder Betriebssystemsystems genutzt werden, die die Benutzer bei einem bestimmten Füllstand der Festplatte warnen oder nur noch dem Systemadministrator Schreibrechte einräumen.

4 Weiterführende Informationen

4.1 Literatur

- [ISiClient] Absicherung eines PC-Clients (ISi-Client),
  (zuletzt abgerufen am 27.09.2017)
  https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Isi-Reihe/Isi-Client/client_node.html

- [NISTSP800123] NIST Special Publication 800-123
  Guide to General Server Security, NIST, 07.2008
  https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Allgemeiner Client" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.36 Identitätsdiebstahl

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.43 Einspielen von Nachrichten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.14	G 0.15	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.28	G 0.30	G 0.31	G 0.36	G 0.39	G 0.40	G 0.43	G 0.45	G 0.46
SYS.2.1.A1	X		X			X	X						X					
SYS.2.1.A2					X	X					X	X	X					X
SYS.2.1.A3				X				X	X	X								
SYS.2.1.A4																	X	X
SYS.2.1.A5			X			X	X				X		X					
SYS.2.1.A6					X	X			X					X	X			
SYS.2.1.A7							X		X									
SYS.2.1.A8					X	X					X	X						X
SYS.2.1.A9			X									X					X	
SYS.2.1.A10						X	X					X					X	
SYS.2.1.A11								X				X						
SYS.2.1.A12								X	X						X			
SYS.2.1.A13					X						X							
SYS.2.1.A14					X				X	X								
SYS.2.1.A15					X	X	X				X				X			X
SYS.2.1.A16			X				X			X	X				X			X
SYS.2.1.A17									X	X								
SYS.2.1.A18		X	X													X		X
SYS.2.1.A19			X			X					X						X	X
SYS.2.1.A20		X			X						X							
SYS.2.1.A21	X	X	X															
SYS.2.1.A22	X		X			X					X		X					
SYS.2.1.A23					X	X		X				X			X		X	
SYS.2.1.A24	X											X		X				
SYS.2.1.A25												X						
SYS.2.1.A26					X		X			X								
SYS.2.1.A27	X		X															
SYS.2.1.A28	X	X	X															X
SYS.2.1.A29					X			X	X						X			
SYS.2.1.A30					X				X			X						
SYS.2.1.A31							X				X				X			
SYS.2.1.A32			X		X	X	X			X	X			X	X		X	X
SYS.2.1.A33					X							X		X				X
SYS.2.1.A34					X							X		X				X
SYS.2.1.A35	X	X	X												X			
SYS.2.1.A36	X		X	X	X		X				X							
SYS.2.1.A37	X		X				X				X		X	X			X	X
SYS.2.1.A38								X	X									
SYS.2.1.A39								X	X			X						
SYS.2.1.A40					X			X										
SYS.2.1.A41								X				X					X	

SYS.2.2: Windows-Clients

SYS.2.2.2 Clients unter Windows 8.1

1 Beschreibung

1.1 Einleitung

Mit Windows 8 hat Microsoft sein Client-Betriebssystem Windows sowie die damit eingeführten Funktionen und Komponenten weiterentwickelt. Neu an Windows 8 ist die auf den Einsatz portabler Geräte mit Touchscreen ausgerichtete Bedienungsführung. Diese bringt ein neues Bedienkonzept für Anwendungen mit sich. Neben den klassischen Desktop-Anwendungen hat Microsoft dazu eine Klasse mobiler Anwendungen zur Nutzung unter Windows 8 vorgesehen, die sogenannten "Apps". Diese sind konsequent auf die Steuerung durch Berührung ausgelegt. Zusätzlich können sie als "Kachel" auf dem Bildschirm Anzeigefunktionen wahrnehmen. Einige Anwendungen, allen voran der mit Windows 8 ausgelieferte Internet Explorer, stehen entsprechend in zwei Varianten für Windows 8 zur Verfügung. Seit der Markteinführung von Windows 8 hat Microsoft einige Verbesserungen vorgenommen und in das Betriebssystem integriert, das damit die Versionsnummer 8.1 erhält.

1.2 Zielsetzung

Zielsetzung dieses Bausteins ist der Schutz von Informationen, die durch und auf Windows 8.1-Clients verarbeiten werden.

1.3 Abgrenzung

Dieser Baustein ist auf alle Zielobjekte anzuwenden, auf denen das Betriebssystem Windows 8.1 betrieben werden. Soweit die beschriebenen Sicherheitsanforderungen und Gefährdungen ausschließlich für Windows 8 gelten, ist dies explizit in den Texten ausgewiesen. Die Anforderungen aus dem Baustein SYS.2.1 Allgemeiner Client sind in jedem Fall ebenfalls zu erfüllen. Der vorliegende Baustein präzisiert und ergänzt Anforderungen, die für Windows 8.1 spezifisch sind. Für Anwendungsprogramme, die auf den Windows-Clients verwendet werden, sind die Anforderungen der entsprechenden Bausteine zu erfüllen, beispielsweise APP.1.1 Office-Produkte oder APP.1.6 Browser. Beim Einsatz in einer Windows-Domäne sind die Anforderungen der entsprechenden Bausteine wie APP.2.2 Active Directory zu erfüllen.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Windows 8.1 von besonderer Bedeutung:

2.1 Auf Windows ausgerichtete Schadprogramme

Schadprogramme bieten einem Angreifer umfangreiche Kommunikations- als auch Steuerungsmöglichkeiten und besitzen eine Vielzahl von Funktionen. Unter anderem können Schadprogramme gezielt Passwörter ausforschen, Systeme fernsteuern, Schutzsoftware deaktivieren und Daten ausspionieren. Ein Wechseldatenträger könnte so manipuliert werden, dass Schadsoftware ausgeführt und installiert wird, wenn der Wechseldatenträger eingelegt oder angeschlossen wurde. Als Schaden ist hier insbesondere der Verlust oder die Verfälschung von Informationen oder Anwendungen von größter Tragweite. Aber auch ein Imageverlust und finanzieller Schaden, der folglich durch Schadprogramme entstehen kann, ist von großer Bedeutung. Windows ist aufgrund seiner großen Verbreitung ein primäres Ziel für Angriffe mit Schadprogrammen, so dass hier eine große Bedrohung durch zahlreiche Angreifer und Angriffsarten besteht.

2.2 Software-Schwachstellen oder -Fehler

Windows 8.1 ist inklusive seiner zahlreichen mitgelieferten Anwendungen ein sehr komplexes Software-Produkt. Werden Software-Fehler darin nicht rechtzeitig erkannt, können die bei der Anwendung entstehenden Abstürze oder Fehler zu weitreichenden Folgen führen (z. B. falsche Berechnungsergebnisse, Fehlentscheidungen der Leitungsebene und Verzögerungen beim Ablauf der Geschäftsprozesse). Durch Software-Schwachstellen oder -Fehler können schwerwiegende Sicherheitslücken in einzelnen Anwendungen, dem gesamten IT-System oder sogar allen damit vernetzten IT-Systemen entstehen. Sicherheitslücken in Windows können unter Umständen von Angreifern ausgenutzt werden, um Schadsoftware einzuschleusen, unerlaubt Daten auszulesen oder zu manipulieren.

2.3 Integrierte Cloud-Funktionalitäten

Windows 8.1 bringt zahlreiche Funktionen mit, mit denen Daten in den Cloud-Diensten von Microsoft abgelegt und darüber synchronisiert werden. Dadurch besteht die Gefahr, Cloud-Diensten unbewusst (oder zumindest unbedacht) auch für möglicherweise sensible oder personenbezogene Daten zu nutzen. Gleichzeitig kann auch gegen Datenschutzgesetze verstoßen werden, wenn Daten bei Dritten, vor allem im Ausland gespeichert werden. Meldet sich ein Benutzer mit bereits aktiviertem Microsoft-Account an ein neues Gerät an, werden dort automatisch die von ihm genutzten Microsoft-Cloud-Dienste eingerichtet. So können Daten des Unternehmens ungewollt auf die privaten Geräte der Mitarbeiter synchronisiert werden. Als weiteres Beispiel bietet Windows 8 als Standardeinstellung die Möglichkeit, den Bitlocker-Recovery-Schlüssel direkt über den Microsoft-Account in der Cloud zu sichern. Damit werden kritische kryptographische Geheimnisse in die Hände Dritter gegeben.

2.4 Beeinträchtigung von Software-Funktionen durch Kompatibilitätsprobleme

Software, die auf Windows-Vorgängerversionen erfolgreich betrieben wurde, muss nicht auch mit einer aktuellen Version des Betriebssystems zusammenarbeiten. Mögliche Ursachen sind neue Sicherheitsmerkmale oder Betriebssystemeigenschaften, sowie der Wegfall von Funktionalitäten oder Diensten. In der Folge kann die Software nicht oder nur mit Einschränkungen verwendet werden. Bei neuen Windows-Versionen kann beispielsweise die Aktivierung neuer Sicherheitsmerkmalen zu Kompatibilitätsproblemen führen. Beispiele dafür sind die Benutzerkontensteuerung (UAC) oder bei 64-Bit-Versionen des Betriebssystems Kernel Patch Guard sowie die Notwendigkeit signierter Treiber. Bei neueren Windows-Versionen fallen aber auch Funktionalitäten weg. Ein Beispiel hierfür ist der Wegfall der GINA-Anmeldekomponente in neueren Windows-Versionen, die z. B. von einigen Fingerabdrucklesern verwendet wurde.

2.5 Fehlerhafte Administration oder Nutzung von Geräten und Systemen

Windows-Betriebssysteme sind komplexe Systeme, deren Sicherheit im Wesentlichen durch die eingestellten Parameter bestimmt wird. Dadurch können insbesondere Fehlkonfiguration von Komponenten die Sicherheit beeinträchtigen, sodass es zu Fehlfunktionen kommen kann oder das IT-System kompromittiert wird. Grundsätzlich beinhaltet jede Schnittstelle an einem IT-System nicht nur die Möglichkeit, darüber bestimmte Dienste des IT-Systems berechtigt zu nutzen, sondern auch das Risiko, dass darüber unbefugt auf das IT-System zugegriffen wird. Wenn etwa durch Fehlkonfiguration der Win-

dows-eigenen Authentisierungsmechanismen Benutzerkennungen und zugehörige Passwörter ausgespäht werden können, ist eine unberechtigte Nutzung der damit geschützten Anwendungen oder IT-Systeme denkbar.

Auch eine fehlerhafte oder nicht ordnungsgemäße Nutzung von Geräten, Systemen und Anwendungen kann die Sicherheit unter Windows beeinträchtigen, vor allem, wenn vorhandene Sicherheitsmaßnahmen missachtet oder umgangen werden. Zu großzügig vergebene Rechte, leicht zu erratende Passwörter, nicht ausreichend geschützte Datenträger mit Sicherungskopien oder bei vorübergehender Abwesenheit nicht gesperrte Arbeitsplätze können zu Sicherheitsvorfällen führen. Eine weitere Folge der fehlerhaften Bedienung von Windows-Systemen oder Anwendungen kann das versehentlich Löschen oder Verändern von Daten sein. Dabei ist es ebenfalls möglich, dass vertrauliche Informationen an die Öffentlichkeit gelangen, wenn beispielsweise Zugriffsrechte falsch gesetzt werden.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Windows 8.1 aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Benutzer

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.2.2.2.A1 Geeignete Auswahl einer Windows 8.1-Version

Es MUSS der Funktionsumfang einer Windows-Version vor der Beschaffung auf die Einsatzfähigkeit geprüft und eine geeignete Version ausgewählt werden. Es SOLLTEN bevorzugt 64-Bit Versionen eingesetzt werden, die erweiterte Sicherheitsfeatures enthalten.

SYS.2.2.2.A2 Festlegung eines Anmeldeverfahrens

Abhängig von den Sicherheitsanforderungen MUSS entschieden werden, ob neben dem klassischen Anmeldeverfahren mit Passwort auch andere Mechanismen wie PIN erlaubt sein sollen. Dies MUSS entsprechend auf allen Clients eingestellt werden.

SYS.2.2.2.A3 Einsatz von Viren-Schutzprogrammen

Sofern nicht gleich- oder höherwertige Maßnahmen zum Schutz des IT-Systems vor einer Infektion mit Schadsoftware getroffen wurden, MUSS ein Virenschutz-Programm auf Windows 8-Clients eingesetzt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Clients unter Windows 8.1. Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.2.2.2.A4 Beschaffung von Windows 8.1

Die Anforderungen gemäß der Windows Hardware Certification Requirements SOLLTEN bei der Beschaffung von Windows 8.1 bzw. der entsprechenden Hardware für das Windows 8.1-System berücksichtigt werden. Des weiteren SOLLTEN die zu beschaffenden Systeme über eine Firmware-Konfigura-

tionsoberfläche für UEFI SecureBoot und für das TPM (sofern vorhanden) verfügen, die die Kontrolle durch den Eigentümer ermöglicht. Der Beschaffungsprozess von Windows 8.1 SOLLTE die Auswahl eines geeigneten Lizenzmodells enthalten.

SYS.2.2.2.A5 Lokale Sicherheitsrichtlinien

Es SOLLTEN alle sicherheitsrelevanten Einstellungen über Sicherheitsrichtlinien bedarfsgerecht konfiguriert, getestet und regelmäßig überprüft werden. Alle nicht benötigten Anwendungen und Komponenten SOLLTEN mittels Sicherheitsrichtlinien deaktiviert werden. Die Verteilung der Sicherheitseinstellungen auf mehrere Windows-8.1-Clients SOLLTE entsprechend der Gegebenheiten der Institution erfolgen.

SYS.2.2.2.A6 Datei- und Freigabeberechtigungen

Um eine einheitliche restriktive Rechtevergabe zu ermöglichen, SOLLTE ein Berechtigungs- und Zugriffskonzept für Windows vorhanden sein, das geeignete Datei- und Verzeichnisberechtigungen nach dem Need-to-Know-Prinzip für Inhalte auf den Windows-8.1-Clients definiert.

Neben Berechtigungen auf dem lokalen Dateisystem SOLLTE das Berechtigungs- und Zugriffskonzept die Zugriffsrechte für freigegebene Verzeichnisse im Netzzugriff beachten. Eine Prüfung der Berechtigungen der Dateien und Verzeichnisse SOLLTE insbesondere bei Rechnern, die von älteren Betriebssystemversionen aktualisiert wurden, erfolgen.

SYS.2.2.2.A7 Einsatz der Windows-Benutzerkontensteuerung UAC

Um eine restriktive Rechtevergabe zu unterstützen, SOLLTE die Benutzerkontensteuerung (UAC, User Account Control) aktiviert sein. Für Standardbenutzer SOLLTE festgelegt sein, dass die Aufforderung zur Passworteingabe für erhöhte Rechte automatisch abgelehnt wird. Für Administratorkonten SOLLTE die Einstellung von UAC zwischen Bedienbarkeit und Sicherheitsniveau abgewogen werden. Die Entscheidung SOLLTE dokumentiert und die entsprechenden Einstellungen konfiguriert werden. Es SOLLTE regelmäßig geprüft werden, ob die Notwendigkeit noch besteht und die Rechte entsprechend angepasst oder entzogen werden.

SYS.2.2.2.A8 Verwendung der Heimnetzgruppen-Funktion [Benutzer]

Clients SOLLTEN keine Dienste wie Datei- oder Druckerfreigaben anbieten. Eine Sicherheitsrichtlinie (GPO) mit der Einstellung "Beitritt des Computers zu einer Heimnetzgruppe verhindern" SOLLTE für alle Clients gelten. Wird die Funktion aus betrieblichen Gründen eingesetzt, SOLLTEN die Benutzer im Umgang mit den Freigaben der Heimnetzgruppe geschult werden.

SYS.2.2.2.A9 Datenschutz und Datensparsamkeit bei Windows 8.1-Clients [Benutzer]

Werden Microsoft-Konten für die Benutzer angelegt, SOLLTEN nur unbedingt erforderliche Angaben zu den Personen hinterlegt werden. Die SmartScreen-Funktion SOLLTE auf die Verträglichkeit mit internen oder externen Datenschutzvorgaben überprüft und bewertet werden. Bevor eine Anwendung oder App zur Nutzung innerhalb der Institution freigegeben wird, SOLLTE sorgfältig geprüft werden, welche Daten Anwendungen und Apps automatisch an die Microsoft-Cloud übersenden. Anwendungen SOLLTEN so konfiguriert werden, dass keine solchen Daten übertragen werden. Apps mit unerwünschter oder unnötig umfangreicher Datenübertragung an Dritte SOLLTEN nicht verwendet werden.

SYS.2.2.2.A10 Integration von Online-Konten in das Betriebssystem

Die Anmeldung am IT-System und der Domäne SOLLTE nur mit einem Konto eines selbst betriebenen Verzeichnisdienstes, wie z. B. Active Directory, möglich sein. Eine lokale Anmeldung SOLLTE Administratoren vorbehalten sein. Bei Verwendung von Online-Konten zur Anmeldung, z. B. eines Microsoft-Kontos oder Konten anderer Anbieter von Diensten zum Identitätsmanagement, SOLLTE auf ausreichende Sicherheit des Anbieters und auf die Einhaltung des Datenschutzes geachtet werden.

SYS.2.2.2.A11 Konfiguration von Synchronisationsmechanismen in Windows 8.1

Die Synchronisierung von Nutzerdaten mit Microsoft Cloud-Diensten SOLLTE vollständig deaktiviert werden.

SYS.2.2.2.A12 Zentrale Authentifizierung in Windows-Netzwerken

In reinen Windows-Netzen SOLLTE zur zentralen Authentifizierung für SSO (Single Sign On) ausschließlich Kerberos eingesetzt werden. Eine Gruppenrichtlinie SOLLTE die Verwendung älterer Protokolle verhindern. Die Speicherung der LAN-Manager-Hashwerte bei Kennwortänderungen SOLLTE per Gruppenrichtlinie deaktiviert werden. Die Überwachungseinstellungen gemeinsam mit den Serverkomponenten von DirectAccess SOLLTEN sorgfältig auf die Anforderungen des Informationsverbunds abgestimmt werden. Eine Protokollierung auf Clientseite SOLLTE sichergestellt werden.

SYS.2.2.2.A13 Anbindung von Windows 8.1 an AppStores

Die Möglichkeit zur Installation von Apps aus dem Microsoft AppStore SOLLTE deaktiviert werden, sofern sie nicht benötigt wird.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.2.2.2.A14 Anwendungssteuerung mit Software Restriction Policies und AppLocker (CIA)

Anwendungen in Pfaden, die von Benutzern schreibbar sind, SOLLTEN durch Software Restriction Policies (SRP) oder AppLocker an der Ausführung gehindert werden. Die Verwaltung der AppLocker- und SRP-GPO in einem domänenbasierten Netz SOLLTE zentralisiert mittels Gruppenrichtlinienobjekten je Benutzer/Benutzergruppe erfolgen.

AppLocker SOLLTE nach dem Ansatz einer Positivliste genutzt werden. Es sollte alles verboten werden, was nicht explizit erlaubt ist. Bei AppLocker SOLLTEN bevorzugt Regeln auf der Grundlage von Anwendungssignaturen definierter Herausgeber genutzt werden. Versuchte Regelverstöße SOLLTEN protokolliert und geeignet ausgewertet werden.

Für Clients mit besonders hohen Anforderungen an die Sicherheit SOLLTE AppLocker die Ausführung aller ungenehmigten Anwendungen verhindern, statt diese zu protokollieren.

Die Umsetzung der SRP- und AppLocker-Regeln SOLLTEN vor dem Einsatz auf einem produktiven System zunächst auf einem Testsystem oder durch den Betrieb im Überwachungsmodus erprobt werden.

SYS.2.2.2.A15 Verschlüsselung des Dateisystems mit EFS (CI)

Bei erhöhtem Schutzbedarf SOLLTE das Dateisystem verschlüsselt werden. Wird hierzu das Encrypting File System (EFS) verwendet, SOLLTE ein komplexes Passwort für den Schutz der mit EFS verschlüsselten Daten verwendet werden. Zusätzlich SOLLTEN die mit EFS verschlüsselten Dateien durch restriktive Zugriffsrechte geschützt werden. Statt des Administratorkontos SOLLTE ein dediziertes Konto der Wiederherstellungsagent sein. Der private Schlüssel dieses Kontos SOLLTE auf einen externen Datenträger ausgelagert und sicher aufbewahrt sowie aus dem System entfernt werden. Dabei SOLLTEN von allen privaten Schlüsseln Datensicherungen erstellt werden. Beim Einsatz von EFS mit lokalen Benutzerkonten SOLLTE die Registry-Verschlüsselung mittels syskey verwendet werden. Beim Einsatz von EFS SOLLTEN die Benutzer im korrekten Umgang mit EFS geschult werden.

SYS.2.2.2.A16 Verwendung der Windows PowerShell (CIA)

Wenn die Windows PowerShell (WPS) nicht benötigt wird, SOLLTE sie deinstalliert werden. Bei Windows 8.1 lässt sich die PowerShell-Skriptumgebung allerdings nur noch entfernen, wenn auch das .NET-Framework deinstalliert wird. Daher SOLLTE alternativ die Ausführung der WPS-Dateien nur den Gruppen der Administratoren, lokal und Domäne, gestattet werden. Die Protokollierung von Schreib- und Lesezugriffen auf das Windows PowerShell-Profil SOLLTE aktiviert und für eine regelmäßige Kontrolle der Protokolle gesorgt werden. Die Ausführung von Windows PowerShell-Skripten mit dem Befehl "Set-Execution Policy AllSigned" SOLLTE eingeschränkt werden, um zumindest die versehentliche Ausführung unsignierter Skripte zu verhindern.

SYS.2.2.2.A17 Sicherer Einsatz des Wartungscenters (CIA)

In der Sicherheitsrichtlinie SOLLTE der Umgang mit dem Wartungscenter durch die Benutzer definiert werden, Änderungen der Standard-Starteinstellungen der Windows 8-Dienste DPS, WDiSvcHost und WerSvc sind notwendig. Die Einstellungen für "Neueste Problembehandlungen vom Windows-Onlinedienst für Problembehandlung abrufen", "Problemberichte senden", "Regelmäßig Daten über Computerkonfiguration an Microsoft senden", "Windows-Sicherung", "Programm zur Benutzerfreundlichkeit" und "Problembehandlung - andere Einstellungen" SOLLTEN unter Windows 8.1 deaktiviert werden.

SYS.2.2.2.A18 Aktivierung des Last-Access-Zeitstempels (A)

Im Rahmen der Erstellung eines Sicherheitskonzeptes für ein IT-System mit Windows 8.1 SOLLTE geprüft werden, ob der Last-Access-Zeitstempel aktiviert wird, um die Analyse eines Systemmissbrauchs zu erleichtern. Dabei SOLLTEN besonders Performance-Aspekte bei der Prüfung berücksichtigt werden.

SYS.2.2.2.A19 Verwendung der Anmeldeinformationsverwaltung (C)

Die Erlaubnis oder das Verbot der Speicherung von Zugangsdaten im sogenannten "Tresor" SOLLTE in einer Richtlinie festgelegt werden. Ein Verbot SOLLTE technisch durchgesetzt werden.

SYS.2.2.2.A20 Sicherheit beim Fernzugriff über RDP (CIA)

Die Auswirkungen auf die Konfiguration der lokalen Firewall SOLLTE bei der Planung der Remote-Unterstützung berücksichtigt werden. Die Gruppe der berechtigten Benutzer für den Remote-Desktopzugriff SOLLTE durch die Zuweisung entsprechender Benutzerrechte und in der Richtlinie festgelegt werden. Eine Remote-Unterstützung SOLLTE nur nach einer expliziten Einladung über EasyConnect oder auf Grundlage einer Einladungsdatei erfolgen. Bei der Speicherung einer Einladung in einer Datei SOLLTE die Datei mit einem Kennwort geschützt sein. Der aktuell angemeldete Benutzer SOLLTE dem Aufbau einer Sitzung immer explizit zustimmen müssen. Die maximale Gültigkeitsdauer der Einladung SOLLTE eine angemessene Größe haben. Zudem SOLLTE eine starke Verschlüsselung (128 Bit, Einstellung "Höchste Stufe") verwendet werden. Außerdem SOLLTE die automatische Kennwortanmeldung deaktiviert werden. Es SOLLTE geprüft werden, ob Umleitungen der Zwischenablage, Drucker, Dateiablage und Smartcard-Anschlüsse notwendig sind, andernfalls SOLLTEN diese deaktiviert werden. Sofern der Einsatz der Fernsteuerungsmechanismen nicht vorgesehen ist, SOLLTEN diese vollständig deaktiviert werden.

SYS.2.2.2.A21 Einsatz von File und Registry Virtualization (CI)

Es SOLLTE geprüft werden, ob der Betrieb von Altanwendungen noch notwendig ist, die Schreibrechte auf kritische System-Ordner oder Registry-Schlüssel erfordern oder mit Administratorrechten ausgeführt werden müssen. Sofern dies zutrifft, SOLLTE eine Strategie entwickelt werden, um die noch benötigten Altanwendungen auf sichere Alternativen umzustellen. Bis zur Ablösung der Altanwendungen SOLLTE der Einsatz der Windows-Techniken File Virtualization und Registry Virtualization zur Absicherung geprüft werden. Zusätzlich SOLLTE die Registry Virtualization nur auf die notwendigen Registry-Schlüssel Zugriff haben.

4 Weiterführende Informationen

4.1 Literatur

- [MicSAO] Security Auditing Overview ,Microsoft, 07.2013
  https://technet.microsoft.com/en-us/library/dn319078.aspx

- [MicSE] Liste von Sicherheitsereignissen: Windows 8 und Windows Server 2012, Microsoft, (zuletzt abgerufen am 27.09.2017)
  https://www.microsoft.com/en-us/download/confirmation.aspx?id=50034

- [WIN8] Informationen zu Einsatz, Bereitstellung und Verwaltung von Windows 8.1, Micorosoft, (zuletzt abgerufen am 27.09.2017)
  https://technet.microsoft.com/de-de/windows/windows-8.aspx

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Clients unter Windows 8.1" von Bedeutung.

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.36 Identitätsdiebstahl

G 0.39 Schadprogramme

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen Anforderungen	G 0.16	G 0.17	G 0.18	G 0.19	G 0.21	G 0.22	G 0.23	G 0.25	G 0.28	G 0.29	G 0.30	G 0.31	G 0.32	G 0.36	G 0.39	G 0.45	G 0.46
SYS.2.2.2.A1						x			x	x	x	x					
SYS.2.2.2.A2	x			x		x	x			x	x		x				x
SYS.2.2.2.A3				x						x			x		x	x	x
SYS.2.2.2.A4			x														
SYS.2.2.2.A5				x		x				x	x	x			x		x
SYS.2.2.2.A6	x	x	x	x	x					x	x		x				x
SYS.2.2.2.A7						x						x					x
SYS.2.2.2.A8				x							x					x	
SYS.2.2.2.A9				x		x							x	x	x		x
SYS.2.2.2.A10	x		x	x		x		x		x	x	x				x	
SYS.2.2.2.A11	x		x	x		x		x		x	x	x				x	
SYS.2.2.2.A12			x	x													x
SYS.2.2.2.A13				x		x							x	x	x		x
SYS.2.2.2.A14				x		x							x	x	x		x
SYS.2.2.2.A15				x													x
SYS.2.2.2.A16						x					x	x					
SYS.2.2.2.A17												x					
SYS.2.2.2.A18			x			x							x				
SYS.2.2.2.A19	x											x					
SYS.2.2.2.A20				x							x	x	x				x
SYS.2.2.2.A21						x						x					x

SYS.2.2: Windows-Clients

SYS.2.2.3 Clients unter Windows 10

1 Beschreibung

1.1 Einleitung

Mit Windows 10 hat Microsoft sein Client-Betriebssystem Windows an eine neue Unternehmensstrategie angepasst. Verändert hat sich insbesondere auch die Designphilosophie des Betriebssystems weg von dem bisherigen Prinzip des "lokalen Betriebssystems" hin zu einem Dienst ("Windows as a Service"), welcher neben den bisherigen Betriebssystemfunktionalitäten auch darüber hinausgehende, insbesondere cloudbasierte, Anwendungen enthält und deswegen auf eine enge Anbindung an die Server-Infrastruktur des Herstellers angewiesen ist. Der tief verankerte und teilweise nicht beeinflussbare Datenaustausch zwischen Client und Herstellerinfrastruktur sowie die zunehmende Auslagerung von sicherheitskritischen Kernbestandteilen einer Windows-Infrastruktur in die Cloud, wie z. B. Authentifizierung, sind dabei wichtige und vor einem Einsatz unbedingt zu bewertende neue Aspekte im Vergleich zu den bisherigen Windows-Versionen.

1.2 Zielsetzung

Ziel dieses Bausteins ist der Schutz von Informationen, die durch und auf Windows 10-Clients verarbeiten werden.

1.3 Abgrenzung

Aufbauend auf dem Baustein SYS.2.1 Allgemeiner Client, enthält dieser Baustein spezifische Anforderungen, die zum sicheren Betrieb von Clients unter dem Betriebssystem Windows 10 zusätzlich zu den Anforderungen aus dem Baustein SYS.2.1 Allgemeiner Client zu beachten und zu erfüllen sind. Die enthaltenen Anforderungen sind daher auch immer in Verbindung mit den Anforderungen aus dem "Allgemeinen Client" zu betrachten. Ein Schutz gegen fortgeschrittene und andauernde Bedrohungen muss durch die Erfüllung zusätzlicher Anforderungen der unterschiedlichen Schichten des modernisierten IT-Grundschutzes realisiert werden.

2 Gefährdungslage

Die folgenden spezifischen Bedrohungen und Schwachstellen sind für die betrachteten Clients auf Basis von Windows 10 von besonderer Bedeutung:

2.1 Schadprogramme unter Windows 10

Aufgrund der hohen Verbreitung von Windows-Betriebssystemen und der zwischen den Systemgenerationen oftmals vorhandenen Abwärtskompatibilität zu älteren Versionen ist die Gefährdung durch Schadprogramme und unbefugtes Eindringen in das IT-System vergleichsweise hoch. Schadprogramme können eine Vielzahl von Funktionen besitzen und einem Angreifer umfangreiche Steuerungsmöglichkeiten ermöglichen. Unter anderem können Schadprogramme gezielt Passwör-

ter ausforschen, Systeme fernsteuern, Schutzsoftware deaktivieren und Daten ausspionieren. Als Schaden ist hier insbesondere der Verlust oder die Verfälschung von Informationen oder Anwendungen von größter Tragweite. Aber auch ein Imageverlust und finanzieller Schaden, der folglich durch Schadprogramme entstehen kann, ist von großer Bedeutung. Windows ist aufgrund seiner großen Verbreitung ein primäres Ziel für den Angriff mit Schadprogrammen, sodass hier eine große Bedrohung durch zahlreiche Angreifer und Angriffsarten besteht.

2.2 Software-Schwachstellen in Windows 10

Windows 10 ist inklusive seiner zahlreichen mitgelieferten Anwendungen ein sehr komplexes Software-Produkt. Werden Software-Fehler darin nicht rechtzeitig erkannt, können die bei der Anwendung entstehenden Abstürze oder Fehler zu weitreichenden Folgen führen (z. B. falsche Berechnungsergebnisse, Fehlentscheidungen der Leitungsebene und Verzögerungen beim Ablauf der Geschäftsprozesse). Durch Software-Schwachstellen oder -Fehler kann es zu schwerwiegenden Sicherheitslücken in einzelnen Anwendungen, dem gesamten IT-System oder sogar allen damit vernetzten IT-Systemen kommen. Sicherheitslücken in Windows können unter Umständen von Angreifern ausgenutzt werden, um Schadsoftware einzuschleusen, unerlaubt Daten auszulesen oder Manipulationen vorzunehmen.

2.3 Integrierte Cloud-Funktionalitäten

Windows 10 bringt zahlreiche Funktionen mit, mit denen Daten unter Nutzung der Dienste von Microsoft abgelegt und synchronisiert werden ("Cloud-Dienste"). Dadurch besteht die Gefahr, diese unbewusst (oder zumindest unbedacht) auch für möglicherweise sensible oder personenbezogene Daten zu nutzen. Gleichzeitig können sich Verstöße gegen die Datenschutzgesetze ergeben, wenn Daten bei Dritten, in der Regel im Ausland, gespeichert werden. Meldet sich ein Benutzer mit bereits aktiviertem Microsoft-Account an ein neues Gerät an, werden automatisch die von ihm genutzten Microsoft-Cloud-Dienste eingerichtet. So können Daten der Institution ungewollt auf die privaten Geräte der Mitarbeiter synchronisiert werden. Als weiteres Beispiel bietet Windows 10 als Standardeinstellung die Möglichkeit, den Bitlocker-Recovery-Schlüssel direkt über den Microsoft-Account in der Cloud zu sichern und somit kritische kryptographische Geheimnisse in die Hände Dritter zu übergeben.

2.4 Beeinträchtigung von Software-Funktionen durch Kompatibilitätsprobleme

Software, die auf Vorgängerversionen eines Betriebssystems erfolgreich betrieben werden konnte, muss nicht auch grundsätzlich mit der aktuellen Version von Windows 10 zusammenarbeiten. Mögliche Ursachen sind neue Sicherheitsmerkmale oder Betriebssystemeigenschaften, sowie der Wegfall von Funktionalitäten oder Diensten. In der Folge kann die Software nicht oder nur mit Einschränkungen verwendet werden. Beispiele für aktivierte Sicherheitsmerkmale, die bei neuen Windows-Versionen Ursache möglicher Kompatibilitätsprobleme sein können, sind die Benutzerkontensteuerung (UAC), oder bei 64-Bit-Versionen des Betriebssystems Kernel Patch Guard sowie die Notwendigkeit signierter Treiber, die möglicherweise für ältere Geräte nicht mehr zur Verfügung stehen.

2.5 Fehlerhafte Administration oder Nutzung von Windows 10

Windows 10 ist ein komplexes Betriebssystem, dessen Sicherheit im Wesentlichen durch ihre Konfiguration bestimmt wird. Dadurch ergeben sich insbesondere durch Fehlkonfiguration einzelner oder mehrerer Komponenten Beeinträchtigungen der Sicherheit für den Client selbst sowie für die genutzte Infrastruktur. Grundsätzlich beinhaltet jede Schnittstelle an einem IT-System nicht nur die Möglichkeit, darüber bestimmte Dienste des IT-Systems berechtigt zu nutzen, sondern auch das Risiko, dass darüber unbefugt auf das IT-System zugegriffen wird. Wenn etwa durch Fehlkonfiguration der Windows-eigenen Authentisierungsmechanismen Benutzerkennungen und zugehörige Passworte ausgespäht werden können, ist eine unberechtigte Nutzung der damit geschützten Anwendungen oder IT-Systeme möglich.

Auch eine fehlerhafte oder nicht ordnungsgemäße Nutzung von Geräten, Systemen und Anwendungen kann die Sicherheit unter Windows beeinträchtigen, vor allem, wenn vorhandene Sicherheitsmaßnahmen missachtet oder umgangen oder bewusst abgeschaltet werden. Zu großzügig vergebene Rechte, leicht zu erratende Passwörter, nicht ausreichend geschützte Datenträger mit Sicherungskopien oder bei vorübergehender Abwesenheit nicht gesperrte Arbeitsplätze können zu Sicherheitsvorfällen führen.

Eine weitere Folge der fehlerhaften Bedienung von Windows-Systemen oder Anwendungen kann das versehentliche Löschen oder Verändern von Daten sein. Dabei ist es ebenfalls möglich, dass vertrauliche Informationen an die Öffentlichkeit gelangen, wenn beispielsweise Zugriffsrechte falsch gesetzt werden.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz von Windows 10 aufgeführt. Grundsätzlich ist *der IT-Betrieb* für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese werden in den entsprechenden Anforderungen gesondert erwähnt.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Benutzer

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.2.2.3.A1 Planung des Einsatzes von Cloud-Diensten

Windows 10-basierte Geräte sind eng mit den Cloud-Diensten des Herstellers Microsoft verzahnt. Es MUSS daher vor der Verwendung von Windows 10-basierten Geräten eine strategische Festlegung erfolgen, welche enthaltenen Cloud-Services in welchem Umfang genutzt werden sollen bzw. dürfen.

SYS.2.2.3.A2 Geeignete Auswahl einer Windows 10-Version und Beschaffung

Der Funktionsumfang und die Versorgung mit funktionalen Änderungen einer Windows 10-Version MUSS unter Berücksichtigung des ermittelten Schutzbedürfnisses und des Einsatzzwecks ausgewählt und die Umsetzbarkeit der erforderlichen Absicherungsmaßnahmen geprüft werden. Basierend auf dem Ergebnis der Überprüfung MUSS der etablierte Beschaffungsprozess um die Auswahl des entsprechenden Lizenzmodells und Releasepfades (CB, CBB oder LTSB) erweitert werden.

SYS.2.2.3.A3 Geeignetes Patch- und Änderungsmanagement

Um alle Änderungen erfassen und bewerten zu können, MÜSSEN alle Windows 10 Systeme einem Patch- und Änderungsmanagement unterstellt sein. Für komplexe Patches oder Änderungen MÜSSEN in einem Umsetzungsplan Tests, Kontroll- und Abbruchpunkte sowie Prioritäten für die Verteilung definiert sein. Nach einem funktionalen Update des Betriebssystems MUSS überprüft werden, ob alle Anforderungen aus dem IT-Grundschutz und den internen Vorgaben weiterhin erfüllt werden.

SYS.2.2.3.A4 Telemetrie und Datenschutzeinstellungen

Die Telemetriedienste, also die Diagnose- und Nutzungsdaten, die Microsoft zur Identifizierung und Lösung von Problemen, zur Verbesserung der Dienste und Produkte und zur Personalisierung des Systems mit eindeutigen Identifizierungsmerkmalen verknüpft in die U SA überträgt, können im Betriebssystem nicht vollständig abgeschaltet werden. Es MUSS daher durch geeignete Maßnahmen, etwa auf Netzebene, sichergestellt werden, dass diese Daten nicht an Microsoft übertragen werden.

SYS.2.2.3.A5 Schutz vor Schadsoftware

Sofern nicht gleich- oder höherwertige andere mitigierende Maßnahmen zum Schutz des IT-Systems vor einer Infektion mit Schadsoftware getroffen wurden, MUSS der Einsatz einer spezialisierten Komponente zum Schutz vor Schadsoftware auf Windows 10-Clients umgesetzt sein.

SYS.2.2.3.A6 Integration von Online-Konten in das Betriebssystem [Benutzer]

Die Anmeldung am System und der Domäne DARF NUR mit dem Konto eines selbst betriebenen Verzeichnisdienstes möglich sein. Anmeldungen mit lokalen Konten SOLLTEN Administratoren vorbehalten sein. Online-Konten zur Anmeldung, etwa ein Microsoft-Konto oder Konten anderer Anbieter von Identitätsmanagementsystemen, DÜRFEN NICHT verwendet werden, da hier personenbezogene Daten an die Systeme des Herstellers übertragen werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Clients unter Windows 10. Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.2.2.3.A7 Lokale Sicherheitsrichtlinien

Alle sicherheitsrelevanten Einstellungen SOLLTEN bedarfsgerecht konfiguriert, getestet und regelmäßig überprüft werden. Die Sicherheitsrichtlinien SOLLTEN gemäß den Empfehlungen des Betriebssystemherstellers und dem voreingestellten Standardverhalten konfiguriert werden, sofern das Standardverhalten nicht anderen Anforderungen aus dem IT-Grundschutz oder der Organisation widerspricht. Abweichungen MÜSSEN dokumentiert und begründet werden. Alle nicht benötigten Anwendungen und Komponenten SOLLTEN deaktiviert werden. Sicherheitsrichtlinien SOLLTEN in jedem Fall gesetzt werden, auch dann, wenn die Einstellung nicht vom Standardverhalten einer nicht gesetzten Sicherheitsrichtlinie abweicht.

SYS.2.2.3.A8 Zentrale Verwaltung der Sicherheitsrichtlinien von Clients

Alle Einstellungen des Windows 10 Clients SOLLTEN durch ein zentrales Management verwaltet und entsprechend dem ermittelten Schutzbedarf basierend auf den internen Richtlinien konfiguriert sein. Technisch nicht umsetzbare Konfigurationsparameter SOLLTEN dokumentiert, begründet und mit dem Sicherheitsmanagement abgestimmt werden.

SYS.2.2.3.A9 Sichere zentrale Authentisierung der Windows-Clients

Für die zentrale Authentisierung SOLLTE ausschließlich Kerberos eingesetzt werden. Eine Gruppenrichtlinie SOLLTE die Verwendung älterer Protokolle verhindern. Ist dies nicht möglich, MUSS alternativ NTLMv2 eingesetzt werden. Die Authentisierung mittels LAN Manager und NTLMv1 DARF innerhalb der Institution und in einer produktiven Betriebsumgebung NICHT erlaubt werden. Die eingesetzten kryptografischen Mechanismen SOLLTEN entsprechend dem ermittelten Schutzbedarf und basierend auf den internen Richtlinien konfiguriert, dokumentiert und abweichende Einstellungen begründet und mit dem Sicherheitsmanagement abgestimmt sein.

SYS.2.2.3.A10 Konfiguration zum Schutz von Anwendungen in Windows 10

Die Datenausführungsverhinderung für alle Programme und Dienste (Opt-Out Modus) SOLLTE aktiviert werden.

SYS.2.2.3.A11 Schutz der Anmeldeinformationen in Windows 10

Sofern Windows 10 in der Enterprise-Version auf einem Hardware-System direkt (nativ) installiert ist, SOLLTE der Virtual Secure Mode (VSM) aktiviert werden. Zusätzlich zur Aktivierung von VSM SOLLTE Credential Guard gegen Angriffe auf die im System gespeicherten Authentisierungstoken und -hashes aktiviert werden. Ist dies nicht möglich, SOLLTE für den Betrieb des für die Verwaltung der Anmeldeinformationen zuständigen LSAS-Dienstes der geschützte Modus (PPL - Protected Process Light) aktiviert werden. Die Netzwerkanmeldung von lokalen Konten SOLLTE verboten werden.

SYS.2.2.3.A12 Datei- und Freigabeberechtigungen

Der Zugriff auf Dateien und Ordner auf dem lokalen System sowie auf Netzwerkfreigaben SOLLTE gemäß einem Berechtigungs- und Zugriffskonzept konfiguriert werden. Dies umfasst im speziellen auch die standardmäßig vorhandenen administrativen Freigaben auf dem System. Die Schreibrechte für Be-

nutzer SOLLTEN auf einen definierten Bereich im Dateisystem beschränkt werden. Insbesondere SOLLTEN Benutzer keine Schreibrechte in Ordner des Betriebssystems oder von installierten Anwendungen erhalten.

SYS.2.2.3.A13 Einsatz der SmartScreen-Funktionen

Die SmartScreen-Funktion, die aus dem Internet heruntergeladene Dateien und Webinhalte auf mögliche Schadsoftware untersucht und dazu unter Umständen personenbezogene Daten an Microsoft überträgt, SOLLTE deaktiviert werden.

SYS.2.2.3.A14 Einsatz des Sprachassistenten Cortana [Benutzer]

Cortana nutzt personenbezogene Daten wie z. B. Sprachdaten, Benutzereingaben, Kalender- und Kontaktdaten, Namen von bevorzugten Orten und benutzten Anwendungen, die an Microsoft übertragen werden. Aus diesem Grund SOLLTE Cortana deaktiviert werden.

SYS.2.2.3.A15 Einsatz der Synchronisationsmechanismen in Windows 10

Die Synchronisierung von Nutzerdaten mit Microsoft Cloud-Diensten und das Sharing von WLAN-Passwörtern SOLLTE vollständig deaktiviert werden.

SYS.2.2.3.A16 Anbindung von Windows 10 an den Windows Store

Die Verwendung des Windows Store SOLLTE auf die Verträglichkeit mit den Datenschutz- und Sicherheitsvorgaben der Institution überprüft und bewertet werden. Die generelle Installation von Apps auf Windows 10 ist nicht an die Anbindung an den Windows Store gebunden. Daher SOLLTE diese Funktion, sofern sie nicht benötigt wird, deaktiviert werden.

SYS.2.2.3.A17 Verwendung der automatischen Anmeldung

Die Speicherung von Kennwörtern, Zertifikaten und anderen Anmeldeinformationen zur automatischen Anmeldung auf Webseiten und IT-Systemen SOLLTE NICHT erlaubt werden.

SYS.2.2.3.A18 Einsatz der Windows-Remoteunterstützung

Die Auswirkungen auf die Konfiguration der lokalen Firewall SOLLTE bei der Planung der Windows-Remoteunterstützung (hiermit ist nicht RDP gemeint) berücksichtigt werden. Eine Remote-Unterstützung SOLLTE nur nach einer expliziten Einladung erfolgen. Bei der Speicherung einer Einladung in einer Datei SOLLTE diese ein Kennwort aufweisen. Der aktuell angemeldete Benutzer SOLLTE dem Aufbau einer Sitzung immer explizit zu stimmen. Die maximale Gültigkeitsdauer der Einladung für eine Unterstützung aus der Ferne SOLLTE eine angemessene Größe haben. Sofern dieser Service nicht verwendet wird, SOLLTE er vollständig deaktiviert werden.

SYS.2.2.3.A19 Verwendung des Fernzugriffs über RDP [Benutzer]

Die Auswirkungen auf die Konfiguration der lokalen Firewall SOLLTE bei der Planung des Fernzugriffs berücksichtigt werden. Die Gruppe der berechtigten Benutzer für den Remote-Desktopzugriff (RDP) SOLLTE durch die Zuweisung entsprechender Benutzerrechte festgelegt werden. In komplexen Infrastrukturen SOLLTE das RDP-Zielsystem nur durch ein dazwischen geschaltetes RDP-Gateway erreicht werden können. Für die Verwendung von RDP SOLLTE eine Prüfung und deren Umsetzung sicherstellen, ob die nachfolgend aufgeführten Komfortfunktionen im Einklang mit den Schutzbedarf des Zielsystems stehen:

- die Verwendung der Zwischenablage,
- die Einbindung von Druckern,
- die Einbindung von Wechselmedien und Netzlaufwerken
- die Nutzung der Dateiablagen und Smartcard-Anschlüssen

Sofern der Einsatz von Remote-Desktopzugriffen nicht vorgesehen ist, SOLLTEN diese vollständig deaktiviert werden. Die eingesetzten kryptographischen Protokolle und Algorithmen SOLLTEN den internen Vorgaben der Institution entsprechen.

SYS.2.2.3.A20 Einsatz der Benutzerkontensteuerung für privilegierte Konten

Die Konfigurationsparameter der Benutzerkontensteuerung (UAC) SOLLTEN für die privilegierten Konten zwischen Bedienbarkeit und Sicherheitsniveau abgewogen eingesetzt werden. Die Entscheidungen für die zu verwendenden Konfigurationsparameter SOLLTEN dokumentiert werden. Darüber hinaus SOLLTE die Dokumentation alle Konten mit Administratorrechten enthalten sowie eine regelmäßige Prüfung erfolgen, ob die Notwendigkeit zur Rechteerweiterung noch besteht.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.2.2.3.A21 Einsatz des Encrypting File Systems EFS (CI)

Da das Encrypting File System (EFS) die verwendeten Schlüssel mit dem Passwort des Benutzerkontos schützt, SOLLTE ein komplexes Passwort verwendet werden. Zusätzlich SOLLTEN restriktive Zugriffsrechte die mit EFS verschlüsselte Dateien schützen. Statt des Administrators SOLLTE ein dediziertes Konto der Wiederherstellungsagent sein. In diesem Zusammenhang SOLLTE dessen privater Schlüssel gesichert und aus dem System entfernt werden. Dabei SOLLTEN von allen privaten Schlüsseln Datensicherungen erstellt werden. Beim Einsatz von EFS mit lokalen Benutzerkonten SOLLTE die Verschlüsselung der lokalen Passwortspeicher mittels Syskey verwendet werden. Dies kann entfallen, wenn die Betriebssystemfunktion Credential Guard genutzt wird. Beim Einsatz von EFS SOLLTEN die Benutzer im korrekten Umgang mit EFS geschult werden.

SYS.2.2.3.A22 Windows PowerShell (CIA)

Die Ausführung der PowerShell sowie von WPS-Dateien SOLLTE nur Administratoren gestattet werden. Die PowerShell-Ausführung selbst SOLLTE zentral protokolliert und die Protokolle überwacht werden. Die Ausführung von PowerShell-Skripten SOLLTE mit dem Befehl Set-ExecutionPolicy-AllSigned eingeschränkt werden, um die versehentliche Ausführung unsignierter Skripte zu verhindern.

SYS.2.2.3.A23 Erweiterter Schutz der Anmeldeinformationen in Windows 10 (CI)

Auf UEFI-basierten Systemen SOLLTE SecureBoot verwendet und der Status des geschützten Modus für LSASS bei Systemstart überwacht werden (vgl. hierzu SYS.2.2.3.A11 Schutz der Anmeldeinformationen in Windows 10). Ist eine Fernwartung der Client-Systeme mittels RDP vorgesehen, SOLLTE bei Einsatz von Windows 10 in einer Domäne ab dem Funktionslevel 2012 R2 von der Option "restrictedAdmin" Gebrauch gemacht werden.

SYS.2.2.3.A24 Aktivierung des Last-Access-Zeitstempels (A)

Um die Analyse nach einem Systemmissbrauch zu erleichtern, SOLLTE der NTFS Last-Access-Zeitstempel aktiviert werden. Vor der Aktivierung SOLLTE geprüft werden, welche Auswirkungen die Aktivierung auf die Systemleistung hat. Die Ergebnisse der Überprüfung und die Entscheidung über die Aktivierung SOLLTEN dokumentiert werden.

SYS.2.2.3.A25 Umgang mit Fernzugriffsfunktionen der "Connected User Experience and Telemetry" (CI)

Die Komponente "Connected User Experience and Telemetry" (CUET) ist bei Windows 10 fester Bestandteil des Betriebssystems und stellt neben Telemetriefunktionalität auch eine Fernzugriffsmöglichkeit für den Betriebssystemhersteller auf das lokale System bereit. Ein Fernzugriff auf den Windows 10 Client durch den Betriebssystemhersteller SOLLTE netzwerkseitig geloggt und falls erforderlich geblockt werden.

4 Weiterführende Informationen

4.1 Literatur

- [TN408187] Configuring Additional LSA Protection
  Microsoft Technet, 03.2014
  https://technet.microsoft.com/en-us/library/dn408187.aspx

- [TN621547] Credential Guard - Überblick
  Microsoft, (zuletzt abgerufen am 27.09.2017)
  https://docs.microsoft.com/de-de/windows/access-protection/credential-guard/credential-guard-requirements

- [TN986865] Device Guard - Überblick
  Microsoft, (zuletzt abgerufen am 27.09.2017)
  https://technet.microsoft.com/de-de/library/dn986865.aspx

- [WIN10E] Windows 10 Editionen vergleichen
  Microsoft, (zuletzt abgerufen am 27.09.2017)
  https://www.microsoft.com/de-de/WindowsForBusiness/Compare

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Clients unter Windows 10" von Bedeutung.

G 0.15 Abhören

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.36 Identitätsdiebstahl

G 0.39 Schadprogramme

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen Anforderungen	G 0.15	G 0.16	G 0.17	G 0.18	G 0.19	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.28	G 0.29	G 0.30	G 0.31	G 0.32	G 0.36	G 0.39	G 0.45	G 0.46
SYS.2.2.3.A1	X			X	X							X				X		X	X
SYS.2.2.3.A2																			
SYS.2.2.3.A3				X		X	X	X	X	X	X						X		
SYS.2.2.3.A4	X			X	X							X				X			X
SYS.2.2.3.A5						X	X	X			X						X		
SYS.2.2.3.A6	X				X											X			
SYS.2.2.3.A7				X				X		X	X		X	X					
SYS.2.2.3.A8				X				X					X	X	X				
SYS.2.2.3.A9				X				X					X	X					
SYS.2.2.3.A10				X		X	X			X	X						X		
SYS.2.2.3.A11				X							X								
SYS.2.2.3.A12				X	X		X						X		X				X
SYS.2.2.3.A13				X	X							X							X
SYS.2.2.3.A14	X			X	X							X							X
SYS.2.2.3.A15				X	X							X							X
SYS.2.2.3.A16				X	X						X	X							
SYS.2.2.3.A17		X	X	X				X					X						
SYS.2.2.3.A18	X			X				X					X	X					
SYS.2.2.3.A19	X			X	X			X					X	X					
SYS.2.2.3.A20				X	X						X		X	X	X				
SYS.2.2.3.A21		X	X	X	X														
SYS.2.2.3.A22				X			X												
SYS.2.2.3.A23				X	X		X												
SYS.2.2.3.A24				X								X							
SYS.2.2.3.A25	X			X				X				X				X			

SYS.2: Desktop-Systeme

SYS.2.3 Clients unter Unix

1 Beschreibung

1.1 Einleitung

Neben Windows werden auf immer mehr Client-Betriebssystemen Linux oder seltener Unix installiert. Beispiele für klassische Unix-Systeme sind die BSD-Reihe (FreeBSD, OpenBSD und NetBSD), Solaris und AIX. Linux hingegen ist kein klassisches Unix (der Kernel basiert nicht auf dem ursprünglichen Quelltext, aus dem sich die verschiedenen Unix-Derivate entwickelt haben), sondern ein funktionelles Unix-System. Da sich die Konfiguration und der Betrieb von Linux- und Unix-Client ähneln, werden in diesem Baustein alle Betriebssysteme der Unix-Familie betrachtet.

Linux ist freie Software und wird von der Open-Source-Gemeinschaft entwickelt. Daneben gibt es Anbieter, die den Linux-Kernel und die verschiedenen Software-Komponenten zu einer Distribution zusammenfassen und pflegen, sowie weitere Dienstleistungen anbieten. Häufig werden Derivate zu den Distributionen Ubuntu, Debian, Red Hat Enterprise Linux SUSE Linux Enterprise eingesetzt. Darüber hinaus gibt es für spezielle Einsatzzwecke und Geräte zugeschnittene Linux-Distributionen wie Qubes OS, das versucht, ein hohes Maß an Sicherheit durch Virtualisierung zu erreichen, IGEL Linux als Thin Client, LibreElec für den Einsatz eines Home Theater PCs (HTPC) oder Kali Linux, eine auf Sicherheit, Computerforensik und Penetrationstests spezialisierte Distribution. Außerdem können Clients auch Live-Distributionen starten, ohne dass das vorhandene Betriebssystem verändert wird.

Der Marktanteil des Betriebssystems Linux auf Clients hat in den letzten Jahren zugenommen, in speziellen Einsatzumgebungen werden weiterhin "klassische" Unix-Systeme in verschiedenen Derivaten eingesetzt. Durch die Menge der vorausgewählten Softwarepakete einer Standardinstallation der gängigen Linux-Distributionen, beziehungsweise der Unix-Derivate, erhöht sich die Angriffsfläche, gleichzeitig bieten unixähnliche Betriebssysteme aber auch umfangreiche Schutzmechanismen. Typischerweise ist ein solches IT-System vernetzt und wird als Client in einem Client-Server-Netz betrieben. Da Clients oftmals aus Sicherheitsgründen unter Unix oder Linux betrieben werden und wie bei allen Clients nicht auf korrektes Nutzerverhalten vertraut werden kann, kommt der Absicherung von unixähnlichen Clients eine besondere Bedeutung zu.

1.2 Zielsetzung

Zielsetzung dieses Bausteins ist der Schutz von Informationen, die auf Unix-Clients erstellt, bearbeitet, gespeichert oder versendet werden. Die Anforderungen des Bausteins adressieren vorrangig Linux-Clients, können aber generell für Unix-Clients adaptiert werden. Der vorliegende Baustein unterscheidet hier weitgehend nicht zwischen Unix- und Linux, unter dem Begriff "Unix" werden Unix- und Linux-Clients zusammengefasst.

1.3 Abgrenzung

Dieser Baustein enthält grundsätzliche Anforderungen zum Betrieb von unixähnlichen Clients auf handelsüblichen IT-Systemen. Er konkretisiert und ergänzt die Aspekte, die im Bausteinen SYS.2.1 Allgemeiner Client behandelt werden, um Spezifika von Unix-Systemen. Auch wenn es sich bei OS

X von Apple um ein unixartiges Betriebssystem handelt, wird dieses Betriebssystem nicht in diesem Baustein behandelt, Empfehlungen hierzu sind im Baustein SYS.2.4 Client unter Apple OS X zu finden.

Soll der Client nicht selber verwaltet werden, sondern wird dieser durch Dritte verwaltet, sind zusätzlich die Anforderungen des Bausteins OPS.3.1 Outsourcing-Nutzung zu berücksichtigen.

Der Baustein umfasst nur das unixartige Betriebssystem, dass in der Regel bei einer Basisinstallation einer Linux-Desktop-Distribution installiert wird. Der Baustein umfasst insbesondere nicht darauf aufbauende Software wie E-Mail-Clients oder Office-Software, Anforderungen hierzu sind in der Schicht APP.1 Client-Anwendungen des IT-Grundschutz-Kompendiums zu finden. Falls der Client Schnittstellen zum Datenaustausch hat, wie z. B. CD/DVD, USB, Bluetooth oder WLAN, müssen die Sicherheitsvorgaben des Bausteins SYS.3.4 Mobile Datenträger erfüllt werden

Es wird bei diesem Client-Baustein davon ausgegangen, dass neben dem Administrator dauerhaft nur eine unveränderte Person mit einem interaktiven Benutzerkonto aktiv ist. Clients, die von mehreren Personen nacheinander oder gleichzeitig genutzt werden, erfordern zusätzliche Maßnahmen, die im Rahmen dieses Bausteins nicht behandelt werden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für Clients unter Unix von besonderer Bedeutung:

2.1 Schadprogramme

Schadprogramme werden mit dem Ziel entwickelt, unerwünschte und meistens schädliche Funktionen auszuführen. Schadprogramme werden meist heimlich, ohne Wissen und Einwilligung des Benutzers aktiv. Schadprogramme bieten heutzutage einem Angreifer umfangreiche Kommunikations- und Steuerungsmöglichkeiten und besitzen eine Vielzahl von Funktionen. Unter anderem können die Programme gezielt Passwörter ausforschen, Systeme fernsteuern, Schutzfunktionen deaktivieren und Daten ausspionieren. Insbesondere sind Anwender, die auf die von vornherein höhere Sicherheit von unixähnlichen Systemen vertrauen, oftmals sorgloser im Umgang mit unbekannten Dateien.

2.2 Software aus Drittquellen

Bei unixähnlichen IT-Systemen ist es nicht ungewöhnlich, Software selbst herunterzuladen und zu kompilieren, statt fertige Softwarepakete zu installieren. Wenn fertige Softwarepakete genutzt werden, werden diese oft nicht nur aus den vorhanden Paketquellen des Unix-Derivates installiert, sondern werden aus Drittquellen ohne weitere Prüfung bezogen. Jeder dieser alternativen Wege der Softwareinstallation birgt zusätzliche Risiken, indem so fehlerhafte oder inkompatible Software sowie Schadsoftware installiert werden kann.

2.3 Software-Schwachstellen oder -Fehler

Auf unixähnlichen IT-Systemen werden in der Regel eine Vielzahl von Anwendungen zur Installation angeboten. Da jede der installierbaren Anwendungen Software-Schwachstellen und -Fehler haben können, wird die potentielle Angriffsfläche erhöht, wenn bei der Installation nicht darauf geachtet, dass nur die benötigte Software installiert wird.

2.4 Ausnutzbarkeit der Skriptumgebung

Oft werden in unixähnlichen Betriebssystemen Skriptsprachen genutzt. Skripte sind eine Auflistung von einzelnen Kommandos, die in einer Textdatei gespeichert und beispielsweise in der Kommandozeile aufgerufen werden. Durch den großen Funktionsumfang der Skriptumgebungen können Angreifer Skripte umfangreich für ihre Zwecke nutzen. Darüber hinaus können aktivierte Skriptsprachen nur sehr schwer eingedämmt werden.

2.5 Dynamisches Laden von gemeinsam genutzten Bibliotheken

Mit der Kommandozeilenoption LD_PRELOAD wird die angegebene Bibliothek vor allen anderen in einer Anwendung benötigten Bibliotheken geladen und deren Funktionen werden von der Anwendung genutzt. Ein Angreifer könnte das Betriebssystem so manipulieren, dass Schadfunktionen bei der Nutzung von bestimmten Anwendungen mit ausgeführt werden.

2.6 Fehlerhafte Konfiguration

Schon in einer Standardinstallation werden bei unixähnlichen Betriebssystemen zahlreiche Anwendungen installiert, die separat konfiguriert werden müssen. Auch nachinstallierte Anwendungen müssen separat konfiguriert werden, so dass auf unixähnlichen Betriebssystemen unzählige Konfigurationsdateien vorzufinden sind.

Da diese Anwendungen unabhängig voneinander konfiguriert werden, können die Konfigurationsoptionen im Widerspruch zueinander stehen, ohne dass dies aus den einzelnen Einstellungen ersichtlich ist. Beispielsweise kann ein Dienst für eine Fernadministration auf einem Port lauschen, der von Paketfilterregeln blockiert wird oder Samba gibt das eigene Home-Verzeichnis unbeabsichtigt im Netz frei. Auf diese Weise können die Anwendungen ungewollt zusätzliche Funktionen bereitstellen oder wichtige Funktionen nicht anbieten und so die Aufgabenerfüllung am Client erschweren.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Client unter Unix aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Benutzer

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.2.3.A1 Authentisierung von Administratoren und Benutzer [Benutzer]

Um den Client zu nutzen, MÜSSEN sich die Benutzer gegenüber dem IT-System authentisieren. Administratoren DÜRFEN sich nicht im Normalbetrieb als root anmelden. Für die Systemadministrationsaufgaben SOLLTE "sudo" oder eine geeignete Alternative mit einer geeigneten Protokollierung genutzt werden. Es SOLLTE verhindert werden, dass sich mehrere Benutzer auf einem Gerät gleichzeitig einloggen können.

SYS.2.3.A2 Auswahl einer geeigneten Distribution

Es MUSS auf Grundlage der Sicherheitsanforderungen und des Einsatzzwecks ein geeignetes Unix-Derivat bzw. Linux-Distribution ausgewählt werden. Alle vorinstallierten Anwendungsprogramme, die nicht benötigt werden, MÜSSEN deinstalliert werden können. Es MUSS für die geplante Einsatzzeit des Betriebssystems Support angeboten werden. Alle benötigten Anwendungsprogramme SOLLTEN direkt verfügbar sein, ohne dass diese aus Drittquellen bezogen werden müssen.

Es SOLLTEN nur Anwendungsprogramme ausgewählt und installiert werden, für die Support angeboten wird. Betriebssystem und Anwendungsprogramme ohne regelmäßige Sicherheitsupdates SOLLTEN nicht eingesetzt werden. Es SOLLTE auf Distributionen mit einem Rolling-Release-Modell verzichtet werden. Distributionen, bei denen das Betriebssystem selber kompiliert wird, SOLLTEN nicht in Produktivumgebungen eingesetzt werden.

SYS.2.3.A3 Cloud- und Online-Inhalte [Benutzer]

Nur zwingend notwendige Cloud- und Online-Dienste des Betriebssystems DÜRFEN genutzt werden. Die notwendigen Cloud- und Online-Dienste SOLLTEN dokumentiert werden. Die Einstellungen des Betriebssystems MÜSSEN auf Konformität mit den organisatorischen Datenschutz- und Sicherheitsvorgaben überprüft und restriktiv konfiguriert bzw. deaktiviert werden.

SYS.2.3.A4 Einspielen von Updates und Patches

Die Verantwortlichen MÜSSEN sich über bekannt gewordene Schwachstellen informieren. Updates und Patches MÜSSEN so schnell wie möglich eingespielt werden. Vorab SOLLTE auf einem Testsystem überprüft werden, ob die Sicherheitsupdates kompatibel sind und keine Fehler verursachen. Solange keine Patches für bekannte Schwachstellen verfügbar sind, MÜSSEN andere geeignete Maßnahmen getroffen werden, um den Client zu schützen. Der Client SOLLTE zeitnah rebootet werden, nachdem der Kernel aktualisiert wurde. Alternativ MUSS Live-Patching des Kernels aktiviert werden.

SYS.2.3.A5 Sichere Installation von Software-Paketen

Es DÜRFEN nur benötigte Anwendungen installiert werden. Nicht mehr benötigte Anwendungen MÜSSEN deinstalliert werden.

Die Integrität und Authentizität der zu installierenden Softwarepakete MUSS immer geprüft werden. Die Software-Pakete MÜSSEN unter einem unprivilegierten Benutzeraccount entpackt, konfiguriert und übersetzt werden. Erst der letzte Schritt, die eigentliche Installation des übersetzten Programms, DARF mit höheren Privilegien erfolgen. Dabei DARF die zu installierende Software NICHT unkontrolliert in das Wurzeldateisystem des Servers installiert werden.

Wird die Software aus dem Quelltext übersetzt, dann SOLLTEN die gewählten Parameter geeignet dokumentiert werden. Anhand dieser Dokumentation SOLLTE der Quelltext jederzeit nachvollziehbar und reproduzierbar kompiliert werden können. Alle weiteren Installationsschritte SOLLTEN dabei ebenfalls dokumentiert werden, damit sich die Konfiguration im Notfall schnell reproduzieren lässt.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Clients unter Unix. Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.2.3.A6 Automatisches Einbinden von Wechsellaufwerken [Benutzer]

Wechsellaufwerke SOLLTEN nicht automatisch eingebunden werden. Die Einbindung von Wechsellaufwerken SOLLTE so konfiguriert sein, dass alle Dateien als nicht ausführbar markiert sind (Mountoption "noexec").

SYS.2.3.A7 Restriktive Rechtevergabe auf Dateien und Verzeichnisse

Der Zugriff von Benutzern auf Dateien und Verzeichnisse SOLLTE immer auf das erforderliche Minimum beschränkt werden. Dabei SOLLTE in jedem Fall sichergestellt werden, dass Dienste und Anwendungen nur ihre zugeordneten Dateien erstellen, verändern oder löschen dürfen. Auf Verzeichnissen, in denen alle Benutzer Schreibrechte haben (z. B. /tmp) SOLLTE das Sticky-Bit gesetzt werden.

SYS.2.3.A8 Einsatz von Techniken zur Rechtebeschränkung von Anwendungen

Zur Beschränkung der Zugriffsrechte von Anwendungen auf Dateien, Geräte und Netze SOLLTE App-Armor oder SELinux eingesetzt werden. Es SOLLTEN die von der jeweiligen Unix-Derivat bzw. Linux-Distribution am besten unterstützte Lösung eingesetzt werden. Statt Blacklisting SOLLTEN die notwendigen Anwendungen durch Whitelisting reglementiert werden. Erweiterungen zur Rechtebeschränkung SOLLTEN im Enforcement Mode oder mit geeigneten Alternativen verwendet werden.

SYS.2.3.A9 Passwörter auf der Kommandozeile [Benutzer]

Passwörter SOLLTEN NICHT als Parameter an Programme übergeben werden.

SYS.2.3.A10 Absicherung des Bootvorgangs

Der Client SOLLTE durch Vergabe eines Boot-Passworts in der Firmware abgesichert werden. Zusätzlich SOLLTE eine Bootreihenfolge festgelegt werden, bei der von der eingebauten Boot-Festplatte zuerst gebootet wird. Der Bootloader SOLLTE mit einem Passwort so abgesichert werden, dass nur der unveränderte Standardeintrag ohne Passwort genutzt werden kann.

Beim Booten SOLLTE die Integrität vom (Pre-)Bootloader bis zum Kernel geprüft werden. Die hierfür genutzten Schlüssel SOLLTEN bei der Ersteinrichtung überprüft werden. Es SOLLTE geprüft werden, ob hierfür Secure Boot als der Teil der UEFI-Spezifikation oder äquivalente Lösungen genutzt werden können.

SYS.2.3.A11 Verhinderung der Überlastung der Festplatte

Es SOLLTEN Quotas für Benutzer bzw. Dienste eingerichtet werden, die ausreichend Freiraum für das Betriebssystem lassen. Generell SOLLTEN unterschiedliche Partitionen für Betriebssystem und Daten genutzt werden. Alternativ SOLLTEN auch Mechanismen des verwendeten Dateisystems genutzt werden, die ab einem geeigneten Füllstand nur noch dem Benutzer root Schreibrechte einräumen.

SYS.2.3.A12 Einsatz von Appliances als Clients

Es SOLLTE sichergestellt werden, dass Appliances ein ähnliches Sicherheitsniveau wie Clients auf Standard-IT-Systemen erfüllen. Es SOLLTE dokumentiert werden, wie entsprechende Sicherheitsanforderungen mit einer eingesetzten Appliance erfüllt werden. Wenn die Anforderungen nicht zweifelsfrei erfüllt werden können, SOLLTE eine Konformitätserklärung vom Hersteller angefordert werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.2.3.A13 Schutz vor unbefugten Anmeldungen (CIA)

Es SOLLTE eine Zwei-Faktor-Authentisierung verwendet werden.

SYS.2.3.A14 Absicherung gegen Nutzung unbefugter Peripheriegeräte (CIA)

Peripheriegeräte SOLLTEN nur nutzbar sein, wenn sie auf einer zentral verwalteten Whitelist geführt sind. Kernelmodule für Peripheriegeräte SOLLTEN nur geladen und aktiviert werden, wenn das Gerät auf der Whitelist steht.

SYS.2.3.A15 Zusätzlicher Schutz vor der Ausführung unerwünschter Dateien (CI)

Partitionen und Verzeichnisse, in denen Benutzer Schreibrechte haben, SOLLTEN so gemountet werden, dass keine Dateien ausgeführt werden können (/noexec).

SYS.2.3.A16 Zusätzliche Absicherung des Bootvorgangs (CIA)

Bootloader und Kernel SOLLTEN durch selbstkontrolliertes Schlüsselmaterial signiert und nicht benötigtes Schlüsselmaterial entfernt werden.

SYS.2.3.A17 Zusätzliche Verhinderung der Ausbreitung bei der Ausnutzung von Schwachstellen (CI)

Die Nutzung von Systemaufrufen SOLLTE insbesondere für exponierte Dienste und Anwendungen auf die unbedingt notwendigen Systemaufrufe beschränkt werden (z B. durch "seccomp"). Die vorhandenen Standardprofile bzw. -Regeln von "SELinux", "AppArmor" sowie alternativen Erweiterungen SOLLTEN manuell überprüft und gegebenenfalls an die eigene Sicherheitsrichtlinie angepasst werden. Falls erforderlich, SOLLTEN neue Regeln bzw. Profile erstellt werden.

SYS.2.3.A18 Zusätzlicher Schutz des Kernels (CI)

Es SOLLTEN mit speziell gehärteten Kernels geeignete Schutzmechanismen wie Speicherschutz, Dateisystemabsicherung und rollenbasierte Zugriffskontrolle, die die Ausnutzung von Schwachstellen und Ausbreitung im Betriebssystem verhindern sollen, genutzt werden (z. B. "grsecurtiy", "PaX").

SYS.2.3.A19 Festplatten- oder Dateiverschlüsselung (CI)

Festplatten oder die hierauf abgespeicherten Dateien SOLLTEN verschlüsselt werden. Die dazugehörigen Schlüssel SOLLTEN NICHT auf dem IT-System gespeichert sein. Es SOLLTE "AEAD" bei der Festplatten- und Dateiverschlüsselung eingesetzt werden. Alternativ SOLLTE "dm-crypt" in Kombination mit "dm-verity" genutzt werden.

SYS.2.3.A20 Abschaltung kritischer SysRq-Funktionen (CIA)

Es SOLLTEN kritische SysRq-Funktionen deaktiviert werden.

4 Weiterführende Informationen

4.1 Literatur

- [ISiClient] Absicherung eines PC-Clients (ISi-Client),
  (zuletzt abgerufen am 27.09.2017)
  https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Isi-Reihe/Isi-Client/client_node.html

- [NISTSP800123] NIST Special Publication 800-123
  Guide to General Server Security, NIST, 07.2008
  https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Clients unter Unix" von Bedeutung.

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.39 Schadprogramme

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.28	G 0.30	G 0.31	G 0.32	G 0.39	G 0.45	G 0.46
SYS.2.3.A1								x	x	x			
SYS.2.3.A2		x	x				x						
SYS.2.3.A3	x			x								x	x
SYS.2.3.A4		x	x			x	x				x		
SYS.2.3.A5		x	x				x				x		
SYS.2.3.A6			x	x	x	x						x	
SYS.2.3.A7	x		x	x				x	x	x			
SYS.2.3.A8	x		x	x				x	x	x			
SYS.2.3.A9			x	x	x			x	x	x		x	x
SYS.2.3.A10			x	x	x	x						x	
SYS.2.3.A11						x						x	x
SYS.2.3.A12	x	x	x	x	x	x	x	x	x	x	x	x	x
SYS.2.3.A13	x		x	x	x			x	x				
SYS.2.3.A14			x	x		x		x					
SYS.2.3.A15			x	x	x								
SYS.2.3.A16			x	x	x	x						x	
SYS.2.3.A17			x					x	x	x			
SYS.2.3.A18			x	x	x			x	x	x	x	x	x
SYS.2.3.A19	x			x	x								x
SYS.2.3.A20						x			x	x			

SYS.3: Mobile Devices

SYS.3.1 Laptops

1 Beschreibung

1.1 Einleitung

Ein Laptop (oder auch Notebook) ist ein PC, der mobil genutzt werden kann. Er hat eine kompakte Bauform, integriert Peripheriegeräte wie Tastatur und Bildschirm, ist über Akkus zeitweise unabhängig von einer externen Stromversorgung und besteht oft aus speziell für den mobilen Einsatz konzipierten Hardware-Komponenten. Laptops können mit allen üblichen Betriebssystemen wie Windows, Apple macOS oder Linux betrieben werden. Die Geräte sind in den meisten Institutionen verbreitet und ersetzen für einige Mitarbeiter den klassischen Desktop-PC.

Da Laptops häufig mobil genutzt werden, sind sie oft nicht permanent am LAN der Institution angeschlossen, sondern können sich in der Regel per Virtual Private Network (VPN) über das Internet oder andere Datennetze einwählen, um so auf die Ressourcen des LANs zuzugreifen. Auch die Infrastruktur einer klassischen Büroumgebung, wie kontrollierbare Umwelteinflüsse, eine stabile Stromversorgung oder zutrittsgeschütze Bereiche, kann für den mobilen Einsatz von Laptops nicht vorausgesetzt werden.

1.2 Zielsetzung

Ziel des Bausteins ist es, einen sicheren Betrieb von Laptops in Institutionen zu ermöglichen sowie für die spezifischen Gefährdungen dieser Geräteklasse zu sensibilisieren.

1.3 Abgrenzung

Um Risiken durch Fehlbedienung oder den absichtlichen Missbrauch der Laptops auszuschließen, ist es notwendig, die Betriebssystem- und Software-Komponenten sorgfältig auszuwählen und zu installieren. Die hier zu erfüllenden Anforderungen sind abhängig vom Betriebssystem des Laptops und werden daher in den Client-spezifischen Bausteinen beschrieben, beispielsweise SYS.2.2.3 *Client unter Windows 10,* SYS 2.3 *Clients unter Unix* oder *SYS.2.4 Clients unter OS X*. Ebenso sind Anforderungen, die für jede Art von Clients gelten, nicht Bestandteil dieses Bausteins, diese sind in SYS.2.1 *Allgemeiner Client* zu finden.

Auch wird nicht behandelt, wie die jeweilige Datenübertragung einzurichten ist, wie z. B. die WLAN-Konfiguration (siehe NET.2.2 *WLAN-Nutzung*) oder die VPN-Anbindung (siehe NET.3.3 Virtual Private Networks (VPN)).

Um Angriffsversuche und missbräuchliche Nutzung erkennen zu können, sind bei Laptops vor allem organisatorische Anforderungen notwendig. Die notwendigen Anforderungen werden im Rahmen der Umsetzung des Bausteins OPS.1.1.2 *Ordnungsgemäße IT-Administration* und daher nicht hier betrachtet.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich *Laptop* von besonderer Bedeutung:

2.1 Beeinträchtigung durch wechselnde Einsatzumgebung

Laptops werden in sehr unterschiedlichen Umgebungen eingesetzt und sind dadurch vielen Gefährdungen ausgesetzt. Dazu gehören beispielsweise schädigende Umwelteinflüsse, wie zu hohe oder zu niedrige Temperaturen, ebenso wie Staub oder Feuchtigkeit. Bei mobilen Geräten besteht auch stets die Gefahr von Transportschäden. Außerdem kommunizieren Laptops vor allem unterwegs oft mit unbekannten IT-Systemen oder Netzen, was immer ein Gefährdungspotenzial für den eigenen Laptop mit sich bringt. So können dabei beispielsweise Schadprogramme mit übertragen oder schützenswerte Informationen kopiert werden.

2.2 Diebstahl

Mitarbeiter benutzen ihre Laptops regelmäßig auch außerhalb der Institution. Die Geräte werden in privaten Kraftfahrzeugen oder öffentlichen Verkehrsmitteln transportiert, in fremden Büroräumen in Pausen zurückgelassen oder in Hotelzimmern unbewacht aufgestellt. Aufgrund dieser Umfeldbedingungen sind Laptops naturgemäß einem höheren Diebstahlrisiko ausgesetzt. Wird ein Laptop gestohlen, entstehen Kosten für die Wiederbeschaffung sowie für die Wiederherstellung eines arbeitsfähigen Zustandes. Ebenso könnten dadurch aber auch Unbefugten schützenswerte Daten offengelegt werden, wodurch es zu weiteren Schäden kommen kann. Diese wiegen in vielen Fällen deutlich schwerer als der rein materielle Verlust des Gerätes.

2.3 Ungeordneter Benutzerwechsel bei Laptops

Wenn Mitarbeiter nur in Ausnahmefällen mobile IT-Systeme benötigen, wie beispielsweise für selten durchgeführte Dienstreisen, ist es oft zweckmäßiger, wenige Laptops für viele Benutzer vorzuhalten, die weitergereicht werden. Wird jedoch bei einem Benutzerwechsel der Laptop einfach an den nächsten Mitarbeiter übergeben, besteht die Gefahr, dass auf dem Gerät noch schutzbedürftige Daten gespeichert sind und dass es mit Schadsoftware verseucht ist. Zudem ist nach einiger Zeit nicht mehr nachvollziehbar, wer den Laptop wann benutzt hat oder wer ihn zurzeit benutzt. Der ungeordnete Benutzerwechsel ohne Speicherkontrollen und ohne entsprechende Dokumentation kann dazu führen, dass der Laptop nur noch eingeschränkt verfügbar ist und Restdaten auf der Festplatte unbefugt ausgelesen werden können.

2.4 Fehler bei der Synchronisation

Wenn Daten lokal auf einem Laptop bearbeitet werden, müssen sie wann immer es geht mit den Dateiservern der Institution synchronisiert werden, z. B. wenn sich der Mitarbeiter wieder über das VPN einloggt. Dabei können die Daten allerdings auch zerstört werden. Im Allgemeinen muss vor einer Synchronisation eingestellt werden, wie mit Konflikten beim Datenabgleich umzugehen ist: ob beispielsweise bei gleichlautenden Dateien die Version auf dem Laptop oder die von einem anderen Mitarbeiter ebenfalls bearbeitete Version auf dem Server ungefragt aktualisiert wird oder ob der Benutzer das entscheiden soll. Das wird häufig einmal konfiguriert und danach oft wieder vergessen. Werden dann aber Daten in einer anderen Reihenfolge geändert als ursprünglich einmal gedacht, gehen dabei schnell wichtige Informationen verloren.

2.5 Datenverlust bei mobilem Einsatz

Bei Laptops ist das Risiko von Datenverlusten höher als bei stationären Systemen. Ursache können Diebstahl oder Geräteverlust sein, aber auch technische Probleme oder schlichter Strommangel. So können zum Beispiel die Daten eines Laptops temporär nicht verfügbar sein, wenn der Akku leer ist. Sie können unter Umständen, wie z. B. bei älteren Geräten, aber auch vollständig vernichtet sein, wenn neben dem Akku auch die eventuell vorhandene Sicherungsbatterie leer ist und damit alle nicht bereits synchronisierten Daten verloren sind.

2.6 Datendiebstahl mithilfe von Laptops

Mit Laptops können sehr leicht Daten mit anderen IT-Systemen ausgetauscht werden, z. B. über WLAN, Bluetooth oder eine Mobilfunkverbindung. Wo ein offener Zugang zu einem Laptop möglich ist, können Angreifer damit Informationen unauffällig abfragen, verändern oder mitnehmen. Eine nachträgliche Überprüfung oder gar ein Nachweis ist nicht immer möglich, da häufig die Zugriffe nicht entsprechend protokolliert werden. Auch können Angreifer in öffentlichen WLANs, die nicht ausreichend abgesichert sind und über die ein Laptop kommuniziert, alle übermittelten Daten mitschneiden und haben so im schlechtesten Fall Zugriff auf die Dateien im Netz der Institution.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen an Laptops aufgeführt. Grundsätzlich ist der *IT-Betrieb* für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Benutzer, Beschaffungsstelle, Leiter IT

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.3.1.A1 Regelungen zur mobilen Nutzung von Laptops

Es MUSS klar geregelt werden, was Mitarbeiter beachten sollen, wenn sie Laptops mitnehmen. Es MUSS insbesondere festgelegt werden, welche Laptops außer Haus mitgenommen werden dürfen, wer sie mitnehmen darf und welche grundlegenden Sicherheitsmaßnahmen dabei zu beachten sind. Die Benutzer MÜSSEN auf die Regelungen hingewiesen werden.

SYS.3.1.A2 Zugriffsschutz am Laptop [Benutzer]

Auf allen Laptops MUSS ein angemessener Zugriffsschutz vorhanden sein, der verhindert, dass das Gerät unberechtigt benutzt werden kann. Es MUSS geprüft werden, ob alle Mitarbeiter sich an die Regeln für den korrekten Umgang mit dem eingerichteten Zugriffsschutz halten.

SYS.3.1.A3 Einsatz von Personal Firewalls

Auf Laptops MUSS eine Personal Firewall aktiv sein. Die Filterregeln der Firewall MÜSSEN so restriktiv wie möglich sein. Sie MÜSSEN regelmäßig getestet werden. Die Personal Firewall MUSS so konfiguriert werden, dass die Benutzer nicht durch Warnmeldungen belästigt werden, die sie nicht interpretieren können.

SYS.3.1.A4 Einsatz von Antivirenprogrammen [Benutzer]

Abhängig vom installierten Betriebssystem und anderer vorhandener Schutzmechanismen MUSS auf allen Laptops der Institution ein Antivirenprogramm installiert und aktiviert sein. Es MUSS sichergestellt werden, dass sowohl das Scan-Programm als auch die Signaturen stets auf dem aktuellsten Stand sind. Die Benutzer MÜSSEN mit der Antivirensoftware vertraut gemacht werden, besonders auch mit On-Demand-Scans.

Der gesamte Datenbestand der Laptops MUSS regelmäßig auf Schadprogramme geprüft werden. Wenn der Rechner infiziert ist, MUSS im Offlinebetrieb untersucht werden, ob das gefundene Schadprogramm bereits vertrauliche Daten gesammelt, Schutzfunktionen deaktiviert oder Code aus dem Internet nachgeladen hat.

Das Antivirenprogramm MUSS zudem nach Schadsoftware suchen, wenn Dateien ausgetauscht oder übertragen werden. Auch MÜSSEN alle auf dem Laptop benutzten Internet-Dienste (HTTP, FTP) sowie verschlüsselte Daten ausreichend vor Schadprogrammen geschützt werden.

Außerdem MUSS sichergestellt werden, dass die Benutzer keine sicherheitsrelevanten Änderungen an den Einstellungen der Antivirenprogramme vornehmen können.

SYS.3.1.A5 Datensicherung [Benutzer]

Alle Daten, die auf Laptops lokal gespeichert werden, MÜSSEN regelmäßig gesichert werden. Hierfür MÜSSEN abhängig vom Volumen des Datenbestands geeignete Verfahren zur Datensicherung ausgewählt werden. Die Datensicherung MUSS weitgehend automatisiert werden, sodass die Benutzer möglichst wenig Aktionen selbst durchführen müssen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Laptops . Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.3.1.A6 Sicherheitsrichtlinien für Laptops [Leiter IT]

Für Laptops SOLLTE eine Sicherheitsrichtlinie erstellt werden, die regelt, wie die Geräte benutzt werden dürfen. Die Benutzer SOLLTEN hinsichtlich des Schutzbedarfs von Laptops und der auf ihnen befindlichen Daten sensibilisiert werden. Auch SOLLTEN sie auf die spezifischen Gefährdungen bzw. die entsprechenden Anforderungen für die Nutzung aufmerksam gemacht werden. Sie SOLLTEN außerdem darüber informiert werden, welche Art von Informationen sie auf Laptops verarbeiten dürfen.

SYS.3.1.A7 Geregelte Übergabe und Rücknahme eines Laptops [Benutzer]

Wenn Laptops von verschiedenen Personen abwechselnd genutzt werden, SOLLTE geregelt werden, wie Laptops sicher an Mitarbeiter übergeben werden können bzw. wie sie wieder sicher zurückzunehmen sind. Beim Benutzerwechsel eines Laptops SOLLTEN eventuell vorhandene schützenswerte Daten sicher gelöscht werden. Falls der Laptop nach dem Benutzerwechsel nicht neu aufgesetzt wird, SOLLTE sichergestellt sein, dass sich auf dem System bzw. allen damit verbundenen Datenträgern keine Schadsoftware befindet. Mit einem Laptop SOLLTE den Mitarbeitern ein Merkblatt für den sicheren Umgang mit dem Gerät ausgehändigt werden.

SYS.3.1.A8 Sicherer Anschluss von Laptops an Datennetze [Benutzer]

Es SOLLTE geregelt werden, wie Laptops sicher an eigene oder fremde Netze und an das Internet angeschlossen werden. Laptops SOLLTEN wirksam vor Schadcode und vor Angriffen aus Fremdnetzen und aus dem Internet geschützt werden. Dafür SOLLTEN das Betriebssystem und die installierte Software von Laptops immer auf dem aktuellen Stand sein. Es SOLLTEN sich nur zugelassene Laptops am internen Netz der Institution anmelden können. Nicht benötigte Schnittstellen SOLLTEN bei allen Laptops deaktiviert werden.

SYS.3.1.A9 Sicherer Fernzugriff von unterwegs [Benutzer]

Daten, die zwischen einem Laptop von außerhalb und dem internen Netz der Institution übertragen werden, SOLLTEN durch geeignete Maßnahmen ausreichend geschützt werden, zum Beispiel durch ein VPN oder mit TLS. Auch SOLLTE der Laptop selbst abgesichert sein, wenn Daten mit anderen IT-Systemen ausgetauscht werden.

SYS.3.1.A10 Abgleich der Datenbestände von Laptops [Benutzer]

Es SOLLTE geregelt werden, wie Daten von Laptops in den Informationsverbund der Institution übernommen werden. Wenn ein Synchronisationstool benutzt wird, SOLLTE sichergestellt sein, dass Synchronisationskonflikte aufgelöst werden können, der Synchronisationsvorgang protokolliert wird und die Benutzer angewiesen sind, die Synchronisationsprotokolle zu prüfen.

SYS.3.1.A11 Sicherstellung der Energieversorgung [Benutzer]

Alle Benutzer SOLLTEN darüber informiert werden, wie sie die Energieversorgung von Laptops im mobilen Einsatz optimal sicherstellen können. Falls für die Laptops Ersatzakkus verfügbar sind, SOLLTEN diese in entsprechenden Hüllen gelagert und transportiert werden.

SYS.3.1.A12 Verlustmeldung [Benutzer]

Es SOLLTE umgehend gemeldet werden, wenn ein Laptop verloren gegangen ist oder gestohlen wurde. Dafür SOLLTE es in jeder Institution klare Meldewege geben. Wenn verlorene Laptops wieder auftauchen, SOLLTE untersucht werden, ob sie eventuell manipuliert wurden. Sie SOLLTEN komplett neu installiert werden.

SYS.3.1.A13 Verschlüsselung von Laptops

Die Festplatten eines Laptops SOLLTEN verschlüsselt werden. Für die Verschlüsselung SOLLTE ein sicherer Verschlüsselungsalgorithmus eingesetzt werden. Die Schlüssel SOLLTEN zufällig erzeugt und Daten und Schlüssel getrennt aufbewahrt werden.

SYS.3.1.A14 Geeignete Aufbewahrung von Laptops [Benutzer]

Alle Benutzer SOLLTEN darauf hingewiesen werden, wie Laptops außerhalb der Institution geeignet aufbewahrt werden sollen. Auch in den Räumen der Institution SOLLTEN Laptops außerhalb der Nutzungszeiten gegen Diebstahl gesichert bzw. verschlossen aufbewahrt werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.3.1.A15 Geeignete Auswahl von Laptops [Beschaffungsstelle] (A)

Bevor Laptops beschafft werden, SOLLTEN die Verantwortlichen eine Anforderungsanalyse durchführen. Sie SOLLTE auch auf zusätzlich benötigte Hardware, wie z. B. Dockingstations und Monitore, erweitert werden. Anhand der Ergebnisse SOLLTEN alle infrage kommenden Geräte bewertet werden. Die Beschaffungsentscheidung SOLLTE mit den Administratoren und dem technischen Personal abgestimmt sein.

SYS.3.1.A16 Zentrale Administration von Laptops (CI)

Es SOLLTE eine geeignete Vorgehensweise definiert werden, wie Laptops zentral zu administrieren sind, da sich so nicht nur Software und Informationen einfacher verteilen lassen, sondern auch die institutionsseigenen Sicherheitsrichtlinien besser durchgesetzt werden können. Deswegen SOLLTE eine geeignete Vorgehensweise definiert werden, wie Laptops zentral zu administrieren sind. Ein Tool zum zentralen Laptop-Management SOLLTE möglichst alle eingesetzten Betriebssysteme unterstützen.

SYS.3.1.A17 Sammelaufbewahrung (A)

Nicht benutzte Laptops SOLLTEN in einem geeignet abgesicherten Raum vorgehalten werden. Der dafür genutzte Raum SOLLTE den Anforderungen aus *INF.5 Technikraum* entsprechen.

SYS.3.1.A18 Einsatz von Diebstahl-Sicherungen (CIA)

Es SOLLTE geregelt werden, welche Diebstahlsicherungen für Laptops eingesetzt werden sollen. Bei mechanischen Sicherungen SOLLTE besonders auf ein gutes Schloss geachtet werden.

4 Weiterführende Informationen

4.1 Literatur

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Laptops " von Bedeutung.

G 0.04 Verschmutzung, Staub, Korrosion

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.39 Schadprogramme

G 0.45 Datenverlust

Elementare Gefährdungen / Anforderungen	G 0.04	G 0.14	G 0.16	G 0.17	G 0.19	G 0.22	G 0.39	G 0.45
SYS.3.1.A1	x	x	x	x	x	x	x	x
SYS.3.1.A2		x			x	x		
SYS.3.1.A3		x			x		x	
SYS.3.1.A4		x			x			
SYS.3.1.A5				x				x
SYS.3.1.A6	x	x	x	x	x	x	x	x
SYS.3.1.A7		x			x			
SYS.3.1.A8		x			x		x	
SYS.3.1.A9		x			x		x	
SYS.3.1.A10								x
SYS.3.1.A11								x
SYS.3.1.A12		x			x			
SYS.3.1.A13		x			x	x		
SYS.3.1.A14	x	x	x	x	x	x		
SYS.3.1.A15			x		x			
SYS.3.1.A16							x	
SYS.3.1.A17	x			x				
SYS.3.1.A18			x	x	x			

SYS.3.2: Tablet und Smartphone

SYS.3.2.1 Allgemeine Smartphones und Tablets

1 Beschreibung

1.1 Einleitung

Smartphones sind mobile Telefone, die mit einem großen, üblicherweise berührungsempfindlichen Display ausgestattet sind. Smartphones vereinen oft Mobiltelefone, Media-Player, Personal Information Manager und Digitalkamera in einem Gerät und bieten den Benutzern verschiedene Anwendungen und Funktionen, wie z. B. Web-Browser, E-Mail-Client oder GPS. Zudem sind sie mit Mobilfunk-, WLAN- und Bluetooth-Schnittstellen ausgestattet. Tablets sind, vereinfacht gesagt, Smartphones mit großem Formfaktor, mit denen oft nicht über das Mobilfunknetz telefoniert werden kann. Als Phablets werden Hybridgeräte aus Smartphone und Tablet bezeichnet, sie werden im Baustein nicht gesondert hervorgehoben.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, den Verantwortlichen des Sicherheitsmanagements und des IT-Betriebs Informationen zu den typischen Gefährdungen für Smartphones und Tablets zu geben. Außerdem sollen den Verantwortlichen Ansätze gezeigt werden, um schutzbedarfsgerechte Konfigurationsprofile zu erstellen. Diese Konfigurationsprofile können über eine zentrale Infrastruktur zum "Mobile Device Management" (MDM) verteilt und verwaltet werden. Es kann jedoch bei der Vielzahl von unterschiedlichen Betriebssystemen nicht grundsätzlich vorausgesetzt werden, dass die Geräte in ein solches MDM eingebunden sind.

1.3 Abgrenzung

Dieser Baustein geht nicht darauf ein, wie spezifische Betriebssysteme von Smartphones und Tablets abgesichert werden, da dies detailliert in den Bausteinen für die jeweiligen Systeme beschrieben wird, z. B. SYS.3.2.3 iOS (for Enterprise) oder SYS.3.2.4 Android. Sicherheitsanforderungen für den Betrieb eines MDM werden in SYS.3.2.2 Mobile Device Management beschrieben.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Smartphone und Tablet von besonderer Bedeutung:

2.1 Verlust des mobilen Geräts

Da mobile Endgeräte oft klein sind und ständig transportiert werden, können sie leicht vergessen, verloren gehen oder gestohlen werden. Neben dem wirtschaftlichen Schaden wiegt der Verlust der Vertraulichkeit und Integrität der enthaltenen Daten besonders schwer. Über ein entwendetes mobiles Endgerät könnte ein Angreifer auf vertrauliche Informationen oder IT-Ressourcen der Institution zugreifen.

2.2 Fehlende Betriebssystems-Updates

Es erscheinen regelmäßig neue Versionen von mobilen Betriebssystemen sowie Updates. Die Updates und Versionen müssen bei Geräten, die herstellerspezifische Erweiterungen des Betriebssystems haben, erst von den Herstellern in ihre Version integriert und dann verteilt werden. Diese Updates werden in der Regel für die neueste Gerätegeneration und für eine Reihe von älteren Gerätegenerationen bereitgestellt. Allerdings werden nicht alle zurückliegenden Betriebssystem-Versionen im gleichen Umfang mit Updates und Sicherheitsupdates versorgt, teilweise werden Betriebssysteme auch aus wirtschaftlichen Gründen nicht weiterentwickelt. Nachträglich bekannt gewordene Schwachstellen im Betriebssystem einer bereits abgekündigten Gerätegeneration werden dann nicht mehr mit Updates versorgt und nicht mehr geschlossen.

2.3 Software-Schwachstellen in Anwendungen (Apps)

Anwendungen (Apps) können Schwachstellen enthalten, die für lokale Angriffe oder für Angriffe über Netzverbindungen ausgenutzt werden können. Außerdem werden viele Apps nach einiger Zeit von Dritt-Entwicklern nicht mehr weiter gepflegt. Erkannte Sicherheitsmängel können dann nicht durch entsprechende Updates behoben werden.

2.4 Manipulation

Ein Angreifer kann sich Zugang zu den Geräten verschaffen, um gezielt Dateien zu manipulieren. Er könnte beispielsweise die Konfiguration ändern, zusätzliche Dienste starten oder Schadsoftware installieren. Dadurch kann ein Angreifer auf dem manipulierten System beispielsweise die Kommunikationsverbindungen mitschneiden (ungewollter Datenabfluss) oder die Regeln nach seinen Bedürfnissen ändern (z. B. Zugriffe aus dem Internet auf das Intranet erlauben).

2.5 Malware

Wie jedes mit dem Internet verbundene Gerät sind auch mobile Endgräte von Schadsoftware bedroht. Das Infektionsrisiko ist verglichen mit PC-Betriebssystemen noch geringer, jedoch konzentrieren sich die Cyberkriminellen immer mehr auf diese Geräte. Wird ein Gerät infiziert, können Angreifer beispielsweise Daten auslesen, verändern oder löschen.

2.6 Webbasierte Angriffe auf mobile Browser

Auch Browser auf mobilen Endgeräten können vollständige Webseiten und Webinhalte anzeigen. Dadurch können die Geräte von Phishing-Angriffen, Drive-by-Exploits und anderen webbasierten Angriffsformen betroffen sein.

2.7 Missbrauch von Fitness- oder Ortungsdaten

Das Betriebssystem vieler Geräte enthält meist spezielle Funktionen, um Fitness- und Ortungsdaten zu verwalten. Diese oft personenbezogene Daten sind besonders sensibel und stellen ein attraktives Angriffsziel dar, insbesondere wenn sie über einen längeren Zeitraum gesammelt und gespeichert werden, insofern diese Funktionen durch den Benutzer aktiviert wurden.

In der Folge ist der Standort des Mitarbeiters durch einen Angriff auf das Gerät oder die Cloud-ID des Mitarbeiters erkennbar. Das kann neben den datenschutzrechtlichen Auswirkungen auch andere Angriffe auf den Mitarbeiter nach sich ziehen.

2.8 Missbrauch sensitiver Daten im Sperrbildschirm

Viele mobile Betriebssysteme verfügen über eine Funktion, um Mitteilungen von aktivierten Widgets und Push-Nachrichten auf dem Sperrbildschirm anzeigen zu lassen. Hierdurch können sensitive Informationen des Benutzers ungeschützt auf dem Sperrbildschirm unberechtigten Dritten preisgegeben und ausgenutzt werden.

2.9 Gefahren durch private Nutzung mobiler Geräte

Wenn Mitarbeitern firmeneigene Smartphones, Tablets und Phablets ausgehändigt werden, könnten sie die Geräte auch unerlaubt privat benutzen. Dadurch entstehen gleich mehrere Probleme für die Informationssicherheit der Institution. So könnte sich ein Benutzer selbstständig Apps installieren, die jedoch Schadfunktionen enthalten oder er besucht eine Webseite, die das Gerät mit Malware infiziert. Ebenso sind viele vom Benutzer privat installierte Apps ein Risiko für die auf dem Gerät gespeicherten Informationen der Institution, da sie z. B. Adressbücher zu unbekannten Servern übertragen oder direkt auf E-Mails oder Dokumente zugreifen. So können Daten abfließen oder umgekehrt unkontrolliert in die Institution gelangen. Bekannte Beispiele dafür sind Social-Media- und Chat-Apps.

2.10 Gefahren durch Bring Your Own Device (BYOD)

Werden private Endgeräte dienstlich genutzt, können beispielsweise bezüglich der Software-Lizenzen zu rechtlichen Problemen auftreten. Auch wenn im Notfall alle Daten durch das MDM auf dem Gerät gelöscht werden müssen, könnte der Benutzer damit nicht einverstanden sein.

Oft können die IT-Verantwortlichen nicht mehr jedes einzelne vom Mitarbeiter mitgebrachte Gerät daraufhin prüfen, ob es sich auch dienstlich einsetzen lässt. Dadurch können ungeeignete Geräte verwendet und so gegen interne Datenschutz- und Sicherheitsanforderungen verstoßen werden. Zudem sind die Benutzer oft selbst dafür verantwortlich, ihre Geräte zu warten und reparieren zu lassen. Bei einer solchen Reparatur könnten beispielsweise Firmendaten unbefugt eingesehen werden. Falls nicht geregelt ist, was mit den Daten auf dem Gerät geschehen soll, wenn der Mitarbeiter aus dem Unternehmen ausscheidet, könnten diese missbraucht werden.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Smartphone und Tablet aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Benutzer, Fachverantwortliche

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.3.2.1.A1 Festlegung einer Strategie für Smartphones und Tablets

Bevor eine Institution Smartphones oder Tablets bereitstellt, betreibt oder einsetzt, MUSS die generelle Strategie im Hinblick auf die Nutzung und Kontrolle der Geräte festgelegt werden. Hierbei MUSS unter anderem festgelegt werden, wer auf welche Informationen der Institution zugreifen darf.

SYS.3.2.1.A2 Festlegung einer Strategie für den Cloud-Einsatz

Die Institution MUSS für mobile Endgeräte eine generelle Strategie für die Cloud-Nutzung und Informationskontrolle sowie für den Schutz der Informationen festlegen. Der Zugriff und die Nutzung von Cloud-Diensten für Informationen der Institution MUSS geklärt und festgelegt werden. Die Benutzer MÜSSEN regelmäßig über den Einsatz von Cloud-Diensten geschult werden.

SYS.3.2.1.A3 Sichere Grundkonfiguration für mobile Geräte

Alle mobilen Endgeräte MÜSSEN so konfiguriert sein, dass sie den erforderlichen Schutzbedarf angemessen erfüllen. Dafür MUSS eine passende Grundkonfiguration zusammengestellt und dokumentiert werden. Wenn eine Institution ein MDM einsetzt, MUSS bei der Übergabe des mobilen Endgerätes bereits der MDM-Client installiert sein.

SYS.3.2.1.A4 Verwendung eines Zugriffschutzes [Benutzer]

Es MÜSSEN alle Smartphones und Tablets mit einem Gerätesperrcode geschützt werden. Die Nutzung der Bildschirmsperre MUSS vorgeschrieben werden. Die Anzeige von vertraulichen Informationen auf dem Sperrbildschirm MUSS deaktiviert sein. Alle mobilen Geräte MÜSSEN nach wenigen Minuten selbsttätig den Bildschirm sperren. Die Zeitdauer MUSS in Abhängigkeit zum Schutzbedarf stehen.

Nach mehreren fehlgeschlagenen Versuchen den Bildschirm zu entsperren, MUSS sich das mobile Gerät in den Werkszustand zurücksetzen. Es SOLLTEN sich dabei die Daten oder die Verschlüsselungsschlüssel sicher vernichten.

Es SOLLTE vermieden werden, dass die Benutzer bei einem Passwortwechsel vor kurzem verwendete Kennworte nutzen. Die Anzahl der Kennworte, nachdem sich ein Passwort wiederholen darf, SOLLTE festgelegt werden.

Es SOLLTE ein komplexes Gerätepasswort verwendet werden.

SYS.3.2.1.A5 Automatische Updates von Betriebssystem und Apps

Es MUSS ein Prozess für automatische Updates des Betriebssystems und der eingesetzten Apps etabliert sein. Die Aktualisierungen MÜSSEN getestet werden. Nach der Freigabe MÜSSEN die Aktualisierungen zeitnah ausgerollt werden. Bereits bei der Auswahl von zu beschaffenden mobilen Geräten MUSS die Institution darauf achten, dass der Hersteller über den geplanten Nutzungszeitraum Updates für die Geräte bereitstellt. Ältere Geräte, für die keine aktuellen Versionen mehr bereitgestellt werden, MÜSSEN ausgesondert und durch vom Hersteller unterstützte Geräte ersetzt werden.

SYS.3.2.1.A6 Datenschutzeinstellungen

Der Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen MUSS angemessen eingeschränkt werden. Die Datenschutzeinstellungen MÜSSEN so restriktiv wie möglich konfiguriert werden. Insbesondere der Zugriff auf Kamera, Mikrofon und Geodaten MÜSSEN auf Konformität mit den organisationsinternen Datenschutz- und Sicherheitsvorgaben überprüft und restriktiv konfiguriert bzw. deaktiviert werden.

SYS.3.2.1.A7 Verhaltensregeln bei Sicherheitsvorfällen [Fachverantwortliche, Benutzer]

Generell MÜSSEN alle Sicherheitsvorfälle gemeldet und behandelt werden. Gehen Geräte verloren oder werden unberechtigt Änderungen an Gerät und Software festgestellt, MÜSSEN die Verantwortlichen sofort geeignete Gegenmaßnahmen einleiten.

Die möglichen Konsequenzen sicherheitskritischer Ereignisse MÜSSEN untersucht werden. Letztlich MÜSSEN alle erforderlichen Maßnahmen ergriffen werden, um auszuschließen, dass auf vertrauliche und geschäftskritische Informationen der Institution zugegriffen werden kann.

SYS.3.2.1.A8 Keine Installation von Apps aus unsicheren Quellen

Es MUSS unterbunden werden, dass sich Apps aus alternativen Märkten oder aus dem Dateisystem installieren lassen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Allgemeine Smartphones und Tablets. Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.3.2.1.A9 Nutzung von funktionalen Erweiterungen

Funktionalen Erweiterungen SOLLTEN nur restriktiv genutzt werden. Wenn möglich, SOLLTE auf funktionalen Erweiterungen verzichtet werden. Die funktionalen Erweiterungen SOLLTEN keinen automatischen Zugriff auf schützenswerte Informationen haben. Sie SOLLTEN die festgelegte Grundkonfiguration nicht umgehen oder ändern können.

SYS.3.2.1.A10 Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten [Benutzer]

Es SOLLTE eine verbindliche Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten erstellt werden. Diese SOLLTE festlegen, wie mobile Geräte genutzt und gepflegt werden sollen. Darin SOLLTEN die Themen Aufbewahrung und Verlustmeldung behandelt werden. Außerdem SOLLTE klar verboten werden, Verwaltungssoftware zu deinstallieren oder das Gerät zu rooten.

SYS.3.2.1.A11 Verschlüsselung des Dateisystems

Der gesamte Speicher des mobilen Geräts SOLLTE verschlüsselt werden. Auch eventuell vorhandene SD-Karten SOLLTEN verschlüsselt werden.

SYS.3.2.1.A12 Verwendung nicht personalisierter Gerätenamen

Der Gerätename SOLLTE keine Hinweise auf die Institution oder den Benutzer enthalten.

SYS.3.2.1.A13 Regelungen zum Screensharing und Casting

Es SOLLTE entschieden werden, ob Screensharing oder Casting eingesetzt werden soll. Screensharing und Casting SOLLTEN organisatorisch oder technisch eingeschränkt werden. Hierzu SOLLTE eine entsprechende Vereinbarung mit den Benutzern getroffen werden.

SYS.3.2.1.A14 Schutz vor Phishing und Schadprogrammen im Browser

Alle mobilen Endgeräte SOLLTEN vor Schadprogrammen geschützt werden. Im verwendeten Browser SOLLTE "Safe Browsing" bzw. die Funktion zur Warnung vor schädlichen Inhalten aktiviert werden.

SYS.3.2.1.A15 Deaktivierung von Download-Boostern

Download-Booster, die Daten über die Server des Herstellers leiten, SOLLTEN deaktiviert werden.

SYS.3.2.1.A16 Deaktivierung nicht benutzter Kommunikationsschnittstellen [Benutzer]

Nicht benutzte Kommunikationsschnittstellen SOLLTEN deaktiviert werden. Notwendige Schnittstellen SOLLTEN nur in geeigneten Umgebungen aktiviert sein.

SYS.3.2.1.A17 Verwendung der SIM-Karten-PIN

Die Nutzung der SIM-Karte der Institution SOLLTE durch eine PIN geschützt werden. Die Super-PIN / PUK SOLLTE nur im Rahmen der definierten Prozesse von den Verantwortlichen benutzt werden.

SYS.3.2.1.A18 Verwendung eines Fingerabdrucksensors

Wenn ein biometrischer Fingerabdrucksensor genutzt werden soll, SOLLTE geprüft werden, ob ein ähnlicher oder höherer Schutz als mit einem Gerätepasswort erzielt werden kann. Im Zweifelsfall oder bei einem schlechteren Schutz SOLLTE ein biometrischer Fingerabdrucksensor NICHT genutzt werden. Die Benutzer SOLLTEN hinsichtlich der Fälschbarkeit von Fingerabdrücken sensibilisiert werden.

SYS.3.2.1.A19 Verwendung eines Sprachassistenten

Sprachassistenten SOLLTEN nur eingesetzt werden, wenn die Funktion notwendig ist. Ansonsten SOLLTEN sie deaktiviert werden. Generell SOLLTE ein Sprachassistent nicht genutzt werden können, wenn das Gerät gesperrt ist.

SYS.3.2.1.A20 Auswahl und Freigabe von Apps

Apps aus öffentlichen App-Stores SOLLTEN durch die Verantwortlichen geprüft und freigegeben werden. Dazu SOLLTE ein Freigabeprozess entwickelt werden, in dem auch geeignete Bewertungskriterien definiert sind. Alle freigegebenen Apps SOLLTEN intern in einem Standardkatalog veröffentlicht werden.

SYS.3.2.1.A21 Definition der erlaubten Informationen und Applikationen auf mobilen Geräten [Fachverantwortliche, Benutzer]

Die Institution SOLLTE festlegen, welche Informationen auf den mobilen Endgeräten verarbeitet werden dürfen. Grundlage für die Regelung SOLLTEN einerseits die Klassifikation der Institutionsdaten sein und andererseits die Bedingungen, unter denen die Daten auf den Geräten verarbeitet werden.

Die Benutzer der mobilen Endgeräte SOLLTEN nur freigegebene und geprüfte Apps aus als sicher klassifizierte Quellen installieren dürfen.

SYS.3.2.1.A22 Einbindung der Geräte in die interne Infrastruktur via VPN

Mobile Endgeräte SOLLTEN nur mittels eines VPNs in die Infrastruktur der Institution integriert werden. Hierzu SOLLTE ein geeignetes Verfahren ausgewählt und eingesetzt werden. Die Authentisierung SOLLTE bevorzugt durch Zertifikate statt durch den Einsatz klassischer Passworte implementiert und betrieben werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.3.2.1.A23 Zusätzliches Passwort für vertrauliche Anwendungen (CI)

Alle Anwendungen mit vertraulichen Daten SOLLTEN durch ein zusätzliches Passwort geschützt werden.

SYS.3.2.1.A24 Einsatz einer geschlossenen Benutzergruppe (CI)

Das Passwort für den Zugangspunkt (Access Point Name, APN) einer geschlossenen Benutzergruppe SOLLTE komplex sein. Die Authentisierung SOLLTE das CHAP-Protokoll nutzen.

SYS.3.2.1.A25 Nutzung von getrennten Arbeitsumgebungen (CI)

Es SOLLTEN Lösungen für getrennte Arbeitsumgebungen eingesetzt werden. Hierfür SOLLTEN nur zertifizierte Produkte beschafft werden. Die Arbeitsdaten SOLLTEN in der dienstlichen Umgebung verbleiben.

SYS.3.2.1.A26 Nutzung von PIM-Containern (CIA)

Information auf den mobilen Endgeräten SOLLTEN gekapselt werden, zum Beispiel in einem PIM-Container. Zusätzlich SOLLTEN die Daten durch ein Passwort und eine vom Betriebssystem unabhängige Verschlüsselung abgesichert werden.

SYS.3.2.1.A27 Einsatz abgesicherter Betriebssysteme (CIA)

Institution SOLLTEN ein Gerät einsetzen, das für die Verarbeitung von Informationen nach gesetzlichen Informationsschutz-Klassifizierungen zertifiziert ist.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [BSICS052] Mobile Device Management BSI-CS 052
  BSI, Version 1.00, 03.2013
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_052.pdf

- [ISF] The Standard of Good Practice
  Information Security Forum (ISF), 06.2016

- [NIST18001D] SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES
  SPECIAL PUBLICATION 1800-1d, NIST, 07.2015
  https://nccoe.nist.gov/sites/default/files/nccoe/NIST_SP1800-1d_Draft_HIT_Mobile-StandardsControls.pdf

- [NIST800124] Guidelines for Managing the Security of Mobile Devices in the Enterprise
  Special Publication 800-124 Revision 1, NIST, 06.2013
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

- [NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations
  Special Publication 800-53, Revision 4, NIST, 04.2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

- [TR02102] Kryptographische Verfahren- Empfehlungen und Schlüssellängen
  BSI, (zuletzt abgerufen am 27.09.2017)
  https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Allgemeine Smartphones und Tablets" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.38 Missbrauch personenbezogener Daten

G 0.39 Schadprogramme

G 0.42 Social Engineering

G 0.43 Einspielen von Nachrichten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.14	G 0.15	G 0.16	G 0.17	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.24	G 0.25	G 0.26	G 0.28	G 0.29	G 0.30	G 0.31	G 0.32	G 0.36	G 0.37	G 0.38	G 0.39	G 0.42	G 0.43	G 0.45	G 0.46
SYS.3.2.1.A1		x			x	x						x	x			x	x								x	x
SYS.3.2.1.A2	x				x	x			x	x	x					x	x	x	x	x	x		x		x	x
SYS.3.2.1.A3	x	x	x	x		x		x	x	x	x					x	x					x	x		x	x
SYS.3.2.1.A4			x	x		x				x	x					x	x	x	x	x	x		x		x	x
SYS.3.2.1.A5	x	x	x	x		x	x	x	x	x	x	x		x								x			x	x
SYS.3.2.1.A6	x	x				x			x	x	x											x	x		x	x
SYS.3.2.1.A7	x	x	x	x	x				x															x	x	x
SYS.3.2.1.A8																						x				
SYS.3.2.1.A9	x	x				x			x	x	x		x												x	x
SYS.3.2.1.A10			x													x										
SYS.3.2.1.A11	x	x						x							x											x
SYS.3.2.1.A12	x																									x
SYS.3.2.1.A13	x												x													x
SYS.3.2.1.A14																						x				
SYS.3.2.1.A15	x																									x
SYS.3.2.1.A16																										
SYS.3.2.1.A17			x	x																						
SYS.3.2.1.A18																										
SYS.3.2.1.A19	x		x	x		x										x	x	x	x	x	x					x
SYS.3.2.1.A20	x	x				x		x	x	x	x					x	x	x	x	x	x		x		x	x
SYS.3.2.1.A21	x	x				x	x	x	x	x	x	x		x								x		x	x	x
SYS.3.2.1.A22	x	x	x	x		x			x																x	x
SYS.3.2.1.A23	x	x				x			x	x	x											x		x	x	x
SYS.3.2.1.A24																										x
SYS.3.2.1.A25	x	x	x	x		x		x	x	x	x											x		x	x	x
SYS.3.2.1.A26	x	x	x	x		x			x	x	x											x		x	x	x
SYS.3.2.1.A27	x	x	x	x		x		x	x	x	x				x	x						x		x	x	x

SYS.3.2: Tablet und Smartphone

SYS.3.2.2 Mobile Device Management (MDM)

1 Beschreibung

1.1 Einleitung

Smartphones, Tablets und Phablets sind für viele Mitarbeiter ein nicht mehr wegzudenkender Teil ihrer Arbeit. Die IT-Abteilungen müssen jedoch immer mehr solcher Geräte in vielen unterschiedlichen Ausführungen bereitstellen und dabei gleichzeitig für eine angemessene Sicherheit sorgen. Hinzu kommt, dass mobile Endgeräte (Mobile Devices) besonderen Gefahren ausgesetzt sind und die Administration sich in grundlegenden Punkten von anderen IT-Systemen unterscheidet.

Deswegen ist ein Mobile Device Management (MDM) besonders in Institutionen mit einer größeren Anzahl von Smartphones, Tablets und Phablets unabdingbar für einen geregelten und sicheren Betrieb dieser Geräte. Mit einer solchen Software können die Endgeräte zentral verwaltet werden, es lassen sich Sicherheitsregeln durchsetzen und es können Notfallaktionen ausgelöst werden. Ein MDM gewährleistet somit auf allen Geräten einen gleichen oder zumindest vergleichbaren Sicherheitsstandard.

1.2 Zielsetzung

Der Baustein zeigt auf, wie mit einem MDM mobile Endgeräte sicher von Institutionen genutzt und wie das MDM selber sicher betrieben werden kann.

1.3 Abgrenzung

Mobile Endgeräte (Mobile Devices) im Sinne dieses Bausteins sind Smartphones, Tablets und Phablets, auf denen mobile Betriebssysteme wie Android, iOS, Windows Phone sowie BlackBerry OS installiert sind. Die Sicherheitsanforderungen von Notebooks und Tablets mit Desktop-Betriebssystemen werden in anderen Bausteinen beschrieben. Auch geht dieser Baustein nicht darauf ein, wie die Smartphones, Tablets und Phablets verschiedener Hersteller spezifisch abgesichert werden, da dies detailliert in den Bausteinen für die jeweiligen Betriebssysteme beschrieben wird, z. B. SYS.3.2.3 *iOS (for Enterprise)* oder SYS.3.2.4 *Android*.

2 Gefährdungslage

Die folgenden spezifischen Bedrohungen und Schwachstellen sind im Bereich Mobile Device Management (MDM) von besonderer Bedeutung.

2.1 Verlust des Endgeräts

Da mobile Endgeräte oft klein sind und ständig transportiert werden, werden sie leicht vergessen, gehen verloren oder werden gestohlen. Neben dem wirtschaftlichen Schaden wiegt der Verlust der Vertraulichkeit und Integrität der enthaltenen Daten besonders schwer. Es besteht zudem die Gefahr, dass Angreifer über ein entwendetes mobiles Endgerät auf interne IT-Ressourcen der Institution zugreifen können.

2.2 Gefahr durch Schadsoftware

Wie jedes mit dem Internet verbundene Gerät sind auch mobile Endgeräte von Schadsoftware bedroht. Das Infektionsrisiko ist verglichen mit PC-Betriebssystemen derzeit noch geringer, jedoch konzentrieren sich Cyberkriminelle immer mehr auf diese Geräte. Wird ein Gerät infiziert, können Angreifer beispielsweise Daten auslesen, verändern oder löschen oder Zugriff auf interne IT-Ressourcen der Institution erlangen.

2.3 Gefahren durch private Nutzung mobiler Endgeräte

Wenn Mitarbeiter firmeneigene Smartphones, Tablets und Phablets ausgehändigt bekommen, besteht immer die Gefahr, dass sie die Geräte auch unerlaubt privat benutzen. Dadurch entstehen gleich mehrere Probleme für die Informationssicherheit der Institution. So könnten sich Benutzer selbstständig Apps installieren, die Schadfunktionen enthalten, oder Webseiten besuchen, die das Gerät mit Malware infizieren können. Ebenso können vom Benutzer privat installierte Apps ein Risiko für die auf dem Gerät gespeicherten Informationen der Institution sein, wenn sie z. B. direkt auf Kontakte, Kalender, E-Mails oder Dokumente zugreifen können. So können Daten abfließen oder umgekehrt unkontrolliert in die Institution gelangen. Bekannte Beispiele sind dafür sind Social-Media- und Instant-Messaging-Apps.

2.4 Nicht ausreichende Synchronisation mit dem MDM

Damit das MDM die von den Verantwortlichen definierten Regelungen auf den mobilen Endgeräten durchsetzen kann, müssen die Geräte regelmäßig mit dem MDM synchronisiert werden. Wenn ein Gerät über einen längeren Zeitraum nicht mit dem MDM verbunden ist, können beispielsweise neue oder aktualisierte Regelungen nicht aufgespielt werden. Auch können, wenn zu einem verlorenen Gerät keine Verbindung besteht, die Daten nicht mehr aus der Ferne gelöscht werden.

2.5 Fehlerhafte Administration des MDM

MDM-Lösungen sind komplexe Anwendungen mit typischerweise mehreren Hundert unterschiedlichen Regeln. Nicht alle Regeln sind dabei miteinander kombinierbar und umgekehrt hängen viele Regeln voneinander ab. Durch Fehler bei der Administration können die Endgeräte diversen Gefahren ausgesetzt sein, die sich direkt oder indirekt auf die Vertraulichkeit, Verfügbarkeit oder Integrität der Daten und Anwendungen auswirken.

2.6 Ungeeignetes Rechtemanagement im MDM

Das Rechtemanagement des MDM entscheidet, wer welche Einstellungen vornehmen und wer auf welche Daten zugreifen darf. Wenn einem Mitarbeiter eine falsche Rolle zugeordnet wird, besteht die Gefahr, dass ihm zu hohe Rechte eingeräumt werden. So könnte er beispielsweise Daten unbefugt einsehen oder Einstellungen am Gerät verändern. Auch wäre es möglich, dass er Apps installiert und benutzt, die in der Institution nicht zugelassen sind, beispielsweise zur Nutzung von Cloud-Speicherdiensten. Dadurch können schützenswerte Daten aus der Institution abfließen, oder es wird gegen den gesetzliche Datenschutzbestimmungen verstoßen.

2.7 Keine oder schwache Verschlüsselung der Kommunikation zwischen MDM und Endgerät

Wird die Datenverbindung zwischen dem mobilen Endgerät und dem MDM-Server gar nicht oder mit veralteten Algorithmen verschlüsselt oder werden nicht ausreichende Schlüssellängen eingesetzt, ist die Vertraulichkeit und Integrität aller übertragenen Daten gefährdet. Zum Beispiel könnte ein Angreifer dadurch sein IT-System als MDM-Server ausgeben und so an schützenswerte Informationen gelangen oder auch Einstellungen auf allen mobilen Endgeräten der Institution verändern.

2.8 Unberechtigte Erstellung von Bewegungsprofilen durch das MDM

Mit den meisten MDM-Produkten lässt sich ermitteln, wo sich ein Gerät gerade befindet, und es können standortabhängig Daten oder Apps freigegeben bzw. gesperrt werden (sogenanntes Geofencing). Dadurch entstehen minutiöse Bewegungsprofile der Geräte und somit auch der Benutzer. Werden diese Daten erhoben, ohne den Benutzer geeignet darüber zu informieren, verstoßen die Verantwortlichen unter Umständen gegen datenschutzrechtliche Bestimmungen. Auch besteht die Gefahr, dass Angreifer auf diese Daten zugreifen. Ebenso kann Geofencing dazu missbraucht werden, um Mitarbeiter unzulässig zu kontrollieren.

2.9 Gefahren durch Bring Your Own Device (BYOD)

Werden private Endgeräte dienstlich genutzt, ergeben sich diverse Gefährdungspotentiale. Beispielsweise kann es bezüglich der Software-Lizenzen zu rechtlichen Problemen kommen. Wenn im Notfall dienstliche Daten durch das MDM auf dem Gerät gelöscht werden müssen, kann dies auch Auswirkungen auf die privaten Daten des Benutzers haben. Zudem können die IT-Verantwortlichen nicht mehr jedes einzelne Mitarbeiter-Gerät daraufhin prüfen, ob es sich auch dienstlich einsetzen lässt. Dadurch besteht die Gefahr, dass ungeeignete Geräte verwendet werden und so gegen interne Datenschutz- und Sicherheitsanforderungen verstoßen wird. Zudem sind die Benutzer oft selbst dafür verantwortlich, ihre privaten Geräte zu warten und reparieren zu lassen. Bei einer solchen Reparatur könnten beispielsweise Firmendaten unbefugt eingesehen werden. Die gleiche Gefahr besteht, wenn nicht geregelt ist, was mit den Daten auf dem Gerät geschehen soll, wenn der Mitarbeiter die Institution verlässt.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz von Mobile Device Management (MDM) aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	-

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.3.2.2.A1 Festlegung einer Strategie für das Mobile Device Management

Es MUSS eine Strategie erarbeitet werden, die festlegt, wie Mitarbeiter mobile Endgeräte benutzen dürfen und wie die Geräte in die IT-Strukturen der Institution integriert sind. Grundlage ist dabei der Schutzbedarf der zu verarbeitenden Informationen. Die Strategie MUSS mindestens folgende Aspekte abdecken:

- Darf das MDM als Cloud-Dienst betrieben werden?
- Soll das MDM durch die Institution selbst betrieben werden?

- Welche Compliance-Anforderungen müssen durchgesetzt werden?
- Welche mobilen Geräte und welche Betriebssysteme muss das MDM unterstützen?
- Muss die MDM-Lösung mandantenfähig sein?
- Müssen Cloud-Dienste eingebunden werden?
- Müssen Dokumentenmanagementsysteme eingebunden werden?
- Muss das MDM auch Peripherie-Geräte einbinden und verwalten?
- Welches Betriebsmodell soll eingesetzt werden: private Endgeräte (Bring Your Own Device, BYOD), personalisierte Endgeräte (Eigentum der Institution) oder nicht personalisierte Endgeräte (Eigentum der Institution, gemeinsam genutzt)?

Die Strategie MUSS schriftlich fixiert und vom ISB freigegeben werden.

SYS.3.2.2.A2 Festlegen erlaubter mobiler Endgeräte

Es MUSS festgelegt werden, welche mobilen Endgeräte und Betriebssysteme in der Institution zugelassen sind. Alle erlaubten Geräte und Betriebssysteme MÜSSEN den Anforderungen der MDM-Strategie genügen und die technischen Sicherheitsanforderungen der Institution vollständig erfüllen. Das MDM MUSS so konfiguriert werden, dass nur mit freigegebenen Geräten auf Informationen der Institution zugegriffen werden kann. Wenn neue mobile Endgeräte beschafft werden, MÜSSEN sie auf der Liste der zugelassenen Endgeräte stehen.

SYS.3.2.2.A3 Auswahl einer MDM-Produkts

Wenn eine geeignete MDM-Software beschafft werden soll, MUSS sichergestellt sein, dass sich mit ihr alle in der MDM-Strategie festgelegten Anforderungen erfüllen lassen. Auch MUSS sie sämtliche technischen und organisatorischen Sicherheitsmaßnahmen umsetzen können und alle zugelassen mobilen Endgeräte unterstützten. Weitere Hinweise zur Beschaffung finden sich im Baustein OPS.1.2.6 *Beschaffung, Ausschreibung und Einkauf*.

SYS.3.2.2.A4 Verteilung der Grundkonfiguration auf mobile Endgeräte

Alle mobilen Endgeräte MÜSSEN so schnell wie möglich in das MDM integriert werden, damit sie nach den Richtlinien der Institution konfiguriert und verwaltet werden können. Wenn die Geräte die Grundkonfiguration erhalten, MÜSSEN sie sich im Werkszustand befinden. Bei bereits benutzten Geräten MÜSSEN vorher alle institutionsbezogenen Daten gelöscht werden. Ein nicht über MDM konfiguriertes Endgerät DARF NICHT auf Informationen der Institution zugreifen können.

SYS.3.2.2.A5 Sichere Grundkonfiguration für mobile Endgeräte

Alle mobilen Endgeräte MÜSSEN so konfiguriert sein, dass sie den Schutzbedarf angemessen erfüllen. Dafür MUSS eine passende Grundkonfiguration zusammengestellt und dokumentiert werden. Einzelheiten dazu werden in den spezifischen Geräte-Bausteinen definiert.

Wenn mobile Endgeräte an Mitarbeiter übergeben werden, MUSS darauf bereits der MDM-Client installiert sein. Andernfalls MUSS es den Benutzern selbst möglich sein, den Client zu installieren.

SYS.3.2.2.A6 Protokollierung

Das MDM MUSS alle sicherheitsrelevanten Ereignisse und Konfigurationsänderungen protokollieren. Die erhobenen Daten DÜRFEN NICHT von unbefugten Personen eingesehen werden und MÜSSEN unveränderbar gespeichert werden. Auch MÜSSEN bei der Protokollierung gesetzliche und interne Regelungen eingehalten werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Mobile Device Management (MDM). Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.3.2.2.A7 Auswahl und Freigabe von Apps

Apps aus öffentlichen App-Stores SOLLTEN durch die Verantwortlichen geprüft und freigegeben werden. Dazu SOLLTE ein Freigabeprozess entwickelt werden, in dem auch geeignete Bewertungskriterien definiert sind. Alle freigegebenen Apps SOLLTEN intern in einem Standardkatalog veröffentlicht werden und dort für die Benutzer verfügbar sein.

SYS.3.2.2.A8 Festlegung erlaubter Informationen auf mobilen Endgeräten

Die Institution SOLLTE festlegen, welche Informationen die mobilen Endgeräte unter welchen Bedingungen verarbeiten dürfen. Grundlage für die Regelung SOLLTE einerseits die Klassifikation bzw. Schutzbedarf der Informationen sein und andererseits die Bedingungen, unter denen die Daten auf den Geräten verarbeitet werden, etwa in abgeschotteten Containern. Die Verantwortlichen SOLLTEN das MDM auf Basis dieser Regeln konfigurieren, so dass es diese auf allen mobilen Endgeräten durchsetzen kann. Den Benutzern SOLLTEN die Regeln geeignet bekannt gegeben werden.

SYS.3.2.2.A9 Auswahl von Sicherheits-Apps

Um das erforderliche Sicherheitsniveau durchzusetzen, SOLLTEN für das Endgerät geeignete Sicherheits-Apps ausgewählt werden. Die Sicherheits-Apps SOLLTEN durch das MDM automatisch installiert werden.

SYS.3.2.2.A10 Sichere Anbindung der mobilen Endgeräte an die Institution

Die Verbindung der mobilen Endgeräte ins Netz der Institution SOLLTE angemessen abgesichert werden. Wenn Daten zwischen den mobilen Endgeräte und dem IT-Netz der Institution übertragen werden, SOLLTE durch geeignete Maßnahmen (z. B. VPN) verhindert werden, dass Unbefugte sie verändern oder einsehen können.

SYS.3.2.2.A11 Berechtigungsmanagement im MDM

Für das MDM SOLLTE ein Berechtigungskonzept erstellt, dokumentiert und angewendet werden. Den Benutzergruppen und Administratoren SOLLTE das MDM nur so viele Berechtigungen einräumen, wie für die Aufgabenerfüllung notwendig ist (Minimalprinzip). Es SOLLTE regelmäßig überprüft werden, ob die zugeteilten Rechte noch angemessen sind.

SYS.3.2.2.A12 Abgesicherte MDM-Betriebsumgebung

Das MDM selbst SOLLTE durch technische Maßnahmen abgesichert werden, um dem Schutzbedarf der hinterlegten oder verarbeiteten Informationen zu genügen. So SOLLTE beispielsweise das zugrundeliegende Betriebssystem gehärtet werden und alle notwendigen Patches SOLLTEN eingespielt sein.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.3.2.2.A13 Einschränkung der App-Installation mittels Whitelist (CIA)

Bei erhöhtem Schutzbedarf SOLLTEN die Benutzer der mobilen Endgeräte nur freigegebene und geprüfte Apps installieren dürfen. Das MDM SOLLTE verhindern, dass andere Apps installiert werden oder alternativ unbefugt installierte Apps sofort wieder entfernen.

SYS.3.2.2.A14 Benutzung externer Reputation-Services für Apps (CI)

Wenn die Administratoren einer Institution die erlaubten Apps nicht selbst auswählen können und Benutzer selbstständig Apps auf ihren Geräten installieren dürfen, SOLLTE ein sogenannter Reputation-Service eingesetzt werden. Dabei handelt es sich um einen externen Dienst, der Apps nach bestimmten Kriterien untersucht und die Ergebnisse als Service bereitstellt. Das MDM SOLLTE dann mithilfe dieser Informationen die Installation von Apps zumindest einschränken.

SYS.3.2.2.A15 Nutzung von PIM-Containern (CI)

Um Information auf den mobilen Endgeräten vor Spionage-Apps zu schützen, SOLLTEN diese gekapselt werden, zum Beispiel in einem PIM-Container. Zusätzlich SOLLTEN die Daten durch ein Passwort und eine vom Betriebssystem unabhängige Verschlüsselung abgesichert werden.

SYS.3.2.2.A16 Nutzung von getrennten Arbeitsumgebungen (CI)

Ist es den Mitarbeitern erlaubt, dienstliche Geräte auch privat zu nutzen, SOLLTEN Lösungen für getrennte Arbeitsumgebungen auf dem Endgerät eingesetzt werden. Wenn möglich, SOLLTEN dafür nur zertifizierte Produkte (z. B. nach Common Criteria) beschafft werden.

SYS.3.2.2.A17 Kontrolle der Nutzung von mobilen Endgeräten (I)

Mit MDM-Lösungen lässt sich kontrollieren, wie die mobilen Endgeräte benutzt werden. Es SOLLTEN angemessene Kriterien definiert werden, aufgrund derer die Geräte zu überwachen sind, ohne gegen gesetzliche oder interne Regelungen zu verstoßen.

SYS.3.2.2.A18 Besonders abgesicherte Betriebssysteme (CIA)

Es gibt mehrere Anbieter besonders abgesicherter mobiler Endgeräte, die teilweise zertifiziert sind für die Verarbeitung von Informationen nach gesetzlichen Informationsschutz-Klassifizierungen. Wenn ein sehr hoher Schutzbedarf besteht, SOLLTE die Institution ein solches Gerät einsetzen und in das MDM integrieren.

SYS.3.2.2.A19 Geofencing (CI)

Mittels Geofencing-Richtlinien ist es möglich, bestimmte Funktionen oder Apps nur an vorher definierten Orten zu erlauben oder auch zu verbieten. Mithilfe einer Schutzbedarfsanalyse SOLLTEN Bereiche identifizieren werden, an denen diese zusätzlichen Sicherheitsmaßnahmen nötig sind. Anschließend SOLLTEN sie unter Beachtung gesetzlicher und interner Regelungen umgesetzt werden.

4 Weiterführende Informationen

4.1 Literatur

- [BSICS052] Mobile Device Management BSI-CS 052
  BSI, Version 1.00, 03.2013
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_052.pdf

- [BYOD] Überblickspapier Consumerisation und BYOD
  BSI, Version 1.2, 07.2013
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_BYOD_pdf.pdf

- [NIST18001D] SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES
  SPECIAL PUBLICATION 1800-1d, NIST, 07.2015
  https://nccoe.nist.gov/sites/default/files/nccoe/NIST_SP1800-1d_Draft_HIT_Mobile-StandardsControls.pdf

- [NIST800124] Guidelines for Managing the Security of Mobile Devices in the Enterprise Special Publication 800-124 Revision 1, NIST, 06.2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Mobile Device Management (MDM)" von Bedeutung.

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.13 Abfangen kompromittierender Strahlung

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.25 Ausfall von Geräten oder Systemen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.38 Missbrauch personenbezogener Daten

G 0.39 Schadprogramme

G 0.45 Datenverlust

Elementare Gefährdungen Anforderungen	G 0.11	G 0.13	G 0.14	G 0.15	G 0.16	G 0.17	G 0.18	G 0.19	G 0.21	G 0.22	G 0.23	G 0.24	G 0.25	G 0.28	G 0.29	G 0.30	G 0.31	G 0.32	G 0.36	G 0.37	G 0.38	G 0.39	G 0.45
SYS.3.2.2.A1							x								x								
SYS.3.2.2.A2							x																
SYS.3.2.2.A3	x						x																x
SYS.3.2.2.A4		x	x						x	x	x					x	x		x			x	
SYS.3.2.2.A5		x	x						x	x	x					x	x		x			x	
SYS.3.2.2.A6																x	x	x		x			
SYS.3.2.2.A7			x		x			x	x	x	x	x	x		x	x	x	x	x			x	
SYS.3.2.2.A8			x			x																	
SYS.3.2.2.A9			x		x	x		x	x	x	x			x		x			x		x		x
SYS.3.2.2.A10				x	x					x													
SYS.3.2.2.A11																x					x		
SYS.3.2.2.A12											x					x		x			x		
SYS.3.2.2.A13			x		x			x		x	x			x		x			x			x	
SYS.3.2.2.A14			x		x			x		x	x			x		x			x			x	
SYS.3.2.2.A15			x		x			x		x	x			x		x			x				
SYS.3.2.2.A16			x		x			x		x	x			x		x			x				
SYS.3.2.2.A17															x	x	x	x		x			
SYS.3.2.2.A18		x	x	x					x	x	x			x	x	x		x	x	x	x	x	x
SYS.3.2.2.A19			x																				

SYS.3.2: Tablet und Smartphone

SYS.3.2.3 iOS (for Enterprise)

1 Beschreibung

1.1 Einleitung

Mobilgeräte sind ständige Begleiter in der heutigen Informationsgesellschaft. Sie sind ständig online, das heißt mit dem Internet oder dem internen Institutionsnetz verbunden, und bieten damit jederzeit Zugriff auf digitale Informationen. Die Kommunikation geschieht über diverse Schnittstellen, Beispiele sind GSM/UMTS/LTE, WLAN, Bluetooth.

Aufgrund von modernen, einfachen Bedienkonzepten sowie hoher Leistungsfähigkeit sind Smartphones und Tablets heutzutage weit verbreitet. Dazu zählen auch die von der Firma Apple produzierten Mobilgeräte iPhone und iPad mit dem Betriebssystem iOS. Ursprünglich wurden diese Geräte für den privaten Gebrauch konzipiert. Durch die Umgestaltung der Infrastrukturen und der Art der Informationserhebung und Verarbeitung finden sie jedoch immer häufiger auch Verwendung im beruflichen Umfeld und lösen teilweise sogar Notebooks ab.

Durch die Integration von Business-Funktionen wurde iOS seit der Version 4 schrittweise für den Einsatz in Unternehmen und Behörden ausgebaut und Funktionen für die Verwaltung aus Sicht einer Institution integriert. Hierzu gehören unter anderem Apples Programm zur zentralisierten Geräteregistrierung sowie Optionen wie Single Sign-on (SSO).

1.2 Zielsetzung

Ziel dieses Bausteins ist es, aufzuzeigen, wie mit iOS (for Enterprise) betriebene Geräte sicher in Institutionen eingesetzt werden können. Dazu werden Anforderungen für Einstellungen der iOS-basierten Endgeräte aufgestellt, die in Form von Konfigurationsprofilen auf den Endgeräten verteilt werden können. iOS-Konfigurationsprofile enthalten einheitlich definierte Einstellungen z. B. für Sicherheitsrichtlinien oder einzelne Systemaspekte, um iOS-basierte Geräte einheitlich und zentral zu verwalten und automatisch zu konfigurieren.

1.3 Abgrenzung

Der Baustein enthält grundsätzliche Anforderungen, die beim Betrieb von iOS-basierten Geräten, die in die Prozesse der Institution integriert sind, zu beachten und zu erfüllen sind. Anforderungen an die Integration in die Sicherheits- oder Kollaborations-Infrastruktur der Institution sind nicht im Fokus dieses Bausteins. Mit einem sogenannten „Mobile Device Management“ (MDM) besteht die Möglichkeit, die Geräte zentral zu verwalten und Konfigurationsprofile pro Benutzergruppe oder Einsatzzweck auszurollen. Über ein MDM lassen sich auch Sicherungsmaßnahmen einheitlich durchsetzen. Es wird vorausgesetzt, dass die iOS-basierten Geräte in ein solches MDM eingebunden sind. Anforderungen für den Betrieb solcher MDMs finden sich im Baustein SYS.3.2.2 MDM. Für kleinere Umgebungen kann auch der Apple Configurator verwendet werden, um die in diesem Baustein aufgeführten Anforderungen auf mehrere Endgeräte auszurollen. Allgemeine und übergreifende Aspekte zum Betrieb von Smartphones und Tablets unabhängig vom darauf eingesetzten Betriebssystem finden sich im Baustein SYS.3.2.1 Smartphone/Tablet.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich iOS (Apple) von besonderer Bedeutung:

2.1 Fehlende oder schlechte Qualität des Gerätecodes (Passcode)

Mit der sogenannten Codesperre werden iOS-basierte Geräte gegen unbefugten Zugriff gesperrt. Wenn diese Funktion nicht aktiviert wird oder wenn ein leicht zu erratender Code verwendet und dieser dadurch umgangen werden kann, besteht die erhöhte Gefahr, dass Unbefugte auf iOS-basierte Geräte zugreifen. Zudem ist der verwendete Gerätecode ein essentieller Bestandteil für die Entropie bestimmter Verschlüsselungscodes.

2.2 Jailbreak

In den bisherigen Versionen des iOS-Betriebssystems wurden meist Schwachstellen gefunden, die es ermöglichen, das von der Firma Apple etablierte Sicherheitsframework zu unterlaufen und somit auf Systemprozesse und geschützte Speicherbereiche zuzugreifen. Sogenannte „Jailbreaks“ nutzen diese Schwachstellen aus, um beispielsweise alternative App-Stores oder von Apple unerwünschte Erweiterungen nutzen zu können. Jailbreak-Techniken werden von Angreifern verwendet, um Schadprogramme zu installieren oder andere schädliche Manipulationen auf dem iOS-basierten Gerät vorzunehmen.

2.3 Risikokonzentration durch ein Benutzerkonto (Apple ID) für alle Apple-Dienste

Mit der Apple ID besteht ein zentraler Zugang zu allen von der Firma Apple zur Verfügung gestellten Diensten (z. B. iMessage, FaceTime, iCloud, App Store, iTunes, iBook-Store, iPhone-Suche oder Synchronisationsdienste). Wenn Unbefugte Zugriff auf eine nicht ausreichend abgesicherte Apple ID erlangen, können sie unter Umständen diese Apple-Dienste unter einer falschen Identität nutzen, die Verfügbarkeit der Apple-ID-basierten Dienste stören, iOS-basierte Geräte aus der Ferne lokalisieren oder alle Daten zurücksetzen sowie auf Informationen des Cloud-Dienstes „iCloud“ zugreifen. Insbesondere ist es einem Angreifer bei aktivierten iCloud-Backups möglich, die gespeicherten Daten auf ein eigenes iOS-Gerät zu klonen.

2.4 Fehlende Betriebssystem-Updates bei alten Geräten

Es erscheinen regelmäßig neue Versionen des iOS-Betriebssystems und Updates. Diese werden in der Regel für die neueste Gerätegeneration und für eine Reihe von älteren Gerätegenerationen (siehe weiterführende Informationen) bereitgestellt. Allerdings werden nicht alle zurückliegenden Betriebssystem-Versionen im gleichen Umfang mit Updates und Sicherheitsupdates versorgt. Nachträglich bekannt gewordene Schwachstellen im Betriebssystem einer bereits abgekündigten Gerätegeneration werden nicht mehr durch Updates geschlossen.

2.5 Software-Schwachstellen in Apps

Apps für iOS können Schwachstellen enthalten, die für lokale Angriffe oder für Angriffe über Netzverbindungen ausgenutzt werden können. Außerdem werden viele Apps von Drittentwicklern nach einiger Zeit nicht mehr weiter gepflegt. Dadurch besteht die Gefahr, dass erkannte Sicherheitsmängel nicht durch entsprechende Updates behoben werden.

2.6 Tiefere Integration für vorinstallierte Apps und deren Funktionalitäten

Mit dem Betriebssystem liefert Apple bereits tief integrierte und vorinstallierte Apps (z. B. die Apps „Mail“ und „Uhr“) sowie Schnittstellen zu Diensten von Drittanbietern (wie Twitter oder Facebook) aus. Diese Apps werden teilweise mit höheren Berechtigungen als aus dem App Store herunterladbare Apps ausgeführt, wodurch sich die Angriffsfläche des iOS-basierten Geräts vergrößert. Die Verwendung der nicht löschbaren bzw. nicht konfigurierbaren Schnittstellen ist bei dienstlicher Nutzung meist nicht erwünscht und vergrößert ebenfalls die Angriffsfläche des Geräts.

2.7 Missbrauch des Fingerabdrucksensors

Das Betriebssystem iOS enthält spezielle Funktionen, die durch den Fingerabdrucksensor Touch ID vereinfacht genutzt werden können. Dieses sind z. B. das vereinfachte Freischalten des Geräts oder der Einkauf bei iTunes und im App Store. Diese biometrische Sicherheitsfunktion lässt sich mit entsprechendem Aufwand durch den Nachbau eines künstlichen Fingers auf Basis eines digital gesäuberten Fingerabdrucks umgehen. Bis zu 48 Stunden nach der letzten Eingabe des gesetzten Passcodes akzeptiert das Gerät eine Freischaltung über Fingerabdruck, dies ist somit das maximale Zeitfenster für einen Missbrauch.

2.8 Missbrauch von Fitness- oder Ortungsdaten unter iOS

Das Betriebssystem iOS enthält spezielle Funktionen zur Verwaltung von Fitness- und Ortungsdaten. Diese Daten sind besonders sensitiv und stellen ein attraktives Angriffsziel dar, insbesondere wenn sie über einen längeren Zeitraum gesammelt und gespeichert werden.

2.9 Missbrauch sensitiver Daten im gesperrten Zustand

Das Betriebssystem iOS verfügt über eine Funktion, um Mitteilungen von aktivierten Widgets und Push-Nachrichten auf dem Sperrbildschirm anzeigen zu lassen. Dadurch besteht die Gefahr, dass sensitive Informationen des Benutzers ungeschützt auf dem Sperrbildschirm unberechtigten Dritten preisgegeben werden und ausgenutzt werden können. Über den Sprachassistenten Siri besteht zudem auch im gesperrten Zustand die Möglichkeit zum Zugriff auf Telefonfunktionen und Kontaktdaten. Auch dies kann dazu führen, dass unberechtigte Dritte an sensitive Informationen gelangen können.

2.10 Missbrauch in iOS-basierten Geräten gespeicherter Daten

Aufgrund der vielen Funktionen und der Erweiterungsmöglichkeiten enthält ein iOS-basiertes Gerät oft sensitive Daten, z. B. E-Mails, Dokumente, Kurznachrichten, Passwörter, Kreditkarteninformationen oder Gesundheitsdaten. Es besteht die Gefahr, dass diese Daten missbraucht werden, wenn Täter bei Verlust, Diebstahl oder Aussonderung an das Gerät gelangen oder sich technisch Zugriff auf die Daten verschaffen.

2.11 Missbräuchlicher Zugriff auf ausgelagerte Daten

Für eine Reihe iOS-spezifischer Funktionen muss die von der Firma Apple betriebene Infrastruktur verwendet werden. Bei Verwendung der Funktionalitäten iCloud-Schlüsselbund, iMessage, FaceTime, Siri, Continuity, Spotlightvorschläge sowie der iCloud zum Anlegen verschlüsselter Backups oder zum gemeinsamen Arbeiten an Dokumenten erfolgt die Synchronisierung von Daten zwischen unterschiedlichen Geräten oder Benutzern stets über die Infrastruktur der Firma Apple. Ebenfalls werden Push-Nachrichten für iOS-basierte Geräte über diese Infrastruktur weitergeleitet. Es besteht somit prinzipiell die Gefahr, dass Unbefugte auf Apple-Server zugreifen und die dort gespeicherten oder übertragenen Daten für ihre Zwecke missbrauchen.

2.12 Webbasierte Angriffe auf Browser

Browser, aber auch viele andere iOS-basierte Apps, können Webseiten und Webinhalte anzeigen. Dadurch können iOS-basierte Geräte von Phishing-Angriffen, Drive-by-Exploits und anderen webbasierten Angriffsformen betroffen sein.

2.13 Unzureichende Vorgaben zum Lizenz-Management

Das Management von Software-Lizenzen ist eine der Kernaufgaben der IT-Compliance. Somit besteht für eine Institution die Notwendigkeit zur Definition klarer Verantwortlichkeiten und Regelungen. Gerade die Thematik der Lizenzen von Apps wird jedoch häufig nicht ausreichend betrachtet. Im Rahmen der allgemeinen Compliance haben die Verantwortlichen der Institution dafür Sorge zu tragen, dass ihre Mitarbeiter keine Lizenzverstöße begehen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen für iOS-basierte Systeme aufgeführt. Grundsätzlich ist der *IT-Betrieb* für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	-

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.3.2.3.A1 Strategie für die iOS-Nutzung

Dieser Baustein setzt voraus, dass zu verwaltende iOS-Geräte in eine MDM-Infrastruktur integriert sind. Eine begründete Ausnahme unter Betrachtung von wirtschaftlichen Aspekten kann die Verwaltung einer kleineren, einstelligen Anzahl von Geräten ohne Einsatz eines MDM sein. Wird ein MDM eingesetzt, so MUSS die Verwaltung der Geräte zum Zwecke der vereinfachten Administration und des einheitlichen Aufspielens von sicherheitstechnischen sowie sonstigen Einstellungen über das MDM erfolgen. Hierzu MUSS eine Strategie zur iOS-Nutzung vorliegen, in der Aspekte wie Endgeräte-Auswahl oder Backup-Strategien festgelegt werden. Es MUSS außerdem geregelt werden, ob zusätzliche Apps von Drittanbietern genutzt werden sollen.

SYS.3.2.3.A2 Planung des Einsatzes von Cloud-Diensten

iOS-basierte Geräte sind grundsätzlich eng mit iCloud-Diensten des Herstellers Apple verzahnt, dies betrifft grundsätzlich bereits die Aktivierung der Geräte mit einer Apple ID. Es wird keine Apple ID benötigt, wenn das Apple-Programm zur Geräteregistrierung (Device Enrollment Program, DEP) genutzt wird. Sofern auf die Nutzung der Aktivierungssperre verzichtet werden kann, wird ebenfalls keine Verknüpfung der Cloud-Dienste mit einer personalisierten Apple ID benötigt. Es MUSS daher vor der Verwendung von iOS-basierten Geräten eine strategische Festlegung erfolgen, welche Cloud-Services in welchem Umfang genutzt werden sollen bzw. dürfen.

SYS.3.2.3.A3 Verwendung des Gerätecodes

Mit der Aktivierung des Gerätecodes wird die Sicherheit der Daten auf dem iOS-basierten Gerät erhöht und zusätzlich basierend auf der Komplexität des Gerätecodes eine verbesserte Entropie für bestimmte Verschlüsselungscodes zur Verfügung gestellt. Basierend auf dem festgelegten Sicherheitskonzept und dem Schutzbedarf der auf dem iOS-basierten Gerät verarbeiteten bzw. gespeicherten Daten MUSS ein angemessen komplexer Gerätecode verwendet werden.

SYS.3.2.3.A4 Verwendung der Konfigurationsoption "Automatische Sperre"

Basierend auf dem Einsatzzweck und Schutzbedarf MUSS die Zeitspanne für die "Automatische Sperre" des Geräts auf einen möglichst niedrigen Wert eingestellt sein. Durch einen niedrigen Wert wird sichergestellt, dass keine unberechtigte Nutzung des unbeaufsichtigten Geräts möglich ist. Durch eine angemessen kurze Zeitspanne für die automatische Sperre wird der Benutzer bei der Einhaltung der Sicherheitsregelungen der Institution unterstützt, sofern das Gerät nicht durch Interaktion mit der Benutzeroberfläche im ungesperrten Zustand verweilt. Bei der Definition des Zeitraums bis zur Passcode-Abfrage MÜSSEN die Anforderungen an den Schutzbedarf und die Benutzbarkeit beachtet werden.

SYS.3.2.3.A5 Verwendung der Konfigurationsoption "Gerätesperrung"

Um bei einem gesperrten Gerät zu vermeiden, dass Unbefugte auf die Benutzerdateien zugreifen können, MUSS der Zeitraum bis zu einer Passcode-Abfrage definiert sein. Bei der Definition des Zeitraums bis zur Passcode-Abfrage MÜSSEN die Anforderungen an den Schutzbedarf und die Benutzbarkeit beachtet werden.

SYS.3.2.3.A6 Verwendung der Konfigurationsoption "Maximale Anzahl von Fehlversuchen"

Um das systematische Ausspionieren des Passcodes zu verhindern, MUSS eine dem Schutzbedarf gerechte Anzahl maximal möglicher Fehleingaben des Passcodes konfiguriert werden. Bei Überschreiten dieses festgelegten Werts MUSS eine vollständige lokale Löschroutine (Wipe) auf dem iOS-basierten Gerät automatisch initialisiert werden.

SYS.3.2.3.A7 Verhinderung des unautorisierten Löschens von Konfigurationsprofilen

Um eine unautorisierte Löschung von Konfigurationsprofilen zu verhindern, MÜSSEN durch die Verantwortlichen geeignete Regelungen getroffen und umgesetzt sein. Beispielsweise kann die Löschung technisch durch eine passwortgeschützte Authentisierung realisiert werden oder organisatorisch grundsätzlich verboten sein.

SYS.3.2.3.A8 Zeitnahe Aktualisierung des Betriebssystems

Apple stellt in unregelmäßigen Abständen neue Versionen mit integrierten Sicherheitsaktualisierungen des Betriebssystems iOS für aktuell unterstützte Geräte zur Verfügung. Bevor alle iOS-basierten Geräte der Institution auf eine neue Version aktualisiert werden, MUSS diese getestet worden sein. Ziel dieses Validierungsprozesses ist die Verifizierung der bisherigen Funktionen, Sicherheitsmechanismen und die Durchsetzbarkeit von Compliance-Anforderungen. Um aufgetretene Sicherheitslücken zu schließen, MUSS eine Aktualisierung des installierten Betriebssystems zeitnah nach Freigabe auf die Geräte ausgerollt werden. Durch eine aktive Teilnahme an Apples Beta-Programm kann in den meisten Fällen die neue Betriebssystemversion vorab getestet werden, um die Freigabe hinsichtlich der genannten Aspekte zeitnah ermöglichen zu können. Ältere Geräte, für die keine aktuellen iOS-Versionen mehr bereitgestellt werden, MÜSSEN ausgesondert und durch unterstützte Geräte ersetzt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich iOS (for Enterprise). Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.3.2.3.A9 Verwendung eines komplexen Gerätecodes

Basierend auf dem Schutzbedürfnis SOLLTE zum Zwecke der Wahrung der Vertraulichkeit ein komplexes Passwort verwendet werden. Bei der Regelung der Komplexität (Mindestlänge des Codes, Mindestanzahl an Sonderzeichen) SOLLTE eine Balance zwischen Benutzbarkeit, Risikoakzeptanz und Schutzbedürfnis gewahrt werden. Beispielsweise können die in der Institution etablierten Regelungen für mobile Arbeitsmittel (Notebooks) die Grundlage für die umzusetzende Komplexität bilden.

SYS.3.2.3.A10 Verwendung des Fingerabdrucksensors

Bei iOS-basierten Geräten mit biometrischem Fingerabdrucksensor, der sogenannten Touch ID, SOLLTE dieser den Benutzern alternativ zur Entsperrung des Geräts freigegeben werden, wenn gleichzeitig organisatorisch und technisch geregelt wird, dass die Benutzer komplexere Gerätecodes verwenden müssen. Einhergehend mit der Aktivierung der Touch ID SOLLTE eine Sensibilisierung der Benutzer hinsichtlich der Fälschbarkeit von Fingerabdrücken erfolgen.

SYS.3.2.3.A11 Verwendung nicht personalisierter Gerätenamen

Wird ein iOS-basiertes Gerät mit iTunes oder zum Laden mit einem Notebook oder einer Workstation gekoppelt, wird automatisch der Gerätename angezeigt und ermöglicht so Rückschlüsse auf den Besitzer oder die Institution. Um zu verhindern, dass unter Umständen der Benutzer und das Gerätepasswort (Passcode) erraten werden können, SOLLTE der Gerätename keine persönlichen Namens- und Institutionsmerkmale enthalten.

SYS.3.2.3.A12 Verwendung institutionsbezogener Apple IDs

In den allgemeinen Geschäftsbedingungen schließt die Firma Apple die Möglichkeit der Übertragung der Apple ID an einen anderen Mitarbeiter aus. Zum Zwecke der Notfallvorsorge vor Verlust geschäftlicher Daten, die auf dem Gerät selbst oder in der iCloud gespeichert sind, und der Möglichkeit der Weiterverwendung des Geräts SOLLTE das iOS-basierte Gerät mit einer institutionsbezogenen Apple ID verwendet werden.

Als zusätzliche Vorsorgemaßnahme zur Verhinderung des Missbrauchs dienstlicher Zahlungsmittel (Kreditkarten) SOLLTE das Programm für Volumenlizenz (VPP) von Apple verwendet werden.

SYS.3.2.3.A13 Verwendung der Konfigurationsoption "Einschränkungen unter iOS"

Um die Vertraulichkeit und Integrität der verarbeiteten bzw. auf dem Gerät gespeicherten Daten sicherzustellen, SOLLTEN alle nicht benötigten oder erlaubten Funktionen oder Dienste deaktiviert werden. Welche zu deaktivieren sind, muss basierend auf dem Einsatzzweck und dem zugrundeliegenden Schutzbedarf für die Punkte Sperrbildschirm, Unified Communication, Siri, Hintergrundbild, Verbindung mit Host-Systemen und Diagnose- und Nutzungsdaten entschieden werden.

SYS.3.2.3.A14 Verwendung der iCloud-Infrastruktur

Durch die Firma Apple wird allen Benutzern mit einer Apple ID die iCloud-Infrastruktur zur Verfügung gestellt. So besteht z. B. die Möglichkeit, über die iCloud-Infrastruktur Dokumente und Fotos zu teilen, Standortinformationen der hinterlegten Freunde abzurufen oder OS X-basierte und iOS-basierte Geräte um Continuity-Funktionen zu erweitern. Bevor die umfängliche oder selektive Nutzung der iCloud-Infrastruktur freigegeben wird, SOLLTE eine Bewertung der Vereinbarkeit der allgemeinen Geschäftsbedingungen der Firma Apple mit den internen Richtlinien hinsichtlich Verfügbarkeit, Vertraulichkeit, Integrität und Datenschutz erfolgen. Wird die Nutzung der iCloud-Infrastruktur erlaubt, SOLLTE die Authentisierung am iCloud-Webservice durch eine Zwei-Faktor-Authentisierung erfolgen. Durch die Verwendung verwalteter Apps kann die iCloud-Nutzung für einen rein dienstlichen Bedarf zusätzlich auf ein geringes Maß reduziert oder komplett ausgeschlossen werden.

SYS.3.2.3.A15 Verwendung der Continuity-Funktionen

Wurde die Nutzung der iCloud-Infrastruktur nicht grundsätzlich durch das Sicherheitsmanagement der Institution untersagt, SOLLTE eine Bewertung der Vereinbarkeit der Continuity-Funktionen (AirDrop und Handoff) mit den internen Richtlinien unter Berücksichtigung der Aspekte Vertraulichkeit und Integrität erfolgen. Auf Basis der Bewertungsergebnisse SOLLTE geregelt werden, inwieweit technisch bzw. organisatorisch diese Funktionen eingeschränkt werden.

SYS.3.2.3.A16 Verwendung der Konfigurationsoption für AirPlay

Mit AirPlay wird es dem Anwender ermöglicht, an einen AirPlay-Empfänger (wie das Apple-TV) Musik, Videos, Präsentationen oder den kompletten Bildschirminhalt des Geräts zu übertragen. Um einen angemessenen Umgang mit der Funktion AirPlay sicherzustellen, SOLLTE es technische bzw. organisatorische Regelungen geben sowie die Benutzer sensibilisiert werden und im sicherheitskonformen Umgang mit AirPlay Unterstützung erhalten.

SYS.3.2.3.A17 Verwendung der Gerätecode-Historie

Um die Vertraulichkeit des verwendeten Passcodes zu wahren und zu schnelle Wiederholungen vom Benutzer verwendeter Passwörter zu verhindern, SOLLTE im Konfigurationsprofil die Anzahl der eindeutigen Codes bis zur ersten Wiederholung festgelegt sein. Bei der Festlegung des Wertes können beispielsweise die etablierten Regelungen innerhalb der Windows-Domäne oder ähnlichen als Grundlage dienen.

SYS.3.2.3.A18 Verwendung der Konfigurationsoption für den Browser Safari

Der Browser Safari ist in iOS tief integriert und besitzt gegenüber den aus dem App-Store installierten Browsern anderer Anbieter teils höhere Rechte. Die bereits in der Institution etablierten Browserrichtlinien SOLLTEN entsprechend auch für Safari durch technische und organisatorische Maßnahmen umgesetzt werden. Dabei SOLLTEN die bereits etablierten Anforderungen für Browser auf stationären und tragbaren PCs als Grundlage für die Absicherung der iOS-basierten Geräte dienen sowie die Einsatzszenarien und das Einsatzumfeld der Geräte beachtet werden.

SYS.3.2.3.A19 Verwendung der Filteroption für Webseiten

Sind die Geräte nicht in eine vorhandene Proxy- und Reputations-Infrastruktur der Institution eingebunden, SOLLTE für den Browser Safari durch die Nutzung der Filteroptionen auf Basis von erlaubten URLs (diese sind eine Ergänzung der bereits durch Apple vorselektierten URL-Gruppen), Whitelist-URLs, Blacklist-URLs oder durch die Einbindung von Inhaltsfiltern Dritter die Erfüllung gesetzlicher Regelungen und interner Vorgaben erfolgen.

Wird durch die Verantwortlichen in der IT bereits ein Reputation Service oder eine Proxy-Infrastruktur angeboten, lassen sich die iOS-basierten Geräte durch die Hinterlegung eines globalen HTTP-Proxy für alle installierten Browser integrieren. Bei der Verwendung eines globalen nur intern erreichbaren HTTP-Proxies SOLLTE die Integration mittels einer VPN-Verbindung wahlweise permanent oder basierend auf den verwendeten Apps in die Infrastrukturen erfolgen.

SYS.3.2.3.A20 Einbindung der Geräte in die interne Infrastruktur via VPN

Um die Vertraulichkeit und Integrität der Informationen der Institution zu wahren, SOLLTEN die iOS-basierten Geräte mittels VPN in die Infrastruktur integriert werden. In Abhängigkeit von Schutzbedarf, Zweck und technischen Möglichkeiten des VPN-Servers SOLLTE eine VPN-Verbindung auf Basis der Technologien IKEv2, IPSec, L2TP, PPTP oder SSL/TLS realisiert werden. Die Authentisierung SOLLTE bevorzugt durch Einmal-Passwörter und Zertifikate statt durch den Einsatz klassischer Passwörter implementiert und betrieben werden.

SYS.3.2.3.A21 Freigabe von Apps und Einbindung des Apple App Stores

Wenn zusätzliche Apps von Drittanbietern eingesetzt werden (siehe SYS.3.2.3.A1), MUSS durch die Verantwortlichen der interne Software-Freigabeprozess bzgl. der Validierung und Freigabe von Anwendungen (Apps) aus dem Apple App-Store ergänzt werden. Um die institutionsinternen App-Freigabeprozesse zu unterstützen, SOLLTE das eingesetzte MDM eine Filterung auf Basis von Whitelists, Blacklists oder App-Reputationsservices ermöglichen.

Alle freigegebenen Anwendungen SOLLTEN intern in einem Standardkatalog veröffentlicht und den Benutzern zur Verfügung gestellt werden. Als unterstützendes Mittel zur Sicherstellung, dass den autorisierten Anwendern die benötigten Apps zum benötigten Zeitpunkt ausreichend zur Verfügung stehen, kann eine Integration des Programms für Volumenlizenzen (VPP) für Unternehmen der Firma Apple in die MDM-Infrastruktur erfolgen. Ein weiterer Aspekt der Nutzung des VPP ist, dass die verwendeten Apple IDs nicht mit einem Zahlungsmittel hinterlegt sein müssen. Die Zahlungsbestätigung von Apps im App-Store DARF NICHT mit der Touch ID erfolgen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.3.2.3.A22 Durchsetzung von Compliance-Anforderungen (CI)

Einen Verstoß gegen die Regelungen der Institution oder sogar die Manipulation des Betriebssystems zu erkennen, ist über die Abfrage einer von Apple freigegebenen Schnittstelle nicht möglich. Diese Aufgabe SOLLTE durch die vom MDM-Anbieter bereitgestellte Lösung erfolgen. Die folgenden Aktionen sollten bei Verdacht auf Verstoß gegen Regelungen oder Manipulation des Betriebssystems ausgeführt werden. Hierzu sollten entsprechende Funktionen bereitgestellt werden:

1. selbständiges Versenden von Warnhinweisenselbständiges Sperren des GerätsLöschen der vertraulichen Informationen der InstitutionLöschen des kompletten GerätsVerhindern des Zugangs zu Unternehmens-Apps Verhindern des Zugangs zu den Systemen und Informationen der Institution
2. selbständiges Sperren des GerätsLöschen der vertraulichen Informationen der InstitutionLöschen des kompletten GerätsVerhindern des Zugangs zu Unternehmens-Apps Verhindern des Zugangs zu den Systemen und Informationen der Institution
3. Löschen der vertraulichen Informationen der InstitutionLöschen des kompletten GerätsVerhindern des Zugangs zu Unternehmens-Apps Verhindern des Zugangs zu den Systemen und Informationen der Institution
4. Löschen des kompletten GerätsVerhindern des Zugangs zu Unternehmens-Apps Verhindern des Zugangs zu den Systemen und Informationen der Institution
5. Verhindern des Zugangs zu Unternehmens-Apps Verhindern des Zugangs zu den Systemen und Informationen der Institution
6. Verhindern des Zugangs zu den Systemen und Informationen der Institution

Bei Verdacht auf einen Verstoß oder Manipulation muss ein Alarm an die verantwortlichen Administratoren und das Sicherheitsmanagement in der Institution gesandt werden.

SYS.3.2.3.A23 Verwendung der automatischen Konfigurationsprofillöschung (CI)

Durch die Verwendung der automatischen Konfigurationsprofillöschung SOLLTE sichergestellt werden, dass auch nicht permanent online erreichbare Geräte ohne Zutun der IT-Verantwortlichen den bisher gewährten Zugang in die interne Infrastruktur nach Ablauf eines definierten Zeitraums oder an einem bestimmten Tag verlieren, sofern der Zeitraum nicht durch Zugriff auf das interne Netz erneuert wird. Zur Sicherstellung, dass der Benutzer noch im Besitz des Geräts ist, kann diese Methodik auch präventiv verwendet werden.

SYS.3.2.3.A24 Verwendung standortbasierter Policies (CI)

Durch die Hinterlegung einer Geofencing-Richtlinie SOLLTE sichergestellt werden, dass Geräte mit Informationen von hohem Schutzbedarf nicht den zuvor festgelegten geographischen Bereich verlassen. Sollte der geographische Bereich verlassen werden, SOLLTE eine selektive Löschung der klassifizierten Informationen oder eine vollständige Löschung des Geräts erfolgen. Bevor eine selektive oder vollständige Löschung des Geräts erfolgt, müssen die verantwortlichen Administratoren und das Sicherheitsmanagement sowie der Benutzer eine Information, z. B. per Push-Nachricht, E-Mail oder SMS, über diesen Sachverhalt erhalten. Zum Zwecke der besseren Akzeptanz und um dem Benutzer die Möglichkeit zu geben, wieder in den zulässigen geographischen Bereich zurückzukehren, sollte die selektive oder vollständige Löschung um einen hinterlegten Zeitraum kurzzeitig verzögert erfolgen. Der Einsatz von Geofencing-Richtlinien darf nicht gegen interne und gesetzliche Anforderungen verstoßen.

SYS.3.2.3.A25 Verwendung der Konfigurationsoption für AirPrint (CI)

Seitens der Firma Apple wurde die AirPrint-Funktionalität fest in das Betriebssystem eingebaut. Diese Funktion lässt sich nicht grundsätzlich einschalten oder abschalten. Freigegebene AirPrint-Drucker SOLLTEN durch ein Konfigurationsprofil dem Benutzer bereitgestellt werden. Um zu vermeiden, dass Informationen auf nicht vertrauenswürdigen Druckern durch die Benutzer ausgedruckt werden können, SOLLTE sichergestellt sein, dass stets alle Kommunikationsverbindungen über die Infrastruktursysteme der Institution geführt werden.

SYS.3.2.3.A26 Keine Verbindung mit Host-Systemen (CI)

Um zu vermeiden, dass iOS-basierte Geräte unautorisiert mit Notebooks, PCs o. ä. verbunden werden, SOLLTEN die Benutzer iOS-basierte Geräte ausschließlich mit dem MDM verbinden können. Hierdurch wird sichergestellt, dass keine lokalen Backups mittels iTunes oder ähnlichen Programmen erstellt werden können. Zusätzlich werden hierdurch Angriffe unter Zuhilfenahme forensischer Mittel stark erschwert oder komplett verhindert.

SYS.3.2.3.A27 Verwendung der Konfigurationsoption für APN

Bei Verwendung eines institutionsbezogenen Zugangspunkts zum Mobilfunknetz (APN, Access Point Name) bildet dieser die Grundlage zur Eingrenzung des erlaubten Geräte-Pools. Alle Geräte, die diesen APN verwenden, erhalten vom Mobilfunk-Provider einen mit der Institution abgestimmten IP-Adressenbereich. Zur Vermeidung von Sicherheitsvorfällen, die durch zu kurze Passwörter für die Authentisierung verursacht werden, SOLLTE ein komplexes Passwort mit maximal 64 Stellen mit dem Mobilfunk-Provider vereinbart werden. Beim Einsatz eines institutionsbezogenen APN SOLLTE die Authentisierung auf Basis des Protokolls CHAP realisiert sein.

4 Weiterführende Informationen

4.1 Literatur

- [ACSIOS] Allianz für Cybersicherheit: Empfehlung zu iOS - BSI-CS 074
  BSI, Version 1.20, 12.2015
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_074.pdf

- [AppAGB] AGB für iTunes
  Apple (zuletzt abgerufen am 27.09.2017)
  https://www.apple.com/legal/internet-services/itunes/de/terms.html

- [AppAGBCl] Apple AGB iCloud
  Apple (zuletzt abgerufen am 27.09.2017)
  https://www.apple.com/legal/internet-services/icloud/de/terms.html

- [AppAGBGC] AGB für Game-Center
  Apple (zuletzt abgerufen am 27.09.2017)
  https://www.apple.com/legal/internet-services/itunes/gamecenter/de/terms.html

- [AppCon] Appel Configuration
  Apple, (zuletzt abgerufen am 27.09.2017)
  https://support.apple.com/de-de/apple-configurator

- [AppDS] Apple Datenschutzrichtlinie
  Apple (zuletzt abgerufen am 27.09.2017)
  https://www.apple.com/legal/privacy/de-ww/

- [AppLPG] Apple "Legal Process Guidelines"
  Apple, 06.2017
  https://images.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf

- [AppSiup] Apple Sicherheitsupdates
  Apple (zuletzt abgerufen am 27.09.2017)
  https://support.apple.com/de-de/HT201222

- [AppViPro] Abgekündigte und Vintage-Produkte
  Apple, (zuletzt abgerufen am 27.09.2017)
  https://support.apple.com/de-de/HT201624

- [DEP] Programm zur Geräteregistrierung
  Apple, (zuletzt abgerufen am 27.09.2017)
  https://www.support.apple.com/de-de/HT6578

- [Support] Support für Unternehmen und Bildungseinrichtungen
  Apple, (zuletzt abgerufen am 27.09.2017)
  https://www.apple.com/de/support/business-education/

- [TR02102] Kryptographische Verfahren- Empfehlungen und Schlüssellängen
  BSI, (zuletzt abgerufen am 27.09.2017)
  https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

- [VPP] Programm für Volumenlizenz
  Apple, (zuletzt abgerufen am 27.09.2017)
  https://vpp.itunes.apple.com/de/store

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "iOS (for Enterprise)" von Bedeutung.

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.35 Nötigung, Erpressung oder Korruption

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.38 Missbrauch personenbezogener Daten

G 0.39 Schadprogramme

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.09	G 0.11	G 0.14	G 0.16	G 0.19	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.29	G 0.30	G 0.32	G 0.35	G 0.36	G 0.37	G 0.38	G 0.39	G 0.41	G 0.42	G 0.46
SYS.3.2.3.A1			x	x	x	x	x	x	x			x	x	x	x			x	x		x		x
SYS.3.2.3.A2		x	x		x								x				x		x				x
SYS.3.2.3.A3			x	x	x	x	x	x							x		x						x
SYS.3.2.3.A4			x	x	x	x	x	x							x		x						x
SYS.3.2.3.A5			x	x	x	x	x	x							x		x						x
SYS.3.2.3.A6			x	x	x	x	x	x							x		x						x
SYS.3.2.3.A7					x	x	x	x						x	x	x		x	x		x		x
SYS.3.2.3.A8			x		x	x			x	x		x			x					x	x		x
SYS.3.2.3.A9			x	x	x	x	x	x							x		x						x
SYS.3.2.3.A10								x															
SYS.3.2.3.A11			x																			x	
SYS.3.2.3.A12			x	x	x										x	x	x	x			x	x	x
SYS.3.2.3.A13			x	x	x	x	x	x		x		x	x	x	x		x	x	x		x	x	x
SYS.3.2.3.A14	x	x	x	x	x			x					x										
SYS.3.2.3.A15		x			x								x										x
SYS.3.2.3.A16	x		x		x																	x	
SYS.3.2.3.A17			x	x	x	x	x	x							x		x						x
SYS.3.2.3.A18										x		x											
SYS.3.2.3.A19													x										
SYS.3.2.3.A20			x		x															x			x
SYS.3.2.3.A21			x		x	x			x	x		x			x					x	x		x
SYS.3.2.3.A22				x		x	x						x								x		x
SYS.3.2.3.A23		x		x							x			x									
SYS.3.2.3.A24				x										x									x
SYS.3.2.3.A25				x	x								x			x							x
SYS.3.2.3.A26		x	x	x	x	x	x	x				x	x	x	x	x	x		x	x	x	x	x
SYS.3.2.3.A27	x																x		x				

SYS.3.2: Tablet und Smartphone

SYS.3.2.4 Android

1 Beschreibung

1.1 Einleitung

Mobilgeräte sind ständige Begleiter in der heutigen Informationsgesellschaft. Sie sind ständig online, das heißt, mit dem Internet oder dem internen Institutionsnetz verbunden, und bieten damit jederzeit Zugriff auf digitale Informationen. Die Geräte können über diverse Schnittstellen kommunizieren, z. B. Mobilfunk, WLAN oder Bluetooth.

Aufgrund von modernen, einfachen Bedienkonzepten sowie hoher Leistungsfähigkeit sind Smartphones und Tablets heutzutage weit verbreitet. Ursprünglich wurden diese Geräte für den privaten Gebrauch konzipiert. Heute werden sie jedoch auch im beruflichen Umfeld verwendet.

Ein oft genutztes Betriebssystem für Mobiltelefone ist Android. Seit Version 4 wurde Android schrittweise für den Unternehmenseinsatz ausgebaut. So wurden z. B. Funktionen integriert, die es Institutionen erleichtern, Android-Geräte zu verwalten. Auch steigt die Zahl der von Android unterstützten Richtlinien mit jeder Version und es gibt herstellerspezifische Erweiterungen, die zusätzliche Richtlinien erlauben.

1.2 Zielsetzung

Ziel des Bausteins ist es, über typische Gefährdungen für Android-basierte Geräte zu informieren sowie aufzuzeigen, wie Android-Geräte sicher in Institutionen eingesetzt werden können. Auf Basis der im Baustein aufgeführten Anforderungen können zudem Sicherheitsrichtlinien erstellt werden.

1.3 Abgrenzung

Der Baustein enthält grundsätzliche Anforderungen, die beim Betrieb von Android-basierten Geräten zu beachten und zu erfüllen sind. Allgemeine und übergreifende Anforderungen an den Betrieb von Smartphones und Tablets werden nicht in diesem Baustein, sondern in SYS.3.2.1 *Smartphone und Tablet* behandelt. Ebenfalls nicht Bestandteil dieses Bausteins sind die Anforderungen an die zentrale Administration von Android-Geräten, diese sind im Baustein SYS 3.2.3 *MDM* aufgeführt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Android von besonderer Bedeutung:

2.1 Rooten des Gerätes

Viele der bisherigen Versionen von Android enthielten Schwachstellen, die es ermöglichten, das vom Hersteller etablierte Sicherheitskonzept außer Kraft zu setzen. Frei erhältliche Werkzeuge nutzen diese Schwachstellen aus, um anderen Apps Superuser-Rechte (root) erteilen zu können.

Diese Apps können dann auf die Daten des Betriebssystems und die anderer Apps zugreifen. Auch benutzen Schadprogramme diese Schwachstellen, um sich auf dem Gerät zu installieren oder es zu manipulieren. Hierdurch kann das Betriebssystem anders als vorgesehen genutzt und wichtige Sicherheitsfunktionen übergangen werden.

Besonders Zugangsdaten, die Android in geschützten Bereichen lagert, sind betroffen, da eine App mit Superuser-Rechten diese unter Umständen auslesen kann und somit auf die dort abgelegten Informationen zugreifen kann.

2.2 Schadsoftware für das Android-Betriebssystem

Aufgrund der Verbreitung und der offenen Architektur sind Geräte mit Android-Betriebssystem ein beliebtes Ziel für Schadsoftware. Da es bei Android relativ einfach möglich ist, Apps nicht nur aus dem Play Store von Google, sondern auch aus alternativen Stores oder per direktem Download zu installieren, verbreiten sich Schadprogramme oft über diesem Weg. Ein Angreifer könnte so eine beliebte Software mit einer Schadsoftware infizieren und anschließend wieder zum Download zur Verfügung stellen.

2.3 Fehlende Updates für das Android-Betriebssystem

Viele Hersteller liefern Smartphone und Tablets mit veralteten Versionen von Android aus oder stellen keine regelmäßigen oder sogar überhaupt keine Updates zur Verfügung. Da regelmäßig Schwachstellen in Android entdeckt werden, sind solche Endgeräte besonders gefährdet. Diese Problematik betrifft vor allem günstige Geräte und kleinere Hersteller, aber auch große Hersteller und Premium-Modelle bieten oftmals keine ausreichende Versorgung mit Sicherheitsupdates über einen längeren Zeitraum.

2.4 Risikokonzentration durch ein Benutzerkonto (Google-ID) für alle Google-Dienste

Mit der Google-ID können Benutzer zentral auf alle Google-Dienste zugreifen, z. B. auf die Geräteverwaltung, die aufgezeichneten geographische Positionen, Chatsoftware, Cloud-Speicher, den Play Store, Musik-, Buch- und Filmangebote, Datensicherung, Bookmarks, Password-Speicher für Webseiten und Synchronisationsdienste. Auch viele andere Anbieter von Diensten im Internet verwenden die Google-ID, um Benutzer zu authentisieren.

Kann sich ein Angreifer über die Google-ID authentisieren, kann er alle diese Dienste unter der gestohlenen Identität benutzen. Auch kann er auf alle dort gespeicherten Daten zugreifen und Geräte aus der Ferne lokalisieren oder sie zurücksetzen, also alle Daten auf dem Gerät löschen.

2.5 Integration für vorinstallierte Apps und deren Funktionalitäten bei Android-basierten Geräten

Mit dem Betriebssystem liefern die Hersteller oft bereits tief integrierte und vorinstallierte Apps (z. B. Play Store und die zugehörigen Play Services) sowie Schnittstellen zu Diensten von Drittanbietern (Twitter, Facebook, usw.) aus. Diese Apps kann der Anwender teilweise nicht entfernen. Damit vergrößert sich die Angriffsfläche des Android-Betriebssystems. Auch die nicht löschbaren bzw. nicht konfigurierbaren Schnittstellen sind oft in Institutionen nicht erwünscht.

Insgesamt steigt durch die tiefe Integration von Apps und Schnittstellen von Drittanbietern das Risiko, dass das Gerät mit Schadsoftware infiziert wird oder ein Angreifer unberechtigt darauf zugreifen kann. Der Schutz der Daten auf dem Gerät nimmt dadurch ab.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Android aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	-

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.3.2.4.A1 Auswahl von Endgeräten mit Android

Bei der Auswahl eines Endgeräts mit Android MUSS sichergestellt sein, dass der Hersteller regelmäßig Sicherheitsupdates für dieses Gerät bereitstellt. Das Endgerät MUSS mit einer aktuellen Version von Android ausgeliefert werden oder unmittelbar auf diese aktualisiert werden können.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Android. Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.3.2.4.A2 Deaktivieren der Entwickler-Optionen

In allen Android-basierten Geräten SOLLTEN die Entwickleroptionen deaktiviert sein.

SYS.3.2.4.A3 Einsatz des Multi-User- und Gäste-Modus

Es SOLLTE geregelt sein, ob der Multi-User- und Gäste-Modus verwendet werden darf oder eventuell auch muss. Ein Benutzer auf dem Android-basierten Gerät SOLLTE einer natürlichen Person entsprechen.

SYS.3.2.4.A4 Regelung und Konfiguration von Cloud-Print

Cloud-Print SOLLTE nur dann erlaubt sein, wenn sichergestellt ist, dass der Benutzer nur genehmigte Drucker auswählen kann.

SYS.3.2.4.A5 Erweiterte Sicherheitseinstellungen

Es SOLLTEN nur die freigegebenen Sicherheits-Apps sich als Geräteadministrator oder "Trust Agents" eintragen. Das Sicherheitsmanagement SOLLTE das regelmäßig überprüfen.

Weiterhin SOLLTEN es die Einstellungen für "Zugriff auf Nutzungsdaten und Zugriff auf Benachrichtigungen" nur erlaubten Apps ermöglichen, auf diese schützenswerten Daten zuzugreifen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.3.2.4.A6 Einsatz eines Produkts zum Schutz vor Schadsoftware (CIA)

Es SOLLTE auf Android-basierten Geräten eine Software zum Schutz vor Schadsoftware installiert sein. Die Software SOLLTE immer aktuell sein. Es SOLLTE eine Software eingesetzt werden, die in unabhängigen Tests als sehr gut bewertet worde.

SYS.3.2.4.A7 Zusätzliche Firewall (CI)

Auf Android-basierten Geräten SOLLTE eine Firewall installiert und aktiviert sein.

4 Weiterführende Informationen

4.1 Literatur

- [AN2] Two-factor Authentifizierung
  Google, (zuletzt abgerufen am 27.09.2017)
  https://www.google.com/landing/2step/

- [ANH] Android Hilfe
  Google, (zuletzt abgerufen am 27.09.2017)
  https://support.google.com/android/?hl=de

- [ANL] Übersicht Android-basierte Geräte
  Google, (zuletzt abgerufen am 27.09.2017)
  https://www.android.com

- [ANS] Netzwerke und Sicherheit
  Google, (zuletzt abgerufen am 27.09.2017)
  https://www.android.com/security/overview

- [ANU] App Updates
  Google, (zuletzt abgerufen am 27.09.2017)
  https://support.google.com/googleplay/answer/113412?hl=de

- [GAGB] Google AGB
  Google, (zuletzt abgerufen am 27.09.2017)
  https://www.google.com/policies/terms/

- [GPP] Goggle Pirvacy Policy
  Google, (zuletzt abgerufen am 27.09.2017)
  https://www.google.com/policies/privacy/

- [GSUITE] G Suite für Unternehmen und Bildungseinrichtungen
  Google, (zuletzt abgerufen am 27.09.2017)
  https://gsuite.google.com

- [TR02102] Kryptographische Verfahren- Empfehlungen und Schlüssellängen
  BSI, (zuletzt abgerufen am 27.09.2017)
  https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Android" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.21 Manipulation von Hard- oder Software

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.38 Missbrauch personenbezogener Daten

G 0.39 Schadprogramme

G 0.41 Sabotage

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.14	G 0.16	G 0.21	G 0.28	G 0.30	G 0.32	G 0.38	G 0.39	G 0.41	G 0.46
SYS.3.2.4.A1				x				x		
SYS.3.2.4.A2	x		x			x			x	x
SYS.3.2.4.A3					x					
SYS.3.2.4.A4	x	x								x
SYS.3.2.4.A5					x					
SYS.3.2.4.A6	x		x					x		
SYS.3.2.4.A7	x		x					x		

SYS.3: Mobile Devices

SYS.3.4 Mobile Datenträger

1 Beschreibung

1.1 Einleitung

Mobile Datenträger werden für eine Vielzahl von Zwecken eingesetzt, beispielsweise um Daten zu transportieren, zu speichern oder um sie unterwegs zu nutzen. Es gibt zahlreiche verschiedene Varianten von mobilen Datenträgern, hierzu gehören unter anderem externe Festplatten, CD-ROMs, DVDs, Speicherkarten, Magnetbänder und USB-Sticks.

Datenträger können danach klassifiziert werden, ob sie nur lesbar, einmalig beschreibbar oder wiederbeschreibbar sind. Sie können auch nach weiteren Kriterien unterteilt werden, beispielsweise nach der Art der Datenspeicherung (analog oder digital), wie sie bearbeitet werden können (ohne technische Hilfsmittel, wie z. B. Papier, oder nur mit technischen Hilfsmitteln, wie z. B. DVDs) und nach ihrer Bauform (auswechselbare Datenträger oder externe Datenspeicher oder Datenträger, die in andere Geräte integriert sind).

1.2 Zielsetzung

In diesem Baustein wird aufgezeigt, wie die auf mobilen Datenträgern gespeicherten Informationen sicher genutzt werden können und wie einer unbefugten Weitergabe von Informationen über mobile Datenträger vorgebeugt werden sollte.

1.3 Abgrenzung

Dieser Baustein beschäftigt sich nur mit den grundsätzlichen Sicherheitseigenschaften mobiler Datenträger.

Die unterschiedlichen und mitunter komplexen Anforderungen an Geräte, die sich neben ihrer Hauptfunktion zusätzlich als mobile Datenträger verwenden lassen, wie z. B. Smartphones und Tablets, werden darüber hinaus in den Bausteinen angeführt, die sich mit dem jeweiligen Themengebiet beschäftigen. Ebenso werden vertiefende Aspekte, die den Austausch von digitalen, aber auch analogen Datenträgern betreffen, nicht betrachtet.

Mobile Datenträger können bei persönlichen Treffen oder auch per Versand ausgetauscht werden. Der Austausch von digitalen und analogen Datenträgern, um Informationen zwischen verschiedenen Kommunikationspartnern und IT-Systemen zu übertragen, wird in diesem Baustein nicht betrachtet. Hierzu sind die Anforderungen des Bausteins OPS.1.2.3 Datenträgeraustausch umzusetzen.

Neben den digitalen Datenträgern sind z. B. auch Informationen auf Papier oder anderen analogen Datenträgern bei der Sicherheitskonzeption zu berücksichtigen. Diese Aspekte gehen über die grundsätzlichen Sicherheitseigenschaften mobiler Datenträger hinaus und werden deshalb in anderen Bausteinen behandelt (zum Beispiel SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte, NET.4.3 Fax, OPS.1.1.5 Datensicherung oder OPS.1.2.2 Archivierung).

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind bei Mobilen Datenträgern von besonderer Bedeutung:

2.1 Sorglosigkeit im Umgang mit Informationen

Häufig ist zu beobachten, dass in Institutionen organisatorische Regelungen und technische Sicherheitsverfahren für mobile Datenträger vorhanden sind, diese jedoch durch den sorglosen Umgang mit den Vorgaben und der Technik wieder ausgehebelt werden. So ist beispielsweise immer wieder zu beobachten, dass mitgebrachte mobile Datenträger während der Pausen unbeaufsichtigt im Besprechungsraum oder auch im Zugabteil zurückgelassen werden.

2.2 Unzureichende Kenntnis über Regelungen

Wenn Mitarbeitern und Funktionsträgern die Regelungen für den korrekten Umgang mit mobilen Datenträgern nicht hinreichend bekannt sind, können sie sich auch nicht daran halten. So kann es zu zahlreichen Gefährdungen hinsichtlich der Informationssicherheit kommen, zum Beispiel wenn USB-Sticks gedankenlos an IT-Systeme in der Institution angeschlossen werden.

2.3 Datenverlust bei mobilem Einsatz

Bei mobilen Datenträgern ist das Risiko von Datenverlusten höher als bei stationären Systemen. Eine Ursache hierfür können Diebstahl oder der Verlust der Geräte, aber auch technische Probleme oder schlichter Strommangel, sein. Die auf den Datenträgern abgelegten Informationen sind oft unwiederbringlich verloren.

2.4 Defekte Datenträger

Mobile Datenträger sind aufgrund ihrer Größe und Anwendungsfelder für Beschädigungen, Fehler oder Ausfälle anfällig. Ursache sind beispielsweise ständig wechselnde Einsatzumgebungen oder mechanische Einwirkungen.

2.5 Diebstahl

Immer wieder werden mobile Datenträger gestohlen. Je kleiner und begehrter solche Geräte sind, wie beispielsweise USB-Festplatten oder USB-Sticks, desto höher ist dieses Risiko. Neben dem materiellen Verlust kann weiterer Schaden entstehen, wenn sensible Dateien verloren gehen oder offengelegt werden.

2.6 Beeinträchtigung durch wechselnde Einsatzumgebung

Mobile Datenträger werden in sehr unterschiedlichen Umgebungen eingesetzt und sind dadurch vielen Gefährdungen ausgesetzt. Dazu gehören beispielsweise schädigende Umwelteinflüsse, wie zu hohe oder zu niedrige Temperaturen, ebenso wie Staub oder Feuchtigkeit. Zu anderen Problemen, die durch die Mobilität der Geräte entstehen, gehören beispielsweise Transportschäden. Ein weiterer wichtiger Aspekt ist, dass sie oft in Bereichen mit unterschiedlichem Sicherheitsniveau benutzt werden. Die Kommunikation mit unbekannten IT-Systemen und Netzen birgt immer ein Gefährdungspotenzial für das eigene mobile Endgerät. Wenn die Datenträger an anderen IT-Systemen angeschlossen werden, können beispielsweise auch vertrauliche Informationen, die nicht dazu bestimmt sind, weitergegeben zu werden, mit kopiert werden.

2.7 Verbreitung von Schadprogrammen

Mobile Datenträger werden oft benutzt, um Daten zwischen verschiedenen Geräten und dem Arbeitsplatz auszutauschen. Es besteht die Gefahr, dass sich Schadprogramme auf den mobilen Datenträgern einnisten und sich so auf die Arbeitsplatz-Systeme übertragen.

2.8 Datendiebstahl mit mobilen Datenträgern

Mobile Datenträger, wie z. B. USB-Sticks oder Speicherkarten, sind meistens klein, unauffällig und besitzen eine hohe Speicherkapazität. Da fast alle IT-Systeme über eine entsprechende Schnittstelle für den Einsatz austauschbarer Datenträger verfügen, besteht die Gefahr, dass mit ihnen große Datenmengen unbefugt und unauffällig kopiert werden können.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz von Mobilen Datenträgern aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Benutzer, Fachverantwortliche

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.3.4.A1 Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern

Alle Mitarbeiter MÜSSEN für den sicheren Umgang mit mobilen Datenträger sensibilisiert werden. Die Mitarbeiter MÜSSEN zudem darauf hingewiesen werden, wie sie sorgfältig mit den mobilen Datenträgern umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen bzw. um eine lange Lebensdauer zu gewährleisten.

SYS.3.4.A2 Verlustmeldung mobiler Datenträger [Benutzer]

Es MUSS umgehend gemeldet werden, wenn ein dienstlich genutzter mobiler Datenträger verloren oder gestohlen wird. Das SOLLTE auch für private Datenträger, die dienstlich genutzt werden, gelten. Hierfür MUSS es in jeder Institution klare Meldewege und Ansprechpartner geben.

SYS.3.4.A3 Sicherungskopie der übermittelten Daten [Benutzer]

Sind die zu übertragenden Daten auf einem mobilen Datenträger nur zum Zweck der Datenübertragung erstellt bzw. zusammengestellt worden und nicht auf einem weiteren Medium gespeichert, MUSS eine Sicherungskopie dieser Daten vorgehalten werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Mobile Datenträger. Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.3.4.A4 Erstellung einer Richtlinie zum sicheren Umgang mit mobilen Datenträgern [Benutzer]

Es SOLLTE eine Richtlinie erstellt werden, die festlegt, wie mit mobilen Datenträgern umgegangen wird. Folgende grundlegenden Aspekte SOLLTEN hierbei berücksichtigt werden:

- welche mobilen Datenträger tatsächlich genutzt werden und wer diese einsetzen darf,
- welche Daten auf mobilen Datenträgern gespeichert werden dürfen und welche nicht,
- wie die auf mobilen Datenträgern gespeicherten Daten vor unbefugtem Zugriff, Manipulation und Verlust geschützt werden,

- wie die Daten auf den mobilen Datenträgern gelöscht werden sollen,
- ob und wie private Datenträger genutzt werden dürfen,
- mit welchen externen Mitarbeitern oder Dienstleistern Datenträger ausgetauscht werden dürfen und welche Sicherheitsregelungen dabei zu beachten sind,
- wie verhindert wird, dass mobile Datenträger für die unbefugte Weitergabe von Informationen benutzt werden und
- wie gegen die Verbreitung von Schadsoftware über mobile Datenträger vorgebeugt wird.

Außerdem SOLLTE geregelt werden, wie private mobile Datenträger in der Institution genutzt werden dürfen. Zudem SOLLTE regelmäßig überprüft werden, ob die Sicherheitsvorgaben für den Umgang mit mobilen Datenträgern noch aktuell sind.

SYS.3.4.A5 Regelung der Mitnahme von mobilen Datenträgern

Es SOLLTEN klare schriftliche Regeln geben, die festlegen, ob und wie mobile Datenträgern mitgenommen werden dürfen. Darin SOLLTE insbesondere festgelegt werden, welche Datenträger außer Haus transportiert werden dürfen, wer sie außer Haus mitnehmen darf und welche grundlegenden Sicherheitsmaßnahmen dabei zu beachten sind (Virenschutz, Verschlüsselung schützenswerter Informationen, Aufbewahrung, etc.). Die Benutzer SOLLTEN auf die Regelungen hingewiesen werden.

SYS.3.4.A6 Datenträgerverwaltung [Fachverantwortliche]

Es SOLLTE eine geregelte Verwaltung von mobilen Datenträgern geben. Dazu SOLLTEN die Datenträger einheitlich gekennzeichnet werden. Es SOLLTEN Bestandsverzeichnisse geführt werden. Weiterhin SOLLTE im Rahmen der Datenträgerverwaltung gewährleistet sein, dass mobile Datenträger sachgerecht behandelt und aufbewahrt sowie ordnungsgemäß eingesetzt und transportiert werden. Schließlich SOLLTE auch gewährleistet sein, dass sie sicher gelöscht bzw. vernichtet werden.

SYS.3.4.A7 Sicheres Löschen der Datenträger vor und nach der Verwendung [Fachverantwortliche]

Bevor wiederbeschreibbare Datenträger weitergegeben werden, SOLLTEN sie geeignet gelöscht werden, bevor sie verwendet oder ausgesondert werden.

SYS.3.4.A8 Absicherung von Laufwerken und Schnittstellen für Wechselmedien und externe Datenspeicher

Die Laufwerke und Schnittstellen der IT-Systeme zur Nutzung von mobilen Datenträgern SOLLTEN durch technische und organisatorische Maßnahmen gemäß den Sicherheitsvorgaben abgesichert werden. So SOLLTE verhindert werden, dass Inhalte von eingelegten Wechseldatenträgern automatisch ausgeführt werden. Auch SOLLTEN technische Maßnahmen ergriffen werden, damit das IT-System nicht von anderen als den vorgesehenen Quellen gebootet sowie keinen unautorisierten externen Geräte und Datenträger angeschlossen werden können.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.3.4.A9 Kontrolle und Überwachung von Schnittstellen (CI)

Die Nutzung von Schnittstellen, an denen Datenträger angeschlossen werden können, SOLLTE durch eine entsprechende Rechtevergabe auf Ebene des Betriebssystems oder mit Hilfe von Zusatzprogrammen geregelt werden. Es SOLLTE geprüft werden, ob alternativ überwacht werden kann, ob Geräte hinzugefügt werden. Der Anschluss von Datenträgern SOLLTE protokolliert und die Protokolle von den Verantwortlichen regelmäßig ausgewertet werden.

SYS.3.4.A10 Datenträgerverschlüsselung (C)

Mobile Datenträger SOLLTEN bei erhöhtem Schutzbedarf möglichst immer vollständig verschlüsselt werden, auch wenn sie nur gelegentlich für vertrauliche Informationen eingesetzt werden. Es SOLLTE ein sicherer Verschlüsselungsalgorithmus eingesetzt werden. Um den Anforderungen der Vertraulichkeit der zu übertragenden Informationen zu entsprechen, SOLLTEN entsprechende Verschlüsselungsprogramme auf dem IT-System des Absenders und des Empfängers installiert sein.

SYS.3.4.A11 Integritätsschutz durch Checksummen oder Digitale Signaturen (I)

Um beim Datenaustausch mittels mobiler Datenträger lediglich die Integrität von vertraulichen Informationen sicherzustellen, SOLLTE ein Verfahren zum Schutz gegen zufällige oder vorsätzliche Veränderungen eingesetzt werden. Beispiele sind Checksummen-Verfahren, fehlerkorrigierende Codes, Message Authentication Code (MAC) oder "Digitale Signaturen". Die Verfahren zum Schutz vor Veränderungen SOLLTEN dem aktuellen Stand der Technik entsprechen.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [NIST800150] Guide to Cyber Threat Information Sharing
  Special Publication 800-150, National Institute of Standards and Technology (NIST), 10.2016
  http://dx.doi.org/10.6028/NIST.SP.800-150

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Mobile Datenträger" von Bedeutung.

G 0.01 Feuer

G 0.02 Ungünstige klimatische Bedingungen

G 0.03 Wasser

G 0.04 Verschmutzung, Staub, Korrosion

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.38 Missbrauch personenbezogener Daten

G 0.39 Schadprogramme

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen Anforderungen	G 0.01	G 0.02	G 0.03	G 0.04	G 0.14	G 0.16	G 0.17	G 0.19	G 0.21	G 0.22	G 0.23	G 0.24	G 0.25	G 0.26	G 0.29	G 0.30	G 0.38	G 0.39	G 0.41	G 0.42	G 0.45	G 0.46
SYS.3.4.A1	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
SYS.3.4.A2					x					x								x				x
SYS.3.4.A3						x	x	x													x	
SYS.3.4.A4	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
SYS.3.4.A5	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
SYS.3.4.A6	x	x	x	x	x	x	x	x	x			x	x	x		x	x					x
SYS.3.4.A7					x	x	x	x									x	x		x		x
SYS.3.4.A8					x	x	x	x	x		x					x		x			x	x
SYS.3.4.A9					x	x	x	x	x		x					x		x	x		x	x
SYS.3.4.A10					x	x	x	x	x	x	x				x		x		x	x	x	x
SYS.3.4.A11					x	x	x	x	x	x							x		x	x	x	x

SYS.4: Sonstige Systeme

SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte

1 Beschreibung

1.1 Einleitung

Obwohl sehr viele Informationen digital gespeichert sind, kann häufig auf Papierdokumente nicht verzichtet werden. Auch lesen oder bearbeiten viele Personen Dokumente lieber auf Papier als am Bildschirm. Drucker, Kopierer und Multifunktionsgeräte werden daher noch lange unverzichtbare Arbeitsmittel sein, die in so gut wie in allen Büros zu finden sind.

Es ist es oft nicht effizient, jeden einzelnen Arbeitsplatz mit einem solchen Gerät auszustatten. Daher werden häufig zentrale Netzdrucker, Kopierer oder Multifunktionsgeräte eingesetzt, auf denen die Benutzer ihre Dokumente ausdrucken, einscannen oder vervielfältigen können. Da es einige Nachteile hat, wenn Aufträge vom Arbeitsplatz-PC direkt an einen Netzdrucker verschickt werden, setzen die meisten Institutionen zudem einen zentralen Druckserver ein, der die Aufträge annimmt und auf die verfügbaren Drucker verteilt.

Dieser Baustein behandelt die Sicherheit von vernetzten Druckern, Kopierern, Multifunktionsgeräten, Druckservern und Dokumentenscannern. Als Multifunktionsgeräte werden dabei Geräte bezeichnet, die mehrere verschiedene papierverarbeitende Funktionen bieten, die also drucken, kopieren und scannen oder auch Fax-Dienste ermöglichen.

1.2 Zielsetzung

Ziel des Bausteins ist es, zu beschreiben, wie Drucker, Kopierer und Multifunktionsgeräte sicher betrieben werden können, so dass weder Informationen über diese abfließenabfliessen können noch die Sicherheit der internen IT-Netze beeinträchtigt wird.

1.3 Abgrenzung

Bei Druckservern kann es sich um gewöhnliche IT-Systeme handeln, die als entsprechende Server betrieben werden. In diesem Fall müssen betriebssystemspezifische Sicherheitsanforderungen für die Server umgesetzt werden, die dieser Baustein jedoch nicht beschreibt, sondern die in den Bausteinen SYS.1.1 *Allgemeiner Server* und den jeweiligen bBetriebssystem-spezifischen Server-Bausteinen zu finden sind. Auch werden keine Sicherheitsanforderungen für den Netzdienst Samba, mit dem Drucker in Netzen zentral bereitgestellt werden können, definiert. Hierfür ist der Baustein APP.3.4 *Samba* anzuwenden.

Der vorliegende Baustein geht nicht auf Sicherheitsanforderungen für Clients ein, diese sind Bestandteil der Bausteine SYS.2.1 Allgemeiner Client und den jeweiligen betriebssystemspezifischen Client-Bausteinen.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich *Drucker, Kopierer und Multifunktionsgeräte* von besonderer Bedeutung:

2.1 Unzureichende oder falsche Versorgung mit Verbrauchsgütern

Viele Drucker, Kopierer und Multifunktionsgeräte benötigen für einen reibungslosen und unterbrechungsfreien Betrieb bestimmte Verbrauchsgüter in ausreichender Menge. Fehlen diese Verbrauchsgüter oder werden sie falsch eingesetzt, kann der Betriebsablauf empfindlich gestört werden. So kann beispielsweise ungeeignete Tinte einen Tintenstrahldrucker verunreinigen und zu Fehlfunktionen des Druckers führen. In Notfällen kann die Handlungsfähigkeit der Institution stark beeinträchtigt sein und es können hohe Folgekosten entstehen, zum Beispiel wenn sich wichtige Verträge nicht ausdrucken lassen.

2.2 Unerlaubte Einsicht in ausgedruckte Dokumente

Bei Netzdruckern verbleiben oft ausgedruckte Dokumente eine längere Zeit im Ausgabefach. Besonders wenn sich die Drucker nicht im direkten Umfeld befinden, drucken die Benutzer häufig mehrere Dateien aus, bevor sie alle zusammen abholen. Da Etagen- oder Abteilungsdrucker von vielen Mitarbeitern benutzt werden, können so auch unberechtigte Personen Ausdrucke mit schützenswerten Informationen einsehen oder entwenden. Das muss nicht einmal böswillig geschehen: Wenn Mitarbeiter beispielsweise eine längere Zeitspanne auf ihren Ausdruck am Gerät warten müssen, werden sie eventuell die Wartezeit überbrücken und schauen, was andere Kollegen ausgedruckt haben. Auch an Kopierern finden sich immer wieder vertrauliche Dokumente, die dort beispielsweise im Einzug vergessen wurden.

Benutzer suchen häufig nicht nach Ursachen, wenn sie ihre Ausdrucke sich nicht am Drucker finden. Stattdessen vermuten sie IT-Probleme und starten einen neuen Druckauftrag, da sie daran gewöhnt sind, dass mit der Hard- und Software immer wieder Probleme und auch unerklärliche Phänomene auftreten. Die Ausdrucke könnten allerdings auch von anderen mitgenommen worden sein. Ebenso kommt es häufig vor, dass Benutzer an ihrem Arbeitsplatz-Rechner versehentlich einen anderen Drucker ausgewählt haben. Typischerweise suchen dann die Benutzer ihre Ausdrucke am falschen Drucker, finden sie dort nicht und starten einfach einen neuen Druckauftrag, diesmal am Standard-Drucker. Dadurch finden sich an vielen Netzdruckern Fehlausdrucke, die nicht abgeholt werden.

2.3 Fehlerhafter Zugriffsschutz zur Administration

Bei einigen Druckern, Kopierern und Multifunktionsgeräten kann der Zugriff auf die Administrationsschnittstelle nicht abgesichert werden, also auch nicht über eine Passwortabfrage geschützt werden. Mit Administratorrechten könnte ein Angreifer die Geräte manipulieren. Das ist in einigen Fällen nicht nur von Arbeitsplätzen des lokalen Netzes möglich, sondern auch aus dem Internet.

Viele Netzdrucker und Hochleistungskopierer haben eingebaute Webserver, um sie leichter administrieren zu können. Komfort wird hier aber mit zusätzlichen Risiken erkauft: So wird häufig die Webschnittstelle bei der Konfiguration vernachlässigt, sodass interne oder sogar externe Personen die Druckerkonfiguration und -nutzung manipulieren können. Beispielsweise könnten von beliebigen Benutzern absichtlich oder unbeabsichtigt Druckaufträge anderer gelöscht oder die Verfügbarkeit des Gerätes beeinträchtigt werden. Manche Webserver liefern außerdem Diagnosedaten zurück, wenn eine überlange URL angegeben wird. Mit diesen Informationen können Angriffe entwickelt werden.

2.4 Missbrauch der Adressbuchfunktion

Verschiedene Hersteller haben auf Druckern, Kopierern und Multifunktionsgeräten eine Adressbuchfunktion für den integrierten E-Mail- oder Faxversand implementiert. Werden solche Funktionen benutzt, ist es schwierig auszuschließen, dass Daten über den Drucker unberechtigt weitergeleitet werden, z. B. ins Internet.

2.5 Unverschlüsselte Druckerkommunikation

Drucker, Kopierer und Multifunktionsgeräte werden oft nicht lokal angesteuert, sondern über einen Netzanschluss. Der Druckertreiber des jeweiligen lokalen Rechners sendet dazu alle benötigten Informationen direkt an den Drucker oder an einen zentralen Druckerserver, der diese an einen Drucker weiterleitet. Diese Datenübertragung wird nur selten verschlüsselt. Dadurch könnte ein Angreifer direkt über das Netz mitlesen, was ausgedruckt wird.

Unverschlüsselte Kommunikationsschnittstellen zur Administration bilden eine weitere Gefahrenquelle. Bei einem Zugriff über HTTP oder Telnet werden die übertragenen Informationen ungeschützt transportiert. In dem Fall könnte ein Angreifer die Kommunikation und somit beispielsweise das Passwort zur Konfiguration mitlesen und es für Angriffe auf die Vertraulichkeit, Verfügbarkeit und Integrität benutzen.

2.6 Fehlende Netztrennung

Sicherheitsgateways zwischen LAN und Internet werden häufig so konfiguriert, dass der Internet-Zugriff für ganze Subnetze freigeschaltet ist. Andererseits werden Drucker, Kopierer und Multifunktionsgeräte oft dem gleichen Subnetz zugeordnet wie die Arbeitsplatz-PCs, von denen auf diesen Geräten gedruckt wird. Dadurch kann es passieren, dass z. B. auch die Netzdrucker auf das Internet zugreifen können. Wenn die Verbindungen von und zu den Druckern aus dem Internet nicht von den Sicherheitsgateways abgewiesen werden, können unter Umständen sensible Informationen unerwünscht das Netz verlassen. Umgekehrt könnte ein netzfähiges Gerät aber auch unerwünscht Daten aus dem Internet empfangen und eventuell weiter verteilen. Ein Netzdrucker kann dadurch z. B. zu einem Einfallstor für Angriffe aus dem Internet werden.

2.7 Beeinträchtigung von Gesundheit und Umwelt

Laserdrucker und Kopierer nutzen meist Trockentoner, der auf das Papier übertragen wird. Der staubförmige Toner enthält neben dem eigentlichen Farbstoff auch Schwermetalle wie Blei und Cadmium. Dieser Tonerstaub wird nicht komplett auf das Papier übertragen, sodass sich Reste davon im gesamten Raum verteilen können. Auch beim Austausch einer fast leeren Toner-Kartusche kann Toner austreten. So kann der feine gesundheitsgefährdende Tonerstaub eingeatmet werden und sich in der Lunge ablagern. Zusätzlich wird bei einigen Geräten im Betrieb Ozon freigesetzt. Moderne Geräte besitzen aber Filter, die die Freigabe von Ozon verringern.

2.8 Auswertung von Restinformationen

Viele Kopierer, Drucker und Multifunktionsgeräte sind mit einem umfangreichen internen Speicher ausgestattet. Wenn Informationen dort abgelegt wurden, können eventuell auch unberechtigte Personen hierauf zugreifen. Im einfachsten Fall ist es dabei lediglich möglich, das zuletzt gespeicherte Dokument auszudrucken. Problematischer ist es, wenn Angreifer den gesamten Speicher auslesen können, um dessen Inhalt zu analysieren.

Auch wenn die gespeicherten Informationen direkt nach der Verwendung gelöscht werden, könnten die gelöschten Daten rekonstruiert werden. Nicht jedes Gerät überschreibt die Daten zusätzlich zur Löschung noch einmal.

Häufig werden digitale Kopierer oder Drucker nur gemietet. Nach einem vorher festgelegten Zeitraum wird das Gerät dann zurückgegeben und eventuell gegen ein aktuelleres ausgetauscht. Der Vermieter oder der nächste Besitzer des Geräts könnten so Zugriff auf noch vorhandene Informationen im Speicher erhalten.

2.9 Yellow Dots

Auf bestimmten Druckern und Kopierern werden auf das Papier sogenannte "Yellow Dots" (oder auch "Machine Identification Code, "tracking dots", "secret dots") gedruckt. Diese oft undokumentierten Wasserzeichen können das Datum und die Zeit sowie die Seriennummer des Druckers beinhalten und sind

mit dem bloßen Auge kaum zu erkennen. Auf diese Weise kann ein Ausdruck direkt einer Institution oder sogar einem bestimmten Benutzer zugewiesen und so zum Verfasser zurückverfolgt werden. Neben datenschutzrechtlichen Auswirkungen könnten so ungewollt Informationen die Institution verlassen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Drucker, Kopierer und Multifunktionsgeräte aufgeführt. Grundsätzlich ist der *IT-Betrieb* für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Benutzer, Innerer Dienst, Leiter Haustechnik, Leiter IT

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.4.1.A1 Erstellung eines Basis-Konzepts für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten [Leiter IT]

Bevor Drucker, Kopierer und Multifunktionsgeräte beschafft werden, MÜSSEN die Verantwortlichen ein Basis-Konzept für den sicheren Einsatz entwickeln. Darin MUSS geregelt sein, wo die Geräte aufgestellt werden dürfen, wer darauf zugreifen darf und wie sie vor Angriffen geschützt werden sollen.

SYS.4.1.A2 Geeignete Aufstellung von Druckern, Kopierern und Multifunktionsgeräten

Drucker, Kopierer und Multifunktionsgeräte SOLLTENMÜSSEN so aufgestellt werden, dass nur befugte Benutzer zu ihnen Zutritt haben. Zumindest SOLLTEN sie NICHT in Bereichen aufgestellt werden, in denen sich häufig Externe aufhalten, also nicht in der Nähe von Besprechungs-, Veranstaltungs- oder Schulungsräumen. Außerdem SOLLTENMÜSSEN die Benutzer dafür sensibilisiert werden, dass keine vertraulichen Dokumente an den Geräten liegengelassen werden sollten.

SYS.4.1.A3 Regelmäßige Aktualisierung

Es MUSS regelmäßig überprüft werden, ob die Drucker, Kopierer und Multifunktionsgeräte auf dem aktuellen Stand sind. Wenn Sicherheitslücken identifiziert werden, MÜSSEN diese so schnell wie möglich behoben werden. Vorhandene Patches und Updates MÜSSEN sofort eingespielt werden oder anderweitige Sicherheitsmaßnahmen ergriffen werden, wenn keine Patches zur Verfügung stehen. Generell MUSS darauf geachtet werden, dass Patches und Updates nur aus vertrauenswürdigen Quellen bezogen werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Drucker, Kopierer und Multifunktionsgeräte. Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.4.1.A4 Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten [Leiter IT]

Aufbauend auf dem Konzept aus SYS.4.1.A1 Erstellung eines *Basis-Konzepts für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten* SOLLTEN für die jeweiligen Teilkomponenten spezifische Sicherheitskonzepte entwickelt werden. Darin SOLLTEN beispielsweise allgemeine Fragen geregelt werden. Zum Beispiel: Sollen lokale oder netzfähige Drucker verwendet werden? Wer darf welche Funktionen benutzen? Welche Richtlinien soll es geben? Weiterhin SOLLTEN Aspekte geregelt werden wie

- Dokumentenzugriff,
- Patchen der Geräte,
- Schutz der Geräte,
- Verfügbarkeit und
- Verschlüsselung (Speicher und Kommunikation).

Ebenso SOLLTE sichergestellt werden, dass der Speicher der Geräte gelöscht wird, nachdem sie verwendet wurden. Alle getroffenen Entscheidungen SOLLTEN nachvollziehbar dokumentiert werden.

SYS.4.1.A5 Erstellung von Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten

Für den sicheren Umgang mit Druckern, Kopierern und Multifunktionsgeräten MUSS eine Administratorenrichtlinie ausgearbeitet werden. Für Benutzer MUSS außerdem ein Merkblatt erstellt werden, auf dem die Sicherheitsrichtlinien für die Benutzer übersichtlich zusammengefasst sind. Das Merkblatt MUSS allen Benutzern bekannt gemacht werden.

SYS.4.1.A6 Sicherer Einsatz von CUPS

Benutzt eine Institution das netzfähige Drucksystem Common Unix Printing System (CUPS), SOLLTE dessen Konfiguration den festgelegten Regelungen für Drucker, Kopierer und Multifunktionsgeräte entsprechen. Der administrative Zugriff auf den CUPS-Server SOLLTE beschränkt werden. Den Druckserver SOLLTEN (berechtigte) Benutzer nur zum Drucken nutzen können.

SYS.4.1.A7 Beschränkung der Administrationszugriffe auf Drucker, Kopierer und Multifunktionsgeräte

Der Zugriff auf die Konfiguration von Druckern, Kopierern und Multifunktionsgeräten SOLLTE beschränkt werden. Wenn Administratoren die Geräte mittels Fernzugriff konfigurieren, SOLLTE das durch eine Authentisierung und eine verschlüsselte Verbindung geschützt werden. Ebenso SOLLTEN alle nicht benötigten Funktionen von Druckern, Kopierern und Multifunktionsgeräten abgeschaltet sein.

SYS.4.1.A8 Versorgung und Kontrolle der Verbrauchsgüter [Innerer Dienst, Benutzer]

Drucker, Kopierer und Multifunktionsgeräte sind auf Verbrauchsgüter wie Papier oder Toner angewiesen, um funktionieren zu können. Die Versorgung mit diesen Verbrauchsgütern SOLLTE sichergestellt sein. Die Entsorgung der Verbrauchsgüter SOLLTE geregelt sein. Die Verantwortlichkeiten hierfür SOLLTEN geregelt und kommuniziert werden.

SYS.4.1.A9 Protokollierung bei Druckern, Kopierern und Multifunktionsgeräten

Aktivitäten auf Druckern, Kopierern und Multifunktionsgeräten SOLLTEN protokolliert werden. Es SOLLTE abgestimmt sein, was protokolliert wird, wo dies gespeichert wird und wer dies in welchen Zeiträumen auswertet. Nur berechtigte Personen SOLLTEN auf die protokollierten Informationen zugreifen können. Wenn die Verantwortlichen die Protokolle auswerten, SOLLTEN dabei geltenden Gesetze und Vorschriften eingehalten werden, zum Beispiel zum Datenschutz. Unberechtigte SOLLTEN nicht auf die Protokolldaten zugreifen können. Zudem SOLLTE sichergestellt sein, dass alle Geräte eine korrekte Systemzeit haben.

SYS.4.1.A10 Einsatz von netzfähigen Dokumentenscannern

Wenn netzfähige Scanner eingesetzt werden, SOLLTEN nur berechtigte Personen auf die digitalisierten Dokumente zugreifen können. Die gescannten Informationen SOLLTEN sicher zum Client des Erfassenden übertragen werden. Alle Speicherbereiche des Scanners SOLLTEN nach der Benutzung gelöscht werden. Beim Scannen SOLLTEN geeignete Bildkompressionsverfahren verwendet werden.

SYS.4.1.A11 Netztrennung beim Einsatz von Multifunktionsgeräten

Wenn eine Institution Multifunktionsgeräte einsetzt, die sich direkt an das Telefonnetz anschließen lassen, SOLLTE überprüft werden, ob die Fax- und Modem-Funktionalität der Geräte abgeschaltet werden kann. Wird diese Funktion doch benutzt, SOLLTEN unkontrollierte Datenverbindungen zwischen dem LAN und Fremdnetzen zuverlässig unterbunden werden. Netzfähige Drucker, Multifunktionsgeräte und auch Dokumentenscanner SOLLTEN in einem separaten Netzsegment angeschlossen werden, das insbesondere von externen Netzen getrennt ist.

SYS.4.1.A12 Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln [Leiter Haustechnik, Benutzer]

Es SOLLTE sichergestellt und geregelt sein, dass alle schutzbedürftigen Betriebsmittel, die bei Druckern, Kopierern und Multifunktionsgeräten anfallen, ordnungsgemäß entsorgt werden. Damit Mitarbeiter schutzbedürftiges Material entsorgen können, SOLLTEN geeignete Entsorgungseinrichtungen vorhanden sein, z. B. Aktenvernichter.

Wenn das Material erst gesammelt und später entsorgt wird, SOLLTE es vor unberechtigtem Zugriff geschützt sein. Die mit der Entsorgung beauftragten Unternehmen SOLLTEN regelmäßig daraufhin überprüft werden, ob der Entsorgungsvorgang verlässlich ist.

SYS.4.1.A13 Sichere Außerbetriebnahme von Druckern, Kopierern und Multifunktionsgeräten

Bevor *Drucker, Kopierer und Multifunktionsgeräte* entsorgt, zurückgegeben oder ausgetauscht werden, SOLLTEN alle auf ihnen befindlichen Information sicher gelöscht werden. Auch SOLLTEN die Verantwortlichen überprüfen, ob die Speicherinhalte tatsächlich gelöscht sind.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.4.1.A14 Authentisierung bei Druckern, Kopierern und Multifunktionsgeräten (CI)

Es SOLLTEN Geräte mit einer Authentisierungsmöglichkeit eingesetzt werden. Diese Funktion SOLLTE aktiviert und genutzt werden.

SYS.4.1.A15 Informationsschutz bei Druckern, Kopierern und Multifunktionsgeräten (CI)

Bei einem erhöhtem Schutzbedarf SOLLTEN die eingesetzten Drucker, Kopierer und Multifunktionsgeräte Informationen verschlüsselt abspeichern. Auch SOLLTEN Druckaufträge nur verschlüsselt an die Geräte übertragen werden.

Weiterhin SOLLTE durch geeignete Mechanismen sichergestellt werden, dass sich gelöschte Daten aus dem Gerätespeicher nicht wiederherstellen lassen. Letztlich SOLLTEN auch Maßnahmen ergriffen werden, die es Angreifern erschweren, interne Speicherkomponenten von Druckern, Kopierern und Multifunktionsgeräten auszubauen.

SYS.4.1.A16 Notfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten

Die Ausfallzeiten von Druckern, Kopierern und Multifunktionsgeräten SOLLTEN so gering wie möglich sein. Deshalb SOLLTEN bei höherem Schutzbedarf unter anderem

- Ersatzgeräte bereitstehen,
- in Wartungsverträgen auf eine angemessene Reaktionszeit geachtet werden,
- eine Liste mit Fachhändlern geführt werden, um schnell Ersatzgeräte oder -teile beschaffen zu können und
- falls erforderlich, Ersatzteile gelagert werden, die häufig benötigt werden.

4 Weiterführende Informationen

4.1 Literatur

- [ACSD] Datenschutz und Sicherheit in Druckinfrastrukturen
  mc² management consulting GmbH, 12.2016 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/partner/161219_mc2_drucker_sicherheit.pdf

- [CERT] Informationen zu Schwachstellen und Sicherheitslücken von Druckern und zugehörigen Diensten, Warn- und Informationsdienst
  CERT-Bund, (zuletzt abgerufen am 28.09.2017)
  https://www.cert-bund.de/search

- [CSE015] Netzwerk-verbundene Bürogeräte
  CSE 015, V1.0, Allianz für Cyber-Sicherheit, 10.2012 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_015.html

- [CSE069] Sichere Passwörter in Embedded Devices
  CSE 069, V1.0, Allianz für Cyber-Sicherheit vom 12.2013 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_069.html

- [NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations
  Special Publication 800-53, Revision 4, NIST, 04.2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

- [PP0058] IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600-2008 Operational Environment B, IEEE Std 2600.2-2009, IEEE Computer Society, Information Assurance (C/IA) Committee, BSI-CC-PP-0058-2010, 07.2010
  https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0058.html

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Drucker, Kopierer und Multifunktionsgeräte" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.37 Abstreiten von Handlungen

G 0.39 Schadprogramme

Elementare Gefährdungen Anforderungen	G 0.14	G 0.16	G 0.18	G 0.19	G 0.21	G 0.23	G 0.25	G 0.27	G 0.30	G 0.32	G 0.37	G 0.39
SYS.4.1.A1			x									
SYS.4.1.A2	x	x		x	x	x						
SYS.4.1.A3						x	x		x			x
SYS.4.1.A4			x									
SYS.4.1.A5	x			x		x			x	x		
SYS.4.1.A6	x	x		x		x		x		x		x
SYS.4.1.A7	x			x		x			x	x	x	
SYS.4.1.A8			x					x				
SYS.4.1.A9											x	
SYS.4.1.A10	x			x		x			x	x		
SYS.4.1.A11	x			x		x						x
SYS.4.1.A12	x	x		x								
SYS.4.1.A13	x	x		x		x						
SYS.4.1.A14	x			x	x	x			x	x		x
SYS.4.1.A15	x			x		x						
SYS.4.1.A16							x					

SYS.4: Sonstige Systeme

SYS.4.4 Allgemeines IoT-Gerät

1 Beschreibung

1.1 Einleitung

In diesem Baustein werden Geräte mit Funktionalitäten aus dem Bereich Internet of Things (IoT) betrachtet. Dies sind im Gegensatz zu "klassischen" IT-Systemen "intelligente" Gegenstände, die zusätzliche "smarte" Funktionen enthalten. IoT-Geräte werden in der Regel an Datennetze angeschlossen, in vielen Fällen drahtlos, und können sogar oft auf das Internet zugreifen und darüber erreicht werden. Hierdurch können sie Auswirkungen auf die Informationssicherheit des gesamten Informationsverbunds haben.

IoT-Geräte können in Institutionen vorhanden sein, weil sie durch Mitarbeiter oder Externe mitgebracht werden, z. B. Smartwatches oder Wearables. In vielen Institutionen werden aber auch IoT-Geräte beschafft und betrieben, z. B. Geräte wie Brand-, Gas- und andere Warnmelder, Kaffeemaschinen oder Elemente der Gebäudesteuerung wie Kameras und HVAC (Heating, Ventilation and Air Conditioning).

Generell kann zwischen direkt adressierbaren IoT-Geräten und IoT-Geräten, die eine zentrale Steuereinheit voraussetzen, unterschieden werden. Direkt adressierbare Geräte werden in der Regel mit einer eigenen IP-Adresse an ein Datennetz angeschlossen und können autark agieren oder durch eine zentralen Steuereinheit verwaltet werden. Es gibt aber auch IoT-Geräte, die ausschließlich direkt mit Steuereinheiten kommunizieren, z. B. über Funknetze wie Bluetooth oder ZigBee, und somit nicht direkt an Datennetze angeschlossen werden. Die Reichweite dieser Funkverbindungen kann, wenn vorgesehen, über ein separates, vermaschtes Netz vergrößert werden, indem jedes Gerät mit jedem Gerät eine Funkverbindung aufbaut.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, IoT-Geräte so abzusichern, dass über diese weder die Sicherheit der Informationen und IT der eigenen Institution noch die von Außenstehenden beeinträchtigt wird. Daher sollte sowohl ein unautorisierter Datenabfluss als auch die Manipulation der Geräte verhindert werden, speziell mit Blick auf Angriffe auf Dritte.

1.3 Abgrenzung

Dieser Baustein beschäftigt sich allgemein mit IoT-Geräten und soll für ein großes Spektrum unterschiedlicher IoT-Geräte anwendbar sein. Auf dedizierte Sicherheitseigenschaften etwa von Bedien- und Anzeigesystemen oder spezifischen Hard- und Software-Architekturen wird nicht näher eingegangen.

Je nach Ausprägung der IoT-Geräte sind die Übergänge zu Industriellen Steuerungssystemen (ICS-Systemen) oder eingebetteten Systemen fließend. Anforderungen für Geräte, die im Bereich Produktion und Fertigung eingesetzt werden, sind in den Bausteinen der Schicht IND (Industrielle IT) zu finden.

Eingebettete Systeme sind informationsverarbeitende Systeme, die in ein größeres System oder Produkt integriert sind, dort Steuerungs-, Regelungs- und Datenverarbeitungsaufgaben übernehmen und dabei oft nicht direkt vom Benutzer wahrgenommen werden. Für diese ist Baustein SYS.4.3 Eingebettete Systeme umzusetzen.

Anforderungen für die häufig im Kontext eingesetzten Funkstrecken befinden sich in den Bausteinen der Schicht NET.2 Funknetze.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich IoT-Geräte von besonderer Bedeutung:

2.1 Ausspähung über IoT-Geräte

Bei der Entwicklung von IoT-Geräten ist der Aspekt der Informationssicherheit typischerweise ein nicht oder nur nachrangig beachtetes Entwurfsziel. Daher konnten IoT-Geräte immer wieder missbraucht werden, um über diese Informationen über die Nutzer bzw. den Einsatzbereich zu sammeln. So ist es immer wieder zu Vorfällen mit vernetzten bzw. IP-basierten Überwachungskameras gekommen, z. B.:

- 2013 wurden mehrere Banken in verschiedenen Ländern im Zuge der Kampagne "Carbanak" über Überwachungskameras kompromittiert. Die Täter erbeuteten einen dreistelligen Millionenbetrag. Bei diesen Angriffen wurden über die Kameras Bildschirminhalte und Tastatureingaben in den Finanzinstituten ausgespäht.
- 2014 wurden über die Webseite Insecam die Videobilder bzw. -streams von 73.000 unzureichend geschützten Webcams offen zur Verfügung gestellt.
- 2015 infizierte die zu dem Zeitpunkt 8 Jahre alte Schadsoftware Conficker eine Vielzahl von Bodycams verschiedener Polizeien.

2.2 Verwendung von UPnP

In LANs integrierte IoT-Geräte bauen oftmals selbstständig eine Verbindung zum Internet auf, indem sie Router im Netz per UPnP (Universal Plug and Play) so konfigurieren, dass eine Portweiterleitung entsteht. Die Geräte können dann nicht nur ins lokale Netz kommunizieren, sondern sind auch von außerhalb des LANs nicht nur sichtbar, sondern auch erreichbar. Wenn dann eine Schwachstelle im IoT-Gerät durch einen Angreifer ausgenutzt wird, könnte dieses dadurch Teil eines Botnetzes werden, es könnte aber auch weitere Schadsoftware in den Informationsverbund eingeschleust werden. Diese Lücke kann theoretisch zu einem späteren Zeitpunkt auch für andere Aktivitäten genutzt werden.

2.3 Schäden Dritter

Wenn IoT-Geräte nicht regelmäßig gepatcht werden, bleiben bekannte Schwachstellen offen und können für umfangreiche Angriffe ausgenutzt werden. Ein Ziel eines Angriffs könnte dabei sein, die IoT-Geräte in ein Botnetz zu integrieren. In diesem Fall könnten sie beispielsweise dazu genutzt werden, um DDoS-Angriffe (Distributed Denial of Service) auszuführen und die Verfügbarkeit von Diensten einzuschränken.

Beispiel: Ende Oktober 2016 wurde ein DDoS-Angriff auf einen Internetdienstleister durchgeführt, bei dem ein Botnetz benutzt wurde, das zu großen Teilen aus IoT-Geräten bestand. Das sogenannte Mirai-Botnetz hat dabei auf Grund der großen Anzahl der Geräte eine Bandbreite erreicht, die weit über die vorher bekannten Botnetze hinausging. Die Webcams, Kameras, DVR Player, Router und Drucker, die bereits zum Botnetz gehörten, scannten selbstständig das Internet nach weiteren Geräten, um sie mit Schadsoftware zu infizieren und dem Botnetz hinzuzufügen.

2.4 Spionageangriffe mittels Hintertüren in IoT-Geräten

Ende September 2016 wurde bekannt, dass einige Modelle von Überwachungskameras und Raumsensoren mit Hintertüren ausgestattet sind, die Spionage ermöglichen. Dies betrifft insbesondere Überwachungskameras, die in Rechenzentren und Serverräumen eingesetzt werden. Die Hintertüren ermög-

lichten offenbar, auf die Bild- und Videodaten der Kameras zuzugreifen sowie diese Daten auf Server im Internet zu kopieren. So können z. B. Benutzer- und Administrations-Kennwörter kompromittiert werden oder Gerätekonfigurationen, Infrastrukturdetails und sonstige vertrauliche Informationen Dritten zugänglich werden. Dies erleichtert weitergehende Angriffe, indem die Gewohnheiten des Personals ausgenutzt werden.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich IoT aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Beschaffungsstelle, Haustechnik, Informationssicherheitsbeauftragter (ISB)

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.4.4.A1 Einsatzkriterien für IoT-Geräte

IoT-Geräte MÜSSEN ein Minimum an Sicherheitskriterien erfüllen, damit sie in Institutionen eingesetzt werden können. Die Geräte MÜSSEN Update-Funktionen besitzen und der Hersteller MUSS einen Update-Prozess anbieten. Die Geräte MÜSSEN eine Authentisierung ermöglichen. Es DÜRFEN KEINE fest codierten Zugangsdaten im Gerät existieren.

SYS.4.4.A2 Authentisierung

Um ein IoT-Gerät in einer Institution zu nutzen, MUSS eine Authentisierung aktiviert sein. Werden hierfür Passwörter verwendet, MÜSSEN sichere Passwörter benutzt werden. Hierfür SOLLTE es eine Passwort-Richtlinie geben. Diese Passwörter MÜSSEN komplex genug sein, geheim gehalten und regelmäßig gewechselt werden. Voreingestellte Passwörter MÜSSEN geändert werden. Zusätzlich empfiehlt sich die Verwendung von alternativen Authentisierungsmechanismen, wie z. B. zertifikatsbasierte Authentisierung.

SYS.4.4.A3 Regelmäßige Aktualisierung

Es MUSS regelmäßig überprüft werden, ob die IoT-Geräte und zugehörige Komponenten wie Sensoren oder Management-Systeme auf dem aktuellen Stand sind. Wenn Sicherheitslücken identifiziert werden, MÜSSEN diese so schnell wie möglich behoben werden. Vorhandene Patches und Updates MÜSSEN sofort eingespielt werden oder anderweitige Sicherheitsmaßnahmen ergriffen werden, wenn keine Patches zur Verfügung stehen. Generell MUSS darauf geachtet werden, dass Patches und Updates nur aus vertrauenswürdigen Quellen bezogen werden.

SYS.4.4.A4 Aktivieren von Autoupdate-Mechanismen

Automatische Update-Mechanismen (Autoupdate) MÜSSEN aktiviert werden, sofern nicht andere Mechanismen, wie regelmäßige manuelle Wartung oder ein zentrales Softwareverteilungssystem für Updates eingesetzt werden. Wenn für Autoupdate-Mechanismen ein Zeitintervall vorgegeben werden kann, SOLLTE mindestens täglich automatisch nach Updates gesucht und diese installiert werden.

SYS.4.4.A5 Einschränkung des Netzzugriffs

Der Netzzugriff von IoT-Geräten MUSS auf das erforderliche Minimum eingeschränkt und kontrolliert werden. Dazu gehören:

- Verkehrskontrolle an Netzübergängen, z. B. durch Regelwerke auf Firewalls und Access Control Lists (ACLs) auf Routern. Es dürfen nur zuvor definierte ein- und ausgehende Verbindungen erlaubt werden.
- Restriktive Konfiguration des Routings auf IoT-Geräten und Sensoren, insbesondere die Unterdrückung von Default-Routen.
- Signaturen auf Intrusion-Prevention-Systemen (IPS).
- Die IoT-Geräte und Sensoren SOLLTEN in einem eigenen Netzsegment betrieben werden, das ausschließlich mit dem Netzsegment für das Management kommunizieren darf.
- Konfiguration von Virtual Private Networks (VPNs) zwischen den Netzen mit IoT-Geräten und Sensor-Netzen und den Management-Netzen .
- UPnP-Funktion MUSS an allen Routern deaktiviert sein.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Allgemeines IoT-Gerät. Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.4.4.A6 Aufnahme von IoT-Geräten in die Sicherheitsrichtlinie der Institution

In der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die Anforderungen an IoT-Geräte konkretisiert werden. Die Richtlinie SOLLTE allen Personen, die an der Beschaffung und dem Betrieb von IoT-Geräten beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft und die Ergebnisse sinnvoll dokumentiert werden.

SYS.4.4.A7 Planung des Einsatzes von IoT-Geräten

Zum sicheren Betrieb von IoT-Geräten SOLLTE im Vorfeld geplant werden, wo und wie diese eingesetzt werden sollen. Die Planung SOLLTE dabei nicht nur Aspekte betreffen, die klassischerweise mit dem Begriff Informationssicherheit verknüpft werden, sondern auch normale betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen. Dabei SOLLTEN Vorgaben zur Authentisierung, Update-Mechanismen und Netzanbindung definiert werden. Alle Entscheidungen, die in der Planungsphase getroffen wurden, SOLLTEN so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

SYS.4.4.A8 Beschaffungskriterien für IoT-Geräte [Informationssicherheitsbeauftragter (ISB), Beschaffungsstelle]

Der ISB SOLLTE auch bei Beschaffungen von Geräten, die keine offensichtliche IT-Funktionalität haben, beteiligt werden. Bevor IoT-Geräte beschafft werden, SOLLTE festgelegt werden, welche Sicherheitsanforderungen diese erfüllen müssen. Bei der Beschaffung von IoT-Geräten SOLLTEN Aspekte der materiellen Sicherheit ebenso wie Anforderungen an die Sicherheitseigenschaften der Software ausreichend berücksichtigt werden. Es SOLLTE eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. IoT-Geräten mit einem Cloud-Konzept SOLLTEN nicht beschafft werden.

SYS.4.4.A9 Regelung des Einsatzes von IoT-Geräten

Für jedes IoT-Gerät SOLLTE ein Verantwortlicher für den Betrieb benannt sein. Die Verantwortlichen SOLLTEN ausreichend informiert sein über den Umgang mit dem IoT-Gerät. Alle für die Geräte Verantwortlichen, Benutzer und Administratoren SOLLTEN über Verhaltensregeln und Meldewege bei Ausfällen, Fehlfunktionen oder bei Verdacht auf einen Sicherheitsvorfall informiert sein.

SYS.4.4.A10 Sichere Installation und Konfiguration von IoT-Geräten

Es SOLLTE festgelegt werden, unter welchen Rahmenbedingungen IoT-Geräte installiert und konfiguriert werden. Die Installation und Konfiguration der IoT-Geräte SOLLTE nur von autorisierten Personen (Verantwortlich für IoT-Geräte, Administratoren oder vertraglich gebundene Dienstleister) nach einem definierten Prozess durchgeführt werden. Alle Installations- und Konfigurationsschritte SOLLTEN so dokumentiert werden, dass die Installation und Konfiguration durch einen sachkundigen Dritten anhand der Dokumentation nachvollzogen und wiederholt werden kann.

Die Grundeinstellungen von IoT-Geräten SOLLTEN überprüft und nötigenfalls entsprechend den Vorgaben der Sicherheitsrichtlinie angepasst werden. Falls möglich, SOLLTEN IoT-Geräte erst mit IT-Netzen verbunden werden, nachdem die Installation und die Konfiguration abgeschlossen ist, dies gilt vor allem für öffentliche Netze.

SYS.4.4.A11 Verwendung sicherer Protokolle

Daten SOLLTEN nur verschlüsselt übertragen werden. IoT-Geräte SOLLTEN ein auf Verschlüsselung basierendes Protokoll (z. B. SSL/TLS bzw. SSH) unterstützen. Bietet das Produkt selbst keine Verschlüsselung, SOLLTE dies bei der Inbetriebnahme, z. B. über ein Virtual Private Network (VPN), flankierend umgesetzt werden.

SYS.4.4.A12 Sichere Integration in übergeordnete Systeme [Informationssicherheitsbeauftragter (ISB)]

Wenn IoT-Geräte in Zusammenhang mit übergeordneten Management-Systemen eingesetzt werden, SOLLTEN sie ausschließlich mit diesen kommunizieren.

SYS.4.4.A13 Deaktivierung und Deinstallation nicht benötigter Komponenten

Nach der Installation SOLLTE überprüft werden, welche Protokolle, Anwendungen und weitere Tools auf den IoT-Geräten installiert und aktiviert sind. Nicht benötigte Protokolle, Dienste, Benutzerkennungen und Schnittstellen SOLLTEN deaktiviert oder ganz deinstalliert werden. Dies gilt insbesondere für unsichere Dienste, wie z. B. Telnet oder SNMPv1/v2. Die Verwendung von nicht benötigten Funkschnittstellen, z. B. für WLAN, ZigBee, Bluetooth, SOLLTE unterbunden werden.

Wenn dies nicht am Gerät selber möglich ist, SOLLTEN nicht benötigte Dienste über das Sicherheitsgateway (Firewall) eingeschränkt werden. Die getroffenen Entscheidungen SOLLTEN so dokumentiert werden, dass nachvollzogen werden kann, welche Konfiguration für die IoT-Geräte gewählt wurden.

SYS.4.4.A14 Einsatzfreigabe

Bevor IoT-Geräte im produktiven Betrieb eingesetzt und bevor sie an ein produktives Netz angeschlossen werden, SOLLTE eine Einsatzfreigabe erfolgen. Diese SOLLTE dokumentiert werden. Für die Einsatzfreigabe SOLLTE die Installations- und Konfigurationsdokumentation und die Funktionsfähigkeit der IoT-Geräte in einem Test geprüft werden. Sie SOLLTE durch eine in der Institution dafür autorisierte Stelle erfolgen.

SYS.4.4.A15 Restriktive Rechtevergabe

Die Zugriffsberechtigungen auf IoT-Geräte SOLLTEN möglichst restriktiv vergeben werden. Wenn dies über die IoT-Geräte selber nicht möglich ist, SOLLTE überlegt werden, dies netzseitig zu regeln.

SYS.4.4.A16 Beseitigen von Schadprogrammen auf IoT-Geräten

Der IT-Betrieb SOLLTE sich regelmäßig informieren, ob sich die eingesetzten IoT-Geräte mit Schadprogrammen infizieren und wie diese beseitigt werden können. Schadprogramme SOLLTEN unverzüglich beseitigt werden. Kann die Ursache für die Infektion nicht behoben bzw. eine Neuinfektion wirksam verhindert werden, SOLLTEN die betroffenen IoT-Geräte nicht mehr verwendet werden.

SYS.4.4.A17 Überwachung des Netzverkehrs von IoT-Geräten

Es SOLLTE überwacht werden, ob Netzverkehr von den IoT-Geräten oder Sensor-Systemen zu Nicht-Managementsystemen erfolgt.

SYS.4.4.A18 Protokollierung sicherheitsrelevanter Ereignisse bei IoT-Geräten

Sicherheitsrelevante Ereignisse SOLLTEN automatisch protokolliert werden. Falls dies durch die IoT-Geräte selber nicht möglich ist, SOLLTEN hierfür Router oder andere Protokollmechanismen genutzt werden. Die Protokolle SOLLTEN in sinnvollem Umfang ausgewertet werden.

SYS.4.4.A19 Schutz der Administrationsschnittstellen

Abhängig davon, ob IoT-Geräte lokal, direkt über das Netz oder über zentrale netzbasierte Tools administriert werden, SOLLTEN geeignete Sicherheitsvorkehrungen getroffen werden. Die zur Administration verwendeten Methoden SOLLTEN in der Sicherheitsrichtlinie festgelegt werden. Die IoT-Geräte SOLLTEN entsprechend der Sicherheitsrichtlinie administriert werden. Die Administration über das Netz SOLLTE über sichere Protokolle erfolgen.

SYS.4.4.A20 Geregelte Außerbetriebnahme von IoT-Geräten

Bei der Außerbetriebnahme von IoT-Geräten SOLLTE sichergestellt werden, dass keine wichtigen Daten, die eventuell auf den verbauten Datenträgern gespeichert sind, verloren gehen, und dass keine sensitiven Daten zurück bleiben. Es SOLLTE einen Überblick darüber geben, welche Daten wo auf IoT-Geräten gespeichert sind. Es SOLLTE eine Checkliste erstellt werden, die bei der Außerbetriebnahme von IoT-Geräten abgearbeitet werden kann. Diese Checkliste SOLLTE mindestens Aspekte zur Datensicherung weiterhin benötigter Daten und dem anschließenden sicheren Löschen aller Daten umfassen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.4.4.A21 Einsatzumgebung und Stromversorgung [Informationssicherheitsbeauftragter (ISB), Haustechnik] (I)

Es SOLLTE geklärt werden, ob IoT-Geräte in der angedachten Einsatzumgebung betrieben werden dürfen (Schutzbedarf anderer Systeme, Datenschutz). IoT-Geräte SOLLTEN in der Einsatzumgebung vor Diebstahl, Zerstörung und Manipulation geschützt werden.

Es SOLLTE geklärt sein, ob ein IoT-Gerät bestimmte Anforderungen an die physikalische Einsatzumgebung hat, wie z. B. Luftfeuchtigkeit, Temperatur oder Energieversorgung. Falls erforderlich, SOLLTEN dafür ergänzende Maßnahmen bei der Infrastruktur umgesetzt werden.

Wenn IoT-Geräte mit Batterien betrieben werden, SOLLTE der regelmäßige Funktionstest und Austausch der Batterien geregelt werden.

IoT-Geräte SOLLTEN entsprechend ihrer vorgesehenen Einsatzart und des vorgesehenen Einsatzorts vor Staub und Verschmutzungen geschützt werden.

SYS.4.4.A22 Systemüberwachung (A)

Die IoT-Geräte SOLLTEN in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept eingebunden werden, das den Systemzustand und die Funktionsfähigkeit der IoT-Geräte laufend überwacht und Fehlerzustände sowie die Überschreitung definierter Grenzwerte an das Betriebspersonal meldet. Ist eine hohe Verfügbarkeit der IoT-Geräte erforderlich, SOLLTE geprüft werden, ob die verwendeten Geräte diese Anforderung erfüllen oder ob weitere Maßnahmen wie das Einrichten eines Clusters oder die Beschaffung von Standby-Geräten erforderlich sind.

SYS.4.4.A23 Auditierung von IoT-Geräten (CIA)

In sicherheitskritischen Bereichen SOLLTEN alle zum Einsatz kommenden IoT-Geräte durch Experten sicherheitstechnisch überprüft werden.

SYS.4.4.A24 Sichere Konfiguration und Nutzung eines eingebetteten Webservers (CIA)

In IoT-Geräten integrierte Webserver SOLLTEN möglichst restriktiv konfiguriert sein. Es SOLLTEN nur die benötigten Komponenten und Funktionen installiert bzw. aktiviert sei. Der Webserver SOLLTE NICHT unter einem privilegierten Konto betrieben werden, soweit möglich. Sicherheitsrelevante Ereignisse SOLLTEN protokolliert werden. Der Zugang DARF nur nach Authentisierung möglich sein. Die Übertragung SOLLTE verschlüsselt sein.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [ACS1] Sicherheit von IP-basierten Überwachungskameras
  CSE 128, Version 1.0, Allianz für Cyber-Sicherheit, 11.2016
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_128.html

- [ACS2] Spionageangriffe mittels Hintertüren in Überwachungskameras und Raumsensoren
  So schützen Sie Ihr Unternehmen, Expertenkreis Cyber-Sicherheit, Allianz für Cyber-Sicherheit, 10.2016
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/partner/161010_expkr_statement01.pdf

- [DHS] Department of Homeland Security
  Securing the Internet of Things, 12.2016,
  https://www.dhs.gov/securingtheIoT

- [OWASP] Open Web Application Security Project
  OWASP, (zuletzt abgerufen am 28.09.2017)
  https://www.owasp.org

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Allgemeines IoT-Gerät" von Bedeutung.

G 0.02 Ungünstige klimatische Bedingungen

G 0.04 Verschmutzung, Staub, Korrosion

G 0.08 Ausfall oder Störung der Stromversorgung

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.38 Missbrauch personenbezogener Daten

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

Elementare Gefährdungen / Anforderungen	G 0.02	G 0.04	G 0.08	G 0.09	G 0.14	G 0.16	G 0.18	G 0.19	G 0.20	G 0.21	G 0.23	G 0.24	G 0.25	G 0.26	G 0.28	G 0.29	G 0.30	G 0.38	G 0.39	G 0.40
SYS.4.4.A1					x		x	x	x		x			x	x					
SYS.4.4.A2					x			x		x	x						x	x	x	x
SYS.4.4.A3					x		x	x	x	x	x		x	x	x		x	x	x	x
SYS.4.4.A4					x		x	x	x	x	x		x	x	x		x	x	x	x
SYS.4.4.A5					x			x	x	x	x		x	x	x	x	x	x	x	x
SYS.4.4.A6	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
SYS.4.4.A7	x	x	x	x		x	x	x		x	x						x	x	x	x
SYS.4.4.A8					x		x		x		x			x	x					
SYS.4.4.A9	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x					
SYS.4.4.A10					x		x	x		x	x		x		x		x	x	x	x
SYS.4.4.A11					x						x				x		x	x	x	x
SYS.4.4.A12				x	x		x										x			
SYS.4.4.A13					x			x		x	x			x	x		x	x	x	x
SYS.4.4.A14							x		x								x			
SYS.4.4.A15					x			x		x	x				x		x	x	x	x
SYS.4.4.A16																			x	
SYS.4.4.A17				x	x					x	x		x	x	x		x			x
SYS.4.4.A18					x			x		x	x						x			
SYS.4.4.A19					x			x		x	x				x		x	x	x	x
SYS.4.4.A20							x	x												
SYS.4.4.A21	x	x	x			x	x					x	x			x				
SYS.4.4.A22										x	x		x	x						x
SYS.4.4.A23					x		x	x	x	x	x			x	x					
SYS.4.4.A24					x			x			x				x		x			

Bundesamt
für Sicherheit in der
Informationstechnik

IND: Industrielle IT

IND.1	Betriebs- und Steuerungstechnik	**607**
IND.2.1	Allgemeine ICS-Komponente	**620**
IND.2.2	Speicherprogrammierbare Steuerung (SPS)	**629**
IND.2.3	Sensoren und Aktoren	**633**
IND.2.4	Maschine	**637**

IT-Grundschutz

IND: Industrielle IT

IND.1 Betriebs- und Steuerungstechnik

1 Beschreibung

1.1 Einleitung

Betriebstechnik (englisch: Operational Technology (OT)) ist Hard- und Software, die Änderung durch die direkte Überwachung und / oder Steuerung von physikalischen Geräten, Prozessen und Ereignissen im Unternehmen erfasst und bewirkt [GART1].

In der Industrie, zu der unter anderem auch die Kritischen Infrastrukturen gehören, zählen dazu insbesondere industrielle Steuerungssystemen (Industrial Control Systems, ICS) und Automationslösungen, die dort die Steuerungs- und Regelfunktionen aller Art übernehmen. Weitere Beispiele sind Laborgeräte (z. B. automatisierte Mikroskop oder Analysewerkzeuge), Logistiksysteme (Barcodescanner mit Kleinrechner) oder Gebäudeleittechnik.

Die in der Vergangenheit übliche physische Trennung der OT von anderen IT-Systemen und Netzen in Büroanwendungen ist heute aufgrund zunehmender Integrationsanforderungen nur in Ausnahmefällen bei erhöhtem Schutzbedarf anwendbar. Mehrstufige Produktionsschritte und deren übergreifende Steuerung wie auch regulatorische Anforderungen erfordern eine zunehmende Öffnung auch über Organisationsgrenzen hinweg. Diese Entwicklung wird durch den Trend zur Optimierung von Fertigungsprozessen zur Steigerung der Wettbewerbsfähigkeit im Rahmen von Industrie 4.0 beschleunigt.

Da neben OT-spezifischen Komponenten zunehmend IT-Komponenten und Technologien aus der Office-IT in der OT eingesetzt werden, sind diese inzwischen vergleichbaren Gefährdungen ausgesetzt. Zugleich weisen die OT gegenüber der klassischen IT wesentliche Unterschiede auf, die das Anwenden dort etablierter Sicherheitsverfahren erschweren. So kann es Restriktionen aufgrund Herstellervorgaben oder gesetzlichen Anforderungen geben, die Veränderungen an Komponenten verhindern oder erschweren. Ein Beispiel hierfür sind die Anwendung von Sicherheitsupdates oder nachträgliche Härtungsmaßnahmen. Die OT unterliegt in der Regel auch deutlich längeren Lebenszyklen, auch über die Herstellerunterstützung hinaus, so dass auch die Verfügbarkeit von Sicherheitsupdates nicht durchgängig gewährleistet werden kann.

Ein wesentlicher Unterschied ergibt sich für die OT auch aus den oft hohen Verfügbarkeits- und Integritätsanforderungen, während im Vergleich zu Office-IT die Vertraulichkeit häufig von nachrangiger Bedeutung ist. Störungen dieser Systeme können Gefährdungen von Leib, Leben und Umwelt nach sich ziehen und sind zumeist nicht durch einen Neustart zu beheben.

1.2 Zielsetzung

Das Ziel des Bausteins besteht darin, geeignete Anforderungen an die Informationssicherheit der OT aufzuzeigen. Er adressiert komponentenübergreifende, konzeptionelle und architektonische Sicherheitsanforderungen.

Der Baustein ist übergreifend zu modellieren und umzusetzen. Dabei kann eine mehrfache Verwendung in unterschiedlichen Bereichen der OT in einer Institution (Betreiber im Sinne der VDI 2182) nicht ausgeschlossen werden, da in diesen unterschiedliche Anforderungen bzgl. der Informationssicherheit vorliegen.

1.3 Abgrenzung

Die Ausgestaltung der OT kann je nach Zweck, Branche, der eingesetzten IT-Systeme und Technik sowie aufgrund des langen Einsatzzeitraums (zum Teil ohne Updates) selbst bei vergleichbaren Anwendungsfällen stark variieren. Bei der Ausgestaltung der Sicherheitsmaßnahmen auf Basis der Anforderungen aus diesem Baustein sind daher die vorhandenen Besonderheiten zu berücksichtigen. Diese können wesentlichen Einfluss auf die Ausgestaltung des Sicherheitskonzepts nehmen. Der Risikoanalyse kann aus diesem Grund bereits bei der Erstellung eines Sicherheitskonzepts für den normalen Schutzbedarf eine hohe Bedeutung zukommen. Dies kann mehrfache Verwendung des Bausteins für unterschiedliche Bereiche erforderlich machen.

Zusätzlich ist die umgebende Infrastruktur der OT – also Standorte, Anlagen, Gebäude, Räume etc. – durch möglichst spezifisch geeignete Bausteine zu modellieren, um die Schutzwirkung dieses Bausteins zu komplementieren.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Betriebs- und Steuerungstechnik von besonderer Bedeutung:

2.1 Ungeeignete Einbindung der OT in die Sicherheitsorganisation

Durch unterschiedliche Rahmenbedingungen, Kenntnisse und Vorgehensweisen in den Bereichen Office-IT und ICS kann es bei übergreifenden Sicherheitsvorgaben zu Umsetzungsproblemen kommen. Sicherheitsvorgaben aus dem Bereich der IT können einerseits aufgrund technischer oder prozessualer Besonderheiten bei ICS-Systemen nicht umsetzbar sein. Andererseits können ICS-spezifische Informationssicherheits- und Safety-Aspekte (Aspekte der funktionalen Sicherheit) den Zuständigen für Informationssicherheit der Office-IT nicht bekannt sein. Auf diese Weise kann es zu Reibungsverlusten in der Kommunikation und der Umsetzung sowie zu nicht ausreichend behandelten bzw. nicht erkannten Risiken kommen.

2.2 Ungeeignete Einbindung der OT in betriebliche Abläufe

Ungeachtet der zunehmenden Konvergenz von OT und IT sind Besonderheiten vorhanden, die das Übertragen etablierter betrieblicher Abläufe erschweren. Betriebliche Eingriffe im Rahmen des Change- und (Security) Incident-Managements zur sicheren Konfiguration, Störungsbehebung oder dem Einspielen von Sicherheitsupdates etwa können eine erneute behördliche Freigabe oder den Verlust des Herstellersupports nach sich ziehen. Nicht autorisierte Änderungen können die Funktion einer Komponente beeinflussen und damit potenziell auch Auswirkungen auf deren Safety-Funktionen besitzen.

Die OT dient der Überwachung, Steuerung und Automatisierung von technischen Abläufen. Störungen dieser Systeme können zu Produktionsausfällen, technischen oder personellen Schäden und Umweltschäden führen. Diese potenziellen Auswirkungen müssen bei betrieblichen Eingriffen berücksichtigt werden.

2.3 Unzureichender Zugangsschutz

Industrielle Steuerungsanlagen werden immer seltener vollständig autark von der Außenwelt betrieben. Moderne Fertigungs- und Erzeugungsprozesse erfordern einen Informationsaustausch mit vor- und nachgelagerten Produktionsschritten und sind häufig an zentrale Produktionsplanungs- und Steuerungssysteme (Manifacturing Execution System / Enterprise Ressource Planning) einer Institution angebunden. Der elektronische Informationsaustausch erfordert eine Vernetzung der Produktionsanlagen mit Drittnetzen wie der Office-IT oder auch den Netzen von Partnern und Dienstleistern. Anforderun-

gen an interaktive Zugriffe von Büro- oder Mobilarbeitsplätzen als auch betrieblich bedingte Anforderungen an den elektronischen Datenaustausch, etwa zur Bereitstellung von Software und Updates, oder zur Realisierung von Fernzugängen für eine Rufbereitschaft oder für Dienstleister fördern die Vernetzung mit der Außenwelt.

Werden die erforderlichen Kommunikationskanäle zu weit gefasst oder unzureichend gesichert, können Angreifer diese Zugangswege zum netzbasierten Zugriff und zur Kompromittierung des Automatisierungssystems nutzen.

2.4 Unzureichendes Schutzkonzept gegen Schadprogramme für die OT

Industrielle Steuerungsanlagen können sowohl von zielgerichteten Schadsoftware-Angriffe als auch zufällig von Schadprogrammen betroffen sein, die auf die Kompromittierung der Office-IT zielen. Mögliche Infektionswege ergeben sich aus Datentransfers, dem Einsatz von Wechselmedien und mobilen Endgeräten oder fehlender Segmentierung oder Kontrolle des Datenverkehrs.

Auf der anderen Seite kann der Einsatz von Virenschutz-Software auch Risiken für die OT darstellen, wenn keine Herstellerfreigabe für die Umgebung vorliegt oder Fehlerkennungen und aktive Systemeingriffe den Betrieb gefährden. Ein vergleichbares Störungspotenzial (durch die Unterbrechung von Verbindungen) kann sich auch aus dem Betrieb netzbasierter Intrusion Prevention Systeme (IPS) ergeben.

Zusätzlich ist beim Einsatz von Virenschutz-Software eine regelmäßige Aktualisierung notwendig. Wenn dies nicht gewährleistet ist, können neue Angriffe durch Schadsoftware nicht erkannt werden. Dies gilt auch allgemein Angriffe, für die die Virenschutz-Software keine Signaturen besitzt.

2.5 Unsicherer Projektierungsprozess / Anwendungsentwicklungsprozess

Anpassungen und Weiterentwicklungen von IT-Systemen, Anwendungen und Steuerungsprogrammen stellen einen kritischen Eingriff in die Steuerungsanlage dar. Störungen können aus funktionalen Fehlern bei unzureichenden Test- und Validierungsschritten, fehlerhaften oder manipulierten Projektierungsdaten oder Schwachstellen in der Software entstehen, wenn wichtige Sicherheitsfunktionen wie Ein- und Ausgabe- oder Berechtigungsprüfungen unzureichend umgesetzt werden.

Weitere Gefahren können sich aus unsicheren Entwicklungsumgebungen, der ungeeigneten Ablage von Programmcode, Dokumentation oder Projektdaten sowie aus den Datentransferschnittstellen ergeben.

2.6 Unsicheres Administrationskonzept und Fernadministration

Die Verwaltung industrieller Steuerungssysteme erfolgt in bestimmten Fällen abgesetzt über Netzzugriffe. Hierbei werden unterschiedliche öffentliche und private Netze wie z. B. Telefonnetze, Funknetze, Mobilfunknetze und zunehmend das Internet eingesetzt. Sind diese Zugänge unzureichend geplant, unsicher konfiguriert oder werden diese nicht überwacht, so können Angreifer unter Umständen unbefugt auf einzelne OT-Komponeten oder die Infrastruktur zugreifen und so die Sicherheitsmechanismen am Perimeter umgehen.

Lokale Administratoren verfügen ebenfalls über privilegierte Rechte, welche einen Missbrauch durch Innentäter oder über kompromittierte Accounts für Angreifer attraktiv machen.

2.7 Unzureichende Überwachungs- und Detektionsverfahren

Das Überwachen von Betriebszuständen des zu automatisierenden Prozesses ist eine wesentliche Funktion industrieller Steuerungssysteme. So werden gewöhnlich den Prozess betreffende Warnungen (z. B. bei unterschrittenen Füllständen) und technische Parameter (z. B. Temperaturen, Ventilstellungen) abgebildet. Dagegen fehlt es häufig an einer angemessenen Überwachung der unterstützenden IT-Infrastruktur.

Werden ungewöhnliche oder sicherheitsrelevante Ereignisse solcher Betriebsumgebungen nicht oder nur unzureichend überwacht, können Angriffsversuche, Netzengpässe oder absehbare Ausfälle nicht frühzeitig erkannt werden.

Darüber hinaus kann auch eine mangelhafte Auswertung oder unübersichtliche Darstellung der Ereignisse dazu führen, dass Warnungen und Fehler verspätet erkannt werden.

2.8 Unzureichendes Testkonzept

Industrielle Steuerungsanlagen unterliegen oft hohen Verfügbarkeitsanforderungen. Störungen oder technische Ausfälle können unter Umständen schwerwiegende Schäden und hohe Folgekosten nach sich ziehen. Aus diesem Grund sind Systeme oft ausfallsicher konzipiert und redundant ausgelegt.

Werden Änderungen an einer solchen Umgebung nicht sorgfältig geplant, abgestimmt und in einer realitätsnahen Umgebung getestet, besteht die Gefahr, dass logische oder softwaretechnische Fehler übersehen werden und Störungen in der Anlage auftreten. Selbst herstellerseitig freigegebene Updates können bei Modifikationen oder Anpassung von Parametern an der Anlage Störungen verursachen.

2.9 Mangelnde Life Cycle Konzepte

Neben spezifischen OT-Komponenten werden zunehmend Komponenten, Technologien und Software aus der Office-IT eingesetzt, sogenannte Commercial-off-the-shelf-Produkte (COTS). Aufgrund der sehr langen Lebenszyklen in der OT werden diese Komponenten in der Regel deutlich länger betrieben als in der Office-IT üblich, teilweise auch über die Hersteller-Support-Zyklen hinaus.

Dies hat zur Folge, dass nach dem Ablauf der Herstellerunterstützung keine Updates für Schwachstellen mehr zur Verfügung gestellt werden. Dem gegenüber stehen oftmals öffentlich dokumentierte Schwachstellen, sowie Werkzeuge, die diese Schwachstellen ausnutzen. Dies ermöglicht auch nicht versierten Angreifern ein erfolgreiches eindringen in die Systeme. Dies gilt auch, wenn Updates nicht oder nur mit sehr großer Verzögerung eingespielt werden.

Die langen Einsatzzeiten können zudem zu Problemen bei der Beschaffung von Ersatzteilen führen, wenn diese nicht mehr durch den Hersteller produziert werden. Dies gilt auch für mögliches Knowhow zur Pflege und Wartung von Alt-Systemen, dass bei neuen Mitarbeitern nicht mehr vorliegt

2.10 Einsatz unsicherer Protokolle

Die OT-Komponenten kommunizieren untereinander über verschiedene Netzprotokolle und Technologien. Neben Protokollen und Technologien aus der Office-IT (z. B. Ethernet, TCP/ IP, WLAN, GSM) werden ICS-spezifische Protokolle eingesetzt. Diese sind nicht immer unter dem Gesichtspunkt der Informationssicherheit entwickelt worden und bieten demgemäß teilweise keine oder nur eingeschränkte Sicherheitsmechanismen. Informationen werden häufig im Klartext und ohne Integritätssicherung oder Authentisierung übertragen.

Ein Angreifer mit Zugang zum Netz könnte die Inhalte der Kommunikation auslesen oder verändern und auf diese Weise Einfluss auf die Prozesse nehmen, etwa durch Vortäuschen von Sensordaten oder Fälschen von Steuerungsbefehlen. Dies trifft in besonderem Maße auf Protokolle zu, welche für die Kommunikation über frei zugängliche Gebiete eingesetzt werden, etwa bei Funkprotokollen oder im Rahmen der Standortvernetzung (Fernwirktechnik).

2.11 Unsichere Konfigurationen

In der Standardkonfiguration von OT-Komponenten sind Sicherheitsmaßnahmen nicht immer aktiviert, wodurch unbefugt Zugriffe erheblich erleichtert werden. Der Betrieb unsicher konfigurierter Komponenten kann darüber hinaus auch die Sicherheit anderer Komponenten der Umgebung bedrohen, etwa wenn Zugangsdaten zu diesen ausgelesen werden können oder diese in einer Vertrauensstellung zu anderen Systemen stehen.

Beispiele für unsichere Konfigurationen sind etwa der Gebrauch von Standardpasswörtern, die Nutzung von Klartextprotokollen zur Systemverwaltung, der Betrieb nicht erforderlicher Dienste, ungesicherte Schnittstellen, wie z. B. USB oder Firewire-Ports, oder deaktivierte Sicherheitsfunktionen.

2.12 Abhängigkeiten der OT von IT-Netzen

Die OT wird mittlerweile immer weniger völlig autark betrieben. Bestehen Abhängigkeiten zu anderen Systemen, Netzen oder Diensten, so wirken sich Ausfälle oder Sicherheitsvorfälle im IT-Netz auch auf die OT aus.

Insbesondere, wenn diese Systeme und Netze nicht unter der Kontrolle der Institution (des Betreibers der ICS-Infrastruktur) stehen, kann dies zu starken Beeinträchtigungen der Verfügbarkeit der OT und der Prozesse führen. Darüber hinaus kann der Vorfall oder Fehler in der Regel nur mit externer Unterstützung behoben werden.

Beispiele für Abhängigkeiten zu anderen Systemen und Netzen sind Internetanbindungen (sowohl drahtgebunden als auch über Mobilfunk), gemeinsam genutzte Infrastrukturkomponenten, eine Betriebsführung und Überwachung durch Dienstleister oder die Nutzung von Cloud-Diensten.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Betriebs- und Steuerungstechnik aufgeführt. Grundsätzlich ist ICS-Informationssicherheitsbeauftragte (ICS-ISB) für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	ICS-Informationssicherheitsbeauftragter
Weitere Verantwortliche	Bereichs-Sicherheitsbeauftragter, IT-Betrieb

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

IND.1.A1 Einbindung in die Sicherheitsorganisation

Ein Informationssicherheits-Managementsystem (ISMS) für den Betrieb der OT-Infrastruktur MUSS entweder als selbständiges ISMS oder als Teil eines Gesamt-ISMS existieren und MUSS in seinem Geltungsbereich die Definition von Zielen und Werten, Prozessen, Rollen, Verantwortlichkeiten und Vorgaben für die OT explizit umfassen.

Die Leitungsebene der Institution MUSS den Sicherheitsprozess initiieren, steuern und kontrollieren. Die Institution MUSS eine Sicherheitsorganisation aufbauen, welche die Rollen und Verantwortlichkeiten für die Informationssicherheit der OT-Infrastruktur und -Komponenten regelt.

Es MUSS ein Gesamtverantwortlicher für die Informationssicherheit im OT-Bereich bestimmt und innerhalb der Institution bekannt gegeben werden. Gesetzliche, regulatorische und sonstige besonderen Vorgaben für den OT-Bereich sowie die jeweilige Branche bzw. den Sektor MÜSSEN bekannt und ihre Auswirkungen auf die Institution ausgewertet sein.

Es MUSS ein Prozess existieren, wie konkrete Vorgaben (Richtlinien) für bestimmte Themenbereiche im Prozessbereich verfasst, kommuniziert, zur Umsetzung gebracht, fortgeschrieben, bewertet und verbessert werden.

Weiterführende Informationen sind im Baustein ISMS Sicherheitsmanagement beschrieben.

IND.1.A2 Sensibilisierung und Schulung des Personals

Betriebspersonal MUSS regelmäßig zu relevanten IT-Sicherheitsbedrohungen im OT-Bereich informiert und sensibilisiert werden. OT-Verantwortliche MÜSSEN regelmäßig zur Bedrohungslage und Handlungsbedarfen informiert oder geschult werden.

Weiterführende Informationen sind im Baustein ORP.3 Sensibilisierung und Schulung beschrieben.

IND.1.A3 Schutz vor Schadprogrammen

Zur Vorbeugung vor Risiken durch Schadprogramme MUSS ein Konzept zum Schutz vor Schadprogrammen erstellt und umgesetzt werden. Darin MÜSSEN die bedrohten IT-Systeme sowie die möglichen Infektionswege (Außenschnittstellen, Wechselmedien, Service- und Parametrier-/Programmiergeräte) betrachtet und geeignete technische und organisatorische Schutzmaßnahmen festgelegt sein.

Beim Einsatz von Virenschutz-Software auf OT-Komponenten MUSS berücksichtigt werden, ob und in welcher Konfiguration der Betrieb von Virenschutz-Software vom Hersteller unterstützt wird. Ist dies nicht der Fall, MUSS im Rahmen einer Risikoanalyse der Bedarf an alternativen Schutzverfahren geprüft werden.

Eingesetzte Virenschutz-Software MÜSSEN mit aktuellen Signaturen versorgt werden. Das Virenschutzkonzept MUSS die Aktualisierungsstrategie festlegen. Dies umfasst den Bezug von Signaturen, deren Verteilungsverfahren und die Häufigkeit der Aktualisierung. Der Bezug und die Verteilung von Signaturen können automatisiert erfolgen. Der Bezug von Virensignaturen durch OT-Systeme DARF NICHT direkt aus dem Internet erfolgen, sondern MUSS indirekt über einen Proxy- oder Virensignaturverteildienst erfolgen. Die Schnittstellensysteme MÜSSEN in einer eigenständigen Zone (z. B. DMZ) von der OT-Umgebung getrennt betrieben werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Betriebs- und Steuerungstechnik. Sie SOLLTEN grundsätzlich umgesetzt werden.

IND.1.A4 Dokumentation der OT-Infrastruktur

Die sicherheitsrelevanten Parameter der OT-Infrastruktur SOLLTEN dokumentiert sein. In einem Bestandsverzeichnis SOLLTEN alle Software- und Systemkomponenten geführt werden. Hieraus SOLLTEN die eingesetzten Produkt- und Protokollversionen sowie die Zuständigkeiten hervorgehen. Zu den eingesetzten Komponenten SOLLTEN eventuelle Restriktionen der Hersteller oder regulatorische Auflagen wie etwa Zertifizierungen bestimmt sein. Diese Dokumentation und ein Systeminventar SOLLTE beispielsweise in einem Leitsystem geführt werden.

Zusätzlich SOLLTE ein aktueller Netzplan Zonen, Zonenübergänge (Conduits), eingesetzte Kommunikationsprotokolle und -verfahren sowie Außenschnittstellen dokumentieren. Bei den Schnittstellen SOLLTEN aktive Netzkomponenten wie auch manuelle Datentransferverfahren (z. B. durch Wechseldatenträger) berücksichtigt werden. Die Dokumentation SOLLTE Redundanzen, IP-Adressen bzw. -Bereiche und die Zuordnung zu physischen Sicherheitszonen erfassen.

Da die Dokumentation vertrauliche Informationen enthält, sind sämtliche Dokumente sicher abzulegen und mit einer Einstufung bzgl. der Schutzbedarfs zu versehen.

IND.1.A5 Entwicklung eines geeigneten Zonenkonzepts [IT-Betrieb]

Es SOLLTE ein Zonenkonzept vorliegen, welches verschiedene Level mit unterschiedlichen Schutzbedarfen definiert und die komplette OT-Infrastruktur sowie mindestens den Übergang zur Office-IT umfasst. Das Netz SOLLTE den Zonen entsprechend segmentiert sein und der Datenfluss zwischen den Zonen geeignet kontrolliert werden, um Angriffe aufwändiger, unwahrscheinlicher und leichter feststellbar zu machen.

Es SOLLTE auch eine horizontale Segmentierung in unabhängige Funktionsbereiche (etwa Anlagen) erfolgen. Die einzelnen Zonen SOLLTEN so weit wie möglich im Betrieb voneinander unabhängig sein. Insbesondere die Zonen, in denen der technische Prozess gesteuert wird, SOLLTEN bei einem Ausfall der anderen Zonen oder deren bewusster Abkopplung nach einer Kompromittierung eine vorbestimmte Zeitspanne weiter betreibbar sein. Dieser Zeitraum SOLLTE im Rahmen der Risikoanalyse oder alternativ im Rahmen der Notfallplanung definiert und dokumentiert werden. Das Netz SOLLTE daher stabil im Sinn von manipulations- und fehlerresistent konzipiert werden.

Alle Schnittstellen/Verbindungen zwischen den Zonen SOLLTEN einer Risikobetrachtung unterzogen sein. An den Außenschnittstellen SOLLTEN authentisierte Benutzer und integritätsgeschützte Protokolle eingesetzt werden.

IND.1.A6 Änderungsmanagement im OT-Betrieb

Für Änderungen an der OT SOLLTE ein Änderungsprozess (Change Management) definiert, dokumentiert und gelebt werden. Der Änderungsprozess SOLLTE gewährleisten, dass Änderungen geplant, dokumentiert, angemessen, auf unerwünschte Seiteneffekte und Funktionalität getestet, objektiv auf sicherheitsrelevante oder betriebliche Auswirkungen bewertet und freigegeben werden.

Es SOLLTE ein Konzept zur sicheren Erprobung von Änderungen vorliegen. Die Systemzeit der OT-Infrastruktur SOLLTE synchron gehalten werden. Dies SOLLTE mit einer externen Referenz erfolgen.

Weitere Informationen sind im Baustein OPS.1.2.1 Änderungsmanagement beschrieben.

IND.1.A7 Etablieren einer Berechtigungsverwaltung

Die Institution SOLLTE einen Prozess zur Verwaltung von Benutzerzugänge und zugeordneten Berechtigungen für den Zugriff auf die OT etablieren. Die Berechtigungsverwaltung SOLLTE den Prozess, die Durchführung und die Dokumentation für die Beantragung, Einrichtung und den Entzug von Berechtigungen umfassen.

Die Berechtigungsverwaltung SOLLTE gewährleisten, dass Berechtigungen nach dem Minimalprinzip vergeben und regelmäßig überprüft werden. In der Berechtigungsverwaltung SOLLTEN die Zugriffe auf IT-Systeme für Mitarbeiter, Administratoren und Dritte geregelt sein. Jeder Beteiligte SOLLTE regelmäßig zu den einzuhaltenden Regelungen geschult werden. Die Einhaltung SOLLTE überprüft und Fehlverhalten sanktioniert werden.

Weitere Informationen sind im Baustein ORP.4 Identitäts- und Berechtigungsmanagement beschrieben.

IND.1.A8 Sichere Administration [IT-Betrieb]

Für die Erstkonfiguration, Verwaltung (Administration) und Fernwartung in der OT SOLLTEN entweder sichere Protokolle oder aber abgetrennte Administrationsnetze mit entsprechendem Schutzbedarf genutzt werden. Der Zugang zu diesen Schnittstellen SOLLTE auf die Berechtigten eingeschränkt sein. Es SOLLTE nur der Zugriff auf die Systeme und Funktionen gewährt sein, welche für die jeweilige Administrationsaufgabe benötigt werden.

Die Systeme und Kommunikationskanäle, mit denen die Administration oder Fernwartung durchgeführt wird, SOLLTEN das gleiche Schutzniveau aufweisen wie die verwalteten OT-Komponenten. Jede Fernwartung und -überwachung SOLLTE durch die Institution autorisiert, überwacht und gesteuert werden. Dazu SOLLTE der Fernwartungszugang nur für die Nutzung aktiviert und danach wieder deaktiviert werden. Dies SOLLTE dokumentiert werden

Dabei SOLLTE darauf geachtet werden, dass es nicht möglich ist, unerwünschte Tunnel zur Umgehung von Sicherheitsmaßnahmen aufzubauen. Bei höherem Schutzbedarf SOLLTE zudem für kritische administrative Schritte ein Vier-Augen-Prinzip gelten.

IND.1.A9 Restriktiver Einsatz von Wechseldatenträgern und mobilen Endgeräten

Für die Nutzung von Wechseldatenträgern und mobilen Endgeräten SOLLTEN Regelungen für den Umgang aufgestellt und bekannt gemacht werden. Grundsätzlich SOLLTE der Einsatz von Wechseldatenträgern und mobilen Endgeräten in ICS-Umgebungen beschränkt werden. Für Medien und Geräte von Dienstleistern SOLLTEN ein Genehmigungsprozess und eine Anforderungsliste existieren. Die Vorgaben SOLLTEN jedem Dienstleister bekannt sein und von diesen schriftlich bestätigt werden.

Auf den OT-Komponenten SOLLTEN alle nicht benötigten Schnittstellen deaktiviert werden. An den aktiven Schnittstellen kann die Nutzung auf bestimmte Geräte bzw. Medien eingeschränkt werden.

Weitere Informationen sind im Baustein SYS.3.4 Mobile Datenträger beschrieben.

IND.1.A10 Monitoring, Protokollierung und Detektion [Bereichs-Sicherheitsbeauftragter]

Zur Begrenzung der möglichen Auswirkungen von Sicherheitsvorfällen SOLLTEN betriebs- und sicherheitsrelevante Ereignisse zeitnah identifiziert werden. Hierzu SOLLTE ein geeignetes Log- und Event-Management entwickelt und umgesetzt werden. Das Log- und Event-Management SOLLTE angemessene Maßnahmen zur Erhebung und Erkennung von sicherheitsrelevanten Ereignissen sowie einen Reaktionsplan (Security Incident Response) umfassen.

Der Reaktionsplan SOLLTE Verfahren zur Sicherheitsvorfallbehandlung festlegen. Darin abgedeckt sein SOLLTEN Klassifizierung von Ereignissen, Meldewege und Festlegung der einzubeziehenden Organisationseinheiten, Reaktionspläne zur Schadensbegrenzung, Analyse und Wiederherstellung von Systemen und Diensten sowie die Dokumentation und Nachbereitung von Vorfällen. Der Reaktionsplan SOLLTE regelmäßig getestet und auf Aktualität geprüft werden.

IND.1.A11 Sichere Beschaffung und Systementwicklung

Für Beschaffungen, Planungen oder Entwicklungen von ICS SOLLTEN Regelungen zur Informationssicherheit getroffen und dokumentiert werden. Die Unterlagen SOLLTEN Teil der Ausschreibung sein.

Bei Beschaffungen, Planungen oder Entwicklungen SOLLTE die Informationssicherheit in dem gesamten Lebenzyklus berücksichtigt werden. Voraussetzungen und Umsetzungshinweise für einen sicheren Betrieb von OT-Komponenten von Herstellern oder Integratoren SOLLTEN frühzeitig eingeplant und umgesetzt werden. Die Einhaltung und Umsetzung SOLLTE dokumentiert werden

Die Institution SOLLTE dokumentieren, wie sich das System in die Konzepte für Zonierung, Berechtigungs-, Schwachstellen-Management und Virenschutz einfügt und diese gegebenenfalls anpassen. Es SOLLTE geregelt sein, wie der Betrieb aufrechterhalten werden kann, falls einer der Partner keine Dienstleistungen mehr anbietet.

Weitere Informationen sind im Bausteinen OPS.2.1 Outsourcing-Nutzung beschrieben.

IND.1.A12 Etablieren eines Schwachstellen-Managements

Für den sicheren Betrieb einer ICS-Umgebung SOLLTE die Institution ein Schwachstellen-Management etablieren. Das Schwachstellen-Management SOLLTE Lücken in Software, Komponenten, Protokollen und Außenschnittstellen der Umgebung identifizieren und mögliche Handlungserfordernisse und -möglichkeiten (z. B. ein Patchmanagement) ableiten, bewerten und umsetzen.

Grundlage dafür SOLLTEN Schwachstellenmeldungen (Advisories) von Herstellern oder öffentlich verfügbare CERT-Meldungen sein. Ergänzend hierzu können organisatorische und technische Audits zur Schwachstellenanalyse durchgeführt werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

IND.1.A13 Notfallplanung für OT (A)

Bei hoher Verfügbarkeit SOLLTEN Notfallpläne für den Ausfall und für die Kompromittierung jeder Zone definiert, dokumentiert, nach jeder größeren Änderung getestet und regelmäßig geübt sein (siehe hierzu auch BSI-Standard 100-4).

Zudem SOLLTE ein wirksames Ersatzverfahren für den Ausfall der (Fern-) Administrationsmöglichkeit definiert, dokumentiert und getestet sein.

IND.1.A14 Starke Authentisierung an OT-Komponenten (CIA)

Zur sicheren Authentisierung von privilegierten Anwendern in Steuerungssystemen SOLLTE ein zentraler Verzeichnisdienst eingerichtet werden. Die Authentisierung SOLLTE durch den Einsatz mehrerer Faktoren (Wissen, Besitz, Biometrie) zusätzlich abgesichert werden.

Bei der Planung SOLLTE darauf geachtet werden, dass daraus entstehende Abhängigkeiten in der Benutzerauthentisierung bekannt sind und bei der Umsetzung der Lösung berücksichtigt werden.

Der zentrale Verzeichnisdienst SOLLTE NICHT zur Authentisierung von betrieblich erforderlichen technischen Konten dienen. Beim Einsatz eines Verzeichnisdienstes SOLLTEN lokale System- und Anwendungskennungen für Notfallsituationen eingerichtet und sicher hinterlegt werden.

Authentisierungssysteme, welche sensible Authentisierungsdaten verwalten, SOLLTEN angemessen vor unbefugtem Zugriff gesichert, Änderungen nachvollziehbar dokumentiert und auf Auffälligkeiten überwacht werden.

IND.1.A15 Prüfung und Überwachung von Berechtigungen (CIA)

Um die effektive Verifikation von Berechtigungen zu ermöglichen, SOLLTE die Institution ein Bestandsverzeichnis führen, welches alle vergebenen Zutritts-, Zugangs und Zugriffsrechte auf kritische Systeme enthält. Das Verzeichnis SOLLTE einerseits Antwort darauf geben können, welche Rechte ein bestimmter Benutzer effektiv hat, und andererseits, wer an einem bestimmten System über welche Rechte verfügt.

Alle kritischen administrativen Tätigkeiten SOLLTEN protokolliert werden. Der IT-Betrieb SOLLTE NICHT die Protokolle löschen oder manipulieren können.

IND.1.A16 Stärkere Abschottung der Zonen (IA)

Bei hoch schutzbedürftigen oder schlecht auf System- und Netzebene absicherbaren ICS-Umgebungen SOLLTEN vorbeugend Schnittstellensystemen mit Sicherheitsprüffunktionen eingesetzt werden um Risiken aus Außenanbindungen vorbeugen.

Wie in IND.1.A5 Entwicklung eines geeigneten Zonenkonzepts gefordert, SOLLTEN alle Außenschnittstellen der Umgebung einer Risikobetrachtung unterzogen werden. Aus den hiermit ermittelten Risiken SOLLTEN spezifische Einzelsicherungsmaßnahmen abgeleitet werden.

Durch Realisierung einer oder mehrerer Anbindungszonen (DMZ) in P-A-P-Struktur (durch Firewalls gekapselte Application Layer Gateways) KÖNNEN durchgängige Außenverbindungen terminiert werden und erforderliche Sicherheitsprüfungen (Virenschutz, Formatierung von Daten, Prüfung und Filterung von Inhalten, Medienbrüche) erfolgen, ohne dass Anpassungen an der ICS-Anlage notwendig sind.

Die Umsetzung dieser Anforderung erhöht die Perimetersicherheit. Ergänzende organisatorische und technische Maßnahmen SOLLTEN identifiziert und umgesetzt werden, um Risiken aus vorsätzlicher und versehentlicher Umgehung des Perimeters, wie etwa durch den Einsatz von Wechseldatenträgern oder Mobilgeräten, weiter zu reduzieren.

IND.1.A17 Regelmäßige Sicherheitsüberprüfung (I)

Die Sicherheitskonfiguration von OT-Komponenten SOLLTE in einem angemessenen Zyklus und/oder bedarfsorientiert bei plötzlich auftretenden neuen, bisher unbekannten Gefährdungen überprüft werden. Die Sicherheitsüberprüfung SOLLTE zumindest die exponierten Systeme mit Außenschnittstellen oder Benutzerinteraktion umfassen.

Auch das realisierte Sicherheitskonzept SOLLTE regelmäßig überprüft werden.

Die Sicherheitsüberprüfung SOLLTE als Konfigurationsprüfung oder auch durch automatisierte Konformitätsprüfungen erfolgen.

4 Weiterführende Informationen

4.1 Literatur

- [27019] ISO/IEC TR 27019:2013
  Information technology- Security techniques- Information security management guidelines based in ISO/ IEC 27002 for process control systems specific on the energy utility industry, Internationale Organisation für Normung, 07.2013
  https://www.iso.org/standard/43759.html

- [AHWAST] Ausführungshinweise zur Anwendung des Whitepaper - Anforderungen an sichere Steuerungs- und Telekommunikationssysteme (Version 1.1, 2014)
  BDEW Bundesverband der Energie- und Wasserwirtschaft e.V. und Oesterreichs E-Wirtschaft, Version 1.1, 2014
  https://www.bdew.de/internet.nsf/id/it-sicherheitsempfehlunge?open&ccm

- [CSE] Empfehlungen für Fortbildungs-und Qualifizierungsmaßnahmen im ICS-Umfeld
  BSI-Veröffentlichungen zur Cyber-Sicherheit (BSI-CS 123), Bundesamt für Sicherheit in der Informationstechnik, 11.2015
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_123.pdf

- [ICSSK] ICS-Security-Kompendium
  Bundesamt für Sicherheit in der Informationstechnik (BSI), 2016
  https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS/empfehlungen_node.html

- [ICSSKfH] ICS-Security-Kompendium für Hersteller und Integratoren
  Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.html

- [IEC62443] IEC 62443-2-1:2010 Industrial communication networks - Network and system security - Part 2-1:
  Establishing an industrial automation and control system security program, International Electrotechnical Commission (IEC), 2010
  https://webstore.iec.ch/publication/7030

- [WAST] Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme
  BDEW Bundesverband der Energie- und Wasserwirtschaft e.V, Version 1.1, 01.2015
  https://www.bdew.de/internet.nsf/id/it-sicherheitsempfehlunge?open&ccm

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Betriebs- und Steuerungstechnik" von Bedeutung.

G 0.05 Naturkatastrophen

G 0.06 Katastrophen im Umfeld

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.39 Schadprogramme

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.05	G 0.06	G 0.09	G 0.11	G 0.14	G 0.15	G 0.18	G 0.19	G 0.20	G 0.21	G 0.23	G 0.28	G 0.29	G 0.30	G 0.32	G 0.36	G 0.37	G 0.39	G 0.41	G 0.42	G 0.46
IND.1.A1							x	x	x				x	x							
IND.1.A2		x			x			x								x		x		x	
IND.1.A3					x													x	x		
IND.1.A4			x		x					x	x				x						
IND.1.A5			x	x		x	x														
IND.1.A6			x	x	x												x				
IND.1.A7															x	x	x				
IND.1.A8				x	x			x		x	x			x							
IND.1.A9								x										x	x		x
IND.1.A10															x		x	x	x		
IND.1.A11							x		x		x	x									
IND.1.A12											x	x						x	x		
IND.1.A13	x	x	x	x															x		
IND.1.A14														x	x	x					
IND.1.A15														x	x	x					
IND.1.A16											x				x				x		
IND.1.A17													x	x	x						

IND.2.1 Allgemeine ICS-Komponente

1 Beschreibung

1.1 Einleitung

Eine ICS-Komponente ist eine elektronische Komponente, die eine Maschine oder Anlage steuert oder regelt. Sie ist damit Bestandteil eines industriellen Steuerungssystems (engl. Industrial Control System, ICS) oder allgemeiner einer Betriebstechnik (engl. Operational Technology, OT). Solche Komponenten können Speicherprogrammierbare Steuerungen (SPS, engl. Programmable Logic Controller, PLC), Sensoren, Aktoren, eine Maschine oder andere Teile eines ICS sein.

Aufgrund der im OT-Umfeld typischen hohen Verfügbarkeitsanforderungen und der oft extremen Umgebungsbedingungen (Klima, Staub, Vibration, Korrosion) wurden ICS-Komponenten schon immer als robuste Geräte mit hoher Zuverlässigkeit und langer Lebensdauer konstruiert.

ICS-Komponenten werden normalerweise über Spezialsoftware des jeweiligen Herstellers konfiguriert bzw. programmiert. Das wird entweder über sogenannte Programmiergeräte (z. B. als Anwendung unter Windows oder Linux) oder über eine Engineering-Station durchgeführt, die die Anwendungsprogramme in die speicherprogrammierbaren Steuerungen lädt.

Die Rolle des Beauftragten für Informationssicherheit für den Bereich der industriellen Automatisierung wird je nach Art und Ausrichtung der Institution anders genannt. Eine weitere Bezeichnung neben ICS-Informationssicherheitsbeauftragter (ICS-ISB) ist auch Industrial Security Officer.

1.2 Zielsetzung

Ziel des Bausteins ist die Absicherung aller Arten von ICS-Komponenten, unabhängig von Hersteller, Bauart, Einsatzzweck und -ort. Er kann für ein einzelnes Gerät oder ein aus mehreren Komponenten aufgebautes modulares Gerät verwendet werden.

1.3 Abgrenzung

Die Anforderungen sind für eine generische Komponente erarbeitet. Für spezifischere ICS-Komponenten sind unter IND.2 *ICS-Komponenten* zusätzliche Bausteine verfügbar, in denen Anforderungen beschrieben sind, die über die generischen Anforderungen dieses Bausteins hinausgehen und eventuell umgesetzt werden müssen.

Der Baustein enthält keine organisatorischen Anforderungen zur Absicherung einer ICS-Komponente. Dafür müssen die Anforderungen des Bausteins IND.1 *Betriebs- und Steuerungstechnik* umgesetzt werden.

IT-Grundschutz

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Allgemeine ICS-Komponente von besonderer Bedeutung:

2.1 Beeinträchtigung durch schädliche Umgebungseinflüsse

ICS-Komponenten in industriellen Umgebungen sind häufig besonderen Bedingungen ausgesetzt, die den sicheren Betrieb beeinträchtigen können. Beispiele hierfür sind extreme Wärme, Kälte, Feuchtigkeit, Staub, Vibration oder auch ätzend oder korrodierend wirkende Atmosphären. Häufig treten auch mehrere Faktoren gleichzeitig auf. Durch solche schädlichen Umgebungseinflüsse können ICS-Komponenten schneller verschleißen und früher ausfallen.

2.2 Unvollständige Dokumentation

ICS-Komponenten sind oft unvollständig dokumentiert, sodass nicht alle Produktfunktionen bekannt sind. Besonders lückenhaft sind häufig die Angaben über die verwendeten Dienste, Protokolle und Kommunikationsports sowie zur Berechtigungsverwaltung. Das erschwert die Gefährdungsanalyse, da Schnittstellen, Funktionen sowie sicherheitsrelevante Mechanismen übersehen werden. Dadurch können potenzielle Gefährdungen nicht berücksichtigt werden. Zudem kann nicht oder nur eingeschränkt auf neue Schwachstellen einer ICS-Komponente reagiert werden, wenn die verwendeten Dienste und Ports nicht vollständig erfasst sind.

2.3 Unsichere Systemkonfiguration

Die Standardkonfiguration von ICS-Komponenten ist häufig darauf ausgelegt, dass die Komponenten korrekt funktionieren und sich leicht in Betrieb nehmen lassen. Sicherheitsmechanismen spielen dabei oft keine hinreichende Rolle. So sind in der Standardeinstellung häufig alle Dienste, Protokolle und Anschlüsse eingeschaltet und bleiben aktiv, auch wenn sie nicht benutzt werden. Ebenso bleiben voreingestellte Berechtigungen häufig unverändert.

Es ist für Angreifer leicht, solche Komponenten zu übernehmen und zu manipulieren. Ebenso ist es möglich, dass ein Angreifer die unsichere Systemkonfiguration ausnutzt, um die ICS-Komponente als Ausgangspunkt für weitere Angriffe zu nutzen. In der Folge können geschäftskritische Informationen abfließen oder auch der gesamte Betrieb der Institution beeinträchtigt werden.

2.4 Unzureichendes Benutzer- und Berechtigungsmanagement

Einige ICS-Komponenten verfügen über ein eigenes Benutzer- und Berechtigungsmanagement. Ist dieses unzureichend konzipiert, kann es passieren, dass Mitarbeiter gemeinsam Benutzerkonten nutzen oder dass Berechtigungen von ausgeschiedenen Mitarbeitern oder Dienstleistern nicht gelöscht werden. Insgesamt können so unberechtigte Personen auf ICS- Komponenten zugreifen.

2.5 Unzureichende Protokollierung

Bei ICS-Komponenten beschränkt sich die Protokollierung häufig auf prozessrelevante Ereignisse. Für die Informationssicherheit relevante Daten werden oft nicht aufgezeichnet. Dadurch lassen sich Sicherheitsvorfälle nur schwer detektieren und auch hinterher nicht mehr rekonstruieren.

2.6 Manipulation und Sabotage einer ICS-Komponente

Die vielfältigen Schnittstellen von ICS-Komponenten führen zu einem erhöhten Manipulationsrisiko für Systeme, Software und übertragene Informationen. Je nach Motivation und Kenntnissen des Täters kann sich das lokal aber auch standortübergreifend auswirken. Zudem können Status- und Alarmmeldungen oder sonstige Messwerte unterdrückt oder verändert werden.

Manipulierte Messwerte können Fehlentscheidungen von ICS-Komponenten bzw. des Bedienpersonals nach sich ziehen. Manipulierte Systeme können dazu genutzt werden, um andere Systeme oder Standorte anzugreifen oder um eine laufende Manipulation zu vertuschen.

2.7 Einsatz unsicherer Protokolle

Die im Umfeld industrieller Steuerungsanlagen eingesetzten Protokolle bieten teilweise keine oder nur eingeschränkte Sicherheitsmechanismen. Technische Informationen wie Mess- und Steuerwerte werden häufig im Klartext und ohne Integritätssicherung oder Authentifizierung übertragen. Ein Angreifer mit Zugang zum Übertragungsmedium kann dann die Inhalte der Kommunikation auslesen und verändern oder Steuerbefehle einschleusen und so Handlungen provozieren bzw. den Betrieb direkt beeinflussen. Ein Angriff auf Protokollebene ist auch dann möglich, wenn die ICS-Komponente ansonsten sicher konfiguriert ist und selbst keine Schwachstellen aufweist.

2.8 Denial-of-Service-(DoS)-Angriffe

Ein Angreifer kann den Betrieb von ICS-Komponenten durch DoS-Angriffe beeinträchtigen. Bei unter Echtzeitbedingungen ablaufenden Prozessen kann bereits eine kürzere Störung zu Informations- oder Kontrollverlust führen.

2.9 Schadprogramme

Die von Schadprogrammen ausgehende Bedrohung verschärft sich auch in industriellen Steuerungsanlagen immer mehr. Infektionsmöglichkeiten ergeben sich durch Schnittstellen zur Außenwelt und zur Office-IT (vertikale Integration) aber auch durch mobile Endgeräte wie Service-Notebooks oder durch Wechseldatenträger bei der Programmierung und Wartung von ICS-Komponenten. Durch letztere können Schadprogramme auch in isolierte Umgebungen (Überwindung des "air gap") eingebracht werden.

2.10 Ausspionieren von Informationen

ICS-Komponenten enthalten häufig detaillierte Informationen über den geregelten oder überwachten Prozess bzw. Vorgang. Auch aus sonstigen übertragenen Werten, wie Mess- oder Steuerungsdaten, lassen sich diese Informationen teilweise rekonstruieren. Gleiches gilt für Steuerungsprogramme oder -parameter.

Angreifer könnten hier an Geschäftsgeheimnisse gelangen (Industriespionage), z. B. Rezepte, Verfahren oder anderes geistiges Eigentum. Auch können sie Informationen über die Funktionsweise einer ICS-Komponente und ihrer Sicherheitsmechanismen gewinnen, die sie für weitere Angriffe benutzen können.

2.11 Unzureichende Sicherheitsanforderungen bei der Beschaffung

Aus mangelndem Bewusstsein für die Risiken und aus Kostengründen wird bei der Beschaffung häufig die Informationssicherheit nicht berücksichtigt. Dadurch können in ICS-Komponenten mitunter schwerwiegende Schwachstellen enthalten sein, die sich später nur sehr aufwändig beheben lassen.

2.12 Manipulierte Firmware

Bei ICS-Komponenten lässt sich neben dem Anwendungsprogramm auch das Betriebssystem (Firmware) verändern. Hierdurch kann manipulierte Software in das System gelangen. Die internen Speicher könnten durch ein kompromittiertes Programmiergerät, über eine lokale Datenschnittstelle (z. B. USB) oder über eine andere bestehende Netzverbindung durch einen Angreifer verändert werden. Ebenso könnte ein Software-Update auf dem Weg vom Hersteller zum Betreiber manipuliert worden sein. Schließlich könnte eine Komponente mit bereits kompromittierter Firmware beim Betreiber eintreffen, etwa bei manipulierter Lieferkette (engl. supply chain) oder Einkauf aus unsicheren Quellen. Ein Angreifer erhält dadurch die Möglichkeit, Prozesse und Abläufe zu verändern bzw. zu verfälschen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Allgemeine ICS-Komponente aufgeführt. Grundsätzlich ist der ICS-Informationssicherheitsbeauftragte (ICS-ISB) für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem

festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	ICS-Informationssicherheitsbeauftragter
Weitere Verantwortliche	ICS-Administrator, Leitstellen-Operator, Wartungspersonal

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

IND.2.1.A1 Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen [ICS-Administrator]

Es MUSS sichergestellt werden, dass nur berechtigte Mitarbeiter auf Konfigurations- und Wartungsschnittstellen von ICS-Komponenten zugreifen können. Die Konfiguration DARF NUR nach einer Freigabe an der ICS-Komponente oder einer Authentisierung geändert werden.

Standardmäßig eingerichtete bzw. herstellerseitig gesetzte Passwörter MÜSSEN gewechselt werden. Der Wechsel MUSS dokumentiert und das Passwort sicher hinterlegt werden. Standardmäßig eingerichtete bzw. herstellerseitig gesetzte Benutzerkonten SOLLTEN gewechselt werden.

IND.2.1.A2 Nutzung sicherer Protokolle für die Konfiguration und Wartung [ICS-Administrator, Wartungspersonal]

Für die Konfiguration und Wartung von ICS-Komponenten MÜSSEN sichere Protokolle benutzt werden. Die Daten DÜRFEN NICHT ungeschützt übertragen werden.

IND.2.1.A3 Protokollierung [ICS-Administrator]

Es MUSS festgelegt werden:

- welche Daten/Ereignisse protokolliert werden sollen,
- wie lange die Protokolldaten aufbewahrt werden und
- wer diese einsehen darf.

Generell MÜSSEN alle sicherheitsrelevanten Systemereignisse protokolliert und bei Bedarf ausgewertet werden.

IND.2.1.A4 Deaktivierung nicht genutzter Dienste, Funktionen und Schnittstellen [ICS-Administrator, Wartungspersonal]

Alle nicht genutzten Dienste, Funktionen und Schnittstellen der ICS-Komponenten MÜSSEN deaktiviert oder deinstalliert werden.

IND.2.1.A5 Deaktivierung nicht benutzter Benutzerkonten [ICS-Administrator]

Nicht benutzte und unnötige Benutzerkonten MÜSSEN deaktiviert werden.

IND.2.1.A6 Netzsegmentierung [ICS-Administrator]

ICS-Komponenten MÜSSEN von der Office-IT getrennt werden. Sind ICS-Komponenten von anderen Diensten im Netz abhängig, SOLLTE das ausreichend dokumentiert werden. ICS-Komponenten SOLLTEN so wenig wie möglich mit anderen ICS-Komponenten kommunizieren.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Allgemeine ICS-Komponente. Sie SOLLTEN grundsätzlich umgesetzt werden.

IND.2.1.A7 Backups [Leitstellen-Operator]

Von Programmen und Daten MÜSSEN regelmäßig und nach Systemänderungen Backups erstellt werden.

IND.2.1.A8 Schutz vor Schadsoftware [ICS-Administrator]

ICS-Komponenten SOLLTEN durch geeignete Mechanismen vor Schadprogrammen geschützt werden. Wird dafür ein Virenschutzprogramm benutzt, SOLLTEN das Programm und die Virensignaturen immer auf dem aktuellen Stand sein. Wenn die Ressourcen auf der ICS-Komponente nicht ausreichend oder die Echtzeitanforderung durch den Einsatz von Virenschutzprogrammen gefährdet werden könnte, SOLLTEN alternative Maßnahmen, wie z. B. die Abschottung der Komponente oder des Produktionsnetzes, ergriffen werden.

IND.2.1.A9 Dokumentation der Kommunikationsbeziehungen [ICS-Administrator]

Es SOLLTE dokumentiert werden, mit welchen Systemen eine ICS-Komponente welche Daten austauscht. Außerdem SOLLTEN die Kommunikationsverbindungen neu integrierter ICS-Komponenten dokumentiert werden.

IND.2.1.A10 Systemdokumentation [Leitstellen-Operator, ICS-Administrator]

Es SOLLTE eine erweiterte Systemdokumentation erstellt werden. Darin SOLLTEN Besonderheiten im Betrieb (z. B. Sicherung, Regelwartungsmaßnahmen, Austausch und Wiederherstellung von Komponenten, Leistungen Dritter) und die Möglichkeiten zur Systemverwaltung (z. B. Fernzugriff) festgehalten werden. Außerdem SOLLTE dokumentiert werden, wenn ICS-Komponenten verändert wurden. Es SOLLTE sichergestellt sein, dass nur berechtigte Mitarbeiter auf die Systemdokumentation zugreifen können. Auch SOLLTE die Dokumentation im Störungsfall noch verfügbar sein.

IND.2.1.A11 Wartung der ICS-Komponenten [Wartungspersonal, Leitstellen-Operator, ICS-Administrator]

Bei der Wartung einer ICS-Komponente SOLLTEN immer die aktuellen und freigegebenen Sicherheitsupdates eingespielt werden. Updates für das Betriebssystem SOLLTEN erst nach Freigabe durch den Hersteller einer Komponente installiert werden oder die Aktualisierung SOLLTE in einer Testumgebung getestet werden, bevor diese in einer produktiven Komponente eingesetzt wird. Für kritische Sicherheitsupdates SOLLTE kurzfristig eine Wartung durchgeführt werden.

IND.2.1.A12 Beschaffung von ICS-Komponenten [Leitstellen-Operator, ICS-Administrator]

Für ICS-Komponenten SOLLTEN einheitliche und dem Schutzbedarf angemessene Anforderungen an die Informationssicherheit definiert werden. Diese SOLLTEN berücksichtigt werden, wenn neue ICS-Komponenten beschafft werden.

IND.2.1.A13 Geeignete Inbetriebnahme der ICS-Komponenten [ICS-Administrator]

Bevor ICS-Komponenten in Betrieb genommen werden, SOLLTEN sie dem aktuellen intern freigegeben Firmware-, Software- und Patch-Stand entsprechen.

Neue ICS-Komponenten SOLLTEN in die bestehenden Betriebs-, Überwachungs- und Informationssicherheitsmanagement-Prozesse eingebunden werden. Das SOLLTE insbesondere

- die Änderungs- und Berechtigungsverwaltung,
- das Schwachstellenmanagement,
- den Schutz vor Schadsoftware,

- die betriebliche Überwachung sowie Notfallplanung und
- regelmäßige Sicherheitsüberprüfung der Systeme

umfassen.

IND.2.1.A14 Aussonderung von ICS-Komponenten [ICS-Administrator]

Bei der Aussonderung von alten oder defekten ICS-Komponenten SOLLTEN alle schützenswerten Daten sicher gelöscht werden. Es SOLLTE insbesondere sichergestellt sein, dass alle Zugangsdaten nachhaltig entfernt wurden.

IND.2.1.A15 Zentrale Systemprotokollierung und -überwachung [ICS-Administrator]

Alle ICS-Komponenten SOLLTEN ihre Protokollierungsdaten an ein zentrales System übermitteln. Die protokollierten Daten SOLLTEN regelmäßig ausgewertet werden. Bei sicherheitskritischen Ereignissen SOLLTE eine automatische Alarmierung erfolgen.

IND.2.1.A16 Schutz externer Schnittstellen [ICS-Administrator]

Von außen erreichbare Schnittstellen, z. B. Netzschnittstellen, USB-Ports oder serielle Anschlüsse, SOLLTEN vor Missbrauch geschützt werden.

IND.2.1.A17 Nutzung sicherer Protokolle für die Übertragung von Informationen [ICS-Administrator]

Mess- oder Steuerdaten SOLLTEN vor unberechtigten Zugriffen oder Veränderungen geschützt werden. Bei Anwendungen mit Echtzeitanforderungen SOLLTE geprüft werden, ob dies notwendig und umsetzbar ist. Werden Mess- oder Steuerdaten über öffentliche Netze übertragen, SOLLTEN sie angemessen geschützt werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

IND.2.1.A18 Kommunikation im Störfall [Leitstellen-Operator, ICS-Administrator] (A)

Es SOLLTE alternative und unabhängige Kommunikationsmöglichkeiten geben, die bei einem Störfall benutzt werden können, um handlungsfähig zu bleiben.

IND.2.1.A19 Security-Tests [ICS-Administrator] (CIA)

Mithilfe von regelmäßigen Security-Tests SOLLTE geprüft werden, ob die technischen Sicherheitsmaßnahmen noch effektiv umgesetzt sind. Die Security Tests SOLLTEN nicht im laufenden Anlagenbetrieb erfolgen. Die Tests SOLLTEN auf die Wartungszeiten geplant werden. Die Ergebnisse SOLLTEN dokumentiert werden. Erkannte Risiken SOLLTEN bewertet und behandelt werden.

IND.2.1.A20 Vertrauenswürdiger Code [ICS-Administrator] (IA)

Firmware-Updates oder neue Steuerungsprogramme SOLLTEN nur eingespielt werden, wenn vorher ihre Integrität und Authentizität überprüft wurde.

4 Weiterführende Informationen

4.1 Literatur

- [AHWAST] Ausführungshinweise zur Anwendung des Whitepaper - Anforderungen an sichere Steuerungs- und Telekommunikationssysteme (Version 1.1, 2014)
  BDEW Bundesverband der Energie- und Wasserwirtschaft e.V. und Oesterreichs E-Wirtschaft, Version 1.1, 2014
  https://www.bdew.de/internet.nsf/id/it-sicherheitsempfehlunge?open&ccm

- [ICSSK] ICS-Security-Kompendium
  Bundesamt für Sicherheit in der Informationstechnik (BSI), 2016
  https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS/empfehlungen_node.html

- [ICSSKfH] ICS-Security-Kompendium für Hersteller und Integratoren
  Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.html

- [NIST80082] NIST Special Publication 800-82, Revision 2
  Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology (NIST), 2015
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf

- [WAST] Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme
  BDEW Bundesverband der Energie- und Wasserwirtschaft e.V, Version 1.1, 01.2015
  https://www.bdew.de/internet.nsf/id/it-sicherheitsempfehlunge?open&ccm

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Allgemeine ICS-Komponente" von Bedeutung.

G 0.02 Ungünstige klimatische Bedingungen

G 0.04 Verschmutzung, Staub, Korrosion

G 0.08 Ausfall oder Störung der Stromversorgung

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

G 0.10 Ausfall oder Störung von Versorgungsnetzen

G 0.12 Elektromagnetische Störstrahlung

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.37 Abstreiten von Handlungen

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.41 Sabotage

G 0.43 Einspielen von Nachrichten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.02	G 0.04	G 0.08	G 0.09	G 0.10	G 0.12	G 0.14	G 0.15	G 0.19	G 0.21	G 0.22	G 0.23	G 0.25	G 0.28	G 0.30	G 0.31	G 0.32	G 0.37	G 0.39	G 0.40	G 0.41	G 0.43	G 0.45	G 0.46
IND.2.1.A1							x		x	x		x			x		x				x	x	x	x
IND.2.1.A2							x		x	x		x							x		x			x
IND.2.1.A3									x	x						x		x			x	x		
IND.2.1.A4							x	x	x	x	x	x			x						x			
IND.2.1.A5							x	x	x	x	x	x			x						x			
IND.2.1.A6							x	x		x	x	x			x	x	x		x	x	x			
IND.2.1.A7	x	x	x	x	x	x							x						x	x	x		x	
IND.2.1.A8							x		x	x	x	x	x	x	x				x					
IND.2.1.A9				x			x	x			x							x			x			x
IND.2.1.A10							x		x	x				x	x				x		x	x	x	x
IND.2.1.A11							x		x	x		x		x	x	x	x		x		x			
IND.2.1.A12	x	x				x		x		x			x	x					x					
IND.2.1.A13						x	x	x		x		x	x	x					x		x			
IND.2.1.A14							x		x						x								x	
IND.2.1.A15							x	x		x		x	x	x	x	x	x	x	x	x	x	x		x
IND.2.1.A16							x		x	x	x	x			x				x		x		x	
IND.2.1.A17							x		x	x	x				x			x	x		x			x
IND.2.1.A18				x																			x	
IND.2.1.A19			x	x			x			x		x		x	x				x	x	x			x
IND.2.1.A20							x			x		x		x					x					

IND.2: ICS-Komponenten

IND.2.2 Speicherprogrammierbare Steuerung (SPS)

1 Beschreibung

1.1 Einleitung

Eine speicherprogrammierbare Steuerung (SPS, engl. Programmable Logic Controller, PLC) ist eine ICS-Komponente. Sie übernimmt Steuerungs- und Regelaufgaben in der Betriebstechnik (engl. Operational Technology, OT). Die Grenzen zwischen verschiedenen Geräteklassen und Bauformen sind heute fließend: So kann zum Beispiel auch ein Fernwirkgerät (engl. Remote Terminal Unit, RTU) die Funktionen einer SPS übernehmen oder ein Programmable Automation Controller (PAC) kann versuchen, die Vorteile einer SPS und eines Industrie-PCs zu vereinen. Jedoch ist die SPS immer noch das klassische Automatisierungsgerät, sodass in diesem Baustein diese Begriffe synonym verwendet werden.

Eine SPS verfügt über digitale Ein- und Ausgänge, ein Echtzeitbetriebssystem (Firmware) sowie weitere Schnittstellen für Ethernet oder Feldbusse. Die Verbindung zu Sensoren und Aktoren erfolgt über die analogen oder digitalen Ein- bzw. Ausgänge oder über einen Feldbus. Die Kommunikation mit Prozessleitsystemen findet meist über die Ethernet-Schnittstelle und IP-basierte Netze statt.

Die möglichen Realisierungen sind vielfältig: SPSen können als Baugruppe, Einzelgerät, PC-Einsteckkarte (Slot-SPS) oder als Software-Emulation (Soft-SPS) eingesetzt werden. Am häufigsten anzutreffen sind modulare SPSen, die aus verschiedenen funktionalen Steckmodulen zusammengesetzt werden. Zunehmend werden auch weitere Funktionen wie das Visualisieren, Alarmieren und Protokollieren durch die SPS realisiert.

Aufgrund der im OT-Umfeld typischen hohen Verfügbarkeitsanforderungen und der oft extremen Umgebungsbedingungen (Klima, Staub, Vibration, Korrosion) wurden ICS-Komponenten schon immer als robuste Geräte mit hoher Zuverlässigkeit und langer Lebensdauer konstruiert.

SPSen werden normalerweise über Spezialsoftware des jeweiligen Herstellers konfiguriert bzw. programmiert. Das wird entweder über sogenannte Programmiergeräte (z. B. als Anwendung unter Windows oder Linux) oder über eine Engineering-Station durchgeführt, die die Daten über ein Netz verteilt.

1.2 Zielsetzung

Ziel des Bausteins ist es, alle Arten von speicherprogrammierbaren Steuerungen abzusichern, unabhängig von Hersteller, Bauart, Einsatzzweck und -ort. Er kann für eine einzelne SPS oder eine zusammenhängende, als SPS eingesetzte Baugruppe angewendet werden.

1.3 Abgrenzung

Der vorliegende Systembaustein ist anzuwenden, um alle Arten von speicherprogrammierbaren Steuerungen (d. h. SPSen und Geräte, die gleiche oder ähnliche Funktionen integrieren) abzusichern. Er ergänzt den Baustein IND.2.1 *Allgemeine ICS-Komponente*. Bei der Anwendung ist dieser daher auch zu berücksichtigen.

Der Baustein enthält keine organisatorischen Anforderungen zur Absicherung einer ICS-Komponente. Dafür müssen die Anforderungen des Bausteins IND.1 *Betriebs- und Steuerungstechnik* umgesetzt werden. Ebenso wird der Bereich funktionale Sicherheit (Safety) nicht behandelt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich SPS von besonderer Bedeutung:

2.1 Unvollständige Dokumentation

Speicherprogrammierbare Steuerungen sind oft unvollständig dokumentiert, sodass nicht alle Produktfunktionen bekannt sind. Besonders lückenhaft sind häufig die Angaben über die verwendeten Dienste, Protokolle und Kommunikationsports sowie zur Berechtigungsverwaltung. Das erschwert jedoch die Gefährdungsanalyse, da Schnittstellen, Funktionen sowie sicherheitsrelevante Mechanismen übersehen werden. Dadurch können potenzielle Gefährdungen nicht berücksichtigt werden. Zudem kann nicht oder nur eingeschränkt auf neue Schwachstellen reagiert werden, wenn diese nicht erfasst ist.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich SPS aufgeführt. Grundsätzlich ist der ICS-Informationssicherheitsbeauftragte (ICS-ISB) für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	ICS-Informationssicherheitsbeauftragter
Weitere Verantwortliche	ICS-Administrator

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Speicherprogrammierbare Steuerung (SPS). Sie SOLLTEN grundsätzlich umgesetzt werden.

IND.2.2.A1 Erweiterte Systemdokumentation für speicherprogrammierbare Steuerungen [ICS-Administrator]

Steuerungsprogramme und Konfigurationen SOLLTEN immer archiviert werden, wenn an ihnen etwas verändert wird. Änderungen an der Konfiguration oder der Tausch von Komponenten SOLLTEN vollständig dokumentiert werden.

IND.2.2.A2 Benutzerkontenkontrolle und restriktive Rechtevergabe [ICS-Administrator]

Zugriffsrechte auf Funktionen und Schnittstellen einer SPS SOLLTEN restriktiv vergeben werden. Bestehende Benutzerkonten SOLLTEN regelmäßig daraufhin überprüft werden, ob sie noch erforderlich sind, die zugewiesenen Berechtigungen noch stimmen. Wenn sich an den Zuständigkeiten der Mitarbeiter etwas ändert, SOLLTEN die Berechtigungen umgehend angepasst werden.

IND.2.2.A3 Zeitsynchronisation [ICS-Administrator]

Für die Systemzeit SOLLTE eine zentrale automatisierte Zeitsynchronisation eingerichtet werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

4 Weiterführende Informationen

4.1 Literatur

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Speicherprogrammierbare Steuerung (SPS)" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.41 Sabotage

Elementare Gefährdungen / Anforderungen	G 0.14	G 0.15	G 0.19	G 0.21	G 0.22	G 0.23	G 0.30	G 0.41
IND.2.2.A1				x	x	x		x
IND.2.2.A2	x	x	x	x	x	x	x	x
IND.2.2.A3				x	x			

IND.2.3 Sensoren und Aktoren

1 Beschreibung

1.1 Einleitung

Sensoren sind als elektronische Komponente mit Mikroprozessor und Software ausgeführte Messumformer, die eine physikalische Größe in einen elektrischen Ausgabewert wandeln. Dieser wird als normiertes Einheitssignal (häufig 4 bis 20 mA, 0 bis 10 V) als Daten an einer seriellen Schnittstelle oder als digitale Informationen, die über einen Feldbus oder Ethernet-Protokolle übertragen werden, bereitgestellt. Messumformer stellen neben den Messwerten häufig noch Schnittstellen, über die eine Diagnose und Parametrierung erfolgt, bereit. So kann ein Sensor neben einem elektronischen Ausgabewert auch noch über weitere Schnittstellen verfügen, z. B. WLAN, Bluetooth oder Wireless-HART-Schnittstellen für Parametrierung und Diagnose.

Auf dem Markt gibt es viele unterschiedliche Sensoren, z. B. um physikalische Größen zu messen. Je nach Aufgabe variieren der Funktionsumfang und die Leistungsfähigkeit eines Sensors stark. Die Bandbreite reicht von Sensoren, die lediglich Messwerte liefern und nicht konfiguriert werden müssen, über solche, die eine Kalibrierung, Konfiguration oder Vorverarbeitung von Daten bis hin zur vollständigen Signalverarbeitung (intelligente Sensoren, smart sensors) ermöglichen.

1.2 Zielsetzung

Ziel des Bausteins ist es, alle Arten von intelligenten Sensoren abzusichern, unabhängig von Hersteller, Bauart, Einsatzzweck und -ort. Er kann für einen einzelnen Sensor oder eine zusammenhängende, als Sensor eingesetzte Baugruppe angewendet werden.

1.3 Abgrenzung

Der vorliegende Systembaustein ist anzuwenden, um intelligente Sensoren abzusichern. Er ergänzt den übergeordneten Baustein IND.2.1 *Allgemeine ICS-Komponente* und setzt diesen voraus.

Einfache Sensoren ohne Konfigurationsschnittstellen oder komplexere Verarbeitungslogik werden durch den Baustein nicht erfasst, da sich hier die möglichen Schutzmaßnahmen darauf beschränken, den Zugang zum Sensor abzusichern und zu überwachen, ob er aktiv ist.

Auch behandelt der Baustein nicht den Schutz komplexer drahtloser Sensornetze. Er beschreibt lediglich, wie sich einzelne Sensoren absichern lassen. Weiterhin werden keine Sicherheitsanforderungen für Betriebs- und Steuerungstechnik beschrieben. Dafür muss der Baustein IND.1 *Betriebs- und Steuerungstechnik* umgesetzt werden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Sensoren von besonderer Bedeutung:

IT-Grundschutz

2.1 Unzureichende Sicherheitsanforderungen bei der Beschaffung

Aus mangelndem Bewusstsein für die Risiken und aus Kostengründen wird bei der Beschaffung häufig die Informationssicherheit nicht berücksichtigt. Dadurch können in Sensoren mitunter schwerwiegende Schwachstellen enthalten sein, die sich später nur sehr aufwändig beheben lassen.

Sensoren für ICS-Komponenten in industriellen Umgebungen sind häufig besonderen Bedingungen ausgesetzt, die den sicheren Betrieb beeinträchtigen können. Beispiele hierfür sind extreme Wärme, Kälte, Feuchtigkeit, Staub, Vibration oder auch ätzend oder korrodierend wirkende Atmosphären. Häufig treten auch mehrere Faktoren gleichzeitig auf. Durch solche schädlichen Umgebungseinflüsse können die Sensoren von ICS-Komponenten schneller verschleißen und früher ausfallen oder fehlerhafte Werte messen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Sensoren aufgeführt. Grundsätzlich ist der ICS-Informationssicherheitsbeauftragte (ICS-ISB) für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	ICS-Informationssicherheitsbeauftragter
Weitere Verantwortliche	ICS-Administrator, Wartungspersonal

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

IND.2.3.A1 Installation von Sensoren [ICS-Administrator, Wartungspersonal]

Sensoren MÜSSEN geeignet installiert werden. Die Sensoren MÜSSEN ausreichend robust und zuverlässig unter den vorgesehenen Umgebungsbedingungen (Klima, Staub, Vibration, Korrosion etc.) messen können.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Sensoren und Aktoren. Sie SOLLTEN grundsätzlich umgesetzt werden.

IND.2.3.A2 Kalibrierung von Sensoren [Wartungspersonal]

Wenn notwendig, SOLLTEN Sensoren regelmäßig kalibriert werden. Die Kalibrierungen SOLLTEN geeignet dokumentiert werden. Der Zugang zur Kalibrierung MUSS geschützt sein, da eine bewusste Fehl-Kalibrierung eines Sensors zu einem Angriffsvektor werden kann.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

IND.2.3.A3 Drahtlose Kommunikation (C)

Bei erhöhtem Schutzbedarf SOLLTEN drahtlose Verwaltungsschnittstellen wie Bluetooth, WLAN oder NFC NICHT benutzt werden. Alle nicht benutzten Kommunikationsschnittstellen MÜSSEN deaktiviert werden.

4 Weiterführende Informationen

4.1 Literatur

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Sensoren und Aktoren" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.21 Manipulation von Hard- oder Software

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

Elementare Gefährdungen / Anforderungen	G 0.14	G 0.18	G 0.21	G 0.23	G 0.28	G 0.30
IND.2.3.A1	x	x				x
IND.2.3.A2	x		x		x	x
IND.2.3.A3	x	x	x	x	x	x

IND.2.4 Maschine

1 Beschreibung

1.1 Einleitung

Eine Maschine ist eine technische Vorrichtung, die automatisierte Aufgaben durchführt. Ein typisches Beispiel dafür ist eine Werkzeugmaschine, die Produkte auf eine vorgegebene Art bearbeitet. Dabei wird sie von einem IT-System unter Nutzung eines Programms gesteuert, das die entsprechenden Arbeitsanweisungen und -Schritte vorgibt. Solche Maschinen werden auch als Automaten bezeichnet.

Meistens werden Maschinen von Maschinenbauern konstruiert und mit bestimmten vordefinierten Funktionen ausgestattet. Der Betreiber der Maschine kann allerdings noch die Parameter bestimmen, nach denen sie arbeiten soll. So lassen sich beispielsweise Formen, die gefräst werden sollen oder Kalibrierungen für bestimmte Materialien einstellen. Damit der Betreiber die Parameter verändern kann, verfügen Maschinen über verschiedene Schnittstellen, z. B. für Wechseldatenträger, spezialisierte Programmiergeräte oder Netzzugriffe.

Häufig werden von Maschinenbauern auch Fernwartungsdienstleistungen angeboten, um frühzeitigen Verschleiß zu erkennen oder in Problemsituationen schnell reagieren zu können.

1.2 Zielsetzung

Der Baustein beschreibt, wie elektronisch gesteuerte, halb- oder vollautomatische Maschinen (z. B. CNC-Maschinen) unabhängig von Hersteller, Bauart, speziellem Einsatzzweck und -ort abgesichert werden können.

1.3 Abgrenzung

Der vorliegende Baustein ergänzt den übergeordneten Baustein IND.2.1 *Allgemeine ICS-Komponente* und setzt voraus, dass dieser umgesetzt wurde. Darüber hinaus werden nur Anforderungen für Maschinen definiert, auf deren interne Strukturen eine Institution nicht zugreifen kann.

Auch werden keine Sicherheitsanforderungen für Betriebs- und Steuerungstechnik beschrieben. Dafür muss der Baustein IND.1 *Betriebs- und Steuerungstechnik* umgesetzt werden. Ebenso wird der Bereich funktionale Sicherheit (Safety) nicht behandelt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Maschine von besonderer Bedeutung:

2.1 Ausfall oder Störung durch ungenügende Wartung

Wenn Maschinen nicht regelmäßig gewartet werden, funktionieren sie früher nicht mehr korrekt oder fallen ganz aus. Durch Fehlfunktionen können z. B. Mitarbeiter gefährdet oder die Produktion kann erheblich beeinträchtigt werden.

2.2 Gezielte Manipulationen

Sind die Schnittstellen einer Maschine ungenügend geschützt, können Angreifer die Parameter der Maschine manipulieren, z. B. über lokale Programmiergeräte oder Netzdienste. Dadurch können Werkstücke beschädigt werden oder ganze Produktreihen fehlerhaft sein. Die Angreifer können aber auch die Maschine selbst beschädigen, sodass auch dadurch ein wirtschaftlicher Verlust entsteht.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Maschine aufgeführt. Grundsätzlich ist der ICS-Informationssicherheitsbeauftragte (ICS-ISB) für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	ICS-Informationssicherheitsbeauftragter
Weitere Verantwortliche	ICS-Administrator

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

IND.2.4.A1 Fernwartung durch Maschinen- und Anlagenbauer [ICS-Administrator]

Für die Fernwartung einer Maschine SOLLTE es eine zentrale Richtlinie geben. Darin SOLLTE geregelt werden, wie die jeweiligen Fernwartungslösungen einzusetzen sind und wie Kommunikationsverbindungen geschützt werden. Sie SOLLTE auch beschreiben, welche Aktivitäten während der Fernwartung überwacht werden sollen.

Außerdem SOLLTE NICHT möglich sein, dass über die Fernwartung einer Maschine auf andere Systeme oder Maschinen der Institution zugegriffen werden kann.

Mit einem Dienstleister SOLLTE vereinbart werden, wie er die in der Maschine gespeicherten Informationen verwerten darf.

IND.2.4.A2 Betrieb nach Ende der Gewährleistung [ICS-Administrator]

Es SOLLTE ein Prozess etabliert werden, der gewährleistet, dass die Maschine auch über den Gewährleistungszeitraum hinaus sicher weiterbetrieben werden kann. Hierzu SOLLTEN mit dem Lieferanten weitere Unterstützungsleistungen vertraglich vereinbart werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Maschine. Sie SOLLTEN grundsätzlich umgesetzt werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

4 Weiterführende Informationen

4.1 Literatur

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Maschine" von Bedeutung.

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.14 Ausspähen von Informationen (Spionage)

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.39 Schadprogramme

Elementare Gefährdungen Anforderungen	G 0.11	G 0.14	G 0.18	G 0.21	G 0.22	G 0.30	G 0.39
IND.2.4.A1	x	x	x	x	x	x	
IND.2.4.A2				x			x

Bundesamt
für Sicherheit in der
Informationstechnik

NET: Netze und Kommunikation

NET.1.1	Netzarchitektur und -design	**642**
NET.1.2	Netzmanagement	**653**
NET.2.1	WLAN-Betrieb	**663**
NET.2.2	WLAN-Nutzung	**671**
NET.3.1	Router und Switches	**676**
NET.3.2	Firewall	**686**
NET.3.3	VPN	**696**

IT-Grundschutz

NET.1: Netze

NET.1.1 Netzarchitektur und -design

1 Beschreibung

1.1 Einleitung

Die meisten Institutionen benötigen heute für ihren Geschäftsbetrieb Rechnernetze über die z. B. Informationen und Daten ausgetauscht sowie verteilte Anwendungen realisiert werden. In solche Netze werden nicht nur herkömmliche Endgeräte, Partner-Institutionen und das Internet eingebunden, sondern sie integrieren zunehmend auch mobile Endgeräte und Elemente, die dem Internet of Things (IoT) zugerechnet werden. Darüber hinaus werden über Rechnernetze vermehrt auch Cloud-Dienste sowie Dienste für Unified Communication and Collaboration (UCC) genutzt. Die Vorteile, die sich dadurch ergeben, sind unbestritten. Aber durch die vielen Endgeräte und Dienste steigen jedoch auch die Risiken. Deshalb ist es wichtig, das eigene Netz bereits durch eine sichere Netzarchitektur zu schützen. Hierfür muss zum Beispiel geplant werden, wie ein lokales Netz (Local Area Network, LAN) oder ein Wide Area Network (WAN) sicher aufgebaut werden kann. Ebenso müssen nur eingeschränkt vertrauenswürdige externe Netze, z. B. das Internet oder Kunden-Netze, geeignet angebunden werden.

Um ein hohes Sicherheitsniveau zu gewährleisten, sind zusätzliche sicherheitsrelevante Aspekte zu berücksichtigen: So sollten z. B. verschiedene Mandanten und Gerätegruppen sicher auf Ebene des Netzes getrennt und ihre Kommunikation durch Firewall-Techniken kontrolliert werden. Ein weiteres wichtiges Sicherheitselement speziell im Client-Bereich ist außerdem die Netzzugangskontrolle (siehe NET.1.3 *Network Access Control*).

1.2 Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil der Netzarchitektur und des Netzdesigns zu etablieren.

1.3 Abgrenzung

Der Baustein enthält grundsätzliche Anforderungen, die es zu beachten und erfüllen gilt, wenn Netze geplant, aufgebaut und betrieben werden. Anforderungen für den sicheren Betrieb der entsprechenden Netzkomponenten, inklusive Sicherheitskomponenten wie z. B. Firewalls und Intrusion Detection Systems / Intrusion Prevention Systems (IDS/IPS), sind nicht Gegenstand des vorliegenden Bausteins. Diese werden in der Bausteingruppe NET.3 *Netzkomponenten* behandelt.

Der Fokus dieses Bausteins liegt auf kabelgebundenen Netzen und auf Datenkommunikation. Jedoch müssen allgemeine Anforderungen an die Architektur und das Design, z. B. Sicherheitszonen und -segmente trennen, für alle Netztechniken beachtet und erfüllt werden. Weitergehende spezifische Anforderungen für Netzbereiche wie Wireless LAN (WLAN) oder Speichernetze (Storage Area Networks, SAN) werden in den Bausteingruppen NET.2 *Funknetze* bzw. im Baustein SYS.1.8 *Speichersysteme* behandelt. Darüber hinaus werden auch die Themen UCC und Voice over IP (VoIP) so-

wie die hierfür zugrunde liegende Sicherheitsinfrastruktur nicht in diesem Baustein erörtert, sondern in den entsprechenden Bausteinen NET.4.2 *VoIP* bzw. NET.4.5 *Unified Communications* behandelt.

Spezifische sicherheitstechnische Anforderungen für Virtual Private Clouds und Hybrid Clouds liegen nicht im Fokus dieses Bausteins (siehe dafür OPS.3.2 *Cloud-Anbieter* und OPS.3.4 *Managed Security Services*).

Das Netzmanagement wird im Rahmen der Zonierung und Segmentierung betrachtet, alle weitergehenden Themen des Netzmanagements werden im Baustein NET.1.2 *Netzmanagement* behandelt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Netzarchitektur und -design von besonderer Bedeutung:

2.1 Ausfall oder unzureichende Performance von Kommunikationsverbindungen

Sind die Kommunikationsverbindungen unzureichend dimensioniert oder reicht ihre Leistung aufgrund von technischen Ausfällen oder aufgrund eines Denial-of-Service-(DoS)-Angriffs nicht mehr aus, können z. B. Clients nur noch eingeschränkt mit Servern kommunizieren. Dadurch erhöhen sich die Zugriffszeiten auf interne und externe Dienste (z. B. Cloud-Dienste), die so mitunter nur noch eingeschränkt oder gar nicht mehr nutzbar sind. Auch sind eventuelle geschäftsrelevante Informationen nicht mehr verfügbar. In der Folge kann es beispielsweise zu Produktionsausfällen kommen oder essenzielle Geschäftsprozesse fallen aus.

2.2 Ungenügend abgesicherte Netzzugänge

Ist das interne Netz mit dem Internet verbunden und der Übergang nicht ausreichend geschützt, z. B. weil keine Firewall eingesetzt wird oder sie falsch konfiguriert ist, können Angreifer auf schützenswerte Informationen der Institution zugreifen und diese kopieren oder manipulieren.

2.3 Unsachgemäßer Aufbau von Netzen

Wird ein Netz unsachgemäß aufgebaut oder fehlerhaft erweitert, können unsichere Netztopologien und Netzkonfigurationen entstehen. Angreifer können so leichter Sicherheitslücken finden, ins interne Netz der Institution eindringen und dort Informationen abziehen, Daten manipulieren oder auch ganze Produktionssysteme stören. Auch bleiben Angreifer in einem fehlerhaft aufgebauten Netz, das die Sicherheitssysteme nur eingeschränkt überwachen können, länger unerkannt.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Netzarchitektur und -design aufgeführt. Grundsätzlich ist der Leiter Netze für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	Leiter Netze
Weitere Verantwortliche	IT-Betrieb, Informationssicherheitsbeauftragter (ISB), Leiter IT

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

NET.1.1.A1 Sicherheitsrichtlinie für das Netz [Leiter IT, Informationssicherheitsbeauftragter (ISB)]

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie für das Netz erstellt werden, in der nachvollziehbar Anforderungen und Vorgaben beschrieben sind, wie Netze sicher konzipiert und aufgebaut werden. In der Richtlinie MUSS unter anderem festgelegt werden:

- in welchen Fällen die Sicherheitszonen zu segmentieren sind und in welchen Fällen Benutzergruppen bzw. Mandanten logisch oder sogar physisch zu trennen sind,
- welche Kommunikationsbeziehungen und welche Netz- und Anwendungsprotokolle jeweils zugelassen werden,
- wie der Datenverkehr für Administration und Überwachung netztechnisch zu trennen ist,
- welche institutionsinterne, standortübergreifende Kommunikation (WAN, Funknetze) erlaubt und welche Verschlüsselung im WAN, LAN oder auf Funkstrecken erforderlich ist,
- welche institutionsübergreifende Kommunikation zugelassen ist.

Die Richtlinie MUSS allen im Bereich Netzdesign verantwortlichen Mitarbeitern bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies dokumentiert und mit dem verantwortlichen ISB abgestimmt werden. Es MUSS regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse MÜSSEN sinnvoll dokumentiert werden.

NET.1.1.A2 Dokumentation des Netzes [IT-Betrieb]

Es MUSS eine vollständige Dokumentation des Netzes (inklusive Netzplan) erstellt und nachhaltig gepflegt werden. Darin MÜSSEN die initiale Ist-Aufnahme (einschließlich der Netzperformance) sowie alle durchgeführten Änderungen im Netz enthalten sein. Auch MUSS die logische Struktur des Netzes dokumentiert werden, insbesondere wie die Subnetze zugeordnet und wie das Netz zoniert und segmentiert wird.

NET.1.1.A3 Anforderungsspezifikation für das Netz

Ausgehend von der Sicherheitsrichtlinie (siehe NET.1.1.A1 *Sicherheitsrichtlinie für das Netz*) MUSS eine Anforderungsspezifikation für das Netz erstellt und nachhaltig gepflegt werden. Aus den Anforderungen MÜSSEN sich alle wesentlichen Elemente für Netzarchitektur und -design ableiten lassen.

NET.1.1.A4 Netztrennung in Sicherheitszonen

Das Gesamtnetz MUSS in mindestens folgende drei Sicherheitszonen physisch separiert sein: internes Netz, demilitarisierte Zone (DMZ) und Außenanbindungen (inklusive Internetanbindung sowie Anbindung an andere nicht vertrauenswürdige Netze). Zonenübergänge MÜSSEN durch eine Firewall abgesichert werden. Diese Kontrolle MUSS dem Prinzip der lokalen Kommunikation folgen, sodass von Firewalls ausschließlich erlaubte Kommunikation weitergeleitet wird (Whitelisting).

Nicht vertrauenswürdige Netze (z. B. Internet) und vertrauenswürdige Netze (z. B. Intranet) MÜSSEN durch eine zweistufige Firewall-Struktur, bestehend aus zustandsbehafteten Paketfiltern (Firewall), getrennt werden. Um Internet und externe DMZ netztechnisch zu trennen, MUSS mindestens ein zustandsbehafteter Paketfilter (Firewall) eingesetzt werden.

In der zweistufigen Firewall-Architektur MUSS jeder ein- und ausgehende Datenverkehr durch den äußeren Paketfilter (Firewall) bzw. den internen Paketfilter (Firewall) kontrolliert und gefiltert werden.

Eine P-A-P-Struktur, die aus Paketfilter, Application-Layer-Gateway bzw. Sicherheits-Proxies und Paketfilter besteht, MUSS immer realisiert werden, wenn die Sicherheitsrichtlinie oder die Anforderungsspezifikation dies fordern.

NET.1.1.A5 Client-Server-Segmentierung

Clients und Server MÜSSEN in unterschiedlichen Sicherheitssegmenten platziert werden. Die Kommunikation zwischen diesen Segmenten MUSS mindestens durch einen zustandsbehafteten Paketfilter (Firewall) kontrolliert werden.

Es SOLLTE beachtet werden, dass etwaige Ausnahmen, die es erlauben, Clients und Server in einem gemeinsamen Sicherheitssegment zu positionieren in den entsprechenden anwendungs- und systemspezifischen Bausteinen geregelt werden.

Für Gastzugänge und für Netzbereiche, in denen keine ausreichende interne Kontrolle über die Endgeräte gegeben ist, MÜSSEN dedizierte Sicherheitssegmente eingerichtet werden.

NET.1.1.A6 Endgeräte-Segmentierung im internen Netz

Es DÜRFEN NUR Endgeräte in einem Sicherheitssegment positioniert werden, die einem ähnlichen Sicherheitsniveau entsprechen.

NET.1.1.A7 Absicherung von schützenswerten Informationen

Schützenswerte Informationen MÜSSEN über nach dem derzeitigen Stand der Technik sichere Protokolle übertragen werden, falls nicht über vertrauenswürdige dedizierte Netzsegmente (z. B. innerhalb des Managementnetzes) kommuniziert wird. Können solche Protokolle nicht genutzt werden, MUSS nach Stand der Technik angemessen verschlüsselt und authentisiert werden (siehe NET.3.3 *VPN).*

NET.1.1.A8 Grundlegende Absicherung des Internetzugangs

Der Internetzugang MUSS entsprechend NET.1.1.A4 *Netztrennung in Sicherheitszonen* gestaltet werden. Der Internetverkehr MUSS über die Firewall-Struktur geführt werden. Die Datenflüsse MÜSSEN durch die Firewall-Struktur auf die benötigten Protokolle und Kommunikationsbeziehungen eingeschränkt werden.

NET.1.1.A9 Grundlegende Absicherung der Kommunikation mit nicht vertrauenswürdigen Netzen

Für jedes Netz MUSS festgelegt werden, inwieweit es als vertrauenswürdig einzustufen ist. Netze, die überhaupt nicht vertrauenswürdig sind, MÜSSEN wie das Internet behandelt und entsprechend abgesichert werden.

NET.1.1.A10 DMZ-Segmentierung für Zugriffe aus dem Internet

Die Firewall-Strukur MUSS für alle Dienste bzw. Anwendungen, die aus dem Internet erreichbar sind, um eine sogenannte externe DMZ ergänzt werden. Es SOLLTE ein Konzept zur DMZ-Segmentierung erstellt werden, das die Sicherheitsrichtlinie und die Anforderungsspezifikation nachvollziehbar umsetzt. Abhängig vom Sicherheitsniveau der IT-Systeme MÜSSEN die DMZ-Segmente weitergehend unterteilt werden. Eine externe DMZ MUSS am äußeren Paketfilter angeschlossen werden.

NET.1.1.A11 Absicherung eingehender Kommunikation vom Internet in das interne Netz

Ein IP-basierter Zugriff auf das interne Netz MUSS über einen sicheren Kommunikationskanal erfolgen und auf vertrauenswürdige IT-Systeme und Benutzer beschränkt werden (siehe NET.3.3 *VPN*). Derartige VPN-Gateways SOLLTEN in einer externen DMZ realisiert werden. Es SOLLTE beachtet werden, dass hinreichend gehärtete VPN-Gateways direkt aus dem Internet erreichbar sein können. Die über das VPN-Gateway authentisierten Netzzugriffe ins interne Netz MÜSSEN mindestens die interne Firewall (zur Absicherung des internen Netzes) durchlaufen.

IT-Systeme DÜRFEN via Internet oder externer DMZ NICHT auf das interne Netz zugreifen. Es SOLLTE beachtet werden, dass etwaige Ausnahmen zu dieser Anforderung in den entsprechenden anwendungs- und systemspezifischen Bausteinen (z. B. APP.5.1 *E-Mail/Groupware*, NET.4.2 *VoIP)* geregelt werden.

NET.1.1.A12 Absicherung ausgehender interner Kommunikation zum Internet

Ausgehende Kommunikation aus dem internen Netz zum Internet MUSS an einem Sicherheits-Proxy entkoppelt werden. Die Entkoppelung MUSS außerhalb des internen Netzes erfolgen. Wird eine P-A-P-Struktur eingesetzt, SOLLTE die ausgehende Kommunikation immer durch die Sicherheits-Proxies der P-A-P Struktur entkoppelt werden.

NET.1.1.A13 Netzplanung

Jede Netzimplementierung MUSS geeignet, vollständig und nachvollziehbar geplant werden. Dabei MÜSSEN die Sicherheitsrichtlinie sowie die Anforderungsspezifikation beachtet werden. Darüber hinaus MÜSSEN in der Planung mindestens die folgenden Punkte bedarfsgerecht berücksichtigt werden:

- Anbindung von Internet und, sofern vorhanden, Standortnetz und Extranet,
- Topologie des Gesamtnetzes und der Netzbereiche, d. h. Sicherheitszonen und -segmente,
- Dimensionierung und Redundanz der Netz- und Sicherheitskomponenten, Übertragungsstrecken und Außenanbindungen,
- zu nutzende Protokolle und deren grundsätzliche Konfiguration und Adressierung, insbesondere IPv4/IPv6-Subnetze von Endgerätegruppen,
- Administration und Überwachung (siehe NET.1.2 *Netzmanagement*).

Die Netzplanung MUSS regelmäßig überprüft werden.

NET.1.1.A14 Umsetzung der Netzplanung

Das geplante Netz MUSS fachgerecht umgesetzt werden. Dies MUSS während der Abnahme geprüft werden.

NET.1.1.A15 Regelmäßiger Soll-Ist-Vergleich [Informationssicherheitsbeauftragter (ISB)]

Es MUSS regelmäßig geprüft werden, ob das bestehende Netz dem Soll-Zustand entspricht. Dabei MUSS mindestens geprüft werden, inwieweit es die Sicherheitsrichtlinie und Anforderungsspezifikation erfüllt und inwiefern die umgesetzte Netzstruktur dem aktuellen Stand der Netzplanung entspricht. Dafür MÜSSEN zuständige Personen sowie Prüfkriterien bzw. Vorgaben festgelegt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Netzarchitektur und -design. Sie SOLLTEN grundsätzlich umgesetzt werden.

NET.1.1.A16 Spezifikation der Netzarchitektur

Auf Basis der Sicherheitsrichtlinie und der Anforderungsspezifikation SOLLTE eine Architektur für die Sicherheitszonen inklusive internem Netz, DMZ-Bereich und Außenanbindungen entwickelt und nachhaltig gepflegt werden. Dabei SOLLTEN je nach spezifischer Situation der Institution alle relevanten Architekturelemente betrachtet werden, mindestens jedoch:

- Netzarchitektur des internen Netzes mit Festlegungen dazu, wie Netzvirtualisierungstechniken, Layer-2- und Layer-3-Kommunikation sowie Redundanzverfahren einzusetzen sind,
- Netzarchitektur für Außenanbindungen, inklusive Firewall-Architekturen, sowie DMZ- und Extranet-Design und Vorgaben an die Standortkopplung,
- Festlegung, an welchen Stellen des Netzes welche Sicherheitskomponenten wie Firewalls oder IDS/IPS zu platzieren sind und welche Sicherheitsfunktionen diese realisieren müssen,
- Vorgaben für die Netzanbindung der verschiedenen IT-Systeme,
- Netzarchitektur in Virtualisierungs-Hosts, wobei insbesondere Network Virtualization Overlay (NVO) und die Architektur in Vertikal integrierten Systemen (ViS) zu berücksichtigen sind,
- Festlegungen der grundsätzlichen Architektur-Elemente für eine Private Cloud sowie Absicherung der Anbindungen zu Virtual Private Cloud, Hybrid Cloud und Public Cloud (siehe OPS.3.2 *Cloud-Anbieter* und OPS.3.4 *Managed Security Services*),
- Architektur zur sicheren Administration und Überwachung der IT-Infrastruktur.

NET.1.1.A17 Spezifikation des Netzdesigns

Basierend auf der Netzarchitektur SOLLTE das Netzdesign für die Sicherheitszonen inklusive internem Netz, DMZ-Bereich und Außenanbindungen entwickelt und nachhaltig gepflegt werden. Dafür SOLLTEN die relevanten Architekturelemente detailliert werden, mindestens jedoch:

- zulässige Formen von Netzkomponenten inklusive virtualisierter Netzkomponenten,
- Festlegungen darüber, wie WAN- und Funkverbindungen abzusichern sind,
- Anbindung von Endgeräten an Switching-Komponenten, Verbindungen zwischen Netzelementen sowie Verwendung von Kommunikationsprotokollen,
- Redundanzmechanismen für alle Netzelemente,
- Adresskonzept für IPv4 und IPv6 sowie zugehörige Routing- und Switching-Konzepte,
- virtualisierte Netze in Virtualisierungs-Hosts inklusive NVO,
- Aufbau, Anbindung und Absicherung von Private Clouds sowie sichere Anbindung von Virtual Private Clouds, Hybrid Clouds und Public Clouds,
- Festlegungen zum Netzdesign für die sichere Administration und Überwachung der IT-Infrastruktur.

NET.1.1.A18 P-A-P-Struktur für die Internet-Anbindung

Zwischen den beiden Firewall-Stufen (siehe NET.1.1.A4 *Netztrennung in Sicherheitszonen*) MUSS ein proxy-basiertes Application-Layer-Gateways (ALG) bzw. MÜSSEN entsprechende Sicherheits-Proxies realisiert werden. Diese MÜSSEN jeweils über ein Transfernetz (dual-homed) zur äußeren Firewall und zur internen Firewall angebunden werden. In diesen Transfernetzen DARF NUR das proxy-basierte ALG bzw. DÜRFEN NUR entsprechende Sicherheits-Proxies integriert werden. Jeglicher Datenverkehr MUSS über das ALG bzw. entsprechende Sicherheits-Proxies entkoppelt werden. Ein Transportnetz, das beide Firewall-Stufen direkt miteinander verbindet, DARF NICHT konfiguriert werden. Die interne Firewall MUSS zudem die Angriffsfläche des ALGs bzw. der Sicherheits-Proxies gegenüber Innentätern oder IT-Systemen im internen Netz reduzieren.

Authentisierte und vertrauenswürdige Netzzugriffe, ausgehend von dem VPN-Gateway ins interne Netz, SOLLTEN NICHT das ALG bzw. die Sicherheits-Proxies der P-A-P-Struktur durchlaufen.

NET.1.1.A19 Separierung der Infrastrukturdienste

Server, die grundlegende Dienste für die IT-Infrastruktur bereitstellen, SOLLTEN in einem dedizierten Sicherheitssegment positioniert werden. Die Kommunikation mit ihnen SOLLTE durch einen zustandsbehafteten Paketfilter (Firewall) kontrolliert werden.

NET.1.1.A20 Zuweisung dedizierter Subnetze für IPv4/IPv6-Endgerätegruppen

Unterschiedliche IPv4-/IPv6- Endgeräte SOLLTEN je nach verwendeten Protokoll (IPv4-/IPv6- oder IPv4/IPv6-DualStack) dedizierten Subnetzen zugeordnet werden.

NET.1.1.A21 Separierung des Management-Bereichs

Es SOLLTE durchgängig ein Out-of-Band-Management genutzt werden, um die Infrastruktur zu managen. Dabei SOLLTEN alle Endgeräte, die für das Management der IT-Infrastruktur benötigt werden, in dedizierten Segmenten positioniert werden. Die Kommunikation mit diesen Endgeräten SOLLTE durch einen zustandsbehafteten Paketfilter (Firewall) kontrolliert werden. Die Kommunikation von und zu diesen Management-Segmenten SOLLTE auf die notwendigen Management-Protokolle mit definierten Kommunikations-Endpunkten beschränkt werden.

Der Management-Bereich SOLLTE mindestens die folgenden Sicherheitssegmente umfassen, die abhängig von der Sicherheitsrichtlinie und der Anforderungsspezifikation weiter unterteilt werden SOLLTEN:

- Segment(e) für IT-Systeme, die für die Authentisierung und Autorisierung der administrativen Kommunikation zuständig sind,
- Segment(e) für die Administration der IT-Systeme,
- Segment(e) für die Überwachung und das Monitoring,

- Segment(e), die die zentrale Protokollierung inklusive Syslog-Server und SIEM-Server enthalten,
- Segment(e) für IT-Systeme, die für grundlegende Dienste des Management-Bereichs benötigt werden,
- Segment(e) für die Management-Interface der zu administrierenden IT-Systeme.

Die verschiedenen Management-Interface der IT-Systeme MÜSSEN nach ihrem Einsatzzweck und ihrer Netzplatzierung über einen zustandsbehafteten Paketfilter (Firewall) getrennt werden. Dabei SOLLTEN die IT-Systeme (Management-Interface) zusätzlich folgender Zugehörigkeit über dedizierte Firewalls getrennt werden:

- IT-Systeme, die aus dem Internet erreichbar sind,
- IT-Systeme im internen Netz,
- Sicherheitskomponenten, die sich zwischen den aus dem Internet erreichbaren IT-Systemen und dem internen Netz befinden.

Es MUSS sichergestellt werden, dass die Segmentierung nicht durch die Management-Kommunikation unterlaufen werden kann, d. h. eine Überbrückung von Segmenten MUSS ausgeschlossen werden.

NET.1.1.A22 Spezifikation des Segmentierungskonzepts

Auf Basis der Spezifikationen von Netzarchitektur und Netzdesign SOLLTE ein umfassendes Segmentierungskonzept für das interne Netz, inklusive eventuell vorhandener virtualisierter Netze in Virtualisierungs-Hosts, geplant, umgesetzt, betrieben und nachhaltig gepflegt werden. Das Konzept SOLLTE mindestens die folgenden Punkte umfassen, soweit diese in der Zielumgebung vorgesehen sind:

- Initial anzulegende Sicherheitssegmente und Vorgaben dazu, wie neue Sicherheitssegmente zu schaffen sind und wie Endgeräte in den Sicherheitssegmenten zu positionieren sind.
- Festlegung für die Segmentierung von Entwicklungs- und Testsystemen (Staging)
- Netzzugangskontrolle für Sicherheitssegmente mit Clients
- Anbindung von Netzbereichen, die über Funktechniken oder Standleitung an die Sicherheitssegmente angebunden sind
- Anbindung der Virtualisierungs-Hosts und von virtuellen Maschinen auf den Hosts an die Sicherheitssegmente
- Rechenzentrumsautomatisierung
- Festlegungen dazu, wie Endgeräte einzubinden sind, die mehrere Sicherheitssegmente versorgen, z. B. Load Balancer, und Speicher- sowie Datensicherungslösungen

Abhängig von der Sicherheitsrichtlinie und der Anforderungsspezifikation SOLLTE für jedes Sicherheitssegment konzipiert werden, wie es netztechnisch realisiert werden soll. Darüber hinaus SOLLTE festgelegt werden, welche Sicherheitsfunktionen die Koppelelemente zwischen den Sicherheitssegmenten bereitstellen müssen (z. B. Firewall als zustandsbehafteter Paketfilter oder IDS/IPS).

NET.1.1.A23 Trennung von Sicherheitssegmenten

IT-Systeme mit unterschiedlichem Schutzbedarf SOLLTEN in verschiedenen Sicherheitssegmenten platziert werden. Ist dies nicht möglich, richtet sich der Schutzbedarf nach dem höchsten vorkommenden Schutzbedarf im Sicherheitssegment. Darüber hinaus SOLLTEN die Sicherheitssegmente abhängig von ihrer Größe und den Anforderungen des Segmentierungskonzepts weiter unterteilt werden. Es MUSS sichergestellt werden, dass keine Überbrückung von Segmenten oder gar Zonen möglich ist.

Gehören die VLANs an einem Switch unterschiedlichen Institutionen an, SOLLTE die Trennung entweder physisch erfolgen oder es SOLLTE Verschlüsselung eingesetzt werden, um die übertragenen Informationen vor unbefugtem Zugriff zu schützen.

NET.1.1.A24 Sichere logische Trennung mittels VLAN

Durch ein Virtual LAN (VLAN) DARF KEINE Verbindung zwischen einer Zone vor dem ALG bzw. den Sicherheits-Proxies einer P-A-P-Struktur und dem dahinter liegenden internen Netz geschaffen werden.

Generell MUSS sichergestellt werden, dass keine Überbrückung von Zonen möglich ist, wenn VLANs eingesetzt werden.

NET.1.1.A25 Fein- und Umsetzungsplanung von Netzarchitektur und -design

Eine Fein- und Umsetzungsplanung für die Netzarchitektur und das Netzdesign SOLLTE durchgeführt, dokumentiert, geprüft und nachhaltig gepflegt werden.

NET.1.1.A26 Spezifikation von Betriebsprozessen für das Netz

Für einen sicheren und effektiven Netzbetrieb SOLLTEN Betriebsprozesse bedarfsgerecht erzeugt oder angepasst und dokumentiert werden (siehe Bausteingruppe Kern-IT-Betrieb, insbesondere OPS.1.1.3 *Patch- und Änderungsmanagement*). Dabei SOLLTE insbesondere berücksichtigt werden, wie sich die Zonierung sowie das Segmentierungskonzept auf den IT-Betrieb auswirken.

NET.1.1.A27 Einbindung der Netzarchitektur in die Notfallplanung [Leiter IT]

Initial und in regelmäßigen Abständen SOLLTE nachvollziehbar analysiert werden, wie sich die Netzarchitektur und die abgeleiteten Konzepte auf die Notfallplanung auswirken.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

NET.1.1.A28 Hochverfügbare Netz- und Sicherheitskomponenten (A)

Zentrale Bereiche des internen Netzes sowie die Sicherheitskomponenten SOLLTEN hochverfügbar realisiert werden. Hierzu SOLLTEN die Komponenten redundant ausgelegt und auch intern hochverfügbar realisiert werden.

NET.1.1.A29 Hochverfügbare Realisierung von Netzanbindungen (A)

Die Netzanbindungen (z. B. Internet-Anbindung und WAN-Verbindungen) SOLLTEN vollständig redundant gestaltet werden. Je nach Verfügbarkeitsanforderung SOLLTEN redundante Anbindungen an einen oder verschiedene Anbieter, bedarfsabhängig mit unterschiedlicher Technik und Performance, bedarfsgerecht umgesetzt werden. Auch SOLLTE Wegeredundanz innerhalb und außerhalb der eigenen Zuständigkeit bedarfsgerecht umgesetzt werden. Hierbei SOLLTEN mögliche Single Points of Failures (SPoF) und störende Umgebungsbedingungen berücksichtigt werden.

NET.1.1.A30 Schutz vor Distributed-Denial-of-Service (A)

Um DDoS-Angriffe abzuwehren, SOLLTE per Bandbreitenmanagement die verfügbare Bandbreite gezielt zwischen verschiedenen Kommunikationspartnern und Protokollen aufgeteilt werden.

Um DDoS-Angriffe mit sehr hohen Datenraten abwehren zu können, SOLLTEN Mitigation-Dienste über größere Internet Service Provider (ISPs) eingekauft und deren Nutzung SOLLTE in Verträgen geregelt werden.

NET.1.1.A31 Physische Trennung von Sicherheitssegmenten (CIA)

Abhängig von Sicherheitsrichtlinie und Anforderungsspezifikation SOLLTEN Sicherheitssegmente physisch durch separate Switches getrennt werden.

NET.1.1.A32 Physische Trennung von Management-Segmenten (CIA)

Abhängig von Sicherheitsrichtlinie und Anforderungsspezifikation SOLLTEN Sicherheitssegmente des Management-Bereichs physisch voneinander getrennt werden.

NET.1.1.A33 Mikrosegmentierung des Netzes (CIA)

Um potenzielle Angriffe auf eine geringe Zahl von Endgeräten zu beschränken, SOLLTE das Netz in kleine Segmente mit sehr ähnlichem Anforderungsprofil und selbem Schutzbedarf unterteilt werden. Insbesondere SOLLTE dies für die DMZ-Segmente berücksichtigt werden.

NET.1.1.A34 Einsatz kryptografischer Verfahren auf Netzebene (CI)

Die Sicherheitssegmente SOLLTEN im internen Netz, im Extranet und im DMZ-Bereich mittels kryptografischer Techniken bereits auf Netzebene realisiert werden. Dafür SOLLTEN VPN-Techniken oder IEEE 802.1AE eingesetzt werden.

Wenn innerhalb von internem Netz, Extranet oder DMZ über Verbindungsstrecken kommuniziert wird, die für einen erhöhten Schutzbedarf nicht ausreichend sicher sind, SOLLTE die Kommunikation angemessen auf Netzebene verschlüsselt werden.

NET.1.1.A35 Einsatz von netzbasiertem DLP [Informationssicherheitsbeauftragter (ISB)] (CI)

Auf Netzebene SOLLTEN Systeme zur Data Loss Prevention (DLP) eingesetzt werden, um das Risiko von Datenabflüssen zu verringern.

NET.1.1.A36 Trennung mittels VLAN bei sehr hohem Schutzbedarf

Bei sehr hohem Schutzbedarf SOLLTEN KEINE VLANs eingesetzt werden.

4 Weiterführende Informationen

4.1 Literatur

- [27033-5] ISO/IEC 27033-5:2013
  Information technology - Security techniques - Network Security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs), ISO, 08.2013
  https://www.iso.org/standard/51584.html

- [ISILANA] BSI-Standard zur Internet-Sicherheit (Isi-Reihe):
  Sichere Anbindung von lokalen Netzen an das Internet (Isi-LANA), Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014
  https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-LANA/lana_node.html

- [TL2103] BSI TL-02103 - Version 2.0 "Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf"
  Bundesamt für Sicherheit in der Informationstechnik, 2014
  https://www.bsi.bund.de/DE/Publikationen/TL-sichere-TK-Anlagen/TL02103_htm.html

- [TR21022] BSI Technische Richtlinie, Kryptografische Verfahren
  Verwendung von Transport Layer Security (TLS), Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017
  https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Netzarchitektur und -design" von Bedeutung.

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.43 Einspielen von Nachrichten

Elementare Gefährdungen / Anforderungen	G 0.09	G 0.11	G 0.18	G 0.19	G 0.22	G 0.23	G 0.27	G 0.29	G 0.30	G 0.39	G 0.40	G 0.43
NET.1.1.A1	x	x	x	x	x	x	x	x	x	x	x	x
NET.1.1.A2			x				x	x				
NET.1.1.A3	x	x	x	x	x	x	x		x	x	x	x
NET.1.1.A4	x		x	x		x		x	x	x	x	x
NET.1.1.A5	x			x	x	x		x	x	x	x	x
NET.1.1.A6	x			x	x	x		x	x	x		x
NET.1.1.A7				x	x	x		x				x
NET.1.1.A8			x	x	x	x		x	x	x	x	x
NET.1.1.A9			x	x	x	x		x	x	x	x	x
NET.1.1.A10			x	x	x	x		x	x	x	x	x
NET.1.1.A11			x	x	x	x		x	x	x	x	x
NET.1.1.A12			x	x		x		x	x	x		
NET.1.1.A13	x	x	x	x	x	x	x	x	x	x	x	x
NET.1.1.A14	x	x	x	x	x	x	x	x	x	x	x	x
NET.1.1.A15	x		x				x	x	x			
NET.1.1.A16	x	x	x	x	x	x	x	x	x	x	x	x
NET.1.1.A17	x	x	x	x	x	x	x	x	x	x	x	x
NET.1.1.A18	x		x	x	x	x		x	x	x	x	x
NET.1.1.A19	x			x	x	x			x	x	x	x
NET.1.1.A20	x		x				x					
NET.1.1.A21	x		x		x	x			x	x		x
NET.1.1.A22	x		x	x	x	x	x		x	x	x	x
NET.1.1.A23	x		x	x	x	x			x	x	x	x
NET.1.1.A24	x		x	x	x	x			x			x
NET.1.1.A25	x	x	x	x	x	x	x	x	x	x	x	x
NET.1.1.A26	x		x						x			
NET.1.1.A27	x	x	x					x		x	x	
NET.1.1.A28	x	x					x				x	
NET.1.1.A29	x	x					x				x	
NET.1.1.A30	x	x					x				x	
NET.1.1.A31	x		x	x	x	x				x	x	x
NET.1.1.A32					x	x			x			
NET.1.1.A33	x			x	x	x			x	x		x
NET.1.1.A34				x	x	x		x	x	x		x
NET.1.1.A35				x	x	x		x	x	x	x	
NET.1.1.A36	x		x	x	x	x			x			x

NET.1: Netze

NET.1.2 Netzmanagement

1 Beschreibung

1.1 Einleitung

Ein zuverlässiges Netzmanagement ist Grundvoraussetzung für den sicheren und effizienten Betrieb moderner Netze. Dazu ist es erforderlich, dass das Netzmanagement alle Netzkomponenten umfassend integriert und geeignete Maßnahmen umsetzt, um die Management-Kommunikation und -Infrastruktur zu schützen.

Das Netzmanagement umfasst viele wichtige Funktionen, wie z. B. die Netzüberwachung, die Konfiguration der Komponenten, die Ereignisbehandlung und die Protokollierung. Eine weitere wichtige Funktion ist das Reporting, das als gemeinsame Plattform für Netz und IT-Systeme angelegt werden kann. Alternativ kann es dediziert als einheitliche Plattform oder als Bestandteil der einzelnen Management-Komponenten realisiert werden.

Die Netzmanagement-Infrastruktur besteht aus zentralen Management-Systemen (z. B. SNMP-Server), Administrations-Endgeräten mit Software für Management-Zugriffe, dezentralen Management-Agenten, dedizierten Management-Werkzeugen (z. B. Probes bzw. spezifische Messgeräte), Management-Protokollen (z. B. SNMP oder SSH) sowie Management-Schnittstellen (z. B. dedizierte Ethernet-Ports oder Konsolen-Ports).

1.2 Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil des Netzmanagements zu etablieren.

1.3 Abgrenzung

Dieser Baustein betrachtet die notwendigen Komponenten und konzeptionellen Aufgaben zum Netzmanagement. Das Pendant im Systemmanagement für vernetzte Clients und Server wird im Baustein SYS.5 *Systemmanagement* beschrieben.

Der vorliegende Baustein konkretisiert die grundsätzlichen Vorgaben des Bausteins NET.1.1 *Netz-Architektur und -Design*. Er behandelt außerdem, wie das Netzmanagement aufgebaut und abgesichert sowie die zugehörige Kommunikation geschützt werden kann. Details bezüglich der Absicherung von Netzkomponenten, insbesondere deren Management-Schnittstellen, werden jedoch in den Bausteingruppen NET.2 und NET.3 behandelt.

Das Management der passiven Netzinfrastruktur wird in den Bausteinen der Infrastruktur (Bausteinschicht INF) bzw. der industriellen IT (Bausteinschicht IND) behandelt. Daher werden diese Themen im Rahmen dieses Bausteins nicht ausgeführt.

Die in diesem Baustein thematisierte Protokollierung sollte in ein übergreifendes Protokollierungs- und Archivierungskonzept eingebunden sein. (siehe OPS.1.1.5 *Protokollierung*).

Auf das Thema Outsourcing geht der vorliegende Baustein nicht im Detail ein. Weitergehende Anforderungen dazu beschreibt der Baustein OPS.2.1 *Outsourcing*.

Allgemeine Gesichtspunkte zum sicheren, effizienten und geordneten Betrieb des Netzmanagements werden in diesem Baustein nur beschrieben, wenn es über die allgemeinen Anforderungen des Bausteins OPS.1.1.1 *Allgemeiner IT-Betrieb* hinaus geht.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Netzmanagement von besonderer Bedeutung:

2.1 Unberechtigter Zugriff auf zentrale Netzmanagement-Komponenten

Gelingt es Angreifern, auf Netzmanagement-Lösungen zuzugreifen, z. B. durch ungepatchte Sicherheitslücken oder eine ungenügende Netztrennung, können sie alle dort angeschlossenen Netzkomponenten kontrollieren und neu konfigurieren. So können sie z. B. auf schützenswerte Informationen zugreifen, Netzverkehr umleiten oder auch das gesamte Netz nachhaltig stören.

2.2 Unberechtigter Zugriff auf einzelne Netzkomponenten

Wenn es Angreifern gelingt, auf einzelne Netzkomponenten zuzugreifen, können sie die jeweilige Komponente kontrollieren und manipulieren. Jeder über die Netzkomponente geleitete Datenverkehr kann somit kompromittiert werden. Darüber hinaus können weiterführende Angriffe vorbereitet werden, um tiefer in das Netz der Institution einzudringen.

2.3 Unberechtigte Eingriffe in die Netzmanagement-Kommunikation

Wird die Management-Kommunikation abgehört und manipuliert, können auf diesem Weg aktive Netzkomponenten fehlkonfiguriert bzw. kontrolliert werden. Hierdurch kann die Netzintegrität verletzt und die Verfügbarkeit der Netzinfrastruktur eingeschränkt werden. Außerdem können die übertragenen Daten mitgeschnitten und eingesehen.

2.4 Unzureichende Zeitsynchronisation der Netzmanagement-Komponenten

Wird die Systemzeit der Netzmanagement-Komponenten unzureichend synchronisiert, können die Protokollierungsdaten eventuell nicht miteinander korreliert werden bzw. kann die Korrelation zu eventuell fehlerhaften Aussagen führen, da die unterschiedlichen Zeitstempel von Ereignissen keine gemeinsame Basis aufweisen. Damit kann nicht geeignet auf eingetretene Ereignisse regiert werden und Probleme können nicht beseitigt werden. Dadurch können beispielsweise Sicherheitsvorfälle und Datenabflüsse unerkannt bleiben.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen an das Netzmanagement aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Darüber hinaus ist der Informationssicherheitsbeauftragte (ISB) bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist er dafür verantwortlich, dass alle Anforderungen gemäß den festgelegten Sicherheitsrichtlinien erfüllt und regelmäßig überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese Rollen sind in eckigen Klammern in der Überschrift der jeweiligen Anforderung aufgeführt.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Informationssicherheitsbeauftragter (ISB), Leiter IT, Leiter Netze, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

NET.1.2.A1 Planung des Netzmanagements

Die Netzmanagement-Infrastruktur MUSS geeignet geplant werden. Hierbei SOLLTEN alle in der Sicherheitsrichtlinie und Anforderungsspezifikation adressierten Punkte sowie das Rollen- und Berechtigungskonzept berücksichtigt werden. Mindestens MÜSSEN folgende Themen berücksichtigt werden:

- zu trennende Management-Bereiche,
- Zugriffsmöglichkeiten auf die Management-Server,
- Kommunikation für den Management-Zugriff,
- benutzte Protokolle, z. B. IPv4 und IPv6,

- Anforderungen an Management-Werkzeuge,
- Schnittstellen, um erfasste Ereignis- oder Alarmmeldungen weiterzuleiten,
- Protokollierung, inklusive erforderlicher Schnittstellen zu einer zentralen Protokollierungslösung,
- Reporting und Schnittstellen zu übergreifenden Lösungen,
- korrespondierende Anforderungen an die einzubindenden Netzkomponenten.

NET.1.2.A2 Anforderungsspezifikation für das Netzmanagement [Leiter IT]

Ausgehend von NET.1.2A1 *Planung des Netzmanagements* MÜSSEN Anforderungen an die Netzmanagement-Infrastruktur und -Prozesse spezifiziert werden. Dabei MÜSSEN alle wesentlichen Elemente für das Netzmanagement berücksichtigt werden. Auch SOLLTE die Richtlinie für das Netzmanagement beachtet werden.

NET.1.2.A3 Rollen- und Berechtigungskonzept für das Netzmanagement

Es MUSS ein Rollen- und Berechtigungskonzept für das Netzmanagement erstellt, umgesetzt und gepflegt werden. Das Konzept MUSS die speziellen Tätigkeiten und den zugehörigen Zugriff auf Informationen im Netzmanagement abbilden.

NET.1.2.A4 Grundlegende Authentisierung für den Netzmanagement-Zugriff [Leiter IT, Informationssicherheitsbeauftragter (ISB)]

Für den Management-Zugriff auf Netzkomponenten und auf Managementinformationen MUSS eine geeignete Authentisierung verwendet werden. Dafür MÜSSEN die Vorgaben der Institution für die Authentisierungsgüte und den Umgang mit den Authentisierungsinformationen umgesetzt werden. Auch MÜSSEN alle Default-Passwörter auf den Netzkomponenten geändert werden. Die neuen Passwörter MÜSSEN ausreichend stark sein und regelmäßig geändert werden.

NET.1.2.A5 Einspielen von Updates und Patches

Die verantwortlichen Mitarbeiter MÜSSEN sich regelmäßig über bekannt gewordene Schwachstellen der eingesetzten Netzmanagement-Lösungen informieren und sicherheitsrelevante Updates und Patches so schnell wie möglich einspielen. Nicht sicherheitsrelevante Updates DÜRFEN NICHT die Sicherheit und Stabilität der Netzmanagement-Lösung beeinträchtigen.

NET.1.2.A6 Regelmäßige Datensicherung

Alle eingesetzten Netzmanagement-Lösungen MÜSSEN ins Datensicherungskonzept der Institution eingebunden werden (siehe CON.3 *Datensicherungskonzept*). Hierbei MÜSSEN alle spezifischen Daten für das Netzmanagement berücksichtigt werden. Es MÜSSEN mindestens die Systemdaten für die Einbindung der zu verwaltenden Komponenten bzw. Objekte, Ereignismeldungen, Statistikdaten sowie vorgehaltene Daten für das Konfigurationsmanagement gesichert werden.

NET.1.2.A7 Grundlegende Protokollierung von Ereignissen

Die Netzmanagement-Lösung MUSS in das Protokollierungskonzept der Institution eingebunden werden (siehe OPS.1.1.5 *Protokollierung*). Darüber hinaus MÜSSEN mindestens folgende Ereignisse protokolliert werden: unautorisierte Zugriffe bzw. Zugriffsversuche, Leistungs- oder Verfügbarkeitsschwankungen des Netzes, Fehler in automatischen Prozessen (z. B. bei der Konfigurationsverteilung) sowie eingeschränkte Erreichbarkeit von Netzkomponenten.

NET.1.2.A8 Zeit-Synchronisation

Alle Komponenten des Netzmanagements, inklusive der eingebundenen Netzkomponenten, MÜSSEN eine synchrone Uhrzeit nutzen. Die Uhrzeit MUSS an jedem Standort innerhalb des lokalen Netzes mittels NTP-Service synchronisiert werden. Ist ein separates Management-Netz eingerichtet, MUSS eine NTP-Instanz in diesem Management-Netz positioniert werden.

NET.1.2.A9 Absicherung der Netzmanagement-Kommunikation

Erfolgt die Netzmanagement-Kommunikation über die produktive Infrastruktur, MÜSSEN hierfür nach dem Stand der Technik sichere Protokolle verwendet werden. Ist dies nicht möglich MUSS ein eigens dafür vorgesehenes Administrationsnetz (Out-of-Band-Management) verwendet werden (siehe NET.1.1 *Netzarchitektur und -design*)

NET.1.2.A10 Beschränkung der SNMP-Kommunikation

Im Netzmanagement DÜRFEN keine unsicheren Versionen des Simple Network Management Protocol (SNMP) eingesetzt werden. Ist dies jedoch nicht möglich, MUSS die SNMP-Kommunikation entweder über ein separates Management-Netz erfolgen oder es MUSS SNMPv3 mit Authentisierung und Verschlüsselung benutzt werden. Grundsätzlich SOLLTE über SNMP nur mit den minimal erforderlichen Zugriffsrechten zugegriffen werden. Die Zugangsberechtigung SOLLTEN auf dedizierte Management-Server eingeschränkt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Netzmanagement. Sie SOLLTEN grundsätzlich umgesetzt werden.

NET.1.2.A11 Festlegung einer Sicherheitsrichtlinie für das Netzmanagement [Informationssicherheitsbeauftragter (ISB)]

Für das Netzmanagement SOLLTE eine Sicherheitsrichtlinie erstellt und nachhaltig gepflegt werden. Die Richtlinie SOLLTE allen Personen, die am Netzmanagement beteiligt sind, bekannt und grundlegend für deren Arbeit sein. Es SOLLTE regelmäßig und nachvollziehbar überprüft werden, dass die in der Richtlinie geforderten Inhalte umgesetzt werden. Die Ergebnisse MÜSSEN sinnvoll dokumentiert werden.

Die Sicherheitsrichtlinie SOLLTE festlegen, welche Bereiche des Netzmanagements über zentrale Management-Werkzeuge und -Dienste realisiert werden. Auch SOLLTE sie definieren, inwieweit Aufgaben im Netzmanagement der Institution automatisiert realisiert werden sollen.

Darüber hinaus SOLLTEN Rahmenbedingungen und Vorgaben für die Netztrennung, Zugriffskontrolle, Protokollierung sowie den Schutz der Kommunikation, das eingesetzte Netzmanagement-Werkzeug und die operativen Grundregeln für das Netzmanagement spezifiziert werden.

NET.1.2.A12 Ist-Aufnahme und Dokumentation des Netzmanagements

Es SOLTE eine Dokumentation erstellt werden, die beschreibt, wie die Management-Infrastruktur des Netzes aufgebaut ist. Darin SOLLTEN die initiale Ist-Aufnahme sowie alle durchgeführten Änderungen im Netzmanagement enthalten sein. Insbesondere SOLLTE dokumentiert werden, welche Netzkomponenten mit welchen Management-Werkzeugen verwaltet werden. Außerdem SOLLTEN alle für das Netzmanagement benutzten IT-Arbeitsplätze und -Endgeräte sowie alle Informationsbestände, Manage-

ment-Daten und Informationen über den Betrieb des Netzmanagements erfasst werden. Letztlich SOLLTEN sämtliche Schnittstellen zu Anwendungen und Diensten außerhalb des Netzmanagements dokumentiert werden.

Der so dokumentierte Ist-Zustand der Management-Infrastruktur SOLLTE mit der Dokumentation der Netz-Infrastruktur abgeglichen werden (siehe Baustein NET.1.1 *Netz-Architektur- und Design).*

Die Dokumentation SOLLTE vollständig und immer aktuell sein.

NET.1.2.A13 Erstellung eines Netzmanagement-Konzepts [Leiter IT]

Ausgehend von der Sicherheitsrichtlinie (siehe NET.1.2.A11 *Festlegung einer Sicherheitsrichtlinie für das Netzmanagement*) SOLLTE ein Netzmanagement-Konzept erstellt und nachhaltig gepflegt werden. Dabei SOLLTEN mindestens folgende Aspekte bedarfsgerecht berücksichtigt werden:

- Methoden, Techniken und Werkzeuge für das Netzmanagement,
- Absicherung des Zugangs und der Kommunikation,
- Netztrennung, insbesondere Zuordnung von Netzmanagement-Komponenten zu Sicherheitszonen,
- Umfang des Monitorings und der Alarmierung je Netzkomponente,
- Protokollierung,
- Automatisierung, insbesondere zentrale Verteilung von Konfigurationsdateien auf Switches,
- Meldeketten bei Störungen und Sicherheitsvorfällen,
- Bereitstellung von Netzmanagement-Informationen für andere Betriebsbereiche und
- Einbindung des Netzmanagements in die Notfallplanung.

NET.1.2.A14 Fein- und Umsetzungsplanung

Es SOLLTE eine Fein- und Umsetzungsplanung für die Netzmanagement-Infrastruktur erstellt werden. Hierbei SOLLTEN alle in der Sicherheitsrichtlinie und im Netzmanagement-Konzept adressierten Punkte berücksichtigt werden.

NET.1.2.A15 Konzept für den sicheren Betrieb der Netzmanagement-Infrastruktur

Ausgehend von den Sicherheitsrichtlinien und dem Netzmanagement-Konzept SOLLTE ein Konzept für den sicheren Betrieb der Netzmanagement-Infrastruktur erstellt werden. Darin SOLLTE der Anwendungs- und Systembetrieb für die Netzmanagement-Werkzeuge berücksichtigt werden. Auch SOLLTE geprüft werden, wie sich die Leistungen anderer operativer Einheiten einbinden und steuern lassen.

NET.1.2.A16 Einrichtung und Konfiguration von Netzmanagement-Lösungen

Lösungen für das Netzmanagement SOLLTEN anhand der Sicherheitsrichtlinie (siehe NET.1.2.A11 *Festlegung einer Sicherheitsrichtlinie für das Netzmanagement*), der spezifizierten Anforderungen (siehe NET1.2.A2 *Anforderungsspezifikation für das Netzmanagement*) und der Fein- und Umsetzungsplanung aufgebaut, sicher konfiguriert und in Betrieb genommen werden. Danach SOLLTEN die spezifischen Prozesse für das Netzmanagement eingerichtet werden.

NET.1.2.A17 Regelmäßiger Soll-Ist-Vergleich

Es SOLLTE regelmäßig und nachvollziehbar geprüft werden, inwieweit die Netzmanagement-Lösung dem Sollzustand entspricht. Dabei SOLLTE geprüft werden, ob die bestehende Lösung noch die Sicherheitsrichtlinie und Anforderungsspezifikation erfüllt. Auch SOLLTE geprüft werden, inwieweit die umgesetzte Management-Struktur und die genutzten Prozesse dem aktuellen Stand entsprechen. Weiter SOLLTE verglichen werden, ob die Management-Infrastruktur auf dem aktuellen Stand der Technik ist.

NET.1.2.A18 Schulungen für Management-Lösungen [Leiter IT, Vorgesetzte]

Für die eingesetzten Netzmanagement-Lösungen SOLLTEN Schulungs- und Trainingsmaßnahmen konzipiert und durchgeführt werden. Die Maßnahmen SOLLTEN die individuellen Gegebenheiten im Configuration-, Availability- und Capacity-Management sowie typische Situationen im Fehlermanagement

abdecken. Die Schulungen und Trainings SOLLTEN regelmäßig wiederholt werden, mindestens jedoch, wenn sich größere technische oder organisatorische Änderungen innerhalb der Netzmanagement-Lösung ergeben.

NET.1.2.A19 Starke Authentisierung des Management-Zugriffs

Für den administrativen Zugriff auf Netzkomponenten SOLLTE eine dem Stand der Technik entsprechende Authentisierungsmethode verwendet werden. Die administrativen Zugänge SOLLTEN über einen zentralen Authentisierungsserver mittels personalisierter Konten über entsprechend sichere Protokolle authentisiert werden.

NET.1.2.A20 Absicherung des Zugangs zu Netzmanagement-Lösungen

Der Zugriff auf zentrale Netzmanagement-Lösungen und Management-Informationen SOLLTE durch eine dem Stand der Technik entsprechende Authentisierungsmethode geschützt werden. Die Zugänge SOLLTEN über einen zentralen Authentisierungsserver mittels personalisierter Konten authentisiert werden.

Es MÜSSEN dem Stand der Technik entsprechende Authentisierungs- und Verschlüsselungsmethoden realisiert werden, falls auf Netzmanagement-Werkzeuge von einem Netz außerhalb der Management-Netze, insbesondere aus einem produktiven Netz oder einem unzureichend sicheren Netz, zugegriffen wird.

NET.1.2.A21 Entkopplung der Netzmanagement-Kommunikation

Direkte Management-Zugriffe eines Administrators von einem IT-System außerhalb der Management-Netze auf eine Netzkomponente SOLLTEN vermieden werden. Ist ein solcher Zugriff ohne zentrales Management-Werkzeug notwendig, SOLLTE die Kommunikation entkoppelt werden. Solche Sprungserver SOLLTEN im Management-Netz integriert und in einem getrennten Zugangssegment positioniert sein.

NET.1.2.A22 Beschränkung der Management-Funktionen

Es SOLLTEN nur die benötigten Management-Funktionen aktiviert werden.

NET.1.2.A23 Protokollierung der administrativen Zugriffe

Im Rahmen des Netzmanagements SOLLTEN die Sitzungsdaten aller administrativen Zugriffe protokolliert und gespeichert werden. Hierbei SOLLTEN die datenschutzrechtlichen Bestimmungen eingehalten werden.

Die Protokollierungsdaten SOLLTEN in der Datensicherung ausreichend und gesetzeskonform geschützt werden. Darüber hinaus SOLLTE festgelegt werden, ob und in welchem Umfang Sitzungsdaten für forensische Analysen zu archivieren sind. Wenn Daten archiviert werden, SOLLTE darauf geachtet werden, dass dies gesetzeskonform und revisionssicher durchgeführt wird.

NET.1.2.A24 Zentrale Konfigurationsverwaltung für Netzkomponenten

Software bzw. Firmware und Konfigurationsdaten für Netzkomponenten SOLLTEN automatisch über das Netz verteilt und ohne Betriebsunterbrechung installiert und aktiviert werden können. Die hierfür benötigten Informationen SOLLTEN an zentraler Stelle sicher verfügbar sein sowie in die Versionsverwaltung und die Datensicherung eingebunden werden. Die zentrale Konfigurationsverwaltung SOLLTE nachhaltig gepflegt und regelmäßig auditiert werden.

NET.1.2.A25 Statusüberwachung der Netzkomponenten

Die grundlegenden Performance- und Verfügbarkeits-Parameter der zentralen Netzkomponenten SOLLTEN kontinuierlich überwacht werden. Hierfür SOLLTEN vorab die jeweiligen Schwellwerte ermittelt werden (Baselining).

NET.1.2.A26 Umfassende Protokollierung, Alarmierung und Logging von Ereignissen

Wichtige Ereignisse oder Fehlerzustände SOLLTEN automatisch an ein zentrales Management-System übermittelt und dort protokolliert werden. Dies gilt sowohl für Ereignisse auf Netzkomponenten als auch für Ereignisse auf den Netzmanagement-Werkzeugen. Das zuständige IT-Personal SOLLTE zusätzlich automatisch benachrichtigt werden. Das Alarming und Logging SOLLTE mindestens folgende Punkte beinhalten:

- Ausfall bzw. Nichterreichbarkeit von Netz- oder Managementkomponenten
- Hardware-Fehlfunktionen
- fehlerhafte Anmeldeversuche
- kritische Zustände oder Überlastung von IT-Systemen

Ereignis-Meldungen bzw. Logging-Daten SOLLTEN kontinuierlich oder kumuliert einem zentralen Management-System übermittelt werden. Alarm-Meldungen SOLLTEN direkt bei Auftreten übermittelt werden.

NET.1.2.A27 Einbindung des Netzmanagements in die Notfallplanung

Die Netzmanagement-Lösungen SOLLTEN in die Notfallplanung der Institution eingebunden werden. Dazu SOLLTEN die Netzmanagement-Werkzeuge und die Konfigurationen der Netzkomponenten gesichert und in die Wiederanlaufpläne integriert sein.

NET.1.2.A28 Platzierung der Management-Clients für das In-Band-Management

Für die Administration sowohl der internen als auch externen IT-Systeme SOLLTEN dedizierte Management-Clients eingesetzt werden. Dafür SOLLTE mindestens ein Management-Client am äußeren Netzbereich (für die Administration am Internet anliegender IT-Systeme) und ein weiterer im internen Bereich (für die Administration interner IT-Systeme) platziert werden.

NET.1.2.A29 Einsatz von VLANs in der Management-Zone

Werden Management Netze durch VLANs getrennt, SOLLTE darauf geachtet werden, dass der äußere Paketfilter sowie die daran angeschlossenen Geräte in einem eigenen Teilnetz stehen. Zudem SOLLTE sichergestellt werden, dass das ALG dabei nicht umgangen wird.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

NET.1.2.A30 Hochverfügbare Realisierung der Management-Lösung (A)

Zentrale Management-Lösungen SOLLTEN hochverfügbar betrieben werden. Hierzu SOLLTEN die Server bzw. Werkzeuge inklusive der Netzanbindungen redundant ausgelegt sein. Auch die einzelnen Komponenten SOLLTEN hochverfügbar bereitgestellt werden.

NET.1.2.A31 Grundsätzliche Nutzung von sicheren Protokollen (CIA)

Für das Netzmanagement SOLLTEN ausschließlich sichere Protokolle benutzt werden. Es SOLLTEN alle Sicherheitsfunktionen dieser Protokolle verwendet werden.

NET.1.2.A32 Physische Trennung des Management-Netzes (CIA)

Das Management-Netz SOLLTE physisch getrennt werden.

NET.1.2.A33 Physische Trennung von Management-Segmenten [Leiter Netze] (CIA)

Das Management-Netz SOLLTE in physisch getrennte Sicherheitszonen unterteilt werden. Dabei SOLLTEN physisch getrennte Sicherheitszonen mindestens für das Management von LAN-Komponenten, Sicherheitskomponenten und Komponenten zur Außenanbindung eingerichtet werden.

NET.1.2.A34 Protokollierung von Inhalten administrativer Sitzungen (CI)

Ergänzend zur Protokollierung von Sitzungsdaten (siehe NET.1.2.A22 *Protokollierung der administrativen Zugriffe*) SOLLTEN auch die Inhalte von administrativen Zugriffen protokolliert werden. Alternativ nach dem Vier-Augen-Prinzip vorgegangen werden. Auch die protokollierten Inhalte der administrativen Sitzungen SOLLTEN in der Datensicherung ausreichend und gesetzeskonform geschützt werden.

NET.1.2.A35 Festlegungen zur Beweissicherung (CIA)

Es SOLLTEN Vorgehensweisen zur Beweissicherung und zu forensischen Untersuchungen im Rahmen des Netzmanagements festgelegt und dokumentiert werden. Die erhobenen Protokollierungsdaten SOLLTEN für forensische Analysen gesetzeskonform und revisionssicher archiviert werden.

NET.1.2.A36 Einbindung der Protokollierung des Netzmanagements in eine SIEM-Lösung (CIA)

Die Protokollierung des Netzmanagements SOLLTE in eine Security-Information-and-Event-Management-(SIEM)-Lösung eingebunden werden. Hierzu SOLLTEN die Anforderungskataloge (siehe NET.1.2.A2) zur Auswahl von Netzmanagement-Lösungen hinsichtlich der erforderlichen Unterstützung von Schnittstellen und Übergabeformaten angepasst werden.

NET.1.2.A37 Standort-übergreifende Zeitsynchronisation (CI)

Die Zeitsynchronisation SOLLTE über alle Standorte der Institution sichergestellt werden. Hierfür SOLLTE eine gemeinsame Referenzzeit benutzt werden, z. B. über einen übergeordneten NTP-Server.

NET.1.2.A38 Festlegung von Notbetriebsformen für die Netzmanagement-Infrastruktur (A)

Für eine schnelle Wiederherstellung der Sollzustände von Software bzw. Firmware sowie der Konfiguration der Komponenten in der Netzmanagement-Infrastruktur SOLLTEN hinreichend gute Ersatzlösungen festgelegt werden, mit denen die administrativen Tätigkeiten im Notfall durchgeführt werden können.

4 Weiterführende Informationen

4.1 Literatur

- [ISI] BSI-Standards zur Internet Sicherheit (Isi-Reihe)
  BSI, (zuletzt abgerufen am 28.09.2017)
  https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Reihe_node.html

- [TR21022] BSI Technische Richtlinie, Kryptografische Verfahren
  Verwendung von Transport Layer Security (TLS), Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017
  https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Netzmanagement" von Bedeutung.

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.14 Ausspähen von Informationen (Spionage)

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.43 Einspielen von Nachrichten

Elementare Gefährdungen / Anforderungen	G 0.09	G 0.11	G 0.14	G 0.18	G 0.19	G 0.22	G 0.23	G 0.25	G 0.27	G 0.29	G 0.30	G 0.39	G 0.40	G 0.43
NET.1.2.A1			x	x	x	x	x	x		x	x		x	x
NET.1.2.A2	x	x	x	x	x	x	x	x	x	x	x	x	x	x
NET.1.2.A3			x		x	x				x	x			x
NET.1.2.A4			x		x	x				x	x			x
NET.1.2.A5			x	x	x	x	x				x	x	x	x
NET.1.2.A6			x		x	x	x		x				x	x
NET.1.2.A7		x			x	x				x	x	x	x	
NET.1.2.A8	x		x			x	x	x						
NET.1.2.A9	x		x		x	x	x	x	x	x	x	x	x	x
NET.1.2.A10			x			x	x				x	x	x	x
NET.1.2.A11			x	x	x	x	x	x		x	x		x	x
NET.1.2.A12	x			x					x	x				
NET.1.2.A13	x	x	x	x	x	x	x	x		x	x		x	
NET.1.2.A14	x	x	x	x	x	x	x	x	x	x	x	x	x	x
NET.1.2.A15	x							x	x					
NET.1.2.A16	x	x		x			x	x	x	x	x			
NET.1.2.A17				x			x		x	x				
NET.1.2.A18	x			x	x		x			x				
NET.1.2.A19			x		x	x	x			x	x	x	x	x
NET.1.2.A20			x		x	x	x				x	x	x	x
NET.1.2.A21			x		x	x	x				x	x	x	x
NET.1.2.A22			x		x	x	x				x			
NET.1.2.A23	x	x		x	x	x	x			x	x	x		
NET.1.2.A24	x			x				x						
NET.1.2.A25	x	x		x			x	x	x				x	
NET.1.2.A26	x	x					x	x	x		x	x	x	x
NET.1.2.A27	x	x						x						
NET.1.2.A28	x			x			x				x			
NET.1.2.A29			x		x		x				x			
NET.1.2.A30	x	x		x				x	x				x	
NET.1.2.A31			x		x	x	x			x	x	x	x	x
NET.1.2.A32	x		x		x	x	x	x	x	x	x	x	x	x
NET.1.2.A33	x		x		x	x	x			x	x	x	x	x
NET.1.2.A34						x	x			x	x			x
NET.1.2.A35				x	x	x	x			x	x	x	x	x
NET.1.2.A36	x		x	x	x	x	x	x		x	x	x	x	x
NET.1.2.A37	x	x	x			x	x	x						
NET.1.2.A38	x	x		x				x					x	

NET.2: Funknetze

NET.2.1 WLAN-Betrieb

1 Beschreibung

1.1 Einleitung

Über Wireless LANs (WLANs) können drahtlose lokale Netze aufgebaut oder bestehende drahtgebundene Netze erweitert werden. Bis heute basieren fast alle am Markt verfügbaren WLAN-Komponenten auf dem Standard IEEE 802.11 und seinen Ergänzungen. Eine besondere Rolle nimmt dabei das Hersteller-Konsortium Wi-Fi Alliance ein, das basierend auf dem Standard IEEE 802.11 mit "Wi-Fi" einen Industriestandard geschaffen hat. Dabei bestätigt die Wi-Fi Alliance mit dem Wi-Fi-Gütesiegel, dass ein Gerät gewisse Interoperabilitäts- und Konformitätstests bestanden hat.

Aufgrund der meist einfachen Installation werden WLANs auch dazu eingesetzt, um temporär Netze einzurichten, beispielsweise auf Messen oder kleineren Veranstaltungen. Darüber hinaus können an öffentlichen Plätzen, wie Flughäfen oder Bahnhöfen, Netzzugänge über so genannte Hotspots angeboten werden. Dadurch werden den mobilen Benutzern Verbindungen in das Internet oder ihr Firmennetz ermöglicht. Die Kommunikation findet dann generell zwischen einem zentralen Zugangspunkt, dem Access Point, und der WLAN-Komponente des Endgeräts (z. B. über einen WLAN-USB-Stick oder eine integrierte WLAN-Funktion) statt.

1.2 Zielsetzung

In diesem Baustein soll systematisch aufgezeigt werden, wie WLANs sicher in einer Institution aufgebaut und betrieben werden können.

1.3 Abgrenzung

Der Baustein enthält grundsätzliche Anforderungen, die beachtet und erfüllt werden müssen, wenn WLANs aufgebaut und betrieben werden. Anforderungen für eine sichere Nutzung von WLANs sind nicht Gegenstand des vorliegenden Bausteins. Die sichere Nutzung von WLANs wird im Baustein NET.2.2 *WLAN-Nutzung* behandelt. Ebenso wird hier nicht auf den Betrieb von Hotspots (siehe NET.2.3 *Betrieb von Hotspots*) eingegangen.

WLANs können entsprechend den Bedürfnissen eines Betreibers und der Hardware-Ausstattung, die zur Verfügung steht, in zwei verschiedenen Modi betrieben werden. Im Ad-hoc-Modus kommunizieren zwei oder mehr mobile Endgeräte, die mit einer WLAN-Netzkarte ausgestattet sind, direkt miteinander. Da WLANs im Ad-hoc-Modus sich selbstständig, also ohne feste Infrastruktur, aufbauen und konfigurieren können und somit eine vollvermaschte parallele Netz-Infrastruktur etablieren können, ist der Ad-hoc-Modus in einer zu schützenden Umgebung ungeeignet. Dieser wird im Folgenden nicht weiter betrachtet. In den meisten Fällen werden WLANs im Infrastruktur-Modus betrieben, d. h. die Kommunikation der Clients und die Verbindung in kabelgebundene LAN-Segmente erfolgt über den Access Point.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich WLAN-Betrieb von besonderer Bedeutung:

2.1 Ausfall oder Störung eines Funknetzes

In Funknetzen werden Informationen mittels elektromagnetischer Funkwellen übertragen. Strahlen andere elektromagnetische Quellen im selben Frequenzspektrum Energie ab, können diese die drahtlose Kommunikation stören und im Extremfall den Betrieb des WLANs verhindern. Dies kann durch andere Funksysteme und Geräte, wie beispielsweise Bluetooth, Mikrowellenherde oder andere WLAN-Netze hervorgerufen werden. Darüber hinaus sind auch Denial-of-Service-Angriffe möglich. Werden beispielsweise bestimmte Steuer- und Managementsignale wiederholt gesendet, kann dies dazu führen, dass das Funknetz nicht mehr verfügbar ist.

2.2 Fehlende oder unzureichende Planung des WLAN-Einsatzes

Planungsfehler stellen sich oft als besonders schwerwiegend heraus, da leicht flächendeckende Sicherheitslücken geschaffen werden können. Wird der Einsatz von WLANs nicht oder nur unzureichend geplant, kann sich eine Vielzahl von Problemen ergeben, wie beispielsweise die Folgenden:

- Vertrauliche Daten könnten mitgelesen werden, beispielsweise wenn WLAN-Standards eingesetzt werden, die nicht mehr dem Stand der Technik entsprechen (z. B. WEP zur Verschlüsselung).
- Die Übertragungskapazität kann unzureichend sein. Dadurch können bandbreitenintensive Anwendungen nicht mit der erforderlichen Dienstgüte genutzt werden.

2.3 Fehlende oder unzureichende Regelungen zum WLAN-Einsatz

Bei einer WLAN-Infrastruktur, die nicht zentral administriert wird, sind die Access Points in der Standard-Einstellung meist ohne oder nur mit unzureichenden Sicherheitsmechanismen vorkonfiguriert. Schließt ein Mitarbeiter beispielsweise aufgrund fehlender Regelungen einen ungenehmigten bzw. ungesicherten Access Point an ein internes Netz der Institution an, untergräbt er praktisch sämtliche im LAN ergriffenen Sicherheitsmaßnahmen, wie z. B. das Sicherheitsgateway (Firewall) zum Schutz gegen unberechtigte externe Zugriffe.

2.4 Ungeeignete Auswahl von Authentisierungsverfahren

Wenn Authentikationsverfahren und -mechanismen fehlen oder zu unzureichend sind, können Sicherheitslücken entstehen. Beispielsweise wird im Standard IEEE 802.1X (Port Based Network Access Control) das EAP (Extensible Authentication Protocol) definiert. In einigen der beschriebenen EAP-Methoden sind Schwachstellen enthalten, z. B. ist EAP-MD5 anfällig gegenüber Man-in-the-Middle- bzw. Wörterbuchangriffen. Wird EAP-MD5 eingesetzt, können Passwörter erraten und die Kommunikation kann abgehört werden.

2.5 Fehlerhafte Konfiguration der WLAN-Infrastruktur

Access Points und andere WLAN-Komponenten (z. B. WLAN Controller) bieten eine Vielzahl von Konfigurationseinstellungen, die insbesondere auch Sicherheitsfunktionen betreffen. Werden hier falsche Einstellungen vorgenommen, ist entweder keine Kommunikation über einen Access Point möglich oder die Kommunikation erfolgt ungeschützt bzw. mit einem zu geringen Schutzniveau.

2.6 Unzureichende oder fehlende WLAN-Sicherheitsmechanismen

Im Auslieferungszustand sind WLAN-Komponenten häufig so konfiguriert, dass keine oder nur wenige Sicherheitsmechanismen aktiviert sind. Einige der Mechanismen sind darüber hinaus unzureichend und bieten keinen ausreichenden Schutz. Auch heute noch werden diverse WLAN-Komponenten eingesetzt, die lediglich unzureichende Sicherheitsmechanismen wie z. B. WEP unterstützen. Teilweise können die-

se Geräte nicht einmal auf stärkere Sicherheitsmechanismen aufgerüstet werden. Werden solche Geräte eingesetzt, kann ein Angreifer leicht die gesamte Kommunikation abhören und damit in den Besitz vertraulicher Informationen kommen.

2.7 Abhören der WLAN-Kommunikation

Da es sich bei Funk um ein Medium handelt, das sich mehrere Benutzer teilen können ("Shared Medium"), können die über WLANs übertragenen Daten problemlos mitgehört und aufgezeichnet werden. Wenn die Daten nicht oder nur unzureichend verschlüsselt werden, können übertragene Nutzdaten leicht gewonnen werden. Zudem überschreiten Funknetze bzw. die ausgesendeten Funkwellen nicht selten die Grenzen der selbstgenutzten Räumlichkeiten, so dass Daten auch noch in Bereiche ausgestrahlt werden, die nicht von den Benutzern oder einer Institution kontrolliert und gesichert werden können.

2.8 Vortäuschung eines gültigen Access Points (Rogue Access Point)

Ein Angreifer kann sich als Teil der WLAN-Infrastruktur ausgeben, indem er einen eigenen Access Point mit einer geeignet gewählter SSID in der Nähe eines Clients installiert. Dieser vorgetäuschte Access Point wird als "Rogue Access Point" bezeichnet. Bietet dieser dem WLAN-Client eine stärkere Sendeleistung als der echte Access Point, wird der Client diesen als Basisstation nutzen, falls keine beidseitige Authentisierung erzwungen wird. Zusätzlich könnte auch der echte Access Point durch einen Denial-of-Service-Angriff ausgeschaltet werden. Die Benutzer melden sich an einem Netz an, das nur vorgibt, das Zielnetz zu sein. Dadurch ist es einem Angreifer möglich, die Kommunikation abzuhören. Auch durch Poisoning- oder Spoofing-Methoden kann ein Angreifer eine falsche Identität vortäuschen bzw. den Netzverkehr zu seinen Systemen umlenken. So kann er die Kommunikation belauschen und kontrollieren. Besonders in öffentlichen Funknetzen (sog. Hotspots) ist ein Rogue Access Point ein beliebtes Angriffsmittel.

2.9 Ungeschützter LAN-Zugang am Access Point

Sind Access Points sichtbar und ohne physischen Schutz montiert, kann sich ein Angreifer zwischen die Access Points und die Switch-Infrastruktur schalten, um den gesamten Netzverkehr abzuhören. Selbst wenn die Kommunikation mit WPA2 verschlüsselt wird, stellt dies eine Gefährdung dar, da diese Methoden nur die Luftschnittstelle absichern, die Ethernet-Anbindung aber nicht weiter berücksichtigen.

2.10 Hardware-Schäden

Hardware-Schäden können dazu führen, dass der Funkverkehr gestört wird. Im schlimmsten Fall kann das WLAN sogar komplett ausfallen. Dies betrifft insbesondere WLAN-Geräte, die außerhalb von geschützten Räumen angebracht werden (z. B. um offene Plätze abzudecken). Sie sind zusätzlichen Gefährdungen ausgesetzt, wie beispielsweise vorsätzliche Beschädigungen durch Angreifer oder umweltbedingte Schäden durch Witterung oder Blitzeinschlag.

2.11 Diebstahl eines Access Points

Werden WLAN Access Points ungesichert in Durchgangswegen angebracht, z. B. direkt unter der Decke oder in Bereichen mit starkem Publikumsverkehr installiert, können sie gestohlen werden. Dadurch lässt sich beispielsweise ein Shared-Secret Key für die Authentisierung am RADIUS-Server oder der verwendete Schlüssel (beispielsweise für WPA2-Personal) auslesen. Mit diesen Informationen kann dann unberechtigt auf das WLAN zugegriffen werden.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich WLAN-Betrieb aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Haustechnik, Leiter IT, Planer

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

NET.2.1.A1 Festlegung einer Strategie für den Einsatz von WLANs [Leiter IT]

Bevor in einer Institution WLANs eingesetzt werden, MUSS festgelegt sein, welche generelle Strategie die Institution im Hinblick auf die WLAN-Nutzung einnimmt. Insbesondere MUSS geklärt und festgelegt werden, in welchen Organisationseinheiten, für welche Anwendungen und zu welchem Zweck WLANs eingesetzt und welche Informationen hierüber übertragen werden dürfen. Ebenso MUSS festgelegt werden, in welchen räumlichen Bereichen WLANs aufgebaut werden sollen.

Außerdem MUSS schon in der Planungsphase festgelegt sein, wer für die Administration der unterschiedlichen WLAN-Komponenten zuständig ist, welche Schnittstellen es zwischen den am Betrieb beteiligten Verantwortlichen gibt, und wann welche Informationen zwischen den Zuständigen ausgetauscht werden müssen.

NET.2.1.A2 Auswahl eines geeigneten WLAN-Standards [Planer]

Um eine Eigenstörung des WLANs zu vermeiden, MUSS im Rahmen der WLAN-Planung zuerst ermittelt werden, welche der von der Institution betriebenen Systeme (z. B. Mikrowellengeräte, Bluetooth) in das ISM-Band bei 2,4 GHz sowie in das 5 GHz-Band abstrahlen.

Außerdem MÜSSEN die vorhandenen Sicherheitsmechanismen der einzelnen WLAN-Standards gegeneinander abgewogen werden. Generell MUSS es sichergestellt sein, dass nur als allgemein sicher anerkannte Verfahren zur Authentisierung und Verschlüsselung eingesetzt werden. Erst nachdem die einzelnen Standards ausführlich bewertet worden sind, kann ein bestimmter WLAN-Standard festgelegt werden. Die Entscheidungsgründe MÜSSEN dokumentiert werden.

Geräte, die von anerkannt sicheren Verfahren auf unsichere zurückgreifen müssen, DÜRFEN in der Planung NICHT mehr berücksichtigt werden.

NET.2.1.A3 Auswahl geeigneter Kryptoverfahren für WLAN [Planer]

Um ein WLAN sicher zu betreiben, MUSS die Kommunikation über die Luftschnittstelle komplett kryptographisch abgesichert werden. Kryptographische Verfahren unsicherer als WPA2 DÜRFEN NICHT mehr eingesetzt werden.

Wird WPA2 mit Pre-Shared Keys (WPA2-PSK) verwendet, dann MUSS ein komplexer Schlüssel mit einer Mindestlänge von 20 Zeichen verwendet werden. Außerdem MUSS dieser regelmäßig gewechselt werden.

NET.2.1.A4 Geeignete Aufstellung von Access Points [Haustechnik]

Access Points MÜSSEN zugriffssicher montiert werden. Darüber hinaus MUSS darauf geachtet werden, dass die Ausbreitung der Funkwellen in Bereichen, die nicht durch das WLAN versorgt werden sollen, möglichst stark reduziert ist. Außeninstallationen MÜSSEN vor Witterungseinflüssen und elektrischen Entladungen wie z. B. Blitzschlag geeignet geschützt werden.

NET.2.1.A5 Sichere Basis-Konfiguration der Access Points

Access Points DÜRFEN NICHT in der Konfiguration des Auslieferungszustandes verwendet werden. Voreingestellte SSIDs (Service Set Identifiers), Zugangskennwörter oder kryptographische Schlüssel MÜSSEN direkt nach Inbetriebnahme geändert werden. Außerdem MÜSSEN unsichere Administrationszugänge (z. B. Telnet oder HTTP) abgeschaltet werden. Access Points MÜSSEN verschlüsselt administriert werden.

NET.2.1.A6 Sichere Konfiguration der WLAN-Clients

Um eine interne WLAN-Infrastruktur sicher betreiben zu können, SOLLTEN auch alle damit gekoppelten WLAN-Clients sicher konfiguriert sein. Geeignete Anforderungen für eine sichere Konfiguration von Clients sind im Baustein SYS.2.1 *Allgemeiner Client* und NET.2.2 *WLAN-Nutzung* zu finden. Zusätzlich MÜSSEN folgende WLAN-spezifischen Anforderungen erfüllt werden:

- Wird die WLAN-Schnittstelle über einen längeren Zeitraum nicht genutzt, MUSS diese deaktiviert werden.
- Es MUSS sichergestellt sein, dass mittels der WLAN-Kommunikation keine Sicherheitszonen gekoppelt werden und hierdurch etablierte Schutzmaßnahmen umgangen werden.

NET.2.1.A7 Aufbau eines Distribution Systems [Planer]

Wird ein Distribution System aufgebaut, MUSS prinzipiell entschieden werden, ob physisch oder logisch durch VLANs auf den Access Switches des kabelbasierten LANs getrennt wird.

NET.2.1.A8 Verhaltensregeln bei WLAN-Sicherheitsvorfällen

Bei einem Sicherheitsvorfall MUSS der IT-Betrieb passende Gegenmaßnahmen einleiten (siehe auch DER.2.1 *Incident Management*):

- Am Übergabepunkt der WLAN-Kommunikation ins interne LAN SOLLTE bei einem Angriff auf das WLAN die Kommunikation selektiv pro SSID, Access Point oder sogar für die komplette WLAN-Infrastruktur gesperrt werden.
- Wurden Access Points gestohlen, MÜSSEN festgelegte Sicherheitsmaßnahmen umgesetzt werden, damit der Access Point nicht missbräuchlich verwendet wird.
- Sind WLAN-Clients entwendet worden und wird eine zertifikatsbasierte Authentisierung verwendet, MÜSSEN die Client-Zertifikate gesperrt werden.

Die möglichen Konsequenzen sicherheitskritischer Ereignisse MÜSSEN untersucht werden. Letztlich MUSS ausgeschlossen werden, dass entwendete Geräte unberechtigt verwendet werden, um auf das Netz der Institution zuzugreifen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich WLAN-Betrieb. Sie SOLLTEN grundsätzlich umgesetzt werden.

NET.2.1.A9 Sichere Anbindung von WLANs an ein LAN [Planer]

Werden WLANs an ein LAN angebunden, SOLLTE der Übergang zwischen WLANs und LAN abgesichert werden, beispielsweise durch einen Paketfilter. Der Access Point SOLLTE unter Berücksichtigung der Anforderung NET.2.1.A7 *Aufbau eines Distribution Systems* eingebunden sein.

NET.2.1.A10 Erstellung einer Sicherheitsrichtlinie für den Betrieb von WLANs

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die wesentlichen Kernaspekte für einen sicheren Einsatz von WLANs konkretisiert werden. Die Richtlinie SOLLTE allen Verantwortlichen, die an Aufbau und Betrieb von WLANs beteiligt sind, bekannt sein und Grundlage für deren Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft werden. Die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

NET.2.1.A11 Geeignete Auswahl von WLAN-Komponenten

Ist beschlossen worden, eine WLAN-Infrastruktur aufzubauen, SOLLTE anhand der Ergebnisse der Planungsphase eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden können. Werden WLAN-Komponenten beschafft, SOLLTE neben Sicherheit auch auf Datenschutz und Kompatibilität der WLAN-Komponenten untereinander geachtet werden.

NET.2.1.A12 Einsatz einer geeigneten WLAN-Management-Lösung

Um aus Sicherheitssicht eine optimale Konfiguration der WLAN-Komponenten gewährleisten zu können, SOLLTE eine zentrale Managementlösung eingesetzt werden. Der Leistungsumfang der eingesetzten Lösung SOLLTE im Einklang mit den Anforderungen der WLAN-Strategie sein.

NET.2.1.A13 Regelmäßige Sicherheitschecks in WLANs

WLANs SOLLTEN regelmäßig überprüft werden, ob eventuell Sicherheitslücken existieren. Zusätzlich SOLLTE nach unbefugt installierten Access Points innerhalb der bereitgestellten WLANs gesucht werden. Weiterhin SOLLTE die Performance gemessen werden. Die Ergebnisse von Sicherheitschecks SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTE nachgegangen werden.

NET.2.1.A14 Regelmäßige Audits der WLAN-Komponenten

Bei allen Komponenten der WLAN-Infrastruktur (Access Points, Distribution System, WLAN-Management-Lösung etc.) SOLLTE regelmäßig überprüft werden, ob alle festgelegten Sicherheitsmaßnahmen umgesetzt und diese korrekt konfiguriert sind. Öffentlich aufgestellte Access Points SOLLTEN regelmäßig stichprobenartig darauf geprüft werden, ob es gewaltsame Öffnungs- oder Manipulationsversuche gab. Die Auditergebnisse SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTE nachgegangen werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

NET.2.1.A15 Verwendung eines VPN zur Absicherung von WLANs (CI)

Bei erhöhtem Schutzbedarf SOLLTE ein VPN eingesetzt werden, um die Kommunikation über die WLAN-Infrastruktur zusätzlich abzusichern. Weitere Informationen hierzu sind im Baustein NET.3.3 *VPN* zu finden.

NET.2.1.A16 Zusätzliche Absicherung bei der Anbindung von WLANs an ein LAN (CIA)

Wird eine WLAN-Infrastruktur an ein LAN angebunden, SOLLTE der Übergang zwischen WLANs und LAN entsprechend des höheren Schutzbedarfs zusätzlich abgesichert werden.

NET.2.1.A17 Absicherung der Kommunikation zwischen Access Points (C)

Die Kommunikation zwischen den Access Points über die Funkschnittstelle und das LAN SOLLTE verschlüsselt erfolgen, um die Vertraulichkeit der übermittelten Daten, zum Beispiel Roaming-Informationen oder Zugangsdaten von Benutzern, zu gewährleisten.

NET.2.1.A18 Einsatz von Wireless Intrusion Detection / Wireless Intrusion Prevention Systemen (CIA)

Um Sicherheitsvorfälle und Schwachstellen zeitnah zu entdecken und entsprechende Gegenmaßnahmen direkt einleiten zu können, SOLLTEN Wireless Intrusion Detection Systeme bzw. Wireless Intrusion Prevention Systeme eingesetzt werden.

4 Weiterführende Informationen

4.1 Literatur

- [BSIDKS] Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte
  Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009 https://www.bsi.bund.de/DE/Publikationen/Broschueren/Drahtloskom/drahtloskom.html

- [ISIWLAN] BSI-Standard zur Internet-Sicherheit (ISi-Reihe)
  Sichere Anbindung von lokalen Netzen an das Internet (Isi-LANA), Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014
  https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-LANA/lana_node.html

- [NIST800153] NIST Special Publication 800-153
  Guidelines for Securing Wireless Local Area Networks (WLANs), NIST, 02.2012 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf

- [NIST80097] NIST Special Publication 800-97
  Establishing Wireless Robust Security Networks, A Guide to IEEE 802.11, NIST, 02.2007
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf

- [TR03103] Technische Richtlinie Sicheres Wireless LAN
  Bundesamt für Sicherheit in der Informationstechnik (BSI), 2005 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03103/index_htm.html

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "WLAN-Betrieb" von Bedeutung.

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

G 0.15 Abhören

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.25 Ausfall von Geräten oder Systemen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.43 Einspielen von Nachrichten

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

Elementare Gefährdungen / Anforderungen	G 0.09	G 0.15	G 0.16	G 0.18	G 0.23	G 0.24	G 0.25	G 0.30	G 0.31	G 0.40	G 0.43	G 0.44
NET.2.1.A1				x								
NET.2.1.A2	x	x		x	x			x			x	
NET.2.1.A3		x		x	x			x			x	
NET.2.1.A4	x		x	x		x	x			x		x
NET.2.1.A5		x			x			x	x		x	
NET.2.1.A6		x			x			x	x		x	
NET.2.1.A7		x		x	x							
NET.2.1.A8		x										
NET.2.1.A9		x		x	x				x			
NET.2.1.A10		x		x								
NET.2.1.A11				x								
NET.2.1.A12			x		x		x	x	x	x	x	
NET.2.1.A13					x			x		x	x	
NET.2.1.A14					x			x		x	x	
NET.2.1.A15		x			x			x	x		x	
NET.2.1.A16		x			x			x				
NET.2.1.A17		x			x							
NET.2.1.A18					x			x		x	x	

NET.2: Funknetze

NET.2.2 WLAN-Nutzung

1 Beschreibung

1.1 Einleitung

Über Wireless LANs (WLANs) können drahtlose lokale Netze aufgebaut oder bestehende drahtgebundene Netze erweitert werden. Bis heute basieren fast alle am Markt verfügbaren WLAN-Komponenten auf dem Standard IEEE 802.11 und seinen Ergänzungen. Eine besondere Rolle nimmt dabei das Hersteller-Konsortium Wi-Fi Alliance ein, das basierend auf dem Standard IEEE 802.11 mit "Wi-Fi" einen Industriestandard geschaffen hat. Dabei bestätigt die Wi-Fi Alliance mit dem Wi-Fi-Gütesiegel, dass ein Gerät gewisse Interoperabilitäts- und Konformitätstests bestanden hat.

WLANs bieten einen Gewinn an Komfort und Mobilität, jedoch birgt die Nutzung auch zusätzliches Gefährdungspotenzial für die Sicherheit der Informationen, da drahtlos kommuniziert wird. Daher ist es unabdingbar, dass neben den IT-Verantwortlichen auch die Benutzer zu möglichen Gefahren sensibilisiert sind, die entstehen können, wenn WLANs unsachgemäß verwendet werden. Dies bedeutet, dass die Benutzer über die erforderlichen Kenntnisse verfügen müssen, um Sicherheitsmaßnahmen richtig verstehen und anwenden zu können. Insbesondere muss ihnen bekannt sein, was von ihnen im Hinblick auf Informationssicherheit erwartet wird und wie sie in bestimmten Situationen reagieren sollten, wenn sie WLANs nutzen.

1.2 Zielsetzung

In diesem Baustein soll aufgezeigt werden, wie WLANs sicher genutzt werden können.

1.3 Abgrenzung

Der Baustein enthält grundsätzliche Anforderungen, die bei der Nutzung von WLANs zu beachten und zu erfüllen sind, um den spezifischen Gefährdungen entgegenwirken zu können. Anforderungen, mit deren Hilfe WLANs sicher betrieben werden können, sind dagegen nicht Gegenstand des vorliegenden Bausteins, sondern sind im Baustein NET.2.1 *WLAN-Betrieb* beschrieben. Darüber hinaus geht der Baustein nicht auf allgemeine Aspekte eines Clients ein. Solche Aspekte werden im Baustein SYS2.1 *Allgemeiner Client* behandelt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich WLAN-Nutzung von besonderer Bedeutung:

2.1 Unzureichende Kenntnis über Regelungen

Sind den Benutzern die Regelungen für den korrekten Umgang mit WLANs nicht hinreichend bekannt, können sie sich auch nicht daran halten. Werden WLAN-Clients zum Beispiel gedankenlos an fremde Netze angeschlossen, können die hierüber übertragenen Informationen (z. B. Sitzungs-Cookies, Passwörter) abgehört werden.

2.2 Nichtbeachtung von Sicherheitsmaßnahmen

Aufgrund von Nachlässigkeit und fehlenden Kontrollen kommt es immer wieder vor, dass Personen die ihnen empfohlenen oder angeordneten Sicherheitsmaßnahmen nicht oder nicht im vollen Umfang berücksichtigen. Wird beispielsweise ein WLAN-Client im Ad-hoc-Modus genutzt, obwohl dies ausdrücklich in der Benutzerrichtlinie verboten ist, kann ein anderer Client direkt mit dem WLAN-Client kommunizieren und z. B. unberechtigt auf vertrauliche Dokumente zugreifen, die auf dem Client gespeichert sind.

2.3 Abhören der WLAN-Kommunikation

Da es sich bei Funk um ein Medium handelt, das sich mehrere Benutzer teilen können ("Shared Medium"), können die über WLANs übertragenen Daten problemlos mitgehört und aufgezeichnet werden. Wenn die Daten nicht oder nur unzureichend verschlüsselt werden, können übertragene Nutzdaten leicht gewonnen werden. Zudem überschreiten Funknetze bzw. die ausgesendeten Funkwellen nicht selten die Grenzen der selbstgenutzten Räumlichkeiten, so dass Daten auch noch in Bereiche ausgestrahlt werden, die nicht von den Benutzern oder einer Institution kontrolliert und gesichert werden können.

2.4 Auswertung von Verbindungsdaten bei der drahtlosen Kommunikation

Bei WLANs auf Basis von IEEE 802.11 wird die MAC-Adresse einer WLAN-Karte bei jeder Datenübertragung mit versendet. Da sie unverschlüsselt übertragen wird, können Bewegungsprofile über mobile Nutzer erstellt werden, z. B. wenn diese sich in öffentliche Hotspots einbuchen.

2.5 Vortäuschung eines gültigen Access Points (Rogue Access Point)

Ein Angreifer kann sich als Teil der WLAN-Infrastruktur ausgeben, indem er einen eigenen Access Point mit einer geeignet gewählter SSID in der Nähe eines Clients installiert. Dieser vorgetäuschte Access Point wird als "Rogue Access Point" bezeichnet. Bietet dieser dem WLAN-Client eine stärkere Sendeleistung als der echte Access Point, wird der Client diesen als Basisstation nutzen, falls keine beidseitige Authentisierung erzwungen wird. Zusätzlich könnte auch der echte Access Point durch einen Denial-of-Service-Angriff ausgeschaltet werden. Die Benutzer melden sich an einem Netz an, das nur vorgibt, das Zielnetz zu sein. Dadurch ist es einem Angreifer möglich, die Kommunikation abzuhören. Auch durch Poisoning- oder Spoofing-Methoden kann ein Angreifer eine falsche Identität vortäuschen bzw. den Netzverkehr zu seinen Systemen umlenken. So kann er die Kommunikation belauschen und kontrollieren. Besonders in öffentlichen Funknetzen (sog. Hotspots) ist ein Rogue Access Point ein beliebtes Angriffsmittel.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich WLAN-Nutzung aufgeführt. Grundsätzlich ist der Benutzer für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Benutzer
Weitere Verantwortliche	IT-Betrieb, Leiter IT, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

NET.2.2.A1 Erstellung einer Benutzerrichtlinie für WLAN [Leiter IT]

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MÜSSEN die wesentlichen Kernaspekte für eine sichere WLAN-Nutzung in einer WLAN-Benutzerrichtlinie konkretisiert werden. In einer solchen Benutzerrichtlinie MÜSSEN die Besonderheiten bei der WLAN-Nutzung beschrieben sein, z. B. ob und wie Hotspots genutzt werden dürfen.

Des Weiteren MUSS die Richtlinie, insbesondere im Hinblick auf die Nutzung von eingestuften Informationen, Angaben dazu enthalten, welche Daten im WLAN genutzt und übertragen werden dürfen und welche nicht.

Es MUSS beschrieben sein, wie mit Client-seitigen Sicherheitslösungen umzugehen ist. Die Benutzerrichtlinie MUSS ein klares Verbot enthalten, ungenehmigte Access Points an das LAN der Institution anzuschließen. Außerdem MUSS in der Richtlinie darauf hingewiesen werden, dass die WLAN-Schnittstelle deaktiviert werden MUSS, wenn sie über einen längeren Zeitraum nicht genutzt wird.

Es MUSS regelmäßig überprüft werden, ob die in der Richtlinie geforderten Inhalte richtig umgesetzt worden sind. Die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

NET.2.2.A2 Sensibilisierung und Schulung der WLAN-Benutzer [Vorgesetzte, Leiter IT]

Die Benutzer von WLAN-Komponenten, vornehmlich von WLAN-Clients, MÜSSEN sensibilisiert und zu den in der Benutzerrichtlinie aufgeführten Maßnahmen geschult werden. Den Benutzern MUSS genau erläutert werden, was die WLAN-spezifischen Sicherheitseinstellungen bedeuten und warum sie wichtig sind. Außerdem MÜSSEN sie auf die Gefahren hingewiesen werden, wenn diese Sicherheitseinstellungen umgangen oder deaktiviert werden.

Die Schulungsinhalte MÜSSEN immer entsprechend der jeweiligen Einsatzszenarien angepasst werden. Neben der reinen Schulung zu WLAN-Sicherheitsmechanismen MÜSSEN die Benutzer jedoch auch die WLAN-Sicherheitsrichtlinie ihrer Institution vorgestellt bekommen. Ebenso MÜSSEN sie über die Gefahren sensibilisiert werden, wenn fremde WLANs verwendet werden sollen.

NET.2.2.A3 Absicherung der WLAN-Nutzung in unsicheren Umgebungen [IT-Betrieb]

DÜRFEN externe Hotspots genutzt werden MUSS Folgendes umgesetzt werden:

- Jeder Benutzer eines Hotspots MUSS seine Sicherheitsanforderungen kennen (siehe NET.2.2.A2 Sensibilisierung und Schulung der WLAN-Benutzer) und danach entscheiden, ob bzw. unter welchen Bedingungen ihm die Nutzung des Hotspots erlaubt ist.
- WLANs, die nur sporadisch genutzt werden, SOLLTEN durch die Benutzer aus der Historie gelöscht werden.
- Wenn möglich, SOLLTEN separate Benutzerkonten mit einer sicheren Grundkonfiguration und restriktiven Berechtigungen verwendet werden.
- Es SOLLTE sichergestellt sein, dass sich kein Benutzer mit Administratorrechten von seinem Client aus an externen WLANs anmelden kann.
- Sensible Daten DÜRFEN NUR übertragen werden, wenn entsprechende Sicherheitsmaßnahmen umgesetzt und sichere Protokolle verwendet werden.
- Über öffentlich zugängliche WLANs DÜRFEN die Benutzer NUR über ein Virtual Private Network (VPN) auf interne Ressourcen der Institution zugreifen. Weitere Informationen hierzu sind im Baustein NET.3.3 VPN zu finden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich WLAN-Nutzung. Sie SOLLTEN grundsätzlich umgesetzt werden.

NET.2.2.A4 Verhaltensregeln bei WLAN-Sicherheitsvorfällen

Bei WLAN-Sicherheitsvorfällen SOLLTEN die Benutzer Folgendes umsetzen:

- Sie SOLLTEN ihre Arbeitsergebnisse sichern, den WLAN-Zugriff beenden und die WLAN-Schnittstelle ihres Clients deaktivieren.
- Fehlermeldungen und Abnormalitäten SOLLTEN durch die Benutzer genau dokumentiert werden. Ebenso SOLLTEN die Benutzer dokumentieren, was sie getan haben bevor bzw. während der Sicherheitsvorfall eingetreten ist.
- Die Benutzer SOLLTEN über eine geeignete Eskalationsstufe (z. B. User Help Desk) den IT-Betrieb benachrichtigen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

4 Weiterführende Informationen

4.1 Literatur

- [BSIDKS] Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte
  Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009 https://www.bsi.bund.de/DE/Publikationen/Broschueren/Drahtloskom/drahtloskom.html

- [ISIWLAN] BSI-Standard zur Internet-Sicherheit (ISi-Reihe)
  Sichere Anbindung von lokalen Netzen an das Internet (Isi-LANA), Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014
  https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-LANA/lana_node.html

- [NIST800153] NIST Special Publication 800-153
  Guidelines for Securing Wireless Local Area Networks (WLANs), NIST, 02.2012 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf

- [NIST80097] NIST Special Publication 800-97
  Establishing Wireless Robust Security Networks, A Guide to IEEE 802.11, NIST, 02.2007
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf

- [TR03103] Technische Richtlinie Sicheres Wireless LAN
  Bundesamt für Sicherheit in der Informationstechnik (BSI), 2005 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03103/index_htm.html

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "WLAN-Nutzung" von Bedeutung.

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.43 Einspielen von Nachrichten

Elementare Gefährdungen / Anforderungen	G 0.15	G 0.18	G 0.23	G 0.31	G 0.43
NET.2.2.A1	x	x	x	x	x
NET.2.2.A2	x	x	x	x	x
NET.2.2.A3	x		x		x
NET.2.2.A4			x		

NET.3: Netzkomponenten

NET.3.1 Router und Switches

1 Beschreibung

1.1 Einleitung

Router und Switches bilden das Rückgrat heutiger IT-Netze. Ein Ausfall eines oder mehrerer dieser Geräte kann zum kompletten Stillstand der gesamten IT-Infrastruktur führen. Sie müssen daher besonders abgesichert werden.

Router arbeiten auf der OSI Schicht 3 (Netzschicht) und vermitteln Datenpakete anhand der Ziel-IP-Adresse im IP-Header. Router sind in der Lage, Netze mit unterschiedlichen Topographien zu verbinden. Sie werden verwendet, um lokale Netze zu segmentieren oder um lokale Netze über Weitverkehrsnetze zu verbinden. Ein Router identifiziert eine geeignete Verbindung zwischen dem Quellsystem bzw. Quellnetz und dem Zielsystem bzw. Zielnetz. In den meisten Fällen geschieht das, indem er die Datenpakete an den nächsten Router weitergibt.

Switches arbeiteten ursprünglich auf der OSI-Schicht 2, mittlerweile sind sie jedoch mit unterschiedlichen Funktionen erhältlich. Hersteller kennzeichnen die Geräte meist mit dem OSI-Layer, der unterstützt wird. Dadurch entstanden die Begriffe Layer-2-, Layer-3- und Layer-4-Switch, wobei es sich bei Layer-3- und Layer-4-Switches eigentlich funktional bereits um Router handelt. Die ursprünglich unterschiedlichen Funktionen von Switches und Routern werden somit heute oft auf einem Gerät vereint.

1.2 Zielsetzung

Der Baustein beschreibt, wie Router und Switches sicher betrieben werden.

1.3 Abgrenzung

Es ist eine große Auswahl von unterschiedlichen Routern und Switches von verschiedenen Herstellern am Markt verfügbar. Der Baustein beschreibt keine spezifischen Anforderungen für bestimmte Produkte. Er ist so weit wie möglich herstellerunabhängig gehalten.

Durch die Verschmelzung der Funktionen von Routern und Switches kann der Großteil der Anforderungen sowohl für Router als auch für Switches benutzt werden. Der vorliegende Baustein unterscheidet hier weitgehend nicht zwischen den Gerätearten.

Heute bieten auch nahezu alle Betriebssysteme eine Routing-Funktionalität an. Dieser Baustein benennt keine Anforderungen für aktivierte Routing-Funktionen in Betriebssystemen.

Darüber hinaus werden Aspekte der infrastrukturellen Sicherheit (z. B. geeignete Aufstellung oder Stromversorgung oder Verkabelung) nicht in diesem Baustein aufgeführt, sondern finden sich in den jeweiligen Bausteinen der Schicht INF *Infrastruktur*.

Der vorliegende Baustein beschreibt keine Anforderungen, wie virtuelle Router und Switches abgesichert werden können. Sicherheitsaspekte von virtuellen aktiven Netzkomponenten werden im Baustein NET.1.4 *Netzvirtualisierung* behandelt. Ebenso wird nicht auf eventuell vorhandene

Firewall-Funktionen von Routern und Switches eingegangen. Dazu muss zusätzlich der Baustein NET.3.2 *Firewall* umgesetzt werden. Einige Aspekte des Netzdesigns und -managements sind auch für den Einsatz von Routern und Switches von Bedeutung und werden im Rahmen der entsprechenden Anforderungen erwähnt. Weitere Informationen für den Aufbau, das Design und das Management eines Netzes sind in den Bausteinen NET.1.1 *Netzarchitektur und -design* und NET.1.2 *Netzmanagement* zu finden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für *Router und Switches* von besonderer Bedeutung:

2.1 Distributed Denial of Service (DDoS)

Bei einem DDoS-Angriff auf ein geschütztes Netz beispielsweise per TCP-SYN-Flooding oder UDP Packet Storm kann aufgrund der vielen Netzverbindungen, die verarbeitet werden müssen, der Router ausfallen. Das kann dazu führen, dass bestimmte Dienste im Local Area Network (LAN) nicht mehr verfügbar sind oder das gesamte LAN ausfällt.

2.2 Manipulation

Gelingt es einem Angreifer, unberechtigt auf einen Router oder Switch zuzugreifen, kann er die Geräte neu konfigurieren oder auch zusätzliche Dienste starten. Die Konfiguration lässt sich beispielsweise so verändern, dass Dienste, Clients oder ganze Netzsegmente geblockt werden.

2.3 Software-Schwachstellen oder -Fehler

Hersteller von Routern und Switches veröffentlichen regelmäßig Updates und Patches, um Softwarefehler und bekannt gewordene Schwachstellen in ihren Produkten zu beheben. Werden diese jedoch nicht oder zu spät eingespielt, kann der Router oder Switch erfolgreich angegriffen werden. Dadurch ist es möglich, dass Angreifer die Systeme manipulieren, sodass geschäftskritische Daten abfließen, Dienste ausfallen oder ganze Produktionsprozesse still stehen.

2.4 Fehlerhafte Konfiguration eines Routers oder Switches

Router und Switches werden mit einer Standardkonfiguration ausgeliefert, in der viele Dienste aktiviert sind. Auch verraten Login-Banner beispielsweise die Modell- und Versionsnummer des Gerätes. Werden Router und Switches mit unsicheren Werkeinstellungen produktiv eingesetzt, kann einfacher unberechtigt auf sie zugegriffen werden. Dies kann dazu führen, dass z. B. Dienste nicht mehr verfügbar sind.

2.5 Fehlerhafte Planung und Konzeption

Viele Institutionen planen und konzipieren den Einsatz von Routern und Switches fehlerhaft. So werden unter anderem Geräte beschafft, die nicht ausreichend dimensioniert sind, z. B. hinsichtlich der Port-Anzahl oder der Leistung. In der Folge ist ein Router oder Switch bereits überlastet, wenn er zum ersten Mal eingesetzt wird. Dadurch sind eventuell Dienste oder ganze Netze nicht erreichbar und der Fehler muss aufwändig korrigiert werden.

2.6 Inkompatible aktive Netzkomponenten

Kompatibilitätsprobleme können insbesondere dann entstehen, wenn bestehende Netze um aktive Netzkomponenten anderer Hersteller ergänzt werden oder wenn Netze mit Netzkomponenten unterschiedlicher Hersteller betrieben werden. Werden aktive Netzkomponenten mit unterschiedlichen Implementierungen desselben Kommunikationsverfahrens gemeinsam in einem Netz betrieben, können einzelne Teilbereiche des Netzes, bestimmter Dienste oder sogar das gesamte Netz ausfallen.

2.7 MAC-Flooding

Beim MAC-Flooding schickt ein Angreifer viele Anfragen mit wechselnden Quell-MAC-Adressen an einen Switch. Sobald der Switch dann die Limits der MAC-Adressen, die er speichern kann, erreicht hat, fängt er an, sämtliche Anfragen an alle IT-Systeme im Netz zu schicken. Dadurch kann der Angreifer den Netzverkehr einsehen.

2.8 Spanning-Tree-Angriffe

Bei Spanning-Tree-Angriffen versendet ein Angreifer sogenannte Bridge Protocol Data Units (BPDUs) mit dem Ziel, die Switches dazu zu bringen, seinen eigenen (bösartigen) Switch als Root Bridge anzusehen. Dadurch wird der Netzverkehr über den Switch des Angreifers umgeleitet, sodass er alle über ihn versendeten Informationen mitschneiden kann. In der Folge kann er DDoS-Attacken initiieren und durch falsche BPDUs das Netz dazu zwingen, die Spanning-Tree-Topologie neu aufzubauen, wodurch das Netz ausfallen kann.

2.9 GARP-Attacken

Bei Gratuitous-ARP-(GARP)-Attacken sendet der Angreifer unaufgeforderte ARP-Antworten an bestimmte Opfer oder an alle IT-Systeme im gleichen Subnetz. In dieser gefälschten ARP-Antwort trägt der Angreifer seine MAC-Adresse als Zuordnung zu einer fremden IP-Adresse ein und bringt das Opfer dazu, seine ARP-Tabelle so zu verändern, dass der Netzverkehr nun zum Angreifer anstatt zum validen Ziel gesendet wird. Dadurch kann er die Kommunikation zwischen den Opfern mitschneiden oder sie manipulieren.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz von *Routern und Switches* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist er dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Informationssicherheitsbeauftragter (ISB)

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

NET.3.1.A1 Sichere Grundkonfiguration eines Routers oder Switches

Bevor ein Router oder Switch eingesetzt wird, MUSS er sicher konfiguriert werden. Die Geräte DÜRFEN NUR von dafür autorisierten Personen installiert und konfiguriert werden. Alle Konfigurationsänderungen SOLLTEN nachvollziehbar dokumentiert sein (siehe NET.3.2.A9 *Betriebsdokumentationen*). Die Integrität der Konfigurationsdateien MUSS geeignet geschützt werden. Zugangspasswörter MÜSSEN verschlüsselt gespeichert werden.

Router und Switches MÜSSEN so konfiguriert sein, dass nur zwingend erforderliche Dienste, Protokolle und funktionale Erweiterungen genutzt werden. Nicht benötigte Dienste, Protokolle und funktionale Erweiterungen MÜSSEN deaktiviert oder ganz deinstalliert werden. Ebenfalls MÜSSEN nicht benutzte Schnittstellen auf Routern und Switches deaktiviert oder zumindest einem dafür eingerichteten *Unassigned-VLAN* zugeordnet werden.

Wenn funktionale Erweiterungen benutzt werden, MÜSSEN die Sicherheitsrichtlinien der Institution weiterhin erfüllt sein. Auch SOLLTE begründet und dokumentiert werden, warum solche Erweiterungen eingesetzt werden.

Informationen über den internen Konfigurations- und Betriebszustand MÜSSEN nach außen verborgen werden. Unnötige Auskunftsdienste MÜSSEN deaktiviert werden.

Bevor Router und Switches in Betrieb genommen werden, MÜSSEN die Standard-Benutzerkonten geändert werden. Passwörter dieser Konten MÜSSEN geändert werden. Nicht benutzte Benutzerkonten MÜSSEN deaktiviert werden. Entsprechend dem Rechte- und Rollenkonzept MÜSSEN anschließend die vorgesehenen Benutzerkonten und -rollen eingerichtet werden.

NET.3.1.A2 Einspielen von Updates und Patches

Die Verantwortlichen MÜSSEN sich über bekannt gewordene Schwachstellen informieren. Updates und Patches MÜSSEN so schnell wie möglich eingespielt werden. Vorab SOLLTE auf einem Testsystem überprüft werden, ob die Sicherheitsupdates kompatibel sind und keine Fehler verursachen. Solange keine Patches für bekannte Schwachstellen verfügbar sind, MÜSSEN andere geeignete Maßnahmen getroffen werden, um Router und Switches zu schützen.

Es MUSS darauf geachtet werden, dass Patches und Updates nur aus vertrauenswürdigen Quellen bezogen werden. Sofern vom Hersteller angeboten, SOLLTEN die Update-Prüfsummen verglichen bzw. die digitalen Signaturen überprüft werden.

NET.3.1.A3 Restriktive Rechtevergabe

Es MUSS geregelt werden, wer auf einen Router oder Switch zugreifen darf. Dabei DÜRFEN immer NUR so viele Zugriffsrechte vergeben werden, wie sie für die jeweiligen Aufgaben erforderlich sind (Minimalprinzip). Nicht mehr benötigte Benutzerkonten MÜSSEN entfernt werden. Es MUSS sichergestellt werden, dass mit Administrator-Rechten (bzw. Root-Rechten) nur gearbeitet wird, wenn es notwendig ist.

NET.3.1.A4 Schutz der Administrationsschnittstellen

Alle Administrations- und Management-Zugänge der Router und Switches MÜSSEN auf einzelne Quell-IP-Adressen bzw. -Adressbereiche eingeschränkt werden. Es MUSS sichergestellt sein, dass aus nicht-vertrauenswürdigen Netzen heraus nicht direkt auf die Administrationsschnittstellen zugegriffen werden kann.

Um Router und Switches zu administrieren bzw. zu überwachen, SOLLTEN ausreichend verschlüsselte Protokolle eingesetzt werden. Sollte dennoch auf unverschlüsselte und damit unsichere Protokolle zurückgegriffen werden, MUSS für die Administration ein eigenes Administrationsnetz (Out-of-Band-Management) genutzt werden. Die Managementschnittstellen und die Administrationsverbindungen MÜSSEN durch eine separate Firewall geschützt werden. Für die Schnittstellen MÜSSEN geeignete Zeitbeschränkungen vorgegeben werden.

Alle für das Management-Interface nicht benötigten Dienste MÜSSEN deaktiviert werden. Verfügt eine Netzkomponente über eine dedizierte Hardwareschnittstelle, MUSS der unberechtigte Zugriff auf diese geeignet unterbunden werden.

NET.3.1.A5 Schutz vor Fragmentierungsangriffen

Am Router und Layer-3-Switch MÜSSEN Schutzmechanismen aktiviert sein, um IPv4- sowie IPv6-Fragmentierungsangriffe abzuwehren.

NET.3.1.A6 Notfallzugriff auf Router und Switches

Es MUSS für die Administratoren immer möglich sein, direkt auf Router und Switches zuzugreifen, sodass diese weiterhin lokal administriert werden können, auch wenn das gesamte Netz ausfällt.

NET.3.1.A7 Protokollierung bei Routern und Switches

Ein Router oder Switch MUSS so konfiguriert werden, dass er unter anderem folgende Ereignisse protokolliert:

- Konfigurationsänderungen (möglichst automatisch),

- Reboot,
- Systemfehler,
- Statusänderungen pro Interface, System und Netzsegment,
- Login-Fehler (zumindest dann, wenn sie wiederholt auftreten)

Die Verantwortlichen MÜSSEN darauf achten, dass bei der Protokollierung alle rechtlichen Rahmenbedingung eingehalten werden. Änderungen an der Konfiguration SOLLTEN zudem automatisch protokolliert werden.

NET.3.1.A8 Regelmäßige Datensicherung

Die Konfigurationsdateien von Routern und Switches MÜSSEN regelmäßig gesichert werden. Die Sicherungskopien MÜSSEN so abgelegt werden, dass im Notfall darauf zugegriffen werden kann.

NET.3.1.A9 Betriebsdokumentationen

Die wichtigsten betrieblichen Aufgaben eines Routers oder Switches MÜSSEN geeignet dokumentiert werden. Es SOLLTEN alle Konfigurationsänderungen sowie sicherheitsrelevante Aufgaben dokumentiert werden. Die Dokumentation SOLLTEN vor unbefugten Zugriffen geschützt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Router und Switches. Sie SOLLTEN grundsätzlich umgesetzt werden.

NET.3.1.A10 Erstellung einer Sicherheitsrichtlinie [Informationssicherheitsbeauftragter (ISB)]

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTE eine spezifische Sicherheitsrichtlinie erstellt werden, in der nachvollziehbar Anforderungen und Vorgaben beschrieben sind, wie Router und Switches sicher betrieben werden können. Die Richtlinie SOLLTE allen Administratoren bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, SOLLTE das mit dem ISB abgestimmt und dokumentiert werden. Es SOLLTE regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse SOLLTEN geeignet dokumentiert werden.

NET.3.1.A11 Beschaffung eines Routers oder Switches

Bevor Router oder Switches beschafft werden, SOLLTE eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Es SOLLTE darauf geachtet werden, dass das von der Institution angestrebte Sicherheitsniveau mit den zu beschaffenden Geräten erreicht werden kann. Grundlage für die Beschaffung SOLLTEN daher die Anforderungen aus der Sicherheitsrichtlinie sein.

NET.3.1.A12 Erstellung einer Konfigurations-Checkliste für Router und Switches

ES SOLLTE eine Konfigurations-Checkliste erstellt werden, anhand derer die wichtigsten sicherheitsrelevanten Einstellungen auf Routern und Switches geprüft werden können. Da die sichere Konfiguration stark vom Einsatzzweck abhängt, SOLLTEN die unterschiedlichen Anforderungen der Geräte in der Konfigurations-Checkliste berücksichtigt werden.

NET.3.1.A13 Administration über ein gesondertes Managementnetz

Router und Switches SOLLTEN ausschließlich über ein separates Managementnetz (Out-of-Band-Management) administriert werden. Eine eventuell vorhandene Administrationsschnittstelle über das eigentliche Datennetz (In-Band) SOLLTE deaktiviert werden. Die verfügbaren Sicherheitsmechanismen der eingesetzten Managementprotokolle zur Authentisierung, Integritätssicherung und Verschlüsselung SOLLTEN aktiviert und alle unsicheren Managementprotokolle deaktiviert werden (siehe NET.1.2 *Netz-Management*).

NET.3.1.A14 Schutz vor Missbrauch von ICMP-Nachrichten

ES SOLLTE sichergestellt sein, dass die Protokolle ICMP und ICMPv6 restriktiv gefiltert werden.

NET.3.1.A15 Bogon- und Spoofing-Filterung

Es SOLLTE verhindert werden, dass Angreifer mithilfe gefälschter, reservierter oder noch nicht zugewiesener IP-Adressen in die Router und Switches eindringen können.

NET.3.1.A16 Schutz vor „IPv6 Routing Header Type-0“-Angriffen

Beim Einsatz von IPv6 SOLLTEN Mechanismen eingesetzt werden, die Angriffe auf den Routing-Header des Type-0 erkennen und verhindern.

NET.3.1.A17 Schutz vor DoS- und DDoS-Angriffen

Es SOLLTEN Mechanismen eingesetzt werden, die hochvolumige Angriffe sowie TCP-State-Exhaustion-Angriffe erkennen und abwehren.

NET.3.1.A18 Einrichtung von Access Control Lists

Der Zugriff auf Router und Switches SOLLTE mithilfe von Access Control Lists (ACL) definiert werden. In der ACL SOLLTE anhand der Sicherheitsrichtlinie der Institution festgelegt werden, über welche IT-Systeme oder Netze mit welcher Methode auf einen Router oder Switch zugegriffen werden darf. Für den Fall, dass keine spezifischen Regeln existieren, SOLLTE generell der restriktivere Whitelist-Ansatz bevorzugt werden.

NET.3.1.A19 Sicherung von Switch-Ports

Die Ports eines Switches SOLLTEN vor unberechtigten Zugriffen geschützt werden.

NET.3.1.A20 Sicherheitsaspekte von Routing-Protokollen

Router SOLLTEN sich authentisieren, wenn sie Routing-Informationen austauschen oder Updates für Routing-Tabellen verschicken. Es SOLLTEN ausschließlich Routing-Protokolle eingesetzt werden, die das unterstützen.

Dynamische Routing-Protokolle SOLLTEN ausschließlich in sicheren Netzen verwendet werden. Sie DÜRFEN NICHT in demilitarisierten Zonen (DMZ) eingesetzt werden. In DMZs SOLLTEN stattdessen statische Routen eingetragen werden.

NET.3.1.A21 Identitäts- und Berechtigungsmanagement in der Netzinfrastruktur

Router und Switches SOLLTEN an ein zentrales Identitäts- und Berechtigungsmanagement angebunden werden (siehe ORP.4 *Identitäts- und Berechtigungsmanagement).*

NET.3.1.A22 Notfallvorsorge bei Routern und Switches

Um in Störungssituationen effektiv und schnell reagieren zu können, SOLLTEN Diagnose und Fehlerbehebungen im Vorfeld geplant und vorbereitet werden. Für typische Ausfallszenarien SOLLTEN entsprechende Handlungsanweisungen definiert werden.

Die Notfallplanungen für Router und Switches SOLLTEN mit der übergreifenden Störungs- und Notfallvorsorge abgestimmt sein und sich am allgemeinen Notfallvorsorgekonzept (siehe DER.4 *Notfallmanagement*) orientieren. Es SOLLTE sichergestellt sein, dass die Dokumentationen zur Notfallvorsorge und die darin enthaltenen Handlungsanweisungen in Papierform existiert. Die in der Notfallvorsorge notwendigen Vorgehensbeschreibungen SOLLTEN regelmäßig geprobt werden.

NET.3.1.A23 Revision und Penetrationstests

Router und Switches SOLLTEN regelmäßig auf bekannte Sicherheitsprobleme hin überprüft werden. Auch SOLLTEN regelmäßig Revisionen durchgeführt werden. Dabei SOLLTE z. B. geprüft werden, ob der Istzustand der festgelegten sicheren Grundkonfiguration entspricht. Die Ergebnisse SOLLTEN nachvollziehbar dokumentiert und mit dem Sollzustand abgeglichen werden. Abweichungen SOLLTE nachgegangen werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

NET.3.1.A24 Einsatz von Netzzugangskontrollen (IA)

Es SOLLTE eine Port-based Access Control nach IEEE 802.1x auf Basis von EAP-TLS implementiert werden. Es SOLLTE NICHT eine Implementierung nach den Standards IEEE 802.1x-2001 und IEEE 802.1x-2004 erfolgen.

NET.3.1.A25 Erweiterter Integritätsschutz für die Konfigurationsdateien (I)

Stürzt ein Router oder Switch ab, SOLLTE sichergestellt werden, dass bei der Wiederherstellung bzw. beim Neustart keine alten oder fehlerhaften Konfigurationen (unter anderem ACLs) benutzt werden.

NET.3.1.A26 Hochverfügbarkeit (A)

Die Realisierung einer Hochverfügbarkeitslösung DARF NICHT den Betrieb der Router und Switches bzw. deren Sicherheitsfunktionen behindern oder das Sicherheitsniveau senken. Router und Switches SOLLTEN redundant ausgelegt werden. Dabei SOLLTE darauf geachtet werden, dass die Sicherheitsrichtlinie der Institution eingehalten wird.

NET.3.1.A27 Bandbreitenmanagement für kritische Anwendungen und Dienste (A)

Um Bandbreitenmanagement für kritische Anwendungen und Dienste zu gewährleisten, SOLLTEN Router und Switches Funktionen enthalten und einsetzen, mit denen sich die Applikationen erkennen und Bandbreiten priorisieren lassen.

NET.3.1.A28 Einsatz von zertifizierten Produkten (CI)

Es SOLLTEN Router und Switches mit einer Sicherheits-Evaluierung nach Common Criteria eingesetzt werden, mindestens mit der Stufe EAL4.

4 Weiterführende Informationen

4.1 Literatur

- [8021AD] IEEE 802.1ad
  Provider Bridges, 2006
  http://www.ieee802.org/1/pages/802.1ad.html

- [8021AE] IEEE 802.1AE
  Media Access Control (MAC) Security, 2006
  http://www.ieee802.org/1/pages/802.1ae.html

- [ISI] BSI-Standards zur Internet Sicherheit (Isi-Reihe)
  BSI, (zuletzt abgerufen am 28.09.2017)
  https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Reihe_node.html

- [NIST80046] NIST Special Publication 800-46 Revision 2
  Guide to Enterprise Telework, Remote Access and Bring Your Own Device (BYOD) Security, NIST, 07.2016
  http://dx.doi.org/10.6028/NIST.SP.800-46r2

- [RFC6165] Extensions to IS-IS for Layer-2 Systems
  RFC, 2011
  https://tools.ietf.org/html/rfc6165

- [RFC7348] Virtual EXtensible Local Area Network (VXLAN)
  A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks, 2014
  https://tools.ietf.org/html/rfc7348

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Router und Switches" von Bedeutung.

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.38 Missbrauch personenbezogener Daten

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.42 Social Engineering

G 0.43 Einspielen von Nachrichten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.09	G 0.11	G 0.14	G 0.15	G 0.16	G 0.17	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.29	G 0.30	G 0.31	G 0.32	G 0.36	G 0.37	G 0.38	G 0.40	G 0.42	G 0.43	G 0.45	G 0.46
NET.3.1.A1	x				x	x	x	x		x	x			x														
NET.3.1.A2		x	x	x									x	x				x	x	x	x		x		x			
NET.3.1.A3			x	x									x															
NET.3.1.A4	x	x	x	x								x						x	x	x	x		x					
NET.3.1.A5	x		x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x		x	x	x
NET.3.1.A6			x	x											x							x						
NET.3.1.A7		x																										
NET.3.1.A8		x																				x						
NET.3.1.A9	x	x	x	x																								
NET.3.1.A10												x																
NET.3.1.A11	x	x	x	x								x						x	x	x	x		x					
NET.3.1.A12	x	x	x	x								x						x	x	x	x	x	x					
NET.3.1.A13	x		x	x			x		x			x	x	x	x	x	x	x	x	x	x		x					
NET.3.1.A14	x	x	x	x								x																
NET.3.1.A15	x												x											x		x	x	x
NET.3.1.A16	x												x											x		x	x	x
NET.3.1.A17	x												x											x		x	x	x
NET.3.1.A18	x												x											x		x	x	x
NET.3.1.A19	x												x											x		x	x	x
NET.3.1.A20															x													
NET.3.1.A21												x																
NET.3.1.A22		x	x	x			x					x			x													
NET.3.1.A23	x	x	x	x								x	x					x	x	x	x		x					
NET.3.1.A24	x		x	x								x						x	x	x	x		x					
NET.3.1.A25			x	x	x	x		x		x	x	x																
NET.3.1.A26			x	x																		x						
NET.3.1.A27			x	x	x	x		x		x	x	x																
NET.3.1.A28	x											x	x		x									x		x	x	x

NET.3: Netzkomponenten

NET.3.2 Firewall

1 Beschreibung

1.1 Einleitung

Eine Firewall ist ein System aus soft- und hardwaretechnischen Komponenten, das dazu eingesetzt wird, IP-basiere Datennetze sicher zu koppeln. Dazu wird mit Hilfe einer Firewall-Struktur die technisch mögliche auf die in einer Sicherheitsrichtlinie als sicher definierte Kommunikation eingeschränkt. Sicherheit bedeutet hierbei, dass ausschließlich die erwünschten Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen werden.

Um Netzübergänge abzusichern, wird oft nicht mehr eine einzelne Komponente verwendet, sondern eine ganze Reihe von IT-Systemen, die unterschiedliche Aufgaben übernehmen, z. B. ausschließlich Pakete zu filtern oder Netzverbindungen mithilfe von Proxy-Funktionen strikt zu trennen. Der in diesem Baustein verwendete Begriff Application Level Gateway (ALG) bezeichnet eine Firewallkomponente, die Datenströme auf Basis von Sicherheitsproxys regelt.

Eine Firewall wird am zentralen Übergang zwischen unterschiedlich vertrauenswürdigen Netzen eingesetzt. Unterschiedlich vertrauenswürdige Netze stellen dabei nicht unbedingt nur die Kombination Internet/Intranet dar. Vielmehr können auch zwei institutionsinterne Netze einen unterschiedlich hohen Schutzbedarf besitzen, z. B. hat das Netz der Bürokommunikation meistens einen anderen Schutzbedarf als das Netz der Personalabteilung, in dem besonders schützenswerte, personenbezogene Daten übertragen werden.

1.2 Zielsetzung

Ziel des Bausteins ist es, eine Firewall bzw. eine Firewall-Struktur sicher einsetzen zu können, um Netze mit unterschiedlichen Schutzanforderungen sicher miteinander zu verbinden.

1.3 Abgrenzung

Der vorliegende Baustein baut auf den Baustein NET.1.1 *Netz-Architektur und -design* auf und enthält konkrete Anforderungen, die zu beachten und zu erfüllen sind, wenn netzbasierte Firewalls beschafft, aufgebaut, konfiguriert und betrieben werden.

Um Netze abzusichern, sind meistens weitere Netzkomponenten erforderlich, z. B. Router und Switches. Anforderungen hierzu werden jedoch nicht in diesem Baustein aufgeführt, sondern sind in NET.3.1 *Router und Switches* zu finden. Wenn eine Firewall die Aufgaben eines Routers oder Switches übernimmt, gelten für sie zusätzlich die Anforderungen des Bausteins NET.3.1 *Router und Switches*.

Darüber hinaus wird nicht auf Produkte wie sogenannte Next Generation Firewalls (NGFW) oder Unified Threat Management Firewalls eingegangen, die zusätzlich funktionale Erweiterungen enthalten, z. B. VPN, Systeme zur Intrusion Detection und Intrusion Prevention (IDS/IPS), Virenscanner oder Spam-Filter. Sicherheitsaspekte dieser funktionalen Erweiterungen sind nicht Gegenstand des vorliegenden Bausteins, sondern werden z. B. in den Bausteinen NET.3.3 *VPN*, NET.3.4 *IDS/IPS*, OPS1.1.4 *Schutz vor Schadprogrammen* behandelt.

Ebenso wird nicht auf eine Anwendungserkennung bzw. -filterung eingegangen. Sie ist eine gängige Funktion von Next Generation Firewalls sowie IDS/IPS. Da sich die Implementierungen zwischen den Produkten unterscheiden, wird empfohlen, sie je nach Einsatzszenario individuell zu betrachten. In diesem Baustein wird auch nicht auf die individuellen Schutzmöglichkeiten für extern angebotene Server-Dienste eingegangen, z. B. durch ein Reverse Proxy oder für Webdienste mithilfe einer Web Application Firewall (WAF). Darüber hinaus werden Aspekte der infrastrukturellen Sicherheit (z. B. geeignete Aufstellung oder Stromversorgung) nicht in diesem Baustein aufgeführt, sondern finden sich in den jeweiligen Bausteinen der Schicht INF.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Firewall von besonderer Bedeutung:

2.1 Distributed Denial of Service (DDoS)

Bei einem DDoS-Angriff auf ein geschütztes Netz (z. B. TCP-SYN-Flooding, UDP Packet Storm) kann aufgrund der vielen Netzverbindungen, die verarbeitet werden müssen, die Firewall ausfallen. Das kann dazu führen, dass bestimmte Dienste im Local Area Network (LAN) nicht mehr verfügbar sind oder das gesamte LAN ausfällt.

2.2 Manipulation

Gelingt es einem Angreifer, unberechtigt auf ein Firewall-System oder eine entsprechende Verwaltungsoberfläche zuzugreifen, kann er dort Dateien beliebig manipulieren. So kann er beispielsweise die Konfiguration ändern, zusätzliche Dienste starten oder Schadsoftware installieren. Ebenso kann er auf dem manipulierten System die Kommunikationsverbindungen mitschneiden. Auch lassen sich beispielsweise die Firewall-Regeln so verändern, dass aus dem Internet auf die Firewall und auf das Intranet der Institution zugegriffen werden kann. Weiterhin kann ein Angreifer einen Denial-of-Service-(DoS)-Angriff starten, indem er im Regelwerk den Zugriff auf einzelne Server-Dienste verhindert.

2.3 Software-Schwachstellen oder -Fehler

Firewalls sind komplexe Systeme und besonders am Übergang vom Intranet zum Internet zahlreichen Angriffen ausgesetzt. Hersteller von Firewalls veröffentlichen daher regelmäßig Updates und Patches, um Softwarefehler und bekannt gewordene Schwachstellen in ihren Produkten zu beheben. Werden diese jedoch nicht oder zu spät eingespielt, kann das Firewall-System erfolgreich angegriffen werden. Dadurch ist es möglich, dass Angreifer die Systeme manipulieren und so geschäftskritische Daten abfließen, Dienste ausfallen oder ganze Produktionsprozesse still stehen.

2.4 Umgehung der Firewall-Regeln

Angreifer können mithilfe grundlegender Mechanismen in den Netzprotokollen die Firewall-Regeln umgehen (z. B. durch Fragmentierungsangriffe), um in einen durch die Firewall geschützten Bereich einzudringen. Im geschützten Bereich können sie anschließend weiteren Schaden anrichten (z. B. sensible Daten auslesen, manipulieren oder löschen).

2.5 Fehlerhafte Konfiguration und Bedienungsfehler einer Firewall

Eine fehlerhaft konfigurierte oder falsch bediente Firewall kann sich gravierend auf die Verfügbarkeit von Diensten auswirken. Werden beispielsweise Firewall-Regeln falsch gesetzt, können Netzzugriffe blockiert werden. Weiterhin können fehlerhafte Konfigurationen dazu führen, dass IT-Systeme nicht mehr ganz oder auch gar nicht mehr geschützt sind. Im schlimmsten Fall sind dadurch interne Dienste für Angreifer erreichbar.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Firewall aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Informationssicherheitsbeauftragter (ISB)

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

NET.3.2.A1 Erstellung einer Sicherheitsrichtlinie [Informationssicherheitsbeauftragter (ISB)]

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie erstellt werden, in der nachvollziehbar Anforderungen und Vorgaben beschrieben sind, wie Firewalls sicher betrieben werden können. Die Richtlinie MUSS allen im Bereich Firewalls verantwortlichen Mitarbeitern bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies mit dem ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse MÜSSEN sinnvoll dokumentiert werden.

NET.3.2.A2 Festlegen der Firewall-Regeln

Die gesamte Kommunikation zwischen den beteiligten Netzen MUSS über die Firewall geleitet werden. Es MUSS sichergestellt sein, dass von außen keine unbefugten Verbindungen in das geschützte Netz aufgebaut werden können. Ebenso DÜRFEN KEINE unbefugten Verbindungen aus dem geschützten Netz heraus aufgebaut werden.

Für die Firewall MÜSSEN eindeutige Regeln definiert werden, die festlegen, welche Kommunikationsverbindungen und Datenströme zugelassen werden. Alle anderen Verbindungen MÜSSEN durch die Firewall unterbunden werden (Whitelist-Ansatz). Die Kommunikationsbeziehungen mit angeschlossenen Dienst-Servern (z. B. E-Mail-Servern, Web-Servern), die über die Firewall geführt werden, MÜSSEN in den Regeln berücksichtigt sein.

Es DÜRFEN KEINE IT-Systeme von außen über die Firewall auf das interne Netz zugreifen (siehe Vorgaben aus dem Baustein NET.1.1 *Netz-Architektur und -design)*. Etwaige Ausnahmen zu dieser Anforderung werden in den entsprechenden anwendungs- und systemspezifischen Bausteinen geregelt.

Es MÜSSEN Verantwortliche benannt werden, die Filterregeln entwerfen, umsetzen und testen. Zudem MUSS geklärt werden, wer Filterregeln verändern darf. Die getroffenen Entscheidungen sowie die relevanten Informationen und Entscheidungsgründe MÜSSEN dokumentiert werden.

NET.3.2.A3 Einrichten geeigneter Filterregeln am Paketfilter

Basierend auf den Firewall-Regeln aus NET.3.2.A2 *Festlegen der Firewall-Regeln* MÜSSEN geeignete Filterregeln für den Paketfilter definiert und eingerichtet werden.

Ein Paketfilter MUSS so eingestellt sein, dass er alle ungültigen TCP-Flag-Kombinationen verwirft. Grundsätzlich MUSS immer zustandsbehaftet gefiltert werden. Auch für die verbindungslosen Protokolle UDP und ICMP SOLLTEN zustandsbehaftete Filterregeln konfiguriert werden. Die Firewall MUSS die Protokolle ICMP und ICMPv6 restriktiv filtern.

NET.3.2.A4 Sichere Konfiguration der Firewall

Bevor eine Firewall eingesetzt wird, MUSS sie sicher konfiguriert werden.

Eine Firewall DARF ausschließlich NUR von dafür autorisierten Personen installiert und konfiguriert werden, z. B. Verantwortlichen aus dem eigenen IT-Betrieb oder vertraglich gebundenen Dienstleistern.

Alle Konfigurationsänderungen MÜSSEN nachvollziehbar dokumentiert sein (siehe NET.3.2.A14 *Betriebsdokumentationen*). Die Integrität der Konfigurationsdateien SOLLTE geeignet geschützt werden. Zugangspasswörter MÜSSEN verschlüsselt gespeichert werden.

Eine Firewall MUSS so konfiguriert sein, dass ausschließlich zwingend erforderliche Dienste verfügbar sind. Wenn funktionale Erweiterungen benutzt werden, MÜSSEN die Sicherheitsrichtlinien der Institution weiterhin erfüllt sein. Auch MUSS begründet und dokumentiert werden, warum solche Erweiterungen eingesetzt werden. Nicht benötigte (Auskunfts-) Dienste sowie nicht benötigte funktionale Erweiterungen MÜSSEN deaktiviert oder ganz deinstalliert werden.

Informationen über den internen Konfigurations- und Betriebszustand MÜSSEN nach außen bestmöglich verborgen werden.

NET.3.2.A5 Restriktive Rechtevergabe

Es MUSS geregelt werden, wer auf die Firewall zugreifen darf, z. B. um sie zu konfigurieren oder zu überwachen. Dabei DÜRFEN immer NUR so viele Zugriffsrechte vergeben werden, wie für die jeweiligen Aufgaben erforderlich sind (Need-to-know-Prinzip). Unautorisierte Benutzerkonten MÜSSEN entfernt werden. Es MUSS sichergestellt werden, dass mit Administrator-Rechten (bzw. Root-Rechten) nur gearbeitet wird, wenn es notwendig ist.

NET.3.2.A6 Schutz der Administrationsschnittstellen

Alle Administrations- und Management-Zugänge der Firewall MÜSSEN auf einzelne Quell-IP-Adressen bzw. -Adressbereiche eingeschränkt werden. Es MUSS sichergestellt sein, dass aus nicht-vertrauenswürdigen Netzen heraus nicht auf die Administrationsschnittstellen zugegriffen werden kann.

Um die Firewall zu administrieren bzw. zu überwachen, DÜRFEN NUR sichere Protokolle eingesetzt werden oder es MUSS ein eigens dafür vorgesehenen Administrationsnetz (Out-of-Band-Management) verwendet werden (siehe Vorgaben aus dem Baustein NET.1.1 *Netz-Architektur und -design und NET.1.2 Netz-Management).* Für die Benutzerschnittstellen MÜSSEN geeignete Zeitbeschränkungen vorgegeben werden.

NET.3.2.A7 Notfallzugriff auf die Firewall

Es MUSS immer möglich sein, direkt auf die Firewall zugreifen zu können, sodass weiterhin lokal gearbeitet werden kann, auch wenn das gesamte Netz ausfällt.

NET.3.2.A8 Unterbindung von dynamischem Routing

In den Einstellungen der Firewall MUSS das dynamische Routing deaktiviert sein, es sei denn, der Paketfilter wird entsprechend dem Baustein NET.3.1 *Router und Switches* als Perimeter-Router eingesetzt.

NET.3.2.A9 Protokollierung

Die Firewall MUSS so konfiguriert werden, dass sie mindestens folgende Ereignisse protokolliert:

- abgewiesene Netzverbindungen (Quell- und Ziel-IP-Adressen, Quell- und Zielport oder ICMP/ICMPv6-Typ, Datum, Uhrzeit),

- fehlgeschlagene Zugriffe auf System-Ressourcen aufgrund fehlerhafter Authentisierungen, mangelnder Berechtigung oder nicht vorhandener Ressourcen,
- Fehlermeldungen der Firewall-Dienste und
- allgemeine Systemfehlermeldungen.

Werden Sicherheitsproxys eingesetzt, MÜSSEN Sicherheitsverletzungen und Verstöße gegen Access-Control-Listen (ACLs oder auch kurz Access-Listen) geeignet protokolliert werden: mindestens Art der Protokollverletzung bzw. des ACL-Verstoßes, Quell- und Ziel-IP-Adresse, Quell- und Zielport, Dienst, Datum und Zeit sowie die Verbindungsdauer (falls erforderlich).

Wenn sich ein Benutzer am Sicherheitsproxy authentisiert, MÜSSEN auch Authentisierungsdaten oder ausschließlich die Information über eine fehlgeschlagene Authentisierung protokolliert werden.

Die Verantwortlichen MÜSSEN darauf achten, dass bei der Protokollierung alle rechtlichen Rahmenbedingung eingehalten werden.

NET.3.2.A10 Abwehr von Fragmentierungsangriffen am Paketfilter

Am Paketfilter MÜSSEN Schutzmechanismen aktiviert sein, um IPv4- sowie IPv6-Fragmentierungsangriffe abzuwehren.

NET.3.2.A11 Einspielen von Updates und Patches

Die Verantwortlichen MÜSSEN sich über bekannt gewordene Schwachstellen informieren. Updates und Patches MÜSSEN so schnell wie möglich eingespielt werden. Vorab SOLLTE auf einem Testsystem überprüft werden, ob die Sicherheitsupdates kompatibel sind und keine Fehler verursachen. Solange keine Patches bei bekannten Schwachstellen verfügbar sind, MÜSSEN andere geeignete Maßnahmen getroffen werden, um die Firewall zu schützen.

Es MUSS darauf geachtet werden, dass Patches und Updates nur aus vertrauenswürdigen Quellen bezogen werden. Darauf MUSS auch bei zugehörigen Diensten innerhalb des Firewall-Systems geachtet werden.

NET.3.2.A12 Vorgehen bei Sicherheitsvorfällen

Es MUSS festgelegt werden, wie bei einem festgestellten Angriff reagiert werden soll. Die Aufgaben und Kompetenzen für die betroffenen Mitarbeiter MÜSSEN eindeutig festgelegt werden. Weitere Informationen hierzu siehe DER.2.1 *Incident Management*.

NET.3.2.A13 Regelmäßige Datensicherung

Es MÜSSEN in regelmäßigen Abständen Systemsicherungen der Firewall erstellt werden. Auch bevor eine Firewall neu installiert oder anders konfiguriert wird, MUSS das System gesichert werden. Wenn gesicherte Datenbestände wieder eingespielt werden, MÜSSEN sich die sicherheitsrelevanten Dateien wie Access-Listen, Passwortdateien und Filterregeln auf dem sicherheitstechnisch erforderlichen Konfigurationsstand befinden.

NET.3.2.A14 Betriebsdokumentationen

Die betrieblichen Aufgaben einer Firewall MÜSSEN nachvollziehbar dokumentiert werden. Es MÜSSEN alle Konfigurationsänderungen sowie sicherheitsrelevante Aufgaben dokumentiert werden, insbesondere Änderungen an den System-Diensten und dem Regelwerk der Firewall. Die Dokumentation MUSS vor unbefugten Zugriffen geschützt werden. Änderungen an der Konfiguration MÜSSEN zudem möglichst automatisch protokolliert werden.

NET.3.2.A15 Beschaffung einer Firewall

Bevor eine Firewall beschafft wird, MUSS eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Es MUSS darauf geachtet werden, dass das von der Institution angestrebte Sicherheitsniveau mit der Firewall erreichbar ist. Grundlage für die Beschaffung MUSS daher die Anforderungen aus der Sicherheitsrichtlinie sein.

Wird IPv6 eingesetzt, MUSS der Paketfilter die IPv6-Erweiterungsheader (Extension Header) überprüfen. Zudem MUSS sich IPv6 adäquat zu IPv4 konfigurieren lassen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Firewall. Sie SOLLTEN grundsätzlich umgesetzt werden.

NET.3.2.A16 Aufbau einer „P-A-P“-Struktur

Der Aufbau einer "Paketfilter – Application-Level-Gateway – Paketfilter"-(P-A-P)-Struktur SOLLTE aus mehreren Komponenten mit jeweils zugeeigneter Hard- und Software bestehen. Für die wichtigsten verwendeten Protokolle SOLLTEN Sicherheitsproxys auf Anwendungsschicht vorhanden sein und für andere Dienste zumindest generische Sicherheitsproxys für TCP und UDP. Die Sicherheitsproxys SOLLTEN zudem innerhalb einer abgesicherten Laufzeitumgebung des Betriebssystems ablaufen.

NET.3.2.A17 Deaktivierung von IPv4 oder IPv6

Wenn das IPv4- oder IPv6-Protokoll in einem Netz-Segment nicht benötigt wird, SOLLTE es am jeweiligen Firewall-Netzzugangspunkt (z. B. am entsprechenden Firewall-Interface) deaktiviert werden. Wenn das IPv4- oder IPv6-Protokoll gar nicht benötigt bzw. eingesetzt wird, SOLLTE es auf der Firewall komplett deaktiviert werden.

NET.3.2.A18 Administration über ein gesondertes Managementnetz

Firewalls SOLLTEN ausschließlich über ein separates Managementnetz (Out-of-Band-Management) administriert werden. Eine eventuell vorhandene Administrationsschnittstelle über das eigentliche Datennetz (In-Band) MUSS deaktiviert werden. Die Kommunikation im Managementnetz SOLLTE über Management-Firewalls (siehe NET.1.1 *Netz-Architektur und -design*) auf wenige Managementprotokolle mit genau festgelegten Ursprüngen und Zielen beschränkt werden. Die verfügbaren Sicherheitsmechanismen der eingesetzten Managementprotokolle zur Authentisierung, Integritätssicherung und Verschlüsselung SOLLTEN aktiviert und alle unsicheren Managementprotokolle deaktiviert werden (siehe NET.1.2 *Netz-Management*).

NET.3.2.A19 Schutz vor TCP SYN Flooding, UDP Paket Storm und Sequence Number Guessing am Paketfilter

Am Paketfilter, der Server-Dienste schützt, die aus nicht-vertrauenswürdigen Netzen erreichbar sind, SOLLTE ein Limit für halboffene und offene Verbindungen gesetzt werden.

Am Paketfilter, der Server-Dienste schützt, die aus weniger oder nicht-vertrauenswürdigen Netzen erreichbar sind, SOLLTEN die sogenannten Rate Limits für UDP-Datenströme gesetzt werden.

Am äußeren Paketfilter SOLLTE bei ausgehenden Verbindungen für TCP eine zufällige Generierung von Initial Sequence Numbers (ISN) aktiviert werden, sofern dieses nicht bereits durch Sicherheits-Proxys realisiert wird.

NET.3.2.A20 Absicherung von grundlegenden Internetprotokollen

Um ins Internet zu kommunizieren, SOLLTEN die Protokolle HTTP, SMTP und DNS inklusive ihrer verschlüsselten Versionen über protokollspezifische Sicherheitsproxys geleitet werden.

NET.3.2.A21 Temporäre Entschlüsselung des Datenverkehrs

Verschlüsselte Verbindungen in nicht-vertrauenswürdige Netze SOLLTEN temporär entschlüsselt werden, um das Protokoll zu verifizieren und die Daten auf Schadsoftware zu prüfen. Hierbei MÜSSEN die rechtlichen Rahmenbedingungen beachtet werden.

Die Komponente, die den Datenverkehr temporär entschlüsselt, SOLLTE unterbinden, dass veraltete Verschlüsselungsoptionen (z. B. SSL) und kryptografische Algorithmen (z. B. DES, MD5, SHA1) benutzt werden.

Auch SOLLTE das eingesetzte TLS-Proxy prüfen können, ob Zertifikate vertrauenswürdig sind. Ist ein Zertifikat nicht vertrauenswürdig, SOLLTE es möglich sein, die Verbindung abzuweisen. Eigene Zertifikate SOLLTEN nachrüstbar sein, um auch "interne" Root-Zertifikate konfigurieren und prüfen zu können. Vorkonfigurierte Zertifikate SOLLTEN überprüft und entfernt werden, wenn sie nicht benötigt werden.

NET.3.2.A22 Sichere Zeitsynchronisation

Es SOLLTE eine sichere Zeitsynchronisation mit einem Network-Time-Protocol-(NTP)-Server erfolgen. Die Firewall SOLLTE keine externe Zeitsynchronisation zulassen. Weitere Anforderungen sind dem Baustein NET.1.2 *Netzmanagement* zu entnehmen.

NET.3.2.A23 Systemüberwachung und -Auswertung

Firewalls SOLLTEN in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept eingebunden werden. Weiterhin SOLLTE ein Prozess definiert werden, der regelt, wie Protokolldaten ausgewertet werden sollen und welche Protokolle regelmäßig, sporadisch oder nur anlassbezogen auszuwerten sind. Es SOLLTE ständig überwacht werden, ob die Firewall selbst und die darauf betriebenen Dienste korrekt funktionieren. Bei Fehlern oder wenn Grenzwerte überschritten werden, SOLLTE das Betriebspersonal alarmiert werden. Zudem SOLLTEN automatisch Alarmmeldungen generiert werden, die bei festgelegten Ereignissen ausgelöst werden. Protokolldaten oder Statusmeldungen SOLLTEN nur über sichere Kommunikationswege übertragen werden.

NET.3.2.A24 Revision und Penetrationstests

Die Firewall-Struktur SOLLTE regelmäßig auf bekannte Sicherheitsprobleme hin überprüft werden. Es SOLLTEN regelmäßige Penetrationstests und Revisionen durchgeführt werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

NET.3.2.A25 Erweiterter Integritätsschutz für die Konfigurationsdateien (CI)

Stürzt ein System ab, SOLLTE sichergestellt werden, dass keine alten oder fehlerhaften Konfigurationen (unter anderem Access-Listen) benutzt werden. Dies SOLLTE auch gelten, wenn es einem Angreifer gelingt, die Firewall neuzustarten.

NET.3.2.A26 Auslagerung von funktionalen Erweiterungen auf dedizierte Hardware (CIA)

Um das Angriffspotenzial weiter zu minimieren, SOLLTE eine Institution funktionale Erweiterungen der Firewall auf dedizierte Hard- und Software auslagern.

NET.3.2.A27 Einsatz verschiedener Firewall-Betriebssysteme und -Produkte in einer mehrstufigen Firewall-Architektur (CI)

In einer mehrstufigen Firewall-Architektur SOLLTEN unterschiedliche Betriebssysteme und -Produkte für die äußeren und inneren Firewalls eingesetzt werden, damit sich eine potenzielle Schwachstelle eines Betriebssystems oder eines Produkts weniger weitreichend auswirkt.

NET.3.2.A28 Zentrale Filterung von aktiven Inhalten (CI)

Aktive Inhalte SOLLTEN gemäß den Sicherheitszielen der Institution zentral gefiltert werden. Dafür SOLLTE auch der verschlüsselte Datenverkehr entschlüsselt werden. Die erforderlichen Sicherheitsproxys SOLLTEN es unterstützen, aktive Inhalte zu filtern.

NET.3.2.A29 Einsatz von Hochverfügbarkeitslösungen (A)

Paketfilter und Application-Level-Gateway SOLLTEN hochverfügbar ausgelegt werden. Zudem SOLLTEN zwei voneinander unabhängige Zugangsmöglichkeiten zum externen Netz bestehen, z. B. zwei Internetzugänge von unterschiedlichen Providern. Interne und externe Router sowie alle weiteren beteiligten aktiven Komponenten (z. B. Switches), die zum Verlust der Verfügbarkeit führen können, SOLLTEN ebenfalls hochverfügbarausgelegt sein.

Auch nach einem automatischen Failover SOLLTE die Firewall-Struktur die Sicherheitsanforderungen der Sicherheitsrichtlinie erfüllen (Fail safe bzw. Fail secure).

Die Funktionsüberwachung SOLLTE anhand von zahlreichen Parametern erfolgen und sich nicht auf ein einzelnes Kriterium verlassen. Protokolldateien und Warnmeldungen der Hochverfügbarkeitslösung SOLLTEN regelmäßig kontrolliert werden.

NET.3.2.A30 Bandbreitenmanagement für kritische Anwendungen und Dienste (A)

Um Bandbreitenmanagement für kritische Anwendungen und Dienste zu gewährleisten, SOLLTEN Paketfilter mit entsprechender Bandbreitenmanagement-Funktion an Netzübergängen und am Übergang zwischen verschiedenen Sicherheitszonen eingesetzt werden.

NET.3.2.A31 Einsatz von zertifizierten Produkten (CI)

Es SOLLTEN Firewalls mit einer Sicherheits-Evaluierung nach Common Criteria eingesetzt werden, mindestens mit der Stufe EAL4.

4 Weiterführende Informationen

4.1 Literatur

- [BSICS112] Next Generation Firewalls - Veröffentlichungen zur Cyber-Sicherheit
  Empfehlung von Einsatzmöglichkeiten für den normalen Schutzbedarf, BSI, 04.2015
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/
  infos/20150407_BSI_Empfehlung_NGFW.htm

- [ISILANA] BSI-Standard zur Internet-Sicherheit (Isi-Reihe):
  Sichere Anbindung von lokalen Netzen an das Internet (Isi-LANA), Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014
  https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-LANA/lana_node.html

- [NIST80041] NIST Special Publication 800-41
  Guidelines on Firewalls and Firewall Policy, 09.2009
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

- [TR21022] BSI Technische Richtlinie, Kryptografische Verfahren
  Verwendung von Transport Layer Security (TLS), Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017
  https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Firewall" von Bedeutung.

G 0.08 Ausfall oder Störung der Stromversorgung

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

G 0.14 Ausspähen von Informationen (Spionage)

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.41 Sabotage

G 0.43 Einspielen von Nachrichten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.08	G 0.09	G 0.14	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.24	G 0.25	G 0.26	G 0.27	G 0.28	G 0.29	G 0.30	G 0.31	G 0.32	G 0.39	G 0.40	G 0.41	G 0.43	G 0.45	G 0.46
NET.3.2.A1				x									x											
NET.3.2.A2			x		x				x										x	x	x	x		x
NET.3.2.A3			x		x				x										x	x	x	x		x
NET.3.2.A4		x	x		x		x	x	x		x	x		x		x		x			x		x	x
NET.3.2.A5								x				x									x			x
NET.3.2.A6		x			x		x	x	x		x			x		x		x			x		x	x
NET.3.2.A7		x									x													
NET.3.2.A8								x			x										x	x		
NET.3.2.A9							x	x							x	x	x	x			x	x	x	x
NET.3.2.A10					x																x	x		
NET.3.2.A11						x	x			x				x							x			
NET.3.2.A12				x																	x			
NET.3.2.A13																							x	
NET.3.2.A14				x		x																		
NET.3.2.A15				x		x																		
NET.3.2.A16			x		x			x	x										x	x				
NET.3.2.A17									x															
NET.3.2.A18		x							x							x								
NET.3.2.A19																				x	x			
NET.3.2.A20			x		x									x								x		
NET.3.2.A21								x													x	x		
NET.3.2.A22							x	x							x	x	x	x			x	x	x	x
NET.3.2.A23	x	x							x		x	x	x							x	x			
NET.3.2.A24							x	x	x				x								x			
NET.3.2.A25					x		x	x	x				x										x	x
NET.3.2.A26				x							x		x											
NET.3.2.A27			x		x		x		x			x		x										
NET.3.2.A28																					x			x
NET.3.2.A29	x	x									x													
NET.3.2.A30		x																		x				
NET.3.2.A31						x																		

NET.3: Netzkomponenten

NET.3.3 VPN

1 Beschreibung

1.1 Einleitung

Mithilfe von Virtuellen Privaten Netzen (VPNs) können Sicherheitsmaßnahmen realisiert werden, um schutzbedürftige Daten über nicht-vertrauenswürdige Netze wie das Internet zu übertragen. Ein VPN ist ein Netz, das physisch innerhalb eines anderen Netzes, wie beispielsweise des Internets, betrieben wird, jedoch logisch von diesem Netz getrennt ist. VPNs können mithilfe kryptografischer Verfahren die Integrität und Vertraulichkeit von Daten schützen. Die sichere Authentisierung der Kommunikationspartner ist auch dann möglich, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.

1.2 Zielsetzung

Der Baustein definiert Anforderungen, mit denen sich ein VPN zielgerichtet und sicher planen, umsetzen und betreiben lässt.

1.3 Abgrenzung

Ein VPN im Sinne dieses Bausteins ist ein Netz, das physisch innerhalb eines anderen Netzes betrieben wird, jedoch logisch von diesem Netz getrennt ist. Der Baustein VPN geht nicht auf Grundlagen für sichere Netze ein (siehe dazu NET.1.1 *Netzarchitektur und -design*). Auch deckt er nicht alle mit dem Betrieb eines VPNs zusammenhängenden Prozesse ab. So müssen zusätzlich vor allem die Bausteine OPS.1.1.3 *Patch- und Änderungsmanagement*, ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*, CON.1 *Kryptokonzept*, OPS.1.1.5 *Datensicherung*, DER.4 *Notfallmanagement* und OPS.2.4 *Fernwartung* beachtet werden.

Der vorliegende Baustein muss für jede Art von Fernzugriffen auf den Informationsverbund angewendet werden. Hierzu gehören Verbindungen über Datennetze, wie zum Beispiel Site-to-Site-, End-to-End- oder Remote-Access-VPNs, und über Telekommunikationsverbindungen, wie beispielsweise über analoge Wählleitungen, ISDN- oder Mobiltelefone. Es werden in diesem Baustein nur VPN-Systeme für die Schichten 2 (Sicherungsschicht) bis 4 (Transportschicht) des Open-Systems-Interconnection-(OSI)-Modells abgedeckt.

Empfehlungen, wie die Betriebssysteme der VPN-Endpunkte konfiguriert werden können, sind ebenfalls nicht Bestandteil dieses Bausteins. Entsprechende Anforderungen sind im Baustein SYS.1.1 *Allgemeiner Server* beziehungsweise SYS.2.1 *Allgemeiner Client* sowie den jeweiligen betriebssystemspezifischen Bausteinen des IT-Grundschutz-Kompendiums zu finden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich VPN von besonderer Bedeutung:

2.1 Fehlende oder unzureichende Planung und Reglementierung des VPN-Einsatzes

Bei einem nicht sorgfältig geplanten, aufgebauten oder konfigurierten VPN können Sicherheitslücken entstehen, die alle mit dem VPN vernetzten IT-Systeme beeinträchtigen. Angreifern kann es so möglich sein, auf vertrauliche Informationen der Institution zuzugreifen.

So ist es durch eine unzureichende VPN-Planung und Reglementierung beispielsweise möglich, dass die Benutzer nicht ordnungsgemäß geschult wurden und dadurch das VPN in einer unsicheren Umgebung benutzen oder sich von einem unsicheren Client aus einwählen. Dies ermöglicht es Angreifern eventuell, auf das gesamte Firmennetz zuzugreifen.

Auch wenn die regelmäßige Kontrolle der Zugriffe auf das VPN unzureichend geplant wurde, könnten Angriffe nicht rechtzeitig erkannt werden. Somit kann nicht zeitnah reagiert werden und ein Angreifer kann unbemerkt Daten stehlen oder ganze Prozesse sabotieren.

2.2 Unsichere VPN-Dienstleister

VPN-Verbindungen können bis in kritische Bereiche des Netzes hineinreichen. Greift die Institution auf einen VPN-Dienstleister zurück und hat sie diesen nicht sorgfältig ausgewählt, könnte hierdurch das gesamte Netz der Institution unsicher werden. So könnte beispielsweise ein vom Dienstleister unsicher angebotener VPN-Zugang von Angreifern benutzt werden, um gezielt Informationen zu stehlen.

2.3 Probleme bei der lokalen Speicherung der Authentisierungsdaten für VPNs

Viele VPN-Clients für den Fernzugriff erlauben es, die zur Authentisierung notwendigen Daten lokal zu speichern, sodass sie der Benutzer beim erneuten Verbindungsaufbau nicht noch einmal eingeben muss. Wenn es einem Angreifer gelingt, auf den VPN-Client zuzugreifen, kann er eventuell so die Zugangsdaten auslesen und sich als legitimer Benutzer am Netz anmelden. Somit kann er auf die lokalen Netze und die darin erreichbaren Informationen und Dienste der Institution zugreifen.

2.4 Unsichere Konfiguration der VPN-Clients für den Fernzugriff

Wird ein VPN-Client nicht sicher konfiguriert, könnten die Benutzer dessen Sicherheitsmechanismen falsch oder gar nicht benutzen. Auch verändern sie eventuell die Konfiguration des Clients. Ebenso ist es durch eine unsichere Konfiguration möglich, dass vom Benutzer installierte Software auch die Sicherheit des VPN-Clients gefährdet.

2.5 Unsichere Standard-Einstellungen auf VPN-Komponenten

Die Standard-Einstellungen von VPN-Komponenten weisen nicht immer alle Merkmale einer sicheren Installation auf. Oft wird mehr auf Benutzerfreundlichkeit und problemlose Integration in bestehende Systeme als auf Sicherheit geachtet. Wenn VPN-Komponenten nicht oder nur mangelhaft an die konkreten Sicherheitsbedürfnisse der Institution angepasst werden, können daher Schwachstellen und somit gefährliche Angriffspunkte entstehen. So ist beispielsweise das gesamte VPN und damit das interne Netz der Institution angreifbar, wenn vom Hersteller voreingestellte Passwörter nicht geändert werden.

2.6 Diebstahl von mobilen Endgeräten mit VPN-Client

Mobile Endgeräte werden öfter gestohlen oder gehen anderweitig verloren. Dadurch besteht die Gefahr, dass Angreifer über die dort eingerichtete VPN-Verbindung auf das interne Netz der Institution zugreifen können. Oftmals fehlen auch Verlustmeldeprozesse, sodass z. B. ein gestohlener Laptop nicht zeitnah der richtigen Stelle in der Institution gemeldet wird. Dadurch kann sich der Angreifer möglicherweise lange unbemerkt im internen Netz aufhalten und zahlreiche schützenswerte Informationen kopieren.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich VPN aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Informationssicherheitsbeauftragter (ISB)

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

NET.3.3.A1 Planung des VPN-Einsatzes

Vor der Einführung eines VPNs MUSS eine sorgfältige Planung erfolgen. Dabei MÜSSEN die Verantwortlichkeiten für den VPN-Betrieb festgelegt werden. Es MÜSSEN zudem für das VPN Benutzergruppen und deren Berechtigungen geplant werden. Ebenso MUSS definiert werden, wie erteilte, geänderte oder entzogene Zugriffsberechtigungen zu dokumentieren sind.

NET.3.3.A2 Auswahl eines VPN-Dienstleisters [Informationssicherheitsbeauftragter (ISB)]

Mit einem VPN-Dienstleister MÜSSEN Service Level Agreements (SLAs) ausgehandelt und schriftlich dokumentiert werden. Es MUSS regelmäßig kontrolliert werden, ob der VPN-Dienstleister die vereinbaren SLAs einhält.

NET.3.3.A3 Sichere Installation von VPN-Endgeräten

Das zugrundeliegende Betriebssystem der VPN-Plattform MUSS sicher konfiguriert werden. Wird eine Appliance benutzt, MUSS es dafür einen gültigen Wartungsvertrag geben. Es MUSS sichergestellt werden, dass nur qualifiziertes Personal VPN-Komponenten installiert. Die Installation der VPN-Komponenten sowie eventuelle Abweichungen von den Planungsvorgaben SOLLTEN dokumentiert werden. Die Funktionalität und die gewählten Sicherheitsmechanismen des VPN MÜSSEN vor Inbetriebnahme geprüft werden.

NET.3.3.A4 Sichere Konfiguration eines VPNs

Für VPN-Clients, VPN-Server und VPN-Verbindungen MUSS eine sichere Konfiguration festgelegt werden. Diese SOLLTE geeignet dokumentiert werden. Auch MUSS der zuständige Administrator regelmäßig kontrollieren, ob die Konfiguration noch sicher ist und sie eventuell für alle IT-Systeme anpassen.

NET.3.3.A5 Sperrung nicht mehr benötigter VPN-Zugänge

Es MUSS regelmäßig geprüft werden, ob ausschließlich berechtigte IT-Systeme und Benutzer auf das VPN zugreifen können. Nicht mehr benötigte VPN-Zugänge MÜSSEN zeitnah deaktiviert werden. Der VPN-Zugriff MUSS auf die benötigten Benutzungszeiten beschränkt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich VPN. Sie SOLLTEN grundsätzlich umgesetzt werden.

NET.3.3.A6 Durchführung einer VPN-Anforderungsanalyse

Es SOLLTE eine Anforderungsanalyse durchgeführt werden, um für das jeweilige VPN die Einsatzszenarien zu bestimmen und daraus Anforderungen an die benötigte Hard- und Software-Komponenten ableiten zu können. In der Anforderungsanalyse SOLLTEN folgende Punkte betrachtet werden:

- Geschäftsprozesse,
- Zugriffswege,
- Identifikations- und Authentisierungsverfahren,
- Benutzer und Benutzerberechtigungen,
- Zuständigkeiten und
- Meldewege.

NET.3.3.A7 Planung der technischen VPN-Realisierung

Neben der allgemeinen Planung (siehe NET.3.3.A1 *Planung des VPN-Einsatzes*) SOLLTEN die technischen Aspekte eines VPNs sorgfältig geplant werden. So SOLLTEN für das VPN die Verschlüsselungsverfahren, VPN-Endpunkte, erlaubten Zugangsprotokolle, Dienste und Ressourcen festgelegt werden. Zudem SOLLTEN die Teilnetze (siehe NET.1.1 *Netzarchitektur und -design*) definiert werden, die über das VPN erreichbar sind.

NET.3.3.A8 Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung

Es SOLLTE eine Sicherheitsrichtlinie zur VPN-Nutzung erstellt und den Mitarbeitern bekannt gegeben werden. Die Sicherheitsmaßnahmen SOLLTEN im Rahmen von Schulungen erläutert werden. Wird einem Mitarbeiter ein VPN-Zugang eingerichtet, SOLLTE ihm ein Merkblatt mit den wichtigsten VPN-Sicherheitsmechanismen ausgehändigt werden. Alle VPN-Benutzer SOLLTEN verpflichtet werden, die Sicherheitsrichtlinien einzuhalten.

NET.3.3.A9 Geeignete Auswahl von VPN-Produkten

Bei der Auswahl von VPN-Produkten SOLLTEN die Anforderungen der Institutionen an die Vernetzung unterschiedlicher Standorte und die Anbindung mobiler Mitarbeiter oder Telearbeiter berücksichtigt werden.

NET.3.3.A10 Sicherer Betrieb eines VPNs

Für VPNs SOLLTE ein Betriebskonzept erstellt werden. Darin SOLLTEN die Aspekte Qualitätsmanagement, Überwachung, Wartung, Schulung und Autorisierung beachtet werden.

NET.3.3.A11 Sichere Anbindung eines externen Netzes

Wird ein VPN benutzt, um ein externes Netz anzubinden, SOLLTEN dabei nach dem derzeitigen Stand der Technik sicherere Authentisierungs- und Verschlüsselungsverfahren mit ausreichender Schlüssellänge verwendet werden. Auch das gewählte Verfahren zum Schlüsselaustausch SOLLTE dem Stand der Technik entsprechen. Es SOLLTE sichergestellt werden, dass VPN-Verbindungen nur zwischen den hierfür vorgesehenen IT-Systemen und Diensten aufgebaut werden. Die dabei eingesetzten Tunnel-Protokolle SOLLTEN für den Einsatz geeignet sein.

NET.3.3.A12 Benutzer- und Zugriffsverwaltung bei Fernzugriff-VPNs

Für Fernzugriff-VPNs SOLLTE eine zentrale und konsistente Benutzer- und Zugriffsverwaltung gewährleistet werden. Die genutzten Authentisierungsverfahren SOLLTEN die Anforderungen des Bausteins ORP.4 *Identitäts- und Berechtigungsmanagement* erfüllen.

Werden eigenständige Server für die Benutzer- und Zugriffsverwaltung genutzt, SOLLTE sichergestellt sein, dass diese sicher und konsistent zu den Anforderungen des Bausteins ORP.4 *Identitäts- und Berechtigungsmanagement* eingerichtet und betrieben werden. Weiterhin SOLLTEN die eingesetzten Server vor unbefugten Zugriffen geschützt sein.

NET.3.3.A13 Integration von VPN-Komponenten in eine Firewall

Die VPN-Komponenten SOLLTEN in die Firewall integriert werden, damit der Datenverkehr wirksam kontrolliert und gefiltert werden kann. Es SOLLTE dokumentiert werden, wie die VPN-Komponenten in die Firewall integriert sind.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

4 Weiterführende Informationen

4.1 Literatur

- [27033-5] ISO/IEC 27033-5:2013
  Information technology - Security techniques - Network Security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs), ISO, 08.2013
  https://www.iso.org/standard/51584.html

- [ISIVPN] Virtuelles Privates Netz (ISi-VPN)
  BSI-Leitlinie zur Internet Sicherheit (ISi-L), BSI, 2009
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_vpn_leitlinie_pdf.pdf

- [NIST80077] NIST Special Publication 800-77
  Guide to IPsec VPNs, NIST, 12.2005
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-77.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "VPN" von Bedeutung.

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.14 Ausspähen von Informationen (Spionage)

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.28 Software-Schwachstellen oder -Fehler

G 0.32 Missbrauch von Berechtigungen

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.43 Einspielen von Nachrichten

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.09	G 0.11	G 0.14	G 0.18	G 0.19	G 0.22	G 0.23	G 0.28	G 0.32	G 0.40	G 0.43	G 0.46
NET.3.3.A1				x					x			
NET.3.3.A2		x										
NET.3.3.A3	x			x								
NET.3.3.A4			x		x	x	x		x			
NET.3.3.A5								x				
NET.3.3.A6				x			x		x			
NET.3.3.A7			x		x	x	x				x	x
NET.3.3.A8				x								
NET.3.3.A9	x	x								x		
NET.3.3.A10			x		x	x					x	x
NET.3.3.A11	x	x								x		
NET.3.3.A12									x			
NET.3.3.A13			x		x	x					x	x

Bundesamt
für Sicherheit in der
Informationstechnik

INF: Infrastruktur

INF.1	Allgemeines Gebäude	**703**
INF.2	Rechenzentrum sowie Serverraum	**713**
INF.3	Elektrotechnische Verkabelung	**725**
INF.4	IT-Verkabelung	**732**
INF.7	Büroarbeitsplatz	**739**
INF.8	Häuslicher Arbeitsplatz	**745**
INF.9	Mobiler Arbeitsplatz	**751**
INF.10	Besprechungs-, Veranstaltungs- und Schulungsräume	**758**

IT-Grundschutz

INF: Infrastruktur

INF.1 Allgemeines Gebäude

1 Beschreibung

1.1 Einleitung

Gebäude bilden den äußeren physischen Rahmen für die Durchführung von Geschäftsprozessen. Ein Gebäude umfasst die stationären Arbeitsplätze, die verarbeiteten Informationen sowie die aufgestellte Informationstechnik und gewährleistet für diese somit einen äußeren Schutz. Zudem ermöglichen die Infrastruktureinrichtungen eines Gebäudes häufig erst die Durchführung von Geschäftsprozessen und den IT-Betrieb. Daher ist nicht nur das Bauwerk an sich, also Wände, Decken, Böden, Dach, Fenster sowie Türen zu betrachten, sondern auch alle gebäudeweiten Infrastruktur- und Versorgungseinrichtungen wie Strom, Wasser, Gas, Heizung und Kühlung.

Betrachtet wird ein Gebäude, das von einer oder mehreren Organisationseinheiten einer Institution genutzt wird. Diese können durchaus unterschiedliche Sicherheitsansprüche haben. Zudem muss in alle Überlegungen einfließen, dass ein Gebäude fast immer auch von Institutionsfremden (Bürgern, Kunden, Lieferanten) betreten werden kann und soll. Wenn ein Gebäude von verschiedenen Parteien in derartiger Weise genutzt wird, so müssen Gestaltung und Ausstattung des Gebäudes und das Nutzungskonzept für das Gebäude zueinander passen. Es soll eine optimale Umgebung für die im Gebäude tätigen Menschen sichergestellt werden. Unberechtigte sollen dort keinen Zutritt erhalten, wo sie die Sicherheit beeinträchtigen könnten und die im Gebäude stationierte Technik soll sicher und effizient betrieben werden können.

1.2 Zielsetzung

In diesem Baustein wird beschrieben, welche Anforderungen umzusetzen sind, um ein Gebäude aus Sicht der Informationssicherheit optimal zu nutzen. Die sich aus den Anforderungen ergebenden Maßnahmen hängen von Art und Größe der Institution ab. Anforderungen aus diesem Baustein können auch auf große Liegenschaften mit mehreren Gebäuden oder auf die Nutzung einzelner Gebäudeteile in Mehrparteienhäusern übertragen werden.

1.3 Abgrenzung

Dieser Baustein betrachtet technische und nicht-technische Sicherheitsaspekte bei der Planung und Nutzung von typischen Gebäuden für Unternehmen und Behörden. Dabei wird der gesamte Lebenszyklus von Gebäuden betrachtet, beginnend von der Erstellung eines Anforderungskataloges, über Konzeption, Einrichtung, Nutzung bis hin zu Umbauten oder Auszug.

Die Verkabelung in einem Gebäude wird in den Bausteinen INF.3 Elektrotechnische Verkabelung und INF.4 IT-Verkabelung gesondert betrachtet, spezielle Räumlichkeiten wie Serverräume oder Archivräume in den jeweiligen Bausteinen der Schicht INF.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Allgemeines Gebäude von besonderer Bedeutung:

2.1 Feuer

Gebäude und die darin befindlichen Menschen und Einrichtungen können durch Feuer schwere Schäden erleiden. Neben direkten durch das Feuer verursachten Schäden müssen auch Folgeschäden mitbetrachtet werden. Die größte Gefahrenquelle bei einem Feuer ist der giftige Brandrauch. Die meisten Personenschäden bei einem Feuer entstehen durch Rauchvergiftung. Auch an Einrichtungen und IT-Systemen kann Brandrauch schwere Schäden anrichten.

So entstehen bei der Verbrennung von PVC Chlorgase, die zusammen mit der Luftfeuchtigkeit und dem Löschwasser Salzsäure bilden. Werden die Salzsäuredämpfe über die Klimaanlage verteilt, können auf diese Weise Schäden an empfindlichen elektronischen Geräten entstehen, die in einem vom Brandort weit entfernten Teil des Gebäudes stehen.

2.2 Blitz

Blitze sind die wesentliche während eines Gewitters bestehende Gefährdung für Gebäude und die darin befindliche Informationstechnik. Blitze erreichen bei Spannungen von mehreren 100.000 Volt Ströme bis zu 200.000 Ampere. Diese enorme elektrische Energie wird innerhalb von 50-100 Mikrosekunden freigesetzt und abgebaut. Ein Blitz mit diesen Werten, der in einem Abstand von ca. 2 km einschlägt, verursacht auf elektrischen Leitungen im Gebäude immer noch Spannungsspitzen, die zur Zerstörung empfindlicher elektronischer Geräte führen können. Diese indirekten Schäden nehmen mit abnehmender Entfernung zu.

Schlägt der Blitz direkt in ein Gebäude ein, werden durch die dynamische Energie des Blitzes Schäden hervorgerufen. Dies können Beschädigungen des Baukörpers (Dach und Fassade), Schäden durch auftretende Brände oder Überspannungsschäden an elektrischen Geräten sein.

2.3 Wasser

Wasser kann von außen, beispielsweise durch Regen, Hochwasser oder Überschwemmungen, oder durch innen, beispielsweise durch Defekte wasserführender Leitungen, Schäden an einem Gebäude und seinen Einrichtungen verursachen.

2.4 Elementarschäden und Naturkatastrophen

Je nach Standort eines Gebäudes ist dieses den Risiken durch Elementarschäden und Naturkatastrophen unterschiedlich stark ausgesetzt. Ursachen für Naturkatastrophen können seismische, klimatische oder vulkanische Phänomene sein, wie beispielsweise Erdbeben, Hochwasser, Erdrutsche, Tsunamis, Lawinen und Vulkanausbrüche. Beispiele für extreme meteorologische Phänomene sind Unwetter, Orkane oder Zyklone.

2.5 Umfeld-Gefährdungen

Gebäude können durch Ereignisse in der unmittelbaren Umgebung beschädigt oder in ihrer Nutzbarkeit beeinträchtigt werden, beispielsweise unmittelbar durch das Austreten giftiger Substanzen oder mittelbar durch Rettungsarbeiten, Straßensperrungen oder Evakuierungen.

2.6 Unbefugter Zutritt

Wenn Unbefugte in ein Gebäude oder einzelne Räumlichkeiten gelangen, kann dies verschiedene andere Sicherheitsgefährdungen nach sich ziehen. Unbefugte Personen können durch vorsätzliche Handlungen wie beispielsweise Diebstahl oder Manipulation von Informationen oder IT-Systemen, aber auch durch unbeabsichtigtes Fehlverhalten (z. B. aufgrund mangelnder Fachkenntnisse) Schäden verursachen.

Ziel eines Einbruchs kann der Diebstahl von IT-Komponenten oder anderer leicht veräußerbarer Ware sein, aber auch das Kopieren oder die Manipulation von Daten oder IT-Systemen. Dabei können nicht offensichtliche Manipulationen weit höhere Schäden als direkte Zerstörungsakte verursachen. Schon durch das unbefugte Eindringen können Sachschäden entstehen. Fenster und Türen werden gewaltsam geöffnet und dabei beschädigt, sie müssen repariert oder ersetzt werden.

2.7 Verstoß gegen Gesetze oder Regelungen

Bei der Errichtung von Gebäuden ist eine Vielzahl von Gesetzen und Vorgaben zu beachten, die beispielsweise den Brandschutz oder andere Aspekte der baulichen Sicherheit betreffen. Wenn gegen diese verstoßen wird, fällt dieses unter Umständen lange nicht auf, kann aber katastrophale Auswirkungen nach sich ziehen, wenn beispielsweise Brandschottungen nicht bestimmungsgemäß eingebaut wurden.

2.8 Unzureichende Brandschottungen

Jedes Gebäude, in dem IT betrieben wird, ist von einer Vielzahl von Leitungen und Kabeln durchzogen. Frisch- und Abwasserleitungen, Heizungsrohre, Energieversorgung und Datenübertragung seien als Beispiele genannt. Es ist dabei unvermeidlich, dass solche Rohr- und Kabel-Trassen Brandschutzwände und Geschossdecken queren müssen. Wenn an solchen Stellen keine geeigneten Brandschottungen eingebaut sind, können sich hierüber unter Umständen Brände und Rauch unkontrolliert ausbreiten.

Die hohe Dynamik der IT macht auch im Leitungsnetz immer wieder Nachverlegungen auch über Brandschotts hinweg erforderlich. In welcher Form das korrekt erfolgen kann, ist unmittelbar von dem vorhandenen Schott abhängig und kann sehr unterschiedlich sein. Werden Änderung an einem Brandschott nicht den Vorgaben des jeweiligen Schott-Herstellers entsprechend ausgeführt, besteht die Gefahr, dass es im Fall einer Brandbelastung versagen und der Brand sich so in eigentlich durch das Schott geschützte Bereich ausweiten kann.

2.9 Ausfall der Stromversorgung

Bei einem Stromausfall können ganze Gebäude oder Teile davon unbenutzbar werden. Von der Stromversorgung sind nicht nur die offensichtlichen, direkten Stromverbraucher wie IT oder Beleuchtung abhängig, auch alle Infrastruktureinrichtungen sind heute direkt oder indirekt vom Strom abhängig, z. B. Aufzüge, Klimatechnik, Gefahrenmeldeanlagen, Sicherheitsschleusen, automatische Türschließanlagen, Sprinkleranlagen, Telefonnebenstellenanlagen. Selbst die Wasserversorgung ist in Hoch- oder Tiefgeschossen wegen der zur Druckerzeugung erforderlichen Pumpen Strom abhängig.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich Allgemeines Gebäude aufgeführt. Grundsätzlich ist die Haustechnik für die Erfüllung der Anforderungen zuständig, also die Organisationseinheit, die für die Einrichtungen der Infrastruktur in einem Gebäude oder in einer Liegenschaft verantwortlich ist. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Haustechnik
Weitere Verantwortliche	Bauleiter, Errichterfirma, Informationssicherheitsbeauftragter (ISB), Innerer Dienst, Institutionsleitung, Leiter Organisation, Mitarbeiter, Planer

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

INF.1.A1 Planung der Gebäudeabsicherung [Planer, Informationssicherheitsbeauftragter (ISB)]

Ausgehend von der geplanten oder vorhandenen Nutzung eines Gebäudes und des Schutzbedarf der dort betriebenen Geschäftsprozesse MUSS festgelegt werden, wie das Gebäude abzusichern ist. Bei einem Gebäude MÜSSEN viele verschiedene Sicherheitsaspekte zum Schutz von Personen im Gebäude, dem Schutz der Wirtschaftsgüter und der IT beachtet werden, von Brandschutz über Elektrik bis hin zur Zutrittskontrolle. Die Sicherheitsanforderungen aus den verschiedenen Bereichen MÜSSEN miteinander abgestimmt werden.

INF.1.A2 Angepasste Aufteilung der Stromkreise

Es MUSS regelmäßig überprüft werden, ob die Absicherung und Auslegung der Stromkreise noch den tatsächlichen Bedürfnissen genügen.

INF.1.A3 Einhaltung von Brandschutzvorschriften

Die bestehenden Brandschutzvorschriften sowie die Auflagen der Bauaufsicht MÜSSEN eingehalten werden. Die Fluchtwege MÜSSEN vorschriftsmäßig ausgeschildert und offen gehalten werden. Die örtliche Feuerwehr SOLLTE bei der Brandschutzplanung hinzugezogen werden. Die aus der Bauordnung erwachsenden Vorschriften zum Brandschutz sind für die Anforderungen des Brandschutzes der IT nicht ausreichend. Daher MUSS ein IT-bezogenes Brandschutzkonzept erstellt und umgesetzt werden.

Unnötige Brandlasten MÜSSEN vermieden werden. Dazu gehört die regelmäßige Entsorgung von Altpapier und Verpackungsabfällen.

Es MUSS einen Brandschutzbeauftragten oder eine mit dem Aufgabengebiet betraute Person geben, die auch entsprechend geschult ist.

INF.1.A4 Branderkennung in Gebäuden [Planer]

Gebäude MÜSSEN mit einer ausreichenden Anzahl von Rauchmeldern ausgestattet sein. Bei größeren Gebäuden SOLLTE eine Brandmeldezentrale (BMZ) eingesetzt werden, auf die alle Melder aufgeschaltet sind. Bei Rauchdetektion MUSS eine Alarmierung im Gebäude ausgelöst werden, bei der sichergestellt ist, dass alle im Gebäude anwesenden Personen diese wahrnehmen können. Die Funktionsfähigkeit aller Rauchmelder bzw. aller Komponenten einer Brandmeldeanlage MUSS regelmäßig überprüft werden. Es MUSS regelmäßig kontrolliert werden, dass die Fluchtwege benutzbar und frei von Hindernissen sind, damit das Gebäude in einer Gefahrensituation schnell geräumt werden kann.

INF.1.A5 Handfeuerlöscher

Zur Sofortbekämpfung von Bränden MÜSSEN Handfeuerlöscher in der jeweils geeigneten Brandklasse (DIN EN 3 Tragbare Feuerlöscher) in ausreichender Zahl und Größe im Gebäude zur Verfügung stehen. Die Handfeuerlöscher MÜSSEN regelmäßig geprüft und gewartet werden. Die Mitarbeiter SOLLTEN in die Benutzung der Handfeuerlöscher eingewiesen worden sein.

INF.1.A6 Geschlossene Fenster und Türen [Mitarbeiter]

Fenster und nach außen gehende Türen (Balkone, Terrassen) MÜSSEN in Zeiten, in denen ein Raum nicht besetzt ist, geschlossen werden. Hierfür MUSS es eine entsprechende Anweisung geben. Es MUSS regelmäßig überprüft werden, ob die Fenster und Türen nach Verlassen der Räume verschlossen sind. Brand- und Rauchschutztüren DÜRFEN NICHT dauerhaft offen gehalten werden.

INF.1.A7 Zutrittsregelung und -kontrolle [Leiter Organisation]

Der Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen MUSS geregelt und kontrolliert werden. Es SOLLTE ein Konzept für die Zutrittskontrolle existieren. Die Zahl der zutrittsberechtigten Personen SOLLTE für jeden Bereich auf ein Mindestmaß reduziert werden. Weitere Personen DÜRFEN erst nach

vorheriger Prüfung der Notwendigkeit Zutritt erhalten. Alle erteilten Zutrittsberechtigungen SOLLTEN dokumentiert werden. Die Zutrittskontroll-Maßnahmen MÜSSEN regelmäßig auf ihre Wirksamkeit überprüft werden.

INF.1.A8 Rauchverbot [Mitarbeiter]

Für Räume mit IT oder Datenträgern (Serverraum, Datenträgerarchiv, aber auch Belegarchiv), in denen Brände oder Verschmutzungen zu hohen Schäden führen können, MUSS ein Rauchverbot erlassen werden. Es MUSS regelmäßig kontrolliert werden, dass bei Einrichtung oder Duldung von Raucherzonen der Zutrittsschutz nicht ausgehebelt wird.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Allgemeines Gebäude. Sie SOLLTEN grundsätzlich umgesetzt werden.

INF.1.A9 Sicherheitskonzept für die Gebäudenutzung [Planer, Informationssicherheitsbeauftragter (ISB)]

Es SOLLTE ein Sicherheitskonzept für die Gebäudenutzung geben. Das Sicherheitskonzept für das Gebäude SOLLTE mit dem Gesamt-Sicherheitskonzept der Institution abgestimmt sein. Es SOLLTE regelmäßig aktualisiert werden.

Schützenswerte Räume oder Gebäudeteile SOLLTEN nicht in exponierten oder besonders gefährdeten Bereichen untergebracht sein.

INF.1.A10 Einhaltung einschlägiger Normen und Vorschriften [Errichterfirma, Bauleiter]

Bei Planung, Errichtung und Umbau von Gebäuden sowie dem Einbau von technischen Einrichtungen SOLLTEN alle relevanten Normen und Vorschriften berücksichtigt werden.

INF.1.A11 Abgeschlossene Türen [Mitarbeiter]

Mitarbeiter SOLLTEN angewiesen werden, bei Abwesenheit ihr Büro zu verschließen oder ihre Arbeitsunterlagen wegzuschließen. Es SOLLTE sporadisch überprüft werden, ob dies umgesetzt wird.

INF.1.A12 Schlüsselverwaltung

Für alle Schlüssel des Gebäudes (von Etagen, Fluren und Räumen) SOLLTE ein Schließplan vorliegen. Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln SOLLTE zentral geregelt sein. Reserveschlüssel SOLLTEN vorgehalten und gesichert, aber für Notfälle griffbereit aufbewahrt werden. Nicht ausgegebene Schlüssel SOLLTEN sicher aufbewahrt werden. Jede Schlüsselausgabe SOLLTE dokumentiert werden.

INF.1.A13 Regelungen für Zutritt zu Verteilern

Der Zutritt zu den Verteilern aller Versorgungseinrichtungen in einem Gebäude SOLLTE im Bedarfsfall schnell möglich sein. Der Zutritt zu Verteilern SOLLTE auf einen engen Kreis von Berechtigten beschränkt sein.

INF.1.A14 Blitzschutzeinrichtungen

Es SOLLTE eine Blitzschutzanlage nach geltender Norm installiert sein. Es SOLLTE ein umfassendes Blitz- und Überspannungsschutzkonzept vorhanden sein. Die Fangeinrichtungen bei Gebäuden mit umfangreicher IT-Ausstattung SOLLTEN mindestens der Schutzklasse II gemäß DIN EN 62305 "Blitzschutz" entsprechen. Die Blitzschutzanlage SOLLTE regelmäßig geprüft und gewartet werden.

INF.1.A15 Lagepläne der Versorgungsleitungen

Es SOLLTEN aktuelle Lagepläne aller Versorgungsleitungen existieren. Es SOLLTE geregelt sein, wer die Lagepläne aller Versorgungsleitungen führt und aktualisiert. Die Pläne SOLLTEN so aufbewahrt werden, dass ausschließlich berechtigte Personen darauf zugreifen können, sie aber im Bedarfsfall schnell verfügbar sind.

INF.1.A16 Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile

Lagehinweise auf schutzwürdige Bereiche SOLLTEN vermieden werden. Schutzwürdige Gebäudebereiche SOLLTEN von außen nicht leicht einsehbar sein.

INF.1.A17 Baulicher Rauchschutz [Planer]

Der bauliche Rauchschutz SOLLTE nach Installations- und Umbauarbeiten überprüft werden. Die Funktionsfähigkeit der Rauchschutz-Komponenten SOLLTE regelmäßig überprüft werden.

INF.1.A18 Brandschutzbegehungen

Brandschutzbegehungen SOLLTEN regelmäßig, mindestens ein- bis zweimal im Jahr stattfinden. Bei Brandschutzbegehungen festgestellte Mängel SOLLTEN unverzüglich behoben werden.

INF.1.A19 Frühzeitige Information des Brandschutzbeauftragten

Der Brandschutzbeauftragten SOLLTE über Arbeiten an Leitungstrassen, Fluren, Flucht- und Rettungswegen informiert werden. Er SOLLTE die ordnungsgemäße Ausführung von Brandschutzmaßnahmen kontrollieren.

INF.1.A20 Alarmierungsplan und Brandschutzübungen

Es SOLLTE ein Alarmierungsplan für die im Brandfall zu ergreifenden Maßnahmen erstellt werden. Er SOLLTE periodisch aktualisiert werden. Brandschutzübungen SOLLTEN regelmäßig durchgeführt werden. Der Alarmierungsplan SOLLTE in regelmäßigen Abständen überprüft und aktualisiert werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

INF.1.A21 Unabhängige elektrische Versorgungsstränge (A)

Die IT SOLLTE über zwei voneinander unabhängige Versorgungsstränge gespeist werden.

INF.1.A22 Sichere Türen und Fenster (CIA)

Türen und Fenster SOLLTEN anhand der Schutzziele des zu sichernden Bereichs und dem Schutzbedarf der Institution sowie der passenden Klassifizierung in den einschlägigen Normen ausgewählt werden. Alle raumumschließenden Sicherungsmaßnahmen durch Fenster, Türen und Wände SOLLTEN in Bezug auf Einbruch, Brand und Rauch gleichwertig und angemessen sein. Es SOLLTE regelmäßig überprüft werden, dass die Sicherheitstüren und -fenster funktionstüchtig sind.

INF.1.A23 Bildung von Sicherheitszonen [Planer] (C)

Räume ähnlichen Schutzbedarfs SOLLTEN in Zonen zusammengefasst werden, um vergleichbare Risiken einheitlich behandeln und Kosten für erforderliche Sicherheitsmaßnahmen reduzieren zu können. Es SOLLTE ein Sicherheitszonenkonzept für Gebäude und Grundstück entwickelt und dokumentiert werden.

INF.1.A24 Selbsttätige Entwässerung (A)

Alle wassergefährdeten Bereiche SOLLTEN mit einer selbsttätigen Entwässerung ausgestattet sein. Die Funktionstüchtigkeit aktiver und passiver Entwässerungseinrichtungen SOLLTE regelmäßig geprüft werden.

INF.1.A25 Geeignete Standortauswahl [Institutionsleitung] (A)

Bei Auswahl oder Planung eines Gebäude-Standortes SOLLTE geprüft werden, welche Umfeldbedingungen Einfluss auf die Informationssicherheit haben könnten. Es SOLLTE eine Übersicht über standortbedingte Gefährdungen geben. Diesen Gefährdungen SOLLTE mit zusätzlichen kompensierenden Maßnahmen begegnet werden.

INF.1.A26 Pförtner- oder Sicherheitsdienst (CIA)

Die Aufgaben des Pförtner- bzw. Sicherheitsdienstes SOLLTEN klar dokumentiert sein. Die Pförtner SOLLTEN alle Personenbewegungen an der Pforte und an allen anderen Eingängen beobachten bzw. kontrollieren. Alle Mitarbeiter und Besucher SOLLTEN sich bei den Pförtnern legitimieren. Besucher SOLLTEN zu den Besuchten begleitet bzw. an der Pforte abgeholt werden. Die Pförtner SOLLTEN rechtzeitig darüber informiert werden, wenn sich Zutrittsberechtigungen ändern.

INF.1.A27 Einbruchsschutz (CIA)

Es SOLLTEN ausreichende und den örtlichen Gegebenheiten angepasste Maßnahmen zum Einbruchsschutz umgesetzt werden. Gleichwertigkeit und Durchgängigkeit des Einbruchsschutzes bei der Planung, der Umsetzung und im Betrieb SOLLTEN regelmäßig durch eine fachkundige Person begutachtet werden. Die Regelungen zum Einbruchsschutz SOLLTEN den Mitarbeitern bekannt sein.

INF.1.A28 Klimatisierung für Menschen (IA)

In größeren Gebäuden SOLLTE die Luftversorgung durch raumlufttechnische (RLT-) Anlagen geleistet werden. Die RLT-Anlagen SOLLTEN auf die tatsächliche Nutzung des Gebäudes ausgelegt sein. Sie SOLLTEN RLT-Anlagen regelmäßig gewartet werden.

INF.1.A29 Organisatorische Vorgaben für die Gebäudereinigung (CIA)

Es SOLLTE kontrolliert werden, ob die Mitarbeiter der beauftragten Reinigungsfirma die ausgegebenen Schlüssel bzw. Ausweise vertragsgemäß verwenden. Die Reinigungskräfte SOLLTEN über den Umgang mit der IT ausreichend informiert sein. Reinigungskräfte SOLLTEN in besonders sensitiven Bereichen bei der Arbeit beaufsichtigt werden.

INF.1.A30 Auswahl eines geeigneten Gebäudes (CIA)

Bei der Auswahl eines geeigneten Gebäudes SOLLTE geprüft werden, ob alle für die spätere Nutzung relevanten Sicherheitsanforderungen auch umgesetzt werden können. Für jedes Gebäude SOLLTEN im Vorfeld die vorhandenen Gefährdungen und die erforderlichen schadensvorbeugenden oder -reduzierenden Maßnahmen dokumentiert werden.

INF.1.A31 Auszug aus Gebäuden [Innerer Dienst] (C)

Im Vorfeld des Auszugs SOLLTE ein Bestandsverzeichnis aller für die Informationssicherheit relevanten Dinge (Hardware, Software, Datenträger, Ordner, Schriftstücke etc.) erstellt werden. Nach dem Auszug SOLLTEN alle Räume nach zurückgelassenen Dingen durchsucht werden.

INF.1.A32 Brandschott-Kataster (A)

Es SOLLTE ein Brandschott-Kataster geführt werden. In diesem SOLLTEN alle Arten von Schotts individuell aufgenommen werden. Nach Arbeiten an Brandschotts SOLLTEN die Änderungen im Kataster spätestens nach 4 Wochen eingetragen werden.

INF.1.A33 Anordnung schützenswerter Gebäudeteile (CIA)

Schützenswerte Räume oder Gebäudeteile SOLLTEN NICHT in exponierten oder besonders gefährdeten Bereichen untergebracht sein. Falls sich schützenswerte Räume in exponierter Lage befinden, SOLLTEN ausreichende Maßnahmen ergriffen werden, sie zu sichern. Dies SOLLTE dokumentiert werden.

INF.1.A34 Gefahrenmeldeanlage (A)

Es SOLLTE eine den Räumlichkeiten und den Risiken angemessene Gefahrenmeldeanlage geben. Die Gefahrenmeldeanlage SOLLTE regelmäßig gewartet bzw. geprüft werden. Es SOLLTE geprüft werden, ob die Empfänger von Gefahrenmeldungen in der Lage sind, technisch und personell angemessen auf den Alarm zu reagieren.

4 Weiterführende Informationen

4.1 Literatur

- [27001A11] ISO/IEC 27001:2013 - Annex A.11 Physical and enviornmental security
  ISO, Information technology - Security techniques - Information security management systems - Requirements, insbesondere Annex A, A.11 Physical and environmental security, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [ISFCF19] The Standard of Good Practice - AREA CF19 Physical and Environmental Security
  insbesondere AREA CF19 Physical and Environmental Security, ISF, 06.2014

- [NIST80053PEP] NIST Special Publication 800-53 Revision 4 - APPENDIX PAGE F-213
  Assesing Security and Privacy Controls for Federal Information Systems and Organizations, insbesondere APPENDIX F-PS PAGE F-213, FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION, NIST, 2013
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Allgemeines Gebäude" von Bedeutung.

G 0.01 Feuer

G 0.02 Ungünstige klimatische Bedingungen

G 0.03 Wasser

G 0.04 Verschmutzung, Staub, Korrosion

G 0.05 Naturkatastrophen

G 0.06 Katastrophen im Umfeld

G 0.07 Großereignisse im Umfeld

G 0.08 Ausfall oder Störung der Stromversorgung

G 0.10 Ausfall oder Störung von Versorgungsnetzen

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.34 Anschlag

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

Elementare Gefährdungen Anforderungen	G 0.01	G 0.02	G 0.03	G 0.04	G 0.05	G 0.06	G 0.07	G 0.08	G 0.10	G 0.16	G 0.18	G 0.29	G 0.34	G 0.44
INF.1.A1	x	x	x	x	x	x	x	x	x		x	x	x	x
INF.1.A2								x						
INF.1.A3	x			x	x	x					x	x		
INF.1.A4	x										x	x		
INF.1.A5	x										x	x		
INF.1.A6			x				x			x				x
INF.1.A7							x			x				x
INF.1.A8	x			x										
INF.1.A9		x					x			x	x		x	x
INF.1.A10											x	x		
INF.1.A11										x				x
INF.1.A12	x		x							x	x			x
INF.1.A13								x	x					x
INF.1.A14	x				x			x	x		x			
INF.1.A15								x	x					
INF.1.A16													x	
INF.1.A17	x										x	x		
INF.1.A18	x			x							x	x		
INF.1.A19	x										x			
INF.1.A20	x				x	x							x	
INF.1.A21								x	x					
INF.1.A22	x						x			x			x	x
INF.1.A23							x			x			x	x
INF.1.A24			x		x									
INF.1.A25		x	x		x	x		x	x		x			
INF.1.A26										x				x
INF.1.A27										x				x
INF.1.A28		x												
INF.1.A29				x				x		x				x
INF.1.A30		x	x		x	x		x	x		x			x
INF.1.A31										x	x			x
INF.1.A32														
INF.1.A33														
INF.1.A34	x													

INF: Infrastruktur

INF.2 Rechenzentrum sowie Serverraum

1 Beschreibung

1.1 Einleitung

Heute werden fast alle strategischen und operativen Funktionen und Aufgaben durch Informationstechnik (IT) maßgeblich unterstützt oder sind ohne IT nicht auszuführen. Dadurch steigen die Anforderungen an die Leistungsfähigkeit und Verfügbarkeit der IT-Systeme und deren Anbindung an die Netzumgebung stetig. Um diesem Leistungsbedarf gerecht zu werden, um entsprechende Reserven vorzuhalten und um die IT auch wirtschaftlich betreiben zu können, konzentrieren Behörden und Unternehmen jeglicher Größe ihre IT-Landschaft in Rechenzentren.

Ein Rechenzentrum (RZ) ist wie folgt definiert:

1. Hat eine IT-nutzende Institution nur einen zentralen IT-Betriebsbereich, ist dieser gemeinsam mit den erforderlichen Supportbereichen grundsätzlich immer wie ein RZ entsprechend dem Schutzbedarf zu behandeln. Unter "IT-Betriebsbereich" sind Räume zu verstehen, in denen die Hardware aufgebaut ist und betrieben wird, die der Bereitstellung von Diensten und Daten dient. Das RZ umfasst neben dem IT-Betriebsbereich alle weiteren technischen Supportbereiche (Stromversorgung, Kälteversorgung, Löschtechnik, Sicherheitstechnik etc.), die dem bestimmungsgemäßen Betrieb und der Sicherheit des IT-Betriebsbereichs dienen.
2. Wird die IT der Institution innerhalb eines Gebäudes oder einer Liegenschaft verteilt in mehreren Bereichen betrieben und sind diese Bereiche untereinander und zu den IT-Nutzern hin durch hauseigene LAN-Verbindungen angeschlossen, ist mindestens der funktional bedeutendste dieser Bereiche als RZ zu behandeln. Des Weiteren sind Bereiche, von deren ordnungsgemäßem Betrieb 50 % und mehr Nutzer abhängig sind oder aus denen heraus 50 % und mehr an Diensten und Daten (gemessen an der Gesamtheit der Bereiche) bereitgestellt werden, als RZ zu behandeln.
3. Ist die IT-nutzende Institution an mehreren, räumlich voneinander getrennten Standorten angesiedelt und sind diese durch andere als hauseigene LAN-Verbindungen miteinander gekoppelt, ist jeder der Standorte entsprechend (1) separat zu betrachten und zu behandeln.
4. Ein IT-Betriebsbereich, in dem für kritische Geschäftsprozesse (Prozesse, deren Störung oder Ausfall zu wesentlichen Beeinträchtigungen der Erledigung primärer Aufgaben einer Institution führen) erforderliche IT angesiedelt ist, ist immer als RZ zu behandeln, unabhängig von Größe oder Anteilsregeln aus Nummer (2).
5. IT-Betriebsbereiche, aus denen heraus Dienste oder Dienstleistungen für Dritte erbracht werden, sind immer als RZ zu betrachten. Dabei ist es unerheblich, ob dies gegen Entgelt erfolgt oder nicht.
6. Besteht ein begründetes Interesse, einen IT-Betriebsbereich gemeinsam mit seinem Supportbereich abweichend von den vorgenannten Regelungen als Serverraum zu behandeln, ist dies samt der sich daraus ergebenden Reduzierungen von Sicherheitsanforderungen zu begründen.

Weicht ein Rechenzentrum von dieser Definition ab, wird der betrachtete IT-Betriebsbereich als Serverraum bezeichnet. Diese Definition orientiert sich ausschließlich an der Bedeutung der IT-Struktur für die Aufgabenerfüllung der nutzenden Institution und steht damit im methodischen Einklang mit der DIN EN 50600.

Soll ein Serverraum abgesichert werden, können die Anforderungen dieses Bausteins entsprechend reduziert werden. Dies muss jedoch stichhaltig und nachvollziehbar begründet werden (entsprechend 6.) und es müssen mindestens die Basis-Anforderungen umgesetzt werden.

1.2 Zielsetzung

Der Baustein richtet sich einerseits an Institutionen, die ein Rechenzentrum betreiben und im Rahmen einer Revision prüfen möchten, ob sie geeignete Sicherheitsmaßnahmen umgesetzt haben. Andererseits kann der Baustein auch dazu benutzt werden, die Sicherheitsmaßnahmen abzuschätzen, die umgesetzt werden müssen, wenn die IT in einem Rechenzentrum zentralisiert werden soll. Das oberste Ziel der in diesem Baustein beschriebenen Anforderungen ist es, den sicheren Betrieb des Rechenzentrums aufrechtzuerhalten.

1.3 Abgrenzung

Gegenstand dieses Bausteins sind nur Rechenzentren mittlerer Art und Güte. Die hier beschriebenen Sicherheitsanforderungen reichen nicht aus, um Hochsicherheitsrechenzentren, wie sie beispielsweise im Bankenbereich eingesetzt werden, zu schützen. Ein Hochsicherheitsrechenzentrum unterscheidet sich vor allem in den Punkten Hochverfügbarkeit, Desastertoleranz, Redundanz der Komponenten, Widerstandsfähigkeit gegen Elementarschäden, Energie-Effizienz und Datensicherheit von den hier betrachteten mittleren Rechenzentren.

Weiterhin eignet sich der vorliegende Baustein nicht für kleine Informationsverbünde mit z. B. nur einem oder sehr wenigen Servern oder IT-Systemen. Ein Beispiel hierfür ist kleines, mittelständisches Unternehmen (KMU) mit wenigen IT-Arbeitsplätzen und einem Server, der in einem separaten Raum steht. In solchen Fällen genügt es oft, den Baustein INF.6 *Schutzschrank/Technikraum* umzusetzen.

Um den Baustein überschaubar zu halten, wurde bewusst auf technische Details und planerische Größen verzichtet. Nähere Informationen liefern einschlägige Normen, z. B. DIN EN 50600.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für Rechenzentren von besonderer Bedeutung:

2.1 Fehlerhafte Planung

Wenn ein Rechenzentrum konzipiert und dabei nicht berücksichtigt wird, es gegen elementare Gefährdungen abzusichern, besteht ein sehr hohes Ausfallrisiko. So können z. B. Standortrisiken wie Luftverkehr, Erdbeben, Hochwasser oder politische Gesichtspunkte die Betriebssicherheit und Verfügbarkeit gefährden. Ebenso massiv kann es sich auf den Betrieb eines neuen Rechenzentrums auswirken, wenn durch eine fehlerhafte Konzeptionierung nicht genügend Bandbreite verfügbar ist oder die Energieversorgung am gewählten Standort nicht ausreicht.

2.2 Unberechtigter Zutritt

Fehlen Zutrittskontrollen oder sind diese unzureichend, erhöht sich die Gefahr, dass unberechtigte Personen das Rechenzentrum betreten und dort fahrlässig, z. B. aufgrund mangelnder Fachkenntnisse, oder vorsätzlich Schaden anrichten. Angreifer können so z. B. schützenswerte Daten entwenden, Geräte stehlen oder Server manipulieren. Unzureichende Zutrittskontrollen wirken sich somit besonders auf die Verfügbarkeit, Vertraulichkeit und die Integrität von Daten beziehungsweise IT-Komponenten aus.

2.3 Unzureichende Überwachung

Wird die im Rechenzentrum betriebene IT und Infrastruktur unzureichend überwacht und betreut, können Komponenten unbemerkt ausfallen. Dadurch wird eventuell die Verfügbarkeit und fehlerfreie Funktion des Rechenzentrums stark beeinträchtigt. Ausfälle treten zudem oftmals schleichend ein. Ohne eine aktive Überwachung könnten diese zu spät bemerkt werden. Es ist dann oft nicht mehr möglich, rechtzeitig zu reagieren.

2.4 Unzureichende Klimatisierung im Rechenzentrum

IT-Komponenten benötigen eine bestimmte Betriebstemperatur, um korrekt zu funktionieren. Auch setzen sie ihre Energie in zusätzliche Wärme um. Wenn ein Rechenzentrum nicht oder nur unzureichend klimatisiert wird, können die klimatischen Bedingungen im Raum nicht stabil gehalten werden. Ist es dort zu kalt oder zu heiß, unter- oder überschreiten die Geräte eventuell ihre zulässige Betriebstemperatur. Die Folgen sind z. B. Fehlfunktionen und Ausfälle von technischen Komponenten oder auch beschädigte Speichermedien.

2.5 Feuer

Verfügt ein Rechenzentrum über keinen oder nur über einen unzureichenden Brandschutz, besteht die Gefahr, dass ein Feuer entstehen und sich schnell ausbreiten kann. Durch Feuer und Rauch können große Schäden entstehen. Auch lassen sich Brandüberschläge eventuell nicht frühzeitig verhindern.

2.6 Wasser

Durch Undichtigkeiten in der Infrastruktur des Rechenzentrums, Hochwasser, Rohrbruch, defekte Sprinkleranlagen, Kanalisationsschäden oder auch Klimaanlagendefekte kann Wasser in das Rechenzentrum eintreten. Das kann dazu führen, dass Geräte beschädigt werden oder nicht mehr funktionieren. Auch könnte so ein Kurzschluss ausgelöst werden, der zum Totalausfall führt oder sogar einen Brand verursacht.

2.7 Fehlender oder unzureichender Einbruchsschutz

Ein fehlender oder mangelhafter Einbruchsschutz macht es unbefugten Personen leicht, in ein Rechenzentrum einzudringen. Täter können so z. B. IT-Komponenten stehlen oder manipulieren und an vertrauliche Informationen gelangen. Auch könnten sie die Geräte zerstören oder das Rechenzentrum insgesamt beschädigen.

2.8 Ausfall der Stromversorgung

Wenn der Strom ausfällt und es keine redundante Stromversorgung gibt, kann das zu erheblichen Störungen im Betriebsablauf eines Rechenzentrums und damit der Institution führen. So sind bei einem Stromausfall alle vom Rechenzentrum bereitgestellten IT-Services plötzlich nicht erreichbar. Auch können Daten verloren gehen. Weiterhin ist es möglich, dass durch einen plötzlichen Stromausfall IT-Systeme, aktive Netzkomponenten, TK-Systeme oder Überwachungstechnik beschädigt werden.

2.9 Verschmutzung

Staub und andere Verschmutzungen in einem Rechenzentrum können dazu führen, dass die Technik nicht mehr funktioniert. Durch Verschmutzungen fällt sie häufiger aus und verschleißt früher.

2.10 Unzureichende Trassendimensionierung

Wenn Kabeltrassen nicht getrennt geführt und Mindestabstände nicht eingehalten werden, können Störungen der IT des Rechenzentrums auftreten. Auch Erweiterungen des Netzes können problematisch sein, sodass der Schutz vor Feuer- und Rauchentwicklungen eventuell nicht mehr gewährleistet ist. Auch ist zu beachten, dass Löcher für Kabeldurchführungen in Brandwänden nur mit 60 % des Querschnitts

mit Kabeln belegt werden dürfen. 40 % müssen mit Brandschutzmörtel oder einem anderen für Brandschotte zugelassenen Material gefüllt werden. Wird diese Vorschrift nicht beachtet, kann ein Brand aus dem benachbarten Raum zu leicht auf das RZ übergreifen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz von Rechenzentren aufgeführt. Grundsätzlich ist der Leiter IT dafür zuständig, die Anforderungen zu erfüllen. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	Leiter IT
Weitere Verantwortliche	Datenschutzbeauftragter, Haustechnik, IT-Betrieb, Informationssicherheitsbeauftragter (ISB), Mitarbeiter, Planer, Wartungspersonal

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

INF.2.A1 Festlegung von Anforderungen [Planer, IT-Betrieb, Haustechnik, Informationssicherheitsbeauftragter (ISB)]

Für ein Rechenzentrum MÜSSEN angemessene technische und organisatorische Vorgaben definiert und umgesetzt werden.

Wenn ein Rechenzentrum geplant wird oder geeignete Räumlichkeiten ausgewählt werden, MÜSSEN potenzielle Gefährdungen durch Umgebungseinflüsse sowie das Sicherheitsniveau der IT-Komponenten (insbesondere Verfügbarkeit) mitbetrachtet werden. Weiterhin MÜSSEN auch Schutzmaßnahmen vor potenziellen internen und externen Angriffen in die Gesamtbetrachtung einfließen.

Ein Rechenzentrum MUSS insgesamt als geschlossener Sicherheitsbereich konzipiert werden. Es MUSS zudem unterschiedliche Sicherheitszonen aufweisen. Hierfür MÜSSEN Verwaltungs-, Logistik-, Technik- und IT-Flächen klar voneinander getrennt werden. Im Falle eines Serverraums SOLLTE geprüft werden, ob unterschiedliche Sicherheitszonen umsetzbar sind.

Auch MUSS darauf geachtet werden, dass Versorgungsleitungen (z. B. für Wasser oder Gas) möglichst nicht in unmittelbarer Nähe von schutzbedürftigen Technikkomponenten verlaufen. Vorhandene Versorgungsleitungen MÜSSEN zumindest an den kritischen Stellen regelmäßig überprüft werden, ob sie noch dicht sind.

INF.2.A2 Bildung von Brandabschnitten [Planer]

Es MÜSSEN geeignete Brandabschnitte für die Räumlichkeiten eines Rechenzentrums festgelegt werden. Schutzziel für die Brandwand bzw. den Brandabschnitt MUSS nicht nur der Personen- und Gebäudeschutz, sondern auch der Schutz des Inventars und dessen Verfügbarkeit sein. Somit MUSS nicht nur verhindert werden, dass sich ein Brand durch Flammen und heiße Rauchgase ausbreitet, sondern es MÜSSEN auch die Wärmestrahlung und die Ausbreitung von kaltem Rauch blockiert werden. Im Falle eines Serverraums SOLLTE geprüft werden, ob geeignete Brandabschnitte für die Räumlichkeiten umsetzbar sind.

INF.2.A3 Einsatz einer unterbrechungsfreien Stromversorgung [Haustechnik]

Für alle betriebsrelevanten Komponenten des Rechenzentrums MUSS eine unterbrechungsfreie Stromversorgung (USV) installiert werden. Da der Leistungsbedarf von Klimatisierungsanlagen oft zu hoch für eine USV ist, MUSS aber mindestens die Steuerung der Anlagen an die unterbrechungsfreie Stromversorgung angeschlossen werden. Im Falle eines Serverraums SOLLTE je nach Verfügbarkeitsanforderungen der IT-Systeme geprüft werden, ob der Betrieb einer USV notwendig ist.

Die USV MUSS ausreichend dimensioniert sein, sodass alle Komponenten bei einem Ausfall der Versorgung so lange mit Strom versorgt werden, dass kein Datenverlust entsteht.

Bei relevanten Änderungen MUSS überprüft werden, ob die vorhandenen USV-Systeme noch ausreichend dimensioniert sind. Die Batterie der USV MUSS im erforderlichen Temperaturbereich gehalten werden und vorzugsweise in einem getrennten Bereich platziert sein.

Die USV MUSS regelmäßig gewartet und auf Funktionsfähigkeit getestet werden. Dafür MÜSSEN die vom Hersteller vorgesehenen Wartungsintervalle eingehalten werden *(siehe INF.2.A10 Inspektion und Wartung der Infrastruktur)*. Um sicherzustellen, dass die USV die erforderliche Stützzeit bereitstellt, MUSS regelmäßig sowie zusätzlich, wenn sich bei den Verbrauchern etwas ändert, die tatsächliche Stützzeit ermittelt werden.

Wenn IT-Geräte über eine USV versorgt werden, DÜRFEN diese NICHT über geschirmte Leitungen mit weiteren IT-Geräten verbunden werden.

INF.2.A4 Notabschaltung der Stromversorgung [Haustechnik]

Für den Notfall MUSS es geeignete Möglichkeiten geben, das Rechenzentrum spannungsfrei zu schalten. Dafür SOLLTE beispielsweise ein Not-Aus-Schalter installiert werden. Ein solcher Schalter MUSS nicht nur die externe Energieversorgung abtrennen, sondern auch die komplette USV-Anlage abschalten. Alle Not-Aus-Schalter MÜSSEN so geschützt sein, dass sie nicht unbeabsichtigt betätigt werden können.

INF.2.A5 Einhaltung der Lufttemperatur und -feuchtigkeit [Haustechnik]

Um IT-Systeme entsprechend den Hersteller-Empfehlungen zuverlässig betreiben zu können, MUSS sichergestellt werden, dass die Lufttemperatur und Luftfeuchtigkeit im IT-Betriebsbereich innerhalb der vorgeschriebenen Grenzen liegen.

Die tatsächliche Wärmelast in den gekühlten Bereichen MUSS in regelmäßigen Abständen und nach größeren Umbauten durch Berechnung oder Messung überprüft werden.

Auch MUSS eine eventuell vorhandene Klimatisierungseinrichtung regelmäßig gewartet werden. Wenn die beiden Parameter "Temperatur" und "Feuchtigkeit" vom Normwert abweichen, MÜSSEN sie über eine repräsentative Dauer hinweg in einem der Situation angepassten Zeitintervall aufgezeichnet werden.

INF.2.A6 Zutrittskontrolle [IT-Betrieb, Informationssicherheitsbeauftragter (ISB), Haustechnik]

Für den Schutz gegen unbefugten Zutritt zu einem Rechenzentrum MUSS es eine Zutrittskontrolle geben.

Durch eine auf die jeweiligen Erfordernisse abgestimmte Zutrittsregelung MUSS für eigene Mitarbeiter und für nur zeitweilig Beschäftigte sichergestellt werden, dass sie keinen Zutritt zu IT-Systemen außerhalb ihres Tätigkeitsbereiches erhalten.

Außerdem MUSS sichergestellt werden, dass Besucher und Fremdpersonal während aller Arbeiten im Rechenzentrum von der Zutrittskontrolle individuell erfasst sowie beaufsichtigt werden.

Zudem MÜSSEN alle Zutrittsmöglichkeiten zu einem Rechenzentrum überwacht werden. Die Anforderungen der Institution an ein Zutrittskontrollsystem MÜSSEN in einem Konzept ausreichend detailliert dokumentiert werden. Im Falle eines Serverraums SOLLTE geprüft werden, ob eine Überwachung aller Zutrittsmöglichkeiten sinnvoll ist.

Weiterhin MUSS geregelt werden, welche internen und externen Personen für welchen Zeitraum Zutritt erhalten. Dabei MUSS sichergestellt sein, dass keine unnötigen oder zu weitreichenden Zutrittsrechte vergeben werden. Es MUSS regelmäßig kontrolliert werden, ob die Regelungen zum Einsatz einer Zutrittskontrolle eingehalten werden.

INF.2.A7 Verschließen und Sichern [Mitarbeiter, Haustechnik]

Alle Türen des Rechenzentrums MÜSSEN stets verschlossen gehalten werden. Fenster sind möglichst schon bei der Planung zu vermeiden. Falls sie doch vorhanden sind, MÜSSEN sie ebenso wie die Türen stets verschlossen gehalten werden. Türen und Fenster MÜSSEN einen dem Sicherheitsniveau angemessenen Schutz gegen Angriffsversuche und Umgebungseinflüsse (z. B. Feuer und Rauch) bieten. Hierbei ist zu beachten, dass die bauliche Ausführung aller raumbildenden Elemente in Bezug auf die Sicherheit, vor allem hinsichtlich Sicherheitszonen, gleichwertig sein MUSS.

INF.2.A8 Einsatz einer Brandmeldeanlage [Planer]

In einem Rechenzentrum MUSS eine Brandmeldeanlage installiert werden. Diese MUSS alle Flächen überwachen. Alle Meldungen der Brandmeldeanlage MÜSSEN geeignet weitergeleitet werden (siehe dazu auch INF.2.A13 *Planung und Installation von Gefahrenmeldeanlagen*). Die Brandmeldeanlage MUSS regelmäßig gewartet. Es MUSS sichergestellt werden, dass in Räumen, die im Brandabschnitt des Rechenzentrums liegen, keine besonderen Brandlasten vorhanden sind.

INF.2.A9 Einsatz einer Lösch- oder Brandvermeidungsanlage [Planer]

In einem Rechenzentrum MUSS eine Lösch- oder Brandvermeidungsanlage nach aktuellem Stand der Technik installiert sein.

In Serverräumen SOLLTEN hierfür Handfeuerlöscher in ausreichender Zahl und Größe benutzt werden. Die Feuerlöscher MÜSSEN so angebracht werden, dass sie im Brandfall leicht zu erreichen sind. Jeder Löscher MUSS regelmäßig inspiziert und gewartet werden, um die Funktionsfähigkeit im Ernstfall zu gewährleisten. Alle Mitarbeiter MÜSSEN in die Benutzung der Handfeuerlöscher eingewiesen werden.

INF.2.A10 Inspektion und Wartung der Infrastruktur [IT-Betrieb, Haustechnik, Wartungspersonal]

Für alle Komponenten der technischen Infrastruktur MÜSSEN mindestens die empfohlenen oder durch Normen festgelegten Intervalle und Vorschriften für Inspektion und Wartung eingehalten werden. Um nachvollziehen zu können, wann welche Arbeiten durchgeführt wurden, MÜSSEN Inspektionen und Wartungsarbeiten protokolliert werden.

Kabel- und Rohrdurchführungen durch Brandwände MÜSSEN regelmäßig daraufhin geprüft werden, ob die Schotten normgerecht und unversehrt sind. Die Ergebnisse MÜSSEN dokumentiert werden.

INF.2.A11 Automatisierte Überwachung der Infrastruktur [IT-Betrieb, Haustechnik]

Alle Störungsmeldungen der Infrastruktur, z. B. Leckageüberwachung, Klima-, Strom- und USV-Anlagen, MÜSSEN automatisiert überwacht und schnellstmöglich geeignet weitergeleitet werden, z. B. über ein Monitoringsystem.

Im Falle eines Serverraums SOLLTEN IT- und Supportgeräte, die nicht oder nur selten von einer Person bedient werden müssen, mit einer Fernanzeige für Störungen ausgestattet werden. Die verantwortlichen Mitarbeiter MÜSSEN zeitnah alarmiert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Rechenzentrum sowie Serverraum. Sie SOLLTEN grundsätzlich umgesetzt werden.

INF.2.A12 Entwurf und Umsetzung eines Perimeterschutzes für das Rechenzentrum [Planer, Haustechnik]

Die Sicherheitsmaßnahmen zum Perimeterschutz SOLLTEN gleichwertig mit denen des Sicherheitskonzeptes für das Gebäude und seines Umfelds sein. Je nach dem festgelegten Schutzbedarf für das Rechenzentrum und abhängig vom Gelände SOLLTE der Perimeterschutz aus folgenden Komponenten bestehen:

- äußere Umschließung oder Umfriedung,
- Sicherungsmaßnahmen gegen unbeabsichtigtes Überschreiten einer Grundstücksgrenze,
- Sicherungsmaßnahmen gegen beabsichtigtes gewaltloses Überwinden der Grundstücksgrenze,
- Sicherungsmaßnahmen gegen beabsichtigtes gewaltsames Überwinden der Grundstücksgrenze,
- Freiland-Sicherungsmaßnahmen sowie
- äußere Personen- und Fahrzeugidentifikation.

INF.2.A13 Planung und Installation von Gefahrenmeldeanlagen [Planer]

Es SOLLTE ein konsistentes Schutzkonzept für das betrachtete Gebäude erarbeitet werden. Erst danach SOLLTE geplant werden, welche Gefahrenmeldeanlagen für welche Gebäudebereiche des Rechenzentrums benötigt und installiert werden und wie mit Alarmmeldungen umzugehen ist. Das Konzept SOLLTE immer angepasst werden, wenn sich die Nutzung der Gebäudebereiche verändert.

Es SOLLTE eine für das jeweilige Einsatzgebiet angemessene Gefahrenmeldeanlage (GMA) installiert werden. Die Meldungen der GMA SOLLTEN unter Beachtung der dafür geltenden Technischen Anschlussbedingungen (TAB) auf eine Alarmempfangsstelle aufgeschaltet werden. Die Alarmempfangsstelle SOLLTE jederzeit erreichbar und technisch sowie personell in der Lage sein, in geeigneter Weise auf die gemeldete Gefährdung zu reagieren. Der Übertragungsweg zwischen eingesetzter GMA und hilfeleistender Stelle SOLLTE redundant ausgelegt werden. Alle Übertragungswege SOLLTEN regelmäßig getestet werden.

INF.2.A14 Einsatz einer Netzersatzanlage [Planer, Haustechnik]

Die Energieversorgung aus dem Netz eines Energieversorgungs-Unternehmens () SOLLTE um eine Netzersatzanlage (NEA) ergänzt werden. Der Betriebsmittelvorrat einer NEA SOLLTE regelmäßig kontrolliert werden. Um die Schutzwirkung einer NEA aufrechtzuerhalten, SOLLTE sie regelmäßig gewartet werden (siehe INF.2.A10 *Inspektion und Wartung der Infrastruktur*). Bei diesen Wartungen SOLLTEN auch Belastungs- und Funktionstests sowie Testläufe unter Last durchgeführt werden.

INF.2.A15 Überspannungsschutzeinrichtung [Planer, Haustechnik]

Es SOLLTE auf Basis der aktuell gültigen Norm ein Blitz- und Überspannungsschutzkonzept nach dem Prinzip der energetischen Koordination (Anhang C der DIN EN 62305-4) erstellt und umgesetzt werden. Die energetische Koordination der Überspannungsschutzeinrichtungen SOLLTE in einem Konzept dokumentiert und abgenommen werden.

Blitz- und Überspannungsschutzeinrichtungen SOLLTEN periodisch und nach bekannten Ereignissen geprüft und falls erforderlich ersetzt werden. Unabhängig von Umfang und Ausbau des Überspannungsschutzes SOLLTE beachtet werden, dass ein umfassender und durchgängiger Potenzialausgleich aller in den Überspannungsschutz einbezogenen elektrischen Betriebsmittel erforderlich ist. Bei Nachinstallationen SOLLTE darauf geachtet werden, dass der Potenzialausgleich mitgeführt wird.

INF.2.A16 Klimatisierung im Rechenzentrum [Haustechnik]

Es SOLLTE sichergestellt werden, das im Rechenzentrum geeignete klimatische Bedingungen für Lufttemperatur und Luftfeuchtigkeit (siehe INF.2.A5 *Einhaltung der Lufttemperatur und -feuchtigkeit*) sowie zusätzlich für die Bereiche Frischluftanteil und Schwebstoffbelastung geschaffen und aufrechterhalten werden. Die Klimatisierung SOLLTE für das Rechenzentrum ausreichend dimensioniert sein. Alle relevanten Werte SOLLTEN ständig überwacht werden. Weicht ein Wert von der Norm ab, SOLLTE eine automatische Alarmierung stattfinden.

Die Klimatisierungsanlagen SOLLTEN in Rechnerraumbereichen möglichst ausfallsicher sein, z. B. durch redundant ausgelegte Komponenten.

INF.2.A17 Brandfrüherkennung [Planer, Haustechnik]

Um Brände in Rechenzentren bereits in einem sehr frühen Stadium erkennen zu können, SOLLTE eine Anlage zur Brandfrüherkennung installiert werden.

Damit sich Entstehungsbrände nicht weiter ausbreiten können, SOLLTE durch die Brandfrüherkennung eine automatische Spannungsfreischaltung erfolgen. Dabei SOLLTEN die Überwachungsbereiche der Brandfrüherkennung sowie die Wirkungsbereiche der Spannungsfreischaltung hinreichend kleinteilig konzipiert werden, um ein ausgewogenes Verhältnis zwischen dem Brandschutz einerseits und der RZ-Verfügbarkeit andererseits zu erreichen.

Die Anlage zur Brandfrüherkennung SOLLTE dem aktuellen Stand der Technik entsprechen. Auch SOLLTE sie nach den Vorgaben des Herstellers betrieben und regelmäßig gewartet werden.

INF.2.A18 Schutz vor Wasseraustritt [Haustechnik]

In Bereichen, in denen sich IT-Geräte mit zentralen Funktionen befinden, SOLLTEN wasserführende Leitungen vermieden werden. So SOLLTE es beispielsweise keine Heizkörper im Rechenzentrum geben.

Sind wasserführende Leitungen (z. B. für die Kühlung direkt auf der RZ-Fläche) unvermeidbar, SOLLTE sichergestellt sein, dass Wasseraustritte möglichst frühzeitig erkannt und die Auswirkungen minimiert werden. Durch Sichtprüfungen SOLLTEN die vorhandenen Wasserleitungen regelmäßig daraufhin überprüft werden, ob sie noch dicht sind. Meldungen einer Detektionsanlage SOLLTEN an verantwortliche Mitarbeiter gemeldet werden, sodass diese anhand von Reaktionsplänen und einer aktuellen Dokumentation schnell eingreifen können (siehe *INF.2.A13 Planung und Installation von Gefahrenmeldeanlagen*).

INF.2.A19 Durchführung von Funktionstests der technischen Infrastruktur [Haustechnik]

Die technische Infrastruktur eines Rechenzentrums SOLLTE regelmäßig (zumindest 1- bis 2-jährlich) sowie nach Systemumbauten und umfangreichen Reparaturen getestet werden. Die Ergebnisse SOLLTEN dokumentiert werden. Es SOLLTEN besonders ganze Reaktionsketten einem echten Funktionstest unterzogen werden.

INF.2.A20 Regelmäßige Aktualisierungen der Infrastruktur- und Baupläne [Planer]

Baupläne, Trassenpläne, Strangschemata, Fluchtwegpläne, Feuerwehrlaufkarten usw. SOLLTEN nach jeder Umbaumaßnahme oder wenn die Infrastruktur oder die Sicherheitstechnik erweitert wurde, umgehend aktualisiert werden. Außerdem SOLLTEN die Mitarbeiter entsprechend informiert werden. Es SOLLTE mindestens ein Mal innerhalb von drei Jahren überprüft werden, ob alle relevanten Pläne noch aktuell und korrekt sind.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

INF.2.A21 Ausweichrechenzentrum (A)

Es SOLLTE ein geografisch separiertes Ausweichrechenzentrum aufgebaut und eingesetzt werden. Das Ausweichrechenzentrum SOLLTE so dimensioniert sein, dass alle Prozesse der Institution aufrechterhalten werden können. Auch SOLLTE es ständig einsatzbereit sein. Alle Daten der Institution SOLLTEN regelmäßig ins Ausweichrechenzentrum gespiegelt werden.

INF.2.A22 Durchführung von Staubschutzmaßnahmen [Haustechnik] (IA)

Wenn ein bestehendes Rechenzentrum erweitert wird, SOLLTEN geeignete Staubschutzmaßnahmen definiert, geplant und umgesetzt werden. Personen, die selbst nicht an den Baumaßnahmen beteiligt sind, SOLLTEN in ausreichend engen Zeitabständen kontrollieren, ob die Staubschutzmaßnahmen ordnungsgemäß funktionieren und die Regelungen zum Staubschutz eingehalten werden.

INF.2.A23 Sicher strukturierte Verkabelung im Rechenzentrum [Haustechnik] (A)

Kabeltrassen SOLLTEN sorgfältig geplant und ausgeführt werden. Alle Kabel SOLLTEN vor ungewollten mechanischen Beanspruchungen, Manipulationen, Abhörversuchen oder Bränden geschützt sein. Für unterschiedliche Netzarten, z. B. Datennetz, Netz für Gefahrenmeldeanlagen und Stromnetz, SOLLTEN getrennte Kabel benutzt werden. Werden Kabel für verschiedene Netze gemeinsam geführt, SOLLTE sichergestellt sein, dass gegenseitige Störungen minimiert werden. Zudem SOLLTE eine redundante Trassenführung angestrebt werden.

INF.2.A24 Einsatz von Videoüberwachungsanlagen [Planer, Haustechnik, Datenschutzbeauftragter] (IA)

Die Zutrittskontrolle und die Einbruchmeldung SOLLTEN durch Videoüberwachungsanlagen ergänzt werden. Dazu SOLLTEN die für Videoüberwachungsanlagen sinnvollen Flächen identifiziert werden.

Eine geplante Videoüberwachung SOLLTE konsistent in das gesamte Sicherheitskonzept eingebettet werden. Auch SOLLTE bei der Planung, Konzeption und eventuellen Auswertung von Videoaufzeichnungen immer der Datenschutzbeauftragte mit einbezogen werden.

Die für eine Videoüberwachung benötigten zentralen Technikkomponenten SOLLTEN in einer geeigneten Umgebung aufgestellt und geschützt werden. Es SOLLTE regelmäßig überprüft werden, ob die Videoüberwachungsanlage korrekt funktioniert.

INF.2.A25 Redundante Auslegung von unterbrechungsfreien Stromversorgungen [Planer]

Um die Verfügbarkeit eines Rechenzentrums sicherzustellen, SOLLTEN die USV-Anlagen redundant ausgelegt sein. Nach einem Stromausfall SOLLTEN alle für den ordnungsgemäßen Betrieb des Rechenzentrums erforderlichen Komponenten so lange mit Strom versorgt werden können, bis eine alternative Stromquelle angeschlossen werden kann.

INF.2.A26 Redundante Auslegung von Netzersatzanlagen (A)

Bei erhöhtem Schutzbedarf SOLLTEN Netzersatzanlagen redundant ausgelegt werden. Es SOLLTE sichergestellt werden, dass auch diese Anlagen regelmäßig gewartet werden (siehe INF.2.A10 *Inspektion und Wartung der Infrastruktur*).

INF.2.A27 Durchführung von Alarmierungs- und Brandschutzübungen (CA)

Mit den Angestellten der Institution SOLLTEN regelmäßige Alarmierungs- und Brandschutzübungen durchgeführt werden. Diese SOLLTEN auf einem Alarmierungsplan basieren, in dem die zu ergreifenden Maßnahmen dokumentiert sind. Es SOLLTE regelmäßig geprüft werden, ob die Maßnahmen noch korrekt, aktuell und praktikabel sind.

INF.2.A28 Einsatz von höherwertigen Gefahrenmeldeanlagen (IA)

Für Rechenzentrumsbereiche mit erhöhtem Schutzbedarf SOLLTEN ausschließlich Gefahrenmeldeanlagen der VDS-Klasse C benutzt werden.

4 Weiterführende Informationen

4.1 Literatur

- [BKRZ] Leitfaden Betriebssicheres Rechenzentrum
  Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM), 2013 (zuletzt abgerufen 04.10.2017)
  http://www.bitkom.org/Bitkom/Publikationen/Betriebssicheres-Rechenzentrum.html

- [DIN50600-1] DIN EN 50600-1, Informationstechnik - Einrichtungen und Infrastrukturen von Rechenzentren
  Teil 1: Allgemeine Konzepte, DIN, 2012

- [DIN62305-4] IEC 62305-4 (VDE 0185-305 / DIN EN 62305) – Blitzschutz
  Teil 4: Elektrische und elektronische Systemene in baulichen Anlagen, DIN, 2011

- [VdSPeri] Sicherungsleitfaden Perimeter
  VdS Schadenverhütung GmbH, 2012 (zuletzt abgerufen 04.10.2017)
  http://vds.de/fileadmin/vds_publikationen/vds_3143_web.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Rechenzentrum sowie Serverraum" von Bedeutung.

G 0.01 Feuer

G 0.02 Ungünstige klimatische Bedingungen

G 0.03 Wasser

G 0.04 Verschmutzung, Staub, Korrosion

G 0.05 Naturkatastrophen

G 0.06 Katastrophen im Umfeld

G 0.07 Großereignisse im Umfeld

G 0.08 Ausfall oder Störung der Stromversorgung

G 0.10 Ausfall oder Störung von Versorgungsnetzen

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.15 Abhören

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.33 Personalausfall

G 0.34 Anschlag

G 0.41 Sabotage

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

Elementare Gefährdungen / Anforderungen	G 0.01	G 0.02	G 0.03	G 0.04	G 0.05	G 0.06	G 0.07	G 0.08	G 0.10	G 0.11	G 0.15	G 0.16	G 0.24	G 0.25	G 0.26	G 0.29	G 0.30	G 0.31	G 0.32	G 0.33	G 0.34	G 0.41	G 0.44
INF.2.A1					x	x	x									x							
INF.2.A2	x							x	x				x	x									
INF.2.A3								x															
INF.2.A4	x				x			x					x		x								
INF.2.A5		x																					
INF.2.A6												x					x		x				x
INF.2.A7												x					x		x				x
INF.2.A8	x							x	x				x	x									
INF.2.A9	x							x	x				x	x									
INF.2.A10	x							x	x					x									
INF.2.A11									x				x		x			x					
INF.2.A12							x					x					x					x	x
INF.2.A13	x		x	x	x	x	x	x	x			x	x	x	x		x	x			x	x	x
INF.2.A14								x															
INF.2.A15	x													x									
INF.2.A16		x																					
INF.2.A17	x							x	x				x	x									
INF.2.A18			x										x	x									
INF.2.A19								x	x						x	x							
INF.2.A20															x	x	x	x					
INF.2.A21					x	x	x	x	x	x											x		
INF.2.A22		x																					
INF.2.A23								x	x		x				x		x					x	
INF.2.A24												x				x	x					x	
INF.2.A25								x															
INF.2.A26								x															
INF.2.A27																x		x					
INF.2.A28	x		x	x	x	x	x	x	x			x	x	x	x		x	x			x	x	x

INF: Infrastruktur

INF.3 Elektrotechnische Verkabelung

1 Beschreibung

1.1 Einleitung

Die elektrotechnische Verkabelung von IT-Systemen und anderen Geräten umfasst alle Kabel und Verteilungen im Gebäude vom Einspeisepunkt des Verteilungsnetzbetreibers bis zu den Elektro-Anschlüssen der Verbraucher.

Die ordnungsgemäße und normgerechte Ausführung der elektrotechnischen Verkabelung ist Grundlage für den sicheren IT-Betrieb.

1.2 Zielsetzung

Ziel dieses Bausteins ist der Schutz der gesamten elektrotechnischen Verkabelung gegen Ausfall und Störung der Stromversorgung.

1.3 Abgrenzung

Die IT-Verkabelung zur Kommunikation der IT-Systeme wird in einem separaten Baustein behandelt (siehe INF.4 IT-Verkabelung).

2 Gefährdungslage

Folgende spezifischen Bedrohungen und Schwachstellen sind im Bereich elektrotechnische Verkabelung von besonderer Bedeutung:

2.1 Kabelbrand

Wenn ein Kabel in Brand gerät, sei es durch Selbstentzündung oder durch Beflammung, kann dies verschiedene Folgen haben. Einige dieser Folgen sind zum Beispiel Kurzschlüsse, die Unterbrechungen des Schutzleiters, die Entwicklung aggressiver Gase, Feuer oder die Entstehung von Schwelbränden. Kabelbrände bewirken in der Entstehungsphase häufig nur einen geringen Anstieg der Temperatur. Damit besteht die zusätzliche Gefährdung, dass eine erhebliche Verrauchung durch "kalten" Brandrauch entsteht, bevor Rauchmelder ansprechen, die an der Raumdecke angebracht sind.

2.2 Unzureichende Dimensionierung der elektrotechnischen Verkabelung

Bei der Planung von Arbeitsplätzen, Serverräumen oder Rechenzentren wird oft der Fehler begangen, diese ausschließlich am aktuellen Bedarf auszurichten. Dabei wird übersehen, dass durch neue Anforderungen wie die Nutzung weiterer Server die Kapazität des Stromnetzes erweitert werden muss. Eine Erweiterung der elektrotechnischen Verkabelung ist aber nur in dem Umfang möglich, wie es die vorhandenen, verlegten Kabel zulassen oder der zur Verfügung stehende Platz für zusätzliche Kabel und Verteilungen erlaubt.

2.3 Unzureichende Dokumentation der Verkabelung

Ist aufgrund unzureichender Dokumentation die genaue Lage von Leitungen nicht bekannt, so kann es bei Bauarbeiten außerhalb oder innerhalb eines Gebäudes zu Beschädigungen von Leitungen kommen. Es kann nicht davon ausgegangen werden, dass alle Kabel und Leitungen in den Installationszonen gemäß gültiger Normen installiert sind. Eine unzureichende Dokumentation erschwert zudem die Prüfung, Wartung und Reparatur von Leitungen.

2.4 Unzureichende geschützte Verteiler

Unterverteilungen des Stromversorgungsnetzes sind vielfach frei zugänglich und unverschlossen in Fluren oder Treppenhäusern untergebracht. Dadurch ist es jedermann möglich, diese Verteiler zu öffnen, Manipulationen vorzunehmen und gegebenenfalls einen Stromausfall herbeizuführen. Ferner kann von solchen Verteilern eine unmittelbare Gefahr ausgehen, da nach Entnahme von Schraubsicherungen und deren Sockeln ein direktes Berühren spannungsführender Teile möglich ist. Offenstehende Türen an den Verteilerkästen können zudem den Verkehrsweg behindern, auch Verletzungen durch Klemmen und Quetschen an den Scherkanten sind möglich.

2.5 Leitungsbeschädigungen

Je ungeschützter ein Kabel verlegt ist, desto größer ist die Gefahr einer Beschädigung. Eine Beschädigung führt nicht unbedingt sofort zu einem Ausfall von Verbindungen. Auch die zufällige Entstehung unzulässiger Verbindungen ist möglich, wenn beispielsweise Kabelmäntel beziehungsweise Isolierungen nicht mehr vollständig intakt sind. Eine Beschädigung muss dabei nicht zwingend absichtlich erfolgen, sondern kann auch unbeabsichtigt entstehen.

2.6 Spannungsschwankungen und Über- bzw. Unterspannung

Durch Schwankungen der Versorgungsspannung kann es zu Funktionsstörungen und Beschädigungen der IT kommen. Die Schwankungen reichen von extrem kurzen und kleinen Ereignissen, die sich kaum oder gar nicht auf die IT auswirken, bis zu Totalausfällen oder zerstörerischen Überspannungen. Die Ursache dafür kann in allen Bereichen des Stromversorgungsnetzes entstehen, vom Netz des Energieversorgungsunternehmens bis zum Stromkreis, an dem die jeweiligen Geräte angeschlossen sind.

2.7 Verwendung unzureichender Steckdosenleisten

Oft reicht die Zahl fest installierter Steckdosen für die Menge der zu betreibenden Geräte nicht aus. Um diesen Mangel auszugleichen, werden dann typischerweise Steckdosenleisten verwendet. Solche Steckdosenleisten stellen, wenn sie von unzureichender Qualität sind, eine gefährliche Zündquelle und damit eine große Brandgefahr dar. Werden zusätzlich mehrere kleinere Steckdosenleisten hintereinander geschaltet, um ausreichende Steckplätze für alle Geräte bereitzustellen, steigt die Gefahr durch zu geringen Leitungsquerschnitt und Überlastung weiter an.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich elektrotechnischer Verkabelung aufgeführt. Grundsätzlich ist der Leiter Haustechnik für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Leiter Haustechnik
Weitere Verantwortliche	Leiter IT

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

INF.3.A1 Auswahl geeigneter Kabeltypen

Bei der Auswahl von Kabeln MÜSSEN die übertragungstechnischen Notwendigkeiten und die Umgebungsbedingungen bei der Verlegung sowie im Betrieb zu berücksichtigt werden. Bei der Auswahl von Elektrokabeln MÜSSEN die einschlägigen Normen und Vorschriften beachtet werden. In Bezug auf die Umgebungsbedingungen MÜSSEN Faktoren wie z. B. die Temperaturen, Kabelwege, Zugkräfte bei der Verlegung, die Verlegeart und etwaige Störquellen beachtet werden.

INF.3.A2 Planung der Kabelführung [Leiter IT]

Kabel, Kabelwege und Kabeltrassen MÜSSEN vor ihrer Verlegung sowohl aus funktionaler wie auch aus physikalische Sicht ausreichend dimensioniert werden. Dabei MÜSSEN zukünftige elektrotechnische Notwendigkeiten ebenso mit einkalkuliert werden wie genügend Platz für mögliche technische Erweiterungen in Kabelkanälen und -trassen. Bei der gemeinsamen Führung von IT- und Stromverkabelung in einer Trasse MUSS außerdem darauf geachtet werden, das Übersprechen zwischen den einzelnen Kabeln zu vermeiden. Es SOLLTE generell darauf geachtet werden, dass IT-Kabel getrennt von der elektrotechnischen Verkabelung geführt werden. Es MUSS darauf geachtet werden, erkennbare Gefahrenquellen zu umgehen.

INF.3.A3 Fachgerechte Installation

Die Installationsarbeiten der elektrotechnischen Verkabelung MÜSSEN sorgfältig und fachkundig erfolgen. Gleichzeitig MÜSSEN alle relevanten Normen beachtet werden. Die entscheidenden Kriterien für eine fachgerechte Ausführung der elektrotechnischen Verkabelung MÜSSEN daher vom Auftraggeber in allen Phasen überprüft werden. Bei Anlieferung des Materials MUSS geprüft werden, ob die richtigen Kabel und Anschlusskomponenten geliefert wurden. Bei der Verlegung von Stromkabeln MUSS besondere Sorgfalt darauf gelegt werden, dass die Montage keine Beschädigungen hervorruft und dass die Kabelwege so gewählt sind, dass Beschädigungen der verlegten Kabel durch die normale Nutzung des Gebäudes ausgeschlossen sind.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Elektrotechnische Verkabelung. Sie SOLLTEN grundsätzlich umgesetzt werden.

INF.3.A4 Anforderungsanalyse für die elektrotechnische Verkabelung

Grundsätzlich SOLLTE eine Analyse der Anforderungen, die Einfluss auf eine zukunftssichere, bedarfsgerechte und wirtschaftliche Ausführung der elektrotechnischen Verkabelung haben, durchgeführt werden. In ihr SOLLTE zunächst die kurzfristig geplante Nutzung durch die Anwender in der Institution und darauf aufbauend die längerfristige Entwicklung der Nutzung abgeschätzt werden.

INF.3.A5 Abnahme der elektrotechnischen Verkabelung

Die elektrotechnische Verkabelung SOLLTE einem Abnahmeprozess unterzogen werden. Eine Abnahme SOLLTE erst dann erfolgen, wenn alle durchzuführenden Aufgaben abgeschlossen sind, der Ausführende die Maßnahme zur Abnahme gemeldet hat und sich bei den Kontrollen durch den Auftraggeber keine inakzeptablen Mängel gezeigt haben. Der Abnahmetermin SOLLTE zeitlich so gewählt werden, dass die Kontrollen zur Abnahme in ausreichender Zeit vorbereitet werden können. Neben der korrekten Abrechnung und dem tatsächlichen Umfang der Leistungen MÜSSEN bei der Abnahme die Einhaltung der unterschiedlichen Normen für elektrotechnische Verkabelungen kontrolliert werden. Für das Abnahmeprotokoll SOLLTE eine Checkliste vorbereitet werden. Die Checkliste SOLLTE auch Punkte zu allgemeinen Anforderungen an die Betriebsräume enthalten. Das Abnahmeprotokoll MUSS von den Teilnehmern und Verantwortlichen rechtsverbindlich unterzeichnet werden. Das Protokoll SOLLTE Bestandteil der internen Dokumentation der Verkabelung sein.

INF.3.A6 Überspannungsschutz

Jedes elektrisch leitende Netz SOLLTE gegen Überspannungen geschützt werden. Hierfür MUSS ein den gültigen Normen entsprechendes Überspannungsschutzkonzept erstellt werden. Netzersatzanlagen und unterbrechungsfreie Stromversorgungen SOLLTEN in das Konzept mit aufgenommen werden.

INF.3.A7 Entfernen und Deaktivieren nicht mehr benötigter Leitungen

Wenn Stromkabel nicht mehr benötigt werden, SOLLTEN sie fachgerecht und vollständig entfernt werden. Anschließend MÜSSEN die Brandschottungen fachgerecht verschlossen werden. Verkabelung, die mit der vorhandenen Technik sinnvoll als Reserve weiter genutzt werden kann, SOLLTE in einem betriebsfähigen Zustand erhalten bleiben. Solche Kabel MÜSSEN mindestens an den Endpunkten entsprechend gekennzeichnet werden. Grundsätzlich SOLLTE eine Übersicht über nicht mehr benötigte Kabel aufgestellt und anhand dieser Dokumentation die Deaktivierung oder der Abbau/Ausbau der Kabel belegt werden. Anschließend MUSS die entsprechende Dokumentation aktualisiert werden.

INF.3.A8 Brandschutz in Trassen

Zur Vermeidung von Kabelbränden SOLLTEN Trassen ausreichend dimensioniert werden. Darüber hinaus SOLLTE nach Abschluss der Installationsarbeiten die Belegungsdichte der Trassen in vernünftigen Abständen überprüft werden.

INF.3.A9 Dokumentation und Kennzeichnung der elektrotechnischen Verkabelung

Eine Institution SOLLTE sicherstellen, dass sie für ihre elektrotechnische Verkabelung eine interne und eine externe Dokumentation besitzt. Die interne Dokumentation MUSS alle Aufzeichnungen, die die Installation und den Betrieb der Verkabelung betreffen, enthalten. Die interne Dokumentation SOLLTE so umfangreich angefertigt und gepflegt werden, dass der Betrieb und die zukünftige Weiterentwicklung bestmöglich unterstützt werden. Die externe Dokumentation der Verkabelung SOLLTE so möglichst neutral gehalten werden.

INF.3.A10 Neutrale Dokumentation in den Verteilern

In jedem Verteiler SOLLTE sich eine Dokumentation befinden, die den derzeitigen Stand von Rangierungen und Leitungsbelegungen wiedergibt. Diese Dokumentation SOLLTE möglichst neutral gehalten werden und MUSS ein sicheres Schalten ermöglichen Nur bestehende und genutzte Verbindungen, sowie auflaufende Reserveleitungen SOLLTEN darin aufgeführt sein. Es SOLLTEN, soweit nicht ausdrücklich vorgeschrieben, keine Hinweise auf die Nutzungsart der Leitungen gegeben werden. Alle weitergehenden Informationen SOLLTEN in einer Revisionsdokumentation aufgeführt werden.

INF.3.A11 Kontrolle elektrotechnischer Anlagen und Verbindungen

Alle elektrotechnischen Anlagen, Verteiler und Zugdosen der Verkabelung SOLLTEN regelmäßig einer (zumindest stichprobenartigen) Sichtprüfung unterzogen werden. Neben der reinen Sichtkontrolle SOLLTE zusätzlich eine funktionale Kontrolle durchgeführt werden, sofern im Rahmen der DGUV-V3-Prüfung eine solche Kontrolle nicht bereits erfolgt ist. Alle Unregelmäßigkeiten, die bei Sichtkontrollen oder funktionalen Kontrollen festgestellt werden, MÜSSEN unverzüglich dokumentiert und den zuständigen Organisationseinheiten gemeldet werden. Die zuständigen Organisationseinheiten MÜSSEN im Anschluss die festgestellten Unregelmäßigkeiten überprüfen und beheben.

INF.3.A12 Vermeidung elektrischer Zündquellen

Die Nutzung privater Elektrogeräte innerhalb einer Institution SOLLTE klar geregelt werden. Alle Elektrogeräte SOLLTEN vor ihrer Verwendung durch eine Elektrofachkraft geprüft und für sicher befunden werden. Die Verwendung von Steckdosenleisten SOLLTE soweit wie möglich vermieden werden. Fehlende Steckdosen SOLLTEN durch eine Elektrofachkraft in vorhandene Kanalsysteme nachgerüstet oder fachgerecht auf Putz montiert werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

INF.3.A13 Sekundär-Energieversorgung (A)

Die primäre Energieversorgung aus dem Netz eines Energieversorgungs-Unternehmens SOLLTE bei erhöhten Anforderungen an die Verfügbarkeit um Maßnahmen zur Notfall-Versorgung ergänzt werden. Dafür SOLLTE für die abzusichernden Bereiche eine ausreichend dimensionierte zentrale USV und eine Netzersatzanlage (NEA) eingerichtet werden. Es SOLLTE geprüft werden, ob die Anschlüsse an den Netzbetreiber redundant ausgelegt werden sollen. NEA und USV MÜSSEN regelmäßig gewartet werden.

INF.3.A14 A-B-Versorgung (A)

Es SOLLTE geprüft werden, ob über die normale einzügige Stromversorgung wichtiger IT-Komponenten hinaus eine zweizügige, sogenannte A-B-Versorgung geschaffen werden soll. Dabei SOLLTE sichergestellt werden, dass deren Funktionsfähigkeit permanent durch geeignete technische Einrichtungen, z. B. durch die Gebäudeleittechnik (GLT), überwacht wird.

INF.3.A15 Materielle Sicherung der elektrotechnischen Verkabelung (A)

In Räumen mit Publikumsverkehr oder in unübersichtlichen Bereichen eines Gebäudes SOLLTE überlegt werden, Leitungen und Verteiler gegen unbefugte Zugriffe zu sichern. In jedem Fall SOLLTE die Zahl und der Umfang der Stellen, an denen Einrichtungen der Energieversorgung für Unbefugte zugänglich sind, auf ein Mindestmaß reduziert werden.

INF.3.A16 Nutzung von Schranksystemen (A)

Zur Verbesserung der Betriebssicherheit elektrotechnischen Anschlüssen und -verteilern SOLLTEN diese Geräte in Schranksystemen eingebaut oder aufgestellt werden.

Die IT-Hardware SOLLTE, soweit es möglich ist, in Schranksystemen untergebracht werden. Diese SOLLTEN in Tiefe und Breite dem zunehmenden Platzbedarf der Einbaugeräte genügen und mit entsprechenden Zusatzeinrichtungen ausgerüstet oder jederzeit nachrüstbar sein.

INF.3.A17 Brandschott-Kataster (A)

Es SOLLTE ein Brandschott-Kataster geführt werden. In diesem SOLLTEN alle Arten von Schotts individuell aufgenommen werden. Nach Arbeiten an Brandschotts SOLLTEN die Änderungen im Kataster spätestens nach 4 Wochen eingetragen werden.

4 Weiterführende Informationen

4.1 Literatur

- [BGVA3] Berufsgenossenschaftliche Vorschrift für Sicherheit und Gesundheit bei der Arbeit – A3 Elektrische Anlagen und Betriebsmittel
- [DIN4102] DIN 4102:2016-05
  Brandverhalten von Baustoffen und Bauteilen, Beuth Verlag
- [IEC60364] IEC60364- Einrichten von Niederspannungsanlagen
  Beuth Verlag

- [IEC62305] IEC 62305 (VDE 0185-305 / DIN EN 62305) – Blitzschutz
  Normreihe zum Blitzschutz von baulichen Anlagen, (zuletzt abgerufen 05.10.2017)
  https://www.vde.com/resource/blob/936756/5b65d838e75e83f750bd8fa23bb620b1/merkblatt-blitzschutznormen-13-download-data.pdf

- [VDE100] DIN VDE 0100- Bestimmung für das Errichten von Starkstromanlagen mit Notspannungen bis 1000V
  VDE Verlag

- [VDE105] DIN VDE 0105-100 – Betrieb von elektrischen Anlagen
  VDE Verlag

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Elektrotechnische Verkabelung" von Bedeutung.

G 0.01 Feuer

G 0.08 Ausfall oder Störung der Stromversorgung

G 0.12 Elektromagnetische Störstrahlung

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.41 Sabotage

Elementare Gefährdungen / Anforderungen	G 0.01	G 0.08	G 0.12	G 0.18	G 0.25	G 0.26	G 0.27	G 0.41
INF.3.A1		x	x	x	x		x	x
INF.3.A2	x	x	x	x	x			
INF.3.A3		x	x	x	x		x	
INF.3.A4		x	x		x		x	x
INF.3.A5		x	x		x		x	
INF.3.A6		x	x	x				
INF.3.A7	x	x	x					
INF.3.A8	x	x	x					
INF.3.A9		x	x		x			
INF.3.A10		x	x		x			
INF.3.A11		x	x	x	x	x	x	
INF.3.A12	x	x	x					
INF.3.A13		x						x
INF.3.A14		x	x					
INF.3.A15		x	x					
INF.3.A16		x	x			x	x	
INF.3.A17	x							

INF: Infrastruktur

INF.4 IT-Verkabelung

1 Beschreibung

1.1 Einleitung

Die IT-Verkabelung umfasst alle Kommunikationskabel und passiven Komponenten (Rangier- bzw. Spleißverteiler, Patchfelder), die in eigener Hoheit der Institution betrieben werden. Sie ist also die physikalische Grundlage der internen Kommunikationsnetze einer Institution. Die IT-Verkabelung reicht von Übergabepunkten aus einem Fremdnetz (z. B. Anschluss eines TK-Anbieters, DSL-Anbindung eines Internet-Providers) bis zu den Anschlusspunkten der Netzteilnehmer.

1.2 Zielsetzung

Ziel dieses Bausteins ist die IT-Verkabelung so zu schützen, dass die Kommunikation über diese Verbindungen weder mitgehört, noch manipuliert noch gestört werden kann.

1.3 Abgrenzung

Aktive Netzkomponenten (Router, Switches etc.) sind nicht Gegenstand dieses Bausteins. Ebenso ist auch das Thema Funknetze und WLAN ausgeklammert. Diese Themen werden in eigenen Bausteinen des IT-Grundschutz-Kompendiums behandelt. In diesem Baustein wird mit IT-Verkabelung die physische Grundlage eines hersteller- und anwendungsneutralen Kommunikationsnetzes, also eines Local Area Networks (LAN), bezeichnet. Eine Unterscheidung zwischen IT-Verkabelung zum Datentransport und TK-Verkabelung für Telekommunikationsdienste erfolgt nicht.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich IT-Verkabelung von besonderer Bedeutung:

2.1 Kabelbrand

Kabelbrände können erhebliche Schäden nach sich ziehen. Einige dieser Folgen sind zum Beispiel Kurzschlüsse, die Unterbrechung des Schutzleiters, die Entwicklung aggressiver Gase, Feuer oder die Entstehung von Schwelbränden. Kabelbrände bewirken in der Entstehungsphase häufig nur einen geringen Anstieg der Umgebungstemperatur. Damit besteht die zusätzliche Gefährdung, dass eine erhebliche Verrauchung durch "kalten" Brandrauch entsteht, bevor Rauchmelder ansprechen, die an der Raumdecke angebracht sind.

2.2 Unzureichende Netzdimensionierung

Wenn ein IT-Netz nicht ausreichend dimensioniert ist, leidet die Verfügbarkeit. Bei der Planung von Netzen, Trassen, Serverräumen oder Rechenzentren wird oft der Fehler begangen, die funktionale, kapazitive oder sicherheitstechnische Auslegung ausschließlich am aktuellen Bedarf auszurichten. Dabei wird übersehen, dass eine Erweiterung der Kapazität des Netzes durch neue Anforderungen

eben so nötig werden kann wie z. B. durch die Änderung von technischen Standards. Eine Erweiterung von Netzen ist aber nur in dem Umfang möglich, wie es die vorhandenen, verlegten Kabel zulassen oder der zur Verfügung stehende Platz für zusätzliche Kabel erlaubt.

2.3 Unzureichende Dokumentation der Verkabelung

Ist aufgrund unzureichender Dokumentation die genaue Lage von Leitungen nicht bekannt, so kann es bei Bauarbeiten außerhalb oder innerhalb eines Gebäudes zu Beschädigungen von Leitungen kommen. Es kann nicht davon ausgegangen werden, dass alle Kabel und Leitungen in den Installationszonen gemäß gültiger Normen installiert sind. Eine unzureichende Dokumentation erschwert zudem die Prüfung, Wartung und Reparatur von Leitungen.

2.4 Unzulässige Kabelverbindungen

Wenn zwischen IT-Systemen oder anderen technischen Komponenten Kabelverbindungen hergestellt werden, die nicht vorgesehen sind, besteht die Gefahr, dass dadurch Sicherheitsprobleme oder Betriebsstörungen entstehen. Beispielsweise kann es aufgrund solcher unzulässiger Kabelverbindungen passieren, dass unerlaubt auf Netze, Systeme, Informationen oder Anwendungen zugegriffen werden kann. Durch unzulässige Kabelverbindungen können Informationen zusätzlich oder ausschließlich zu falschen Empfängern übertragen werden. Die normale Verbindung kann gestört werden.

2.5 Leitungsbeschädigungen

Je ungeschützter ein Kabel verlegt ist, desto größer ist die Gefahr einer Beschädigung. Eine Beschädigung führt nicht unbedingt sofort zu einem Ausfall von Verbindungen, sondern kann auch sporadische, schwer zu detektierende Übertragungsfehler nach sich ziehen. Auch die zufällige Entstehung unzulässiger Verbindungen ist möglich, wenn beispielsweise Kabelmäntel beziehungsweise Isolierungen nicht mehr vollständig intakt sind. Eine Beschädigung muss dabei nicht zwingend absichtlich erfolgen, sondern kann auch unbeabsichtigt entstehen.

2.6 Leitungsbeeinträchtigung

Die Übertragungseigenschaften von Kabeln mit elektrischer Signalübertragung können durch elektrische und magnetische Felder in ihrem Umfeld negativ beeinflusst werden. Übersprechen ist eine spezielle Form dieser Leitungsbeeinträchtigung. Dabei wird die Störung nicht allgemein im Umfeld, sondern durch Ströme und Spannungen von Signalen erzeugt, die auf eine benachbarte Leitung übertragen werden.

2.7 Abhören und Manipulation von Leitungen

Abhörangriffe auf Leitungen sind eine Gefahr für die Informationssicherheit, die nicht vernachlässigt werden sollte. Grundsätzlich gibt es keine abhörsicheren Kabel. Lediglich hinsichtlich des zum Abhören erforderlichen Aufwands unterscheiden sich die Kabel. Ob eine Leitung tatsächlich abgehört wird, ist nur mit hohem messtechnischem Aufwand feststellbar. Neben dem Abhören von Leitungen stellen weitere bewusste Manipulationen oder gar die Zerstörung von IT-Leitungen eine Gefahr für die Institution dar. Fehlfunktionen von Leitungen können bewusst und in manipulativer Absicht herbeigeführt werden. Solche Manipulationen verfolgen oftmals das Ziel, den IT-Betrieb zu stören oder finanzielle Schäden für die Institution zu verursachen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Bereich IT-Verkabelung aufgeführt. Grundsätzlich ist der Leiter IT für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Leiter IT
Weitere Verantwortliche	Leiter Haustechnik

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

INF.4.A1 Auswahl geeigneter Kabeltypen [Leiter Haustechnik]

Bei der Auswahl von Kabeln MÜSSEN die übertragungstechnischen Notwendigkeiten und die Umgebungsbedingungen bei der Verlegung sowie im Betrieb berücksichtigt werden. Die Auswahl der Kabel aus kommunikationstechnischer Sicht MUSS durch die erforderliche Übertragungsrate und die Entfernung zwischen den Übertragungseinrichtungen bestimmt werden. Im Bezug auf die Umgebungsbedingungen MÜSSEN Faktoren wie z. B. die Temperaturen, Kabelwege, Zugkräfte bei der Verlegung, die Verlegeart und etwaige Störquellen beachtet werden. Des Weiteren MÜSSEN die anzuwendenden Normen und Vorschriften bei der Auswahl der Kabel berücksichtigt werden.

INF.4.A2 Planung der Kabelführung [Leiter Haustechnik]

Kabel, Kabelwege und Kabeltrassen MÜSSEN vor ihrer Verlegung sowohl aus technischer wie auch aus physischer Sicht ausreichend dimensioniert werden. Dabei MÜSSEN zukünftige übertragungstechnische Notwendigkeiten ebenso mit einkalkuliert werden wie genügend Platz für mögliche technische Erweiterungen in Kabelkanälen und -trassen. Bei der gemeinsamen Führung von IT- und Stromverkabelung in einer Trasse MUSS außerdem darauf geachtet werden, das Übersprechen zwischen den einzelnen Kabeln zu vermeiden. Es MUSS darauf geachtet werden, erkennbare Gefahrenquellen zu umgehen.

INF.4.A3 Fachgerechte Installation [Leiter Haustechnik]

Installationsarbeiten an der IT-Verkabelung MÜSSEN sorgfältig und fachkundig erfolgen. Gleichzeitig MÜSSEN alle relevanten Normen beachtet werden. Die entscheidenden Kriterien für eine fachgerechte Ausführung der IT-Verkabelung MÜSSEN vom Auftraggeber in allen Phasen überprüft werden. Bei Anlieferung des Materials MUSS geprüft werden, ob die richtigen Kabel und Anschlusskomponenten geliefert wurden. Bei der Verlegung von IT-Kabeln MUSS besondere Sorgfalt darauf gelegt werden, dass die Montage keine Beschädigungen hervorruft und dass die Kabelwege so gewählt sind, dass Beschädigungen der verlegten Kabel durch die normale Nutzung des Gebäudes ausgeschlossen sind. Zudem MUSS generell darauf geachtet werden, dass IT-Kabel getrennt von der elektrotechnischen Verkabelung geführt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich IT-Verkabelung. Sie SOLLTEN grundsätzlich umgesetzt werden.

INF.4.A4 Anforderungsanalyse für die IT-Verkabelung

Grundsätzlich SOLLTE eine Analyse der Anforderungen, die Einfluss auf eine zukunftssichere, bedarfsgerechte und wirtschaftliche Ausführung der IT-Verkabelung haben, durchgeführt werden. In ihr SOLLTE zunächst die kurzfristig geplante Nutzung durch die Anwender in der Institution und darauf aufbauend die längerfristige Entwicklung der IT-Nutzung abgeschätzt werden. Darüber hinaus MÜSSEN die Schutzziele der Verfügbarkeit, Integrität und Vertraulichkeit bei der Anforderungsanalyse für die IT-Verkabelung mit betrachtet werden.

INF.4.A5 Abnahme der IT-Verkabelung [Leiter Haustechnik]

Die IT-Verkabelung SOLLTE einem Abnahmeprozess unterzogen werden. Diese SOLLTE erst dann erfolgen, wenn alle durchzuführenden Aufgaben abgeschlossen sind, der Ausführende die Maßnahme zur Abnahme gemeldet hat und sich bei den Kontrollen durch den Auftraggeber keine inakzeptablen Mängel gezeigt haben. Der Abnahmetermin SOLLTE zeitlich so gewählt werden, dass die Kontrollen zur Ab-

nahme in ausreichender Zeit vorbereitet werden können. Bei der Abnahme MÜSSEN die Aspekte der Informationssicherheit kontrolliert werden. Für das Abnahmeprotokoll SOLLTE eine Checkliste vorbereitet werden. Die Checkliste SOLLTE auch Punkte zu allgemeinen Anforderungen an die Betriebsräume enthalten. Das Abnahmeprotokoll MUSS von den Teilnehmern und Verantwortlichen unterzeichnet werden.

INF.4.A6 Laufende Fortschreibung und Revision der Netzdokumentation

Die Dokumentation der IT-Verkabelung SOLLTE als ein elementarer Bestandteil einer jeden Veränderung im Netz betrachtet und behandelt werden. Hierbei SOLLTEN alle von der Änderung betroffenen Dokumentationsbereiche leicht erfasst und angepasst werden können. Außerdem SOLLTE geprüft werden, ob der Einsatz eines Dokumentenmanagements für die Netzdokumentation zweckmäßig ist.

INF.4.A7 Entfernen und Deaktivieren nicht mehr benötigter IT-Verkabelung [Leiter Haustechnik]

Wenn IT-Verkabelung nicht mehr benötigt wird, SOLLTE sie fachgerecht und vollständig entfernt werden. IT-Verkabelung, die mit der vorhandenen Technik sinnvoll als Reserve weiter genutzt werden kann, SOLLTE in einem betriebsfähigen Zustand erhalten bleiben. Grundsätzlich SOLLTE eine Übersicht über nicht mehr benötigte Kabel aufgestellt und anhand dieser Dokumentation die Deaktivierung oder der Abbau/Ausbau der Kabel belegt werden. Anschließend MUSS die Dokumentation, in der der Bestand der IT-Verkabelung aufgeführt ist, aktualisiert werden.

INF.4.A8 Brandabschottung von Trassen [Leiter Haustechnik]

Zur Vermeidung von Kabelbränden SOLLTEN Trassen über eine ausreichende Be- und Entlüftung verfügen. Die brandschutztechnischen Auflagen MÜSSEN eingehalten werden. Darüber hinaus SOLLTEN nach Abschluss der Installationsarbeiten die Brandabschottung in regelmäßigen Abständen kontrolliert werden.

INF.4.A9 Dokumentation und Kennzeichnung der IT-Verkabelung

Eine Institution SOLLTE sicherstellen, dass sie für ihre IT-Verkabelung eine interne und eine externe Dokumentation besitzt. Die interne Dokumention MUSS alle Aufzeichnungen, die die Errichtung und den Betrieb der IT-Verkabelung betreffen, enthalten. Die interne Dokumentation SOLLTE so umfangreich angefertigt und gepflegt werden, dass der Betrieb und die zukünftige Weiterentwicklung der IT-Netze bestmöglich unterstützt werden. Die externe Dokumentation der Verkabelung SOLLTE so sparsam wie möglich ausfallen.

INF.4.A10 Neutrale Dokumentation in den Verteilern

In jedem Verteiler SOLLTE sich eine Dokumentation befinden, die den derzeitigen Stand von Rangierungen und Leitungsbelegungen wiedergibt. Diese Dokumentation SOLLTE möglichst neutral gehalten werden. Nur bestehende und genutzte Verbindungen SOLLTEN darin aufgeführt sein. Es SOLLTEN, soweit nicht ausdrücklich vorgeschrieben, keine Hinweise auf die Nutzungsart der Leitungen gegeben werden. Alle weitergehenden Informationen MÜSSEN in einer Revisionsdokumentation aufgeführt werden.

INF.4.A11 Kontrolle bestehender Verbindungen

Alle Verteiler und Zugdosen der Verkabelung SOLLTEN regelmäßig einer (zumindest stichprobenartigen) Sichtprüfung unterzogen werden. Neben der reinen Sichtkontrolle SOLLTE zusätzlich eine funktionale Kontrolle durchgeführt werden. Alle Unregelmäßigkeiten, die bei Sichtkontrollen oder funktionalen Kontrollen festgestellt werden, MÜSSEN unverzüglich dokumentiert und den zuständigen Organisationseinheiten gemeldet werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

INF.4.A12 Redundanzen für die Verkabelung (A)

Es SOLLTE geprüft werden, ob zumindest für wichtige Gebäude eine redundante, über unabhängige Trassen geführte primäre IT-Verkabelung geschaffen werden soll. Ebenso SOLLTE geprüft werden, ob die Anschlüsse an IT- oder TK-Provider redundant ausgelegt werden sollen. Bei hohen oder sehr hohen Verfügbarkeitsanforderungen SOLLTE überlegt werden, in den relevanten Gebäuden die Sekundär- und Tertiärverkabelung redundant auszulegen. Dabei SOLLTE die Sekundärverkabelung über mindestens zwei Steigeschächte geführt werden, die sich in verschiedenen Brandabschnitten des Gebäudes befinden sollten. Wird eine redundante Verkabelung verwendet SOLLTE deren Funktionsfähigkeit regelmäßig geprüft werden.

INF.4.A13 Materielle Sicherung der IT-Verkabelung (IA)

In Räumen mit Publikumsverkehr oder in unübersichtlichen Bereichen eines Gebäudes SOLLTEN Leitungen und Verteiler zusätzlich gegen unbefugte Zugriffe gesichert werden. In jedem Fall SOLLTE die Zahl der Stellen, an denen das verlegte Kabel zugänglich ist, auf ein Mindestmaß reduziert und die Länge der vor unberechtigten Zugriff zu schützenden Verbindungen möglichst klein gehalten werden.

INF.4.A14 Verhinderung von Ausgleichsströmen auf Schirmungen (A)

Die Stromversorgung der IT-Komponenten SOLLTE so gewählt sein, das Störungen durch Ausgleichsströme auf den Schirmungen von Datenleitungen verhindert werden. Je nach Netzform SOLLTEN außerdem Vorkehrungen gegen Einstrahlungen von außen, Abstrahlung durch die Leitung sowie zur Erkennung von Ausgleichsströmen getroffen werden.

INF.4.A15 Nutzung von Schranksystemen (IA)

Zur Verbesserung der Betriebssicherheit von aktiven und passiven Netzkomponenten SOLLTEN diese Geräte in Schranksystemen eingebaut oder aufgestellt werden.

4 Weiterführende Informationen

4.1 Literatur

- [DIN4102] DIN 4102:2016-05
  Brandverhalten von Baustoffen und Bauteilen, Beuth Verlag
- [DIN41494] DIN 41494
  Bauweisen für elektronische Einrichtungen, Beuth Verlag
- [DIN60297] DIN IEC 60297
  Bauweisen für elektronische Einrichtungen, Beuth Verlag
- [EN50173] EN 50173:2007
  Informationstechnik - Anwendungsneutrale Kommunikationskabelanlagen, Beuth Verlag
- [EN50174] EN 50174:2009
  Informationstechnik - Installation von Kommunikationsverkabelung, Beuth Verlag

- [EN50310] EN 50310:2010
  Anwendung von Maßnahmen für Erdung und Potentialausgleich in Gebäuden mit Einrichtungen der Informationstechnik, VDE Verlag, 2010

- [EN50346] EN 50346:2010
  Prüfung installierter Verkabelung, Beuth Verlag, 2010

- [IEC60364] IEC60364- Einrichten von Niederspannungsanlagen
  Beuth Verlag

- [IEEE8023] IEEE8023
  IEEE 802.3 – Standards in Lokalen Netzen, CSMA/CD, Ethernet Working Group, (zuletzt abgerufen am 28.09.2017)
  http://www.ieee802.org/3/

- [ISO11801] ISO/IEC 11801:2010
  Informationstechnik - Anwendungsneutrale Standortverkabelung, ISO, 2010

- [VDE100] DIN VDE 0100- Bestimmung für das Errichten von Starkstromanlagen mit Notspannungen bis 1000V
  VDE Verlag

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "IT-Verkabelung" von Bedeutung.

G 0.01 Feuer

G 0.02 Ungünstige klimatische Bedingungen

G 0.09 Ausfall oder Störung von Kommunikationsnetzen

G 0.12 Elektromagnetische Störstrahlung

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.37 Abstreiten von Handlungen

G 0.41 Sabotage

Elementare Gefährdungen / Anforderungen	G 0.01	G 0.02	G 0.09	G 0.12	G 0.15	G 0.18	G 0.20	G 0.21	G 0.25	G 0.26	G 0.27	G 0.29	G 0.37	G 0.41
INF.4.A1			x	x		x	x		x	x	x			
INF.4.A2	x	x	x	x		x		x	x	x		x		x
INF.4.A3	x		x		x			x	x	x		x	x	x
INF.4.A4	x		x						x	x				x
INF.4.A5		x				x	x	x	x	x	x	x		x
INF.4.A6	x							x	x	x		x	x	x
INF.4.A7						x							x	
INF.4.A8					x			x						
INF.4.A9					x	x							x	
INF.4.A10					x									
INF.4.A11			x	x				x	x	x				
INF.4.A12	x		x						x	x	x			x
INF.4.A13			x		x			x	x					x
INF.4.A14			x	x					x	x				
INF.4.A15					x			x	x					x

INF: Infrastruktur

INF.7 Büroarbeitsplatz

1 Beschreibung

1.1 Einleitung

Ein Büroraum ist der Bereich innerhalb einer Institution, in dem sich ein oder mehrere Mitarbeiter aufhalten, um dort ihre Aufgaben zu erfüllen. In diesem Baustein werden die typischen Gefährdungen und Anforderungen bezüglich der Informationssicherheit für einen Büroraum beschrieben.

1.2 Zielsetzung

Ziel des Bausteins ist der Schutz der Informationen, die in Büroräumen bearbeitet werden.

1.3 Abgrenzung

Dieser Baustein betrachtet technische und nichttechnische Sicherheitsanforderungen für Büroräume. Empfehlungen, wie die IT-Systeme in diesen Räumen konfiguriert und abgesichert werden können, werden in diesem Baustein nicht behandelt. Hinweise dafür sind u. a. in SYS.2.1 *Allgemeiner Client* sowie in den betriebssystemspezifischen Bausteinen zu finden.

Auch auf die Verkabelung von Büroräumen wird nicht eingegangen. Dazu müssen die Bausteine INF.3 *Elektrotechnische Verkabelung* und INF.4 *IT-Verkabelung* gesondert betrachtet werden. Anforderungen zum Brandschutz und Zutrittsregelung in Gebäuden sind im Baustein INF.1 *Allgemeines Gebäude* zu finden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Büroraum von besonderer Bedeutung:

2.1 Unbefugter Zutritt

Fehlen Zutrittskontrollen oder sind diese unzureichend, können unberechtigte Personen einen Büroraum betreten und schützenswerte Daten entwenden, Geräte stehlen oder sie manipulieren. Dadurch kann die Verfügbarkeit, Vertraulichkeit oder Integrität von Geräten und Informationen beeinträchtigt werden. Selbst wenn keine unmittelbaren Schäden erkennbar sind, kann der Betriebsablauf schon dadurch gestört werden, dass untersucht werden muss, wie ein solcher Vorfall möglich war, ob Schäden aufgetreten sind oder Manipulationen vorgenommen wurden.

2.2 Beeinträchtigung durch ungünstige Arbeitsbedingungen

Ein nicht nach ergonomischen Gesichtspunkten eingerichteter Büroraum oder ein ungünstiges Arbeitsumfeld können dazu führen, dass Mitarbeiter dort nicht ungestört arbeiten oder die verwendete IT nicht oder nicht optimal benutzen können. Die Störungen reichen von Lärm oder starkem Kundenverkehr bis zu ungünstiger Beleuchtung und schlechter Belüftung. Dadurch werden Arbeitsabläufe eingeschränkt und Mitarbeiterpotenziale unzureichend genutzt. Es können sich bei der Arbeit auch Fehler einschleichen, wodurch die Integrität von Daten vermindert werden kann.

2.3 Reinigungs- und Fremdpersonal oder Besucher

Bei kleineren bzw. kurzen Besprechungen ist es meist effizienter, den Besuch im Büro zu empfangen. Dabei kann der Besuch ebenso wie auch Reinigungs- und Fremdpersonal auf verschiedene Art und Weise interne Informationen einsehen, Geschäftsprozesse gefährden und IT-Systeme manipulieren, angefangen von der unsachgemäßen Behandlung der technischen Einrichtungen über den Versuch des "Spielens" an IT-Systemen bis zum Diebstahl von Unterlagen oder IT-Komponenten. So kann beispielsweise durch Reinigungspersonal versehentlich eine Steckverbindung gelöst werden oder Wasser in die IT gelangen, auch können Unterlagen verlegt oder sogar mit dem Abfall entsorgt werden.

2.4 Manipulation oder Zerstörung von IT, Zubehör, Informationen und Software im Büroraum

Angreifer können aus unterschiedlichen Beweggründen heraus versuchen, IT-Systeme, Zubehör und andere Datenträger zu manipulieren oder zu zerstören. Die Angriffe können umso wirkungsvoller sein, je später sie durch den Mitarbeiter oder die Institution selbst entdeckt werden, je umfassender die Kenntnisse der Täter und je tiefgreifender die Folgen für einen Arbeitsvorgang sind. Die Manipulationen reichen von der unerlaubten Einsichtnahme in die schützenswerten Daten des Mitarbeiters bis hin zur Zerstörung von Datenträgern oder IT-Systemen. Erhebliche Ausfallzeiten und Prozesseinschränkungen können die Folge sein.

2.5 Diebstahl

Da IT-Geräte immer handlicher werden, ist es umso leichter, sie unbemerkt in die Tasche zu stecken. Durch den Diebstahl von Datenträgern, IT-Systemen, Zubehör, Software oder Daten entstehen einerseits Kosten für die Wiederbeschaffung sowie für die Wiederherstellung eines arbeitsfähigen Zustandes, andererseits Verluste aufgrund mangelnder Verfügbarkeit. Darüber hinaus könnte die Person, die die IT-Geräte entwendet hat, vertrauliche Information einsehen und offenlegen, wodurch es zu weiteren Schäden kommen kann. Diese wiegen in vielen Fällen deutlich schwerer als der rein materielle Verlust des Gerätes.

Gestohlen werden neben teuren IT-Systemen häufig auch mobile Endgeräte, die unauffällig und leicht transportiert werden können. Wenn die Büroräume nicht verschlossen, beaufsichtigt oder die IT-Systeme nicht ausreichend gesichert sind, kann die Technik dementsprechend schnell und unauffällig entwendet werden.

2.6 Fliegende Verkabelung

Je nach Lage der Anschlusspunkte der Steckdosen, der Stromversorgung und des Datennetzes im Büroraum könnten Kabel quer durch den Raum, auch über Verkehrswege hinweg, verlegt werden. Solche "fliegenden" Kabel sind nicht nur Stolperfallen, an denen sich Personen verletzen können. Wenn Personen daran hängen bleiben, können auch IT-Geräte beschädigt werden.

2.7 Vandalismus

Durch Vandalismus wird fremdes Eigentum zerstört oder beschädigt. Die Auswirkungen sind mit denen eines Anschlags sehr verwandt, nur dass Vandalismus nicht wie dieser gezielt geplant und umgesetzt wird, sondern meist Ausdruck spontaner, blinder Zerstörungswut ist. Sowohl Außentäter (enttäuschte Einbrecher) als auch Innentäter (frustrierte oder psychisch labile Mitarbeiter) kommen dafür in Betracht. Mögliche Auslöser für Vandalismus können unter anderem Meinungsverschiedenheiten, persönliche Probleme, Mobbing oder ein schlechtes Betriebsklima sein.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz von Büroräumen aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragter (ISB) für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der ISB ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist er dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	Informationssicherheitsbeauftragter (ISB)
Weitere Verantwortliche	Leiter Haustechnik, Leiter IT, Mitarbeiter, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

INF.7.A1 Geeignete Auswahl und Nutzung eines Büroraumes [Mitarbeiter, Vorgesetzte]

Es DÜRFEN NUR geeignete Räume als Büroraume genutzt werden. Auch MÜSSEN die Büroräume für den Schutzbedarf bzw. das Schutzniveau der dort verarbeiteten Informationen angemessen ausgewählt und ausgestattet sein. So MÜSSEN Büroräume mit Publikumsverkehr in nicht sicherheitsrelevanten Bereichen liegen. Für den Arbeitsplatz und für die Einrichtung eines Büroraumes MUSS die Arbeitsstättenverordnung umgesetzt werden.

INF.7.A2 Geschlossene Fenster und abgeschlossene Türen [Mitarbeiter]

Wenn Mitarbeiter ihre Büroräume verlassen, MÜSSEN alle Fenster geschlossen werden. Befinden sich vertrauliche Informationen in dem Büroraum, SOLLTEN beim Verlassen die Türen abgeschlossen werden. Dies SOLLTE insbesondere in Bereichen mit Publikumsverkehr beachtet werden. Die entsprechenden Vorgaben SOLLTEN in einer geeigneten Anweisung festgehalten werden. Alle Mitarbeiter SOLLTEN dazu verpflichtet werden, die Anweisung umzusetzen. Zusätzlich MUSS regelmäßig geprüft werden, ob beim Verlassen die Fenster geschlossen und, wenn notwendig, die Türen abgeschlossen werden. Ebenso MUSS darauf geachtet werden, dass Brand- und Rauchschutztüren tatsächlich geschlossen werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Büroarbeitsplatz. Sie SOLLTEN grundsätzlich umgesetzt werden.

INF.7.A3 Fliegende Verkabelung

Die Stromanschlüsse und Zugänge zum Datennetz im Büroraum SOLLTEN sich in der Nähe des Ortes befinden, wo die IT-Geräte aufgestellt sind. Verkabelungen, die über den Boden verlaufen, SOLLTEN mit einem Kabelschacht abgedeckt werden.

INF.7.A4 Zutrittsregelungen und -kontrolle

Es SOLLTE gewährleistet werden, dass Unberechtigte die Büroräume nicht betreten können. Dafür SOLLTE ein Sicherheitskonzept erstellt und umgesetzt werden. Zudem SOLLTE regelmäßig überprüft werden, ob die ergriffenen Maßnahmen wirksam sind.

INF.7.A5 Ergonomischer Arbeitsplatz [Leiter Haustechnik]

Die Arbeitsplätze aller Mitarbeiter SOLLTEN ergonomisch eingerichtet sein. Vor allem die Bildschirme SOLLTEN so aufgestellt werden, dass ein ergonomisches und ungestörtes Arbeiten möglich ist. Dabei SOLLTE beachtet werden, dass Bildschirme nicht durch Unbefugte eingesehen werden können. Die Bildschirmarbeitsschutzverordnung (BildscharbV) SOLLTE umgesetzt werden.Alle Arbeitsplätze SOLLTEN für eine möglichst fehlerfreie Bedienung der IT individuell verstellbar sein.

INF.7.A6 Aufgeräumter Arbeitsplatz [Mitarbeiter]

Jeder Mitarbeiter SOLLTE dazu angehalten werden, seinen Arbeitsplatz aufgeräumt zu hinterlassen. Benutzer SOLLTEN dafür sorgen, dass Unbefugte keinen Zugang zu IT-Anwendungen erhalten oder vertrauliche Informationen einsehen können. Alle Mitarbeiter SOLLTEN sorgfältig ihre Arbeitsplätze überprüfen und sicherstellen, dass keine vertraulichen Informationen frei zugänglich sind. Vorgesetzte SOLLTEN sporadisch Arbeitsplätze daraufhin überprüfen, ob dort schutzbedürftige Informationen offen zugreifbar sind.

INF.7.A7 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeiter, Leiter Haustechnik]

Die Mitarbeiter SOLLTEN angewiesen werden, vertrauliche Dokumente und Datenträger verschlossen aufzubewahren, wenn sie nicht verwendet werden. Dafür SOLLTEN geeignete Behältnisse in den Büroräumen oder in deren Umfeld aufgestellt werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

INF.7.A8 Einsatz von Diebstahlsicherungen [Mitarbeiter, Leiter IT] (CIA)

Wenn der Zutritt zu den Räumen nicht geeignet beschränkt werden kann, SOLLTEN für alle IT-Systeme Diebstahlsicherungen eingesetzt werden. In Bereichen mit Publikumsverkehr SOLLTEN generell Diebstahlsicherungen benutzt werden.

4 Weiterführende Informationen

4.1 Literatur

- [27001A12.2] ISO/IEC 27001: 2013 - Annex A.12.2 Protction from malware
  Information technology - Security technigues - Information security management systems - Requirements, insbesondere Annex A, A.12.2 Protection from malware, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [ArbStättV] Arbeitsstättenverordnung
  Bundesministerium für Arbeit und Soziales (BMAS), (zuletzt abgerufen am 28.09.2017)
  http://www.bmas.de/DE/Service/Gesetze/arbeitsstaettenverordnung.html

- [BildscharbV] Bildschirmarbeitsschutzverordnung
  ArbSchG, (zuletzt abgerufen am 28.09.2017)
  https://www.arbeitsschutzgesetz.org/bildscharbv/

- [DIN1627] DIN EN 1627:2011-09
  Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Anforderungen und Klassifizierung, 2011

- [ISFCF19] The Standard of Good Practice - AREA CF19 Physical and Environmental Security insbesondere AREA CF19 Physical and Environmental Security, ISF, 06.2014

- [NIST80053PEP] NIST Special Publication 800-53 Revision 4 - APPENDIX PAGE F-213 Assesing Security and Privacy Controls for Federal Information Systems and Organizations, insbesondere APPENDIX F-PS PAGE F-213, FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION, NIST, 2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Büroarbeitsplatz" von Bedeutung.

G 0.02 Ungünstige klimatische Bedingungen

G 0.13 Abfangen kompromittierender Strahlung

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.02	G 0.13	G 0.14	G 0.15	G 0.16	G 0.18	G 0.21	G 0.22	G 0.23	G 0.24	G 0.30	G 0.44	G 0.46
INF.7.A1	x	x	x	x	x	x				x		x	
INF.7.A2			x		x			x	x	x	x	x	x
INF.7.A3						x							
INF.7.A4			x		x		x	x	x	x	x	x	x
INF.7.A5													
INF.7.A6			x					x					x
INF.7.A7			x	x	x		x	x	x				x
INF.7.A8					x								

INF: Infrastruktur

INF.8 Häuslicher Arbeitsplatz

1 Beschreibung

1.1 Einleitung

Telearbeiter, freie Mitarbeiter oder Selbstständige arbeiten typischerweise von häuslichen Arbeitsplätzen aus. Im Gegensatz zum Arbeitsplatz in einer Büroumgebung nutzen Mitarbeiter bei einem häuslichen Arbeitsplatz einen Arbeitsplatz im eigenen Wohnumfeld. Dabei muss ermöglicht werden, dass die berufliche Sphäre hinreichend von der privaten getrennt ist. Wenn Mitarbeiter häusliche Arbeitsplätze dauerhaft benutzen, müssen zudem diverse rechtliche Anforderungen erfüllt sein, beispielsweise müssen die Arbeitsplätze arbeitsmedizinischen und ergonomischen Bestimmungen entsprechen.

Bei einem häuslichen Arbeitsplatz kann nicht die gleiche infrastrukturelle Sicherheit vorausgesetzt werden, wie sie in den Büroräumen einer Institution anzutreffen ist, so ist z. B. oft der Arbeitsplatz auch für Besucher oder Familienangehörige zugänglich. Deshalb müssen Maßnahmen ergriffen werden, mit denen sich ein Sicherheitsniveau erreichen lässt, das mit einem Büroraum vergleichbar ist.

1.2 Zielsetzung

In diesem Baustein wird aufgezeigt, wie sich die Infrastruktur eines häuslichen Arbeitsplatzes sicher aufbauen und betreiben lässt. Kernziel des Bausteins ist der Schutz der Informationen der Institution am häuslichen Arbeitsplatz.

1.3 Abgrenzung

Der Baustein enthält grundsätzliche Anforderungen, die zu beachten und zu erfüllen sind, um den spezifischen Gefährdungen für einen häuslichen Arbeitsplatz entgegenwirken zu können. Dabei werden jedoch nur spezifische Anforderungen an die Infrastruktur für einen ortsfesten Arbeitsplatz mit Zugang durch Dritte definiert. Sicherheitsanforderungen für die eingesetzten IT-Systeme (z. B. Rechner) und insbesondere für die technischen Anteile der Telearbeit (z. B. Kommunikationsverbindungen) sind dagegen nicht Gegenstand des vorliegenden Bausteins, sondern werden in OPS.1.2.4 *Telearbeit* bzw. in den jeweiligen system-spezifischen Bausteinen beschrieben.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für einen häuslichen Arbeitsplatz von besonderer Bedeutung:

2.1 Fehlende oder unzureichende Regelungen für den häuslichen Arbeitsplatz

Da ein häuslicher Arbeitsplatz räumlich außerhalb der Institution liegt, sind die Mitarbeiter dort weitgehend auf sich allein gestellt. Dadurch können durch fehlende oder unzureichende Regelungen für das häusliche Arbeitsplatzumfeld IT-Probleme mit erhöhten Ausfallzeiten entstehen. Wenn

IT-Probleme nicht per Fernadministration geklärt werden können, muss beispielsweise ein IT-Betreuer aus der Institution erst zum häuslichen Arbeitsplatz fahren, um dort die Probleme zu beseitigen. Wenn der Umgang mit internen und vertraulichen Informationen am häuslichen Arbeitsplatz nicht nachvollziehbar geregelt ist, könnte es passieren, dass Mitarbeiter solche Informationen falsch aufbewahren. Dadurch kann die Vertraulichkeit und Integrität der Informationen gefährdet sein, da nicht ausreichend verhindert werden kann, dass Informationen ausgespäht oder modifiziert werden.

2.2 Unbefugter Zutritt zu schutzbedürftigen Räumen des häuslichen Arbeitsplatzes

Räume eines häuslichen Arbeitsplatzes, in denen schutzbedürftige Informationen aufbewahrt und weiterverarbeitet werden oder in denen schutzbedürftige Geräte stehen, werden dadurch zu schutzbedürftigen Räumen. Wenn unbefugte Personen diese Räume unbeaufsichtigt betreten können, ist die Vertraulichkeit, Integrität und Verfügbarkeit der dort befindlichen Daten und Informationen erheblich gefährdet.

Beispiele:

- Ein Mitarbeiter hatte zuhause zwar ein separates Arbeitszimmer eingerichtet, aber es nicht konsequent abgeschlossen. Als die Kleinkinder kurz unbeaufsichtigt waren, spielten sie in dem nicht verschlossenen Arbeitszimmer. Dabei wurden wichtige Dokumente als Malgrundlage verwendet.
- Als ein Mitarbeiter am häuslichen Arbeitsplatz in eine Projektarbeit vertieft war, bekam er überraschend Besuch. Während er in der Küche Kaffee kochte, wollte der Besucher am nicht gesperrten Rechner schnell etwas im Internet recherchieren und hat diesen dabei versehentlich mit Schadsoftware infiziert.

2.3 Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen am häuslichen Arbeitsplatz

Ein nicht nach ergonomischen Gesichtspunkten eingerichteter häuslicher Arbeitsplatz oder ein ungünstiges Arbeitsumfeld können dazu führen, dass dort nicht ungestört gearbeitet werden kann oder die verwendete IT nicht oder nicht optimal benutzt werden kann. Die Störungen reichen von Lärm oder starkem Kundenverkehr bis zu ungünstiger Beleuchtung und schlechter Belüftung. Dadurch werden Arbeitsabläufe eingeschränkt und Mitarbeiterpotenziale unzureichend genutzt. Es können sich bei der Arbeit auch Fehler einschleichen, die Integrität von Daten kann vermindert werden.

2.4 Ungesicherter Akten- und Datenträgertransport

Wenn Dokumente, Datenträger oder Akten zwischen der Institution und dem häuslichen Arbeitsplatz transportiert werden, besteht die Gefahr, dass diese Daten und Informationen verloren gehen oder auch von unbefugten Dritten entwendet, gelesen oder manipuliert werden. Der Akten- und Datenträgertransport kann auf verschiedene Arten unzureichend gesichert sein:

- Werden Unikate transportiert (fehlendes Backup), können nach Verlust Ziele und Aufgaben nicht wie geplant erreicht werden.
- Fallen unverschlüsselte Datenträger in falsche Hände, kann das zu schwerwiegenden Vertraulichkeitsverlusten führen.
- Wenn unterwegs kein ausreichender Zugriffsschutz vorhanden ist, können Akten oder Datenträger unbemerkt kopiert oder manipuliert werden.

2.5 Ungeeignete Entsorgung der Datenträger und Dokumente

Ist es Mitarbeitern am häuslichen Arbeitsplatz nicht möglich, Datenträger und Dokumente geeignet zu entsorgen, besteht die Gefahr, dass diese in den Hausmüll geworfen werden. Angreifer können jedoch hieraus wertvolle Informationen gewinnen, die sich gezielt für Erpressungsversuche oder zur Wirtschaftsspionage missbrauchen lassen. Die Folgen reichen vom Know-how-Verlust bis zur Existenzgefährdung der Institution, zum Beispiel wenn dadurch wichtige Aufträge nicht zustande kommen oder Partnerschaften scheitern.

2.6 Manipulation oder Zerstörung von IT, Zubehör, Informationen und Software am häuslichen Arbeitsplatz

IT-Geräte, Zubehör, Informationen und Software, die am häuslichen Arbeitsplatz benutzt werden, können unter Umständen einfacher manipuliert oder zerstört werden als in der Institution. Der häusliche Arbeitsplatz ist oft für Kunden, Angehörige und Besucher der Familie zugänglich. Auch sind hier die zentralen Schutzmaßnahmen der Institution nicht vorhanden, zum Beispiel Pförtnerdienste. Wenn IT-Geräte, Zubehör, Informationen oder Software manipuliert oder zerstört werden, ist der Mitarbeiter am häuslichen Arbeitsplatz oft nur noch eingeschränkt arbeitsfähig. Des Weiteren müssen womöglich zerstörte IT-Komponenten, Informationen und Softwarelösungen ersetzt werden, was sowohl finanzielle als auch zeitliche Ressourcen erfordert.

2.7 Gefährdung durch Reinigungs- oder Fremdpersonal

Reinigungs- und Fremdpersonal können interne Informationen, Geschäftsprozesse und IT-Systeme auf verschiedene Art und Weise gefährden, angefangen von der unsachgemäßen Behandlung der technischen Einrichtungen, über den Versuch des "Spielens" an IT-Systemen bis zum Diebstahl von Unterlagen oder IT-Komponenten. So kann beispielsweise durch Reinigungspersonal versehentlich eine Steckverbindung gelöst werden, Wasser in die IT gelangen, Unterlagen verlegt oder sogar mit dem Abfall entfernt werden.

2.8 Erhöhte Diebstahlgefahr am häuslichen Arbeitsplatz

Der häusliche Arbeitsplatz ist meistens nicht so gut abgesichert wie der Arbeitsplatz in einem Unternehmen oder einer Behörde. Durch aufwendigere Vorkehrungen (z. B. Sicherheitstüren, Pförtnerdienst) ist dort die Gefahr, dass jemand unbefugt in das Gebäude eindringt, weitaus geringer als bei einem Privathaus. Einbrecher stehlen meistens vorrangig Gegenstände, die schnell und einfach verkauft werden können. Dabei kann auch dienstliche IT gestohlen werden. Die auf den entwendeten dienstlichen IT-Systemen vorhandenen Informationen besitzen aber oft einen höheren Wert als die IT-Systeme selber. Einbrecher könnten versuchen, durch Erpressung oder Weitergabe der Daten an Konkurrenzunternehmen einen höheren Gewinn als durch den Verkauf der Hardware zu erzielen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz des häuslichen Arbeitsplatzes aufgeführt. Grundsätzlich ist der Mitarbeiter für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Mitarbeiter
Weitere Verantwortliche	Haustechnik, Informationssicherheitsbeauftragter (ISB)

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

INF.8.A1 Sichern von dienstlichen Unterlagen am häuslichen Arbeitsplatz

Dienstliche Unterlagen und Datenträger MÜSSEN am häuslichen Arbeitsplatz so aufbewahrt werden, dass kein Unbefugter darauf zugreifen kann. Daher MÜSSEN ausreichende verschließbare Behältnisse (Schreibtisch, Rollcontainer, Schrank etc.) vorhanden sein. Jeder Mitarbeiter MUSS seinen häuslichen Arbeitsplatz aufgeräumt hinterlassen und sicherstellen, dass keine sensitiven Informationen frei zugänglich sind.

INF.8.A2 Transport von Arbeitsmaterial zum häuslichen Arbeitsplatz [Haustechnik]

Es MUSS geregelt werden, welche Datenträger und Unterlagen am häuslichen Arbeitsplatz bearbeitet und zwischen der Institution und dem häuslichen Arbeitsplatz hin und her transportiert werden dürfen. Generell MÜSSEN Datenträger und andere Unterlagen sicher transportiert werden. Die Regelungen MÜSSEN den Mitarbeitern geeignet bekanntgegeben werden.

INF.8.A3 Schutz vor unbefugtem Zutritt am häuslichen Arbeitsplatz [Haustechnik]

Den Mitarbeitern MUSS bekanntgegeben werden, welche Regelungen und Maßnahmen zum Einbruchs- und Zutrittsschutz zu beachtet sind. So MUSS darauf hingewiesen werden, Fenster zu schließen und Türen abzuschließen, wenn der häusliche Arbeitsplatz nicht besetzt ist.

Es MUSS sichergestellt werden, dass Unbefugte zu keiner Zeit den häuslichen Arbeitsplatz betreten und auf dienstliche IT und Unterlagen zugreifen können. Diese Maßnahmen MÜSSEN in sinnvollen zeitlichen Abständen, mindestens aber bei einer Änderung der häuslichen Verhältnisse überprüft werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Häuslicher Arbeitsplatz. Sie SOLLTEN grundsätzlich umgesetzt werden.

INF.8.A4 Geeignete Einrichtung des häuslichen Arbeitsplatzes [Haustechnik]

Der häusliche Arbeitsplatz SOLLTE durch eine geeignete Raumaufteilung von den privaten Bereichen der Wohnung getrennt sein.

Der häusliche Arbeitsplatz SOLLTE über eine geeignete Einrichtung verfügen, die den ergonomischen Anforderungen entspricht.

Ebenso SOLLTE der häusliche Arbeitsplatz durch geeignete technische Sicherungsmaßnahmen vor Einbrüchen geschützt werden. Die Schutzmaßnahmen SOLLTEN an die örtlichen Gegebenheiten und den vorliegenden Schutzbedarf angepasst sein.

INF.8.A5 Entsorgung von vertraulichen Informationen am häuslichen Arbeitsplatz [Haustechnik]

Vertrauliche Informationen SOLLTEN sicher entsorgt werden, also nicht einfach in den Hausmüll. In einer speziellen Sicherheitsrichtlinie SOLLTE daher geregelt werden, wie schutzbedürftiges Material zu beseitigen ist. Es SOLLTEN die dafür benötigten Entsorgungseinrichtungen verfügbar sein.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

INF.8.A6 Umgang mit dienstlichen Unterlagen bei erhöhtem Schutzbedarf am häuslichen Arbeitsplatz [Informationssicherheitsbeauftragter (ISB)] (CIA)

Wenn Mitarbeiter dienstliche Unterlagen oder Informationen mit erhöhtem Schutzbedarf bearbeiten müssen, SOLLTE überlegt werden, von einem häuslichen Arbeitsplatz ganz abzusehen. Anderenfalls SOLLTE der häusliche Arbeitsplatz durch erweiterte, hochwertige technische Sicherungsmaßnahmen geschützt werden.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [DIN1627] DIN EN 1627:2011-09
  Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Anforderungen und Klassifizierung, 2011

- [ISF] The Standard of Good Practice - Area BA2.3 Protection of Databases
  The Standard of Good Practice, Information Security Forum, ISF, 06.2016

- [NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations
  Special Publication 800-53, Revision 4, NIST, 04.2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Häuslicher Arbeitsplatz" von Bedeutung.

G 0.01 Feuer

G 0.02 Ungünstige klimatische Bedingungen

G 0.03 Wasser

G 0.04 Verschmutzung, Staub, Korrosion

G 0.13 Abfangen kompromittierender Strahlung

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.41 Sabotage

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

Elementare Gefährdungen / Anforderungen	G 0.01	G 0.02	G 0.03	G 0.04	G 0.13	G 0.14	G 0.15	G 0.16	G 0.17	G 0.19	G 0.22	G 0.23	G 0.24	G 0.30	G 0.32	G 0.41	G 0.44
INF.8.A1		x		x		x		x	x	x	x					x	
INF.8.A2						x		x	x	x	x						
INF.8.A3							x	x	x	x			x		x	x	x
INF.8.A4	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x
INF.8.A5						x			x	x							
INF.8.A6	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

INF: Infrastruktur

INF.9 Mobiler Arbeitsplatz

1 Beschreibung

1.1 Einleitung

Eine gute Netzabdeckung sowie leistungsfähige IT-Geräte, wie z. B. Laptops, Smartphones oder Tablets, ermöglichen es Mitarbeitern, nahezu an jedem Platz bzw. von überall zu arbeiten. Das bedeutet, dass dienstliche Aufgaben häufig nicht mehr nur in den Räumen und Gebäuden der Institution erfüllt werden, sondern an wechselnden Arbeitsplätzen in unterschiedlichen Umgebungen, z. B. in Hotelzimmern, Zügen oder bei Kunden. Die dabei verarbeitenden Informationen müssen angemessen geschützt werden.

Das mobile Arbeiten verändert einerseits die Dauer, Lage und Verteilung der Arbeitszeiten und es erhöht andererseits die Anforderungen an die Informationssicherheit, da in mobilen Arbeitsplatz-Umgebungen keine sichere IT-Infrastruktur, wie sie in einer Büroumgebung anzutreffen ist, vorausgesetzt werden kann.

1.2 Zielsetzung

Der Baustein beschreibt Sicherheitsanforderungen an mobile Arbeitsplätze. Ziel ist es, für solche Arbeitsplätze eine mit einem Büroraum vergleichbare Sicherheitssituation herbeizuführen.

1.3 Abgrenzung

Der Baustein enthält grundsätzliche Anforderungen, die zu beachten und zu erfüllen sind, wenn Mitarbeiter häufig nicht nur innerhalb der Räumlichkeiten der Institution arbeiten, sondern an wechselnden Arbeitsplätzen außerhalb.

Er bildet vor allem die organisatorischen, technischen und personellen Anforderungen an die gänzliche oder teilweise mobile Arbeit ab. Um IT-Systeme, Datenträger oder Unterlagen, die beim mobilen Arbeiten genutzt werden, abzusichern, müssen alle relevanten Bausteine wie zum Beispiel SYS.3.1 *Laptop*, SYS.3.2 *Tablet und Smartphone,* SYS.3.4 *Mobile Datenträger,* NET.3.3 *VPN,* SYS.2.1 *Allgemeiner Client, INF.1 Gebäude oder INF.8 Häuslicher Arbeitsplatz* gesondert berücksichtigt werden.

Ebenso sind die Sicherheitsanforderungen an Bildschirmarbeitsplätze, die vom Arbeitgeber fest eingerichtet werden (Telearbeitsplätze) nicht Gegenstand des vorliegenden Bausteins, sondern werden in OPS.1.2.4 *Telearbeit* beschrieben.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich des mobilen Arbeitsplatzes von besonderer Bedeutung:

2.1 Fehlende oder unzureichende Regelungen für mobile Arbeitsplätze

Ist das mobile Arbeiten nicht oder nur unzureichend geregelt, können der Institution unter anderem finanzielle Schäden entstehen. Ist beispielsweise nicht geregelt, welche Informationen außerhalb der Institution transportiert und bearbeitet werden dürfen und welche Schutzvorkehrungen dabei zu beachten sind, können vertrauliche Informationen in fremde Hände gelangen. Diese können dann von Unbefugten möglicherweise zum schwerwiegenden Nachteil der Institution verwendet werden.

2.2 Beeinträchtigung durch wechselnde Einsatzumgebung

Da mobile Datenträger und Endgeräte in sehr unterschiedlichen Umgebungen eingesetzt werden, sind sie einer Vielzahl von Gefährdungen ausgesetzt. Dazu gehören beispielsweise schädigende Umwelteinflüsse (zum Beispiel hohe oder zu niedrige Temperaturen), ebenso wie Staub, Feuchtigkeit oder Transportschäden.

Neben diesen Einflüssen sind auch die Einsatzumgebungen mit ihrem unterschiedlichen Sicherheitsniveau zu berücksichtigten. Besonders Smartphones, Tablets, Laptops und ähnliche mobile Endgeräte sind nicht nur beweglich, sondern können auch mit anderen IT-Systemen kommunizieren. Hierbei können beispielsweise Schadprogramme übertragen oder schützenswerte Informationen kopiert werden. So können eventuell Aufgaben nicht mehr erfüllt, Kundentermine nicht wahrgenommen oder IT-Systeme beschädigt werden.

2.3 Manipulation oder Zerstörung von IT-Systemen, Zubehör, Informationen und Software am mobilen Arbeitsplatz

IT-Systeme, Zubehör, Informationen und Software, die mobil genutzt werden, können unter Umständen einfacher manipuliert oder zerstört werden als in der Institution. Der mobile Arbeitsplatz ist oft für Dritte zugänglich. Auch sind hier die zentralen Schutzmaßnahmen der Institution nicht vorhanden, zum Beispiel Pförtnerdienste. Werden IT-Systeme, Zubehör, Informationen oder Software manipuliert oder zerstört, ist der Mitarbeiter am mobilen Arbeitsplatz oft nur noch eingeschränkt arbeitsfähig. Des Weiteren müssen womöglich zerstörte IT-Komponenten oder Softwarelösungen ersetzt werden, was sowohl finanzielle als auch zeitliche Ressourcen erfordert.

2.4 Verzögerungen durch temporär eingeschränkte Erreichbarkeit

Meist hat ein Mitarbeiter am mobilen Arbeitsplatz keine festen Arbeitszeiten und ist unterwegs mitunter auch schwer erreichbar. Dadurch kann sich der Informationsfluss deutlich verzögern. Selbst wenn die Informationen über E-Mail übermittelt werden, verkürzt sich nicht zwingend die Reaktionszeit, da nicht sichergestellt werden kann, dass der mobile Mitarbeiter die E-Mail zeitnah liest. Die temporär eingeschränkte Erreichbarkeit wirkt sich dabei je nach Situation und Institution unterschiedlich aus, kann aber die Verfügbarkeit von Informationen stark einschränken.

2.5 Ungesicherter Akten- und Datenträgertransport

Wenn Dokumente, Datenträger oder Akten zwischen der Institution und den mobilen Arbeitsplätzen transportiert werden, können diese Informationen und Daten verloren gehen oder auch von unbefugten Dritten entwendet, gelesen oder manipuliert werden. Dadurch können der Institution größere finanzielle Schäden entstehen. Der Akten- und Datenträgertransport kann auf verschiedene Arten unzureichend gesichert sein:

- Werden Unikate transportiert (fehlendes Backup), können nach Verlust Ziele und Aufgaben nicht wie geplant erreicht werden.
- Fallen unverschlüsselte Datenträger in falsche Hände, kann dies zu schwerwiegenden Vertraulichkeitsverlusten führen.
- Ist unterwegs kein ausreichender Zugriffsschutz vorhanden, können Akten oder Datenträger unbemerkt kopiert oder manipuliert werden.

2.6 Ungeeignete Entsorgung der Datenträger und Dokumente

Ist es am mobilen Arbeitsplatz nicht möglich, Datenträger und Dokumente geeignet zu entsorgen, wandern diese meist in den Hausmüll. Auch dort, wo unterwegs gearbeitet wird, werfen Mitarbeiter häufig Entwürfe und andere vermeintlich unnütze Dokumente direkt in den nächsten Papierkorb oder lassen sie einfach liegen, sei es im Hotel oder in der Bahn. Wenn jedoch Datenträger oder Dokumente nicht geeignet entsorgt werden, können Angreifer hieraus wertvolle Informationen entnehmen, die sich gezielt für Erpressungsversuche oder zur Wirtschaftsspionage missbrauchen lassen. Die Folgen reichen vom Know-how-Verlust bis zur Existenzgefährdung der Institution, zum Beispiel wenn dadurch wichtige Aufträge nicht zustande kommen oder Partnerschaften scheitern.

2.7 Vertraulichkeitsverlust schützenswerter Informationen

Am mobilen Arbeitsplatz können Angreifer einfacher auf vertrauliche Informationen zugreifen, die sich auf Festplatten, auf austauschbaren Speichermedien oder auf Papier befinden, besonders wenn sie professionell agieren. Auch können sie Kommunikationsverbindungen abhören. Werden Informationen unberechtigt gelesen oder preisgegeben, hat das jedoch schwerwiegende Folgen für die gesamte Institution. Unter anderem kann der Verlust der Vertraulichkeit dazu führen, dass die Institution gegen Gesetze verstößt oder dass Wettbewerbsnachteile und finanzielle Schäden entstehen.

2.8 Diebstahl oder Verlust von Datenträgern oder Dokumenten

Der mobile Arbeitsplatz ist nicht so gut abgesichert wie der Arbeitsplatz in einem Unternehmen oder einer Behörde. Während einer Bahnfahrt, aus einem Hotelzimmer oder mitunter auch aus Konferenzräumen bei Kunden, können dienstliche IT und Dokumente daher leichter gestohlen werden.

Zudem können IT-Systeme oder Komponenten verloren gehen. Neben dem rein materiellen Schaden durch den unmittelbaren Verlust des mobilen Gerätes kann durch die Offenlegung schützenswerter Daten (z. B. E-Mails, Notizen von Besprechungen, Adressen oder sonstige Dokumente) weiterer (finanzieller und/oder Reputations-)Schaden entstehen.

2.9 Fehlendes Sicherheitsbewusstsein und Sorglosigkeit im Umgang mit Informationen

Häufig ist zu beobachten, dass in Institutionen organisatorische Regelungen und technische Sicherheitsmaßnahmen für tragbare IT-Systeme und mobile Datenträger vorhanden sind, diese jedoch durch den sorglosen Umgang mit den Vorgaben und der Technik wieder ausgehebelt werden. So ist z. B. immer wieder zu beobachten, dass mitgebrachte mobile Datenträger während der Pausen unbeaufsichtigt im Besprechungsraum oder auch im Zugabteil zurückgelassen werden.

Darüber hinaus werden zum Teil Geschenke in Form von Datenträgern, wie z. B. USB-Sticks, von Mitarbeitern angenommen und unüberlegt an das eigene Notebook angeschlossen. Hier kann dann das Notebook mit Schadsoftware infiziert und dadurch können schützenswerte Informationen gestohlen, manipuliert oder verschlüsselt und damit vorübergehend unbrauchbar gemacht werden.

In öffentlichen Verkehrsmitteln oder auch während Geschäftsessen ist immer wieder zu beobachten, dass Menschen offene Gespräche über geschäftskritische Informationen führen. Diese können dann von Außenstehenden leicht mitgehört und möglicherweise zum schwerwiegenden Nachteil des Mitarbeiters oder seiner Institution verwendet werden.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz von mobilen Arbeitsplätzen aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte (ISB) für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	Informationssicherheitsbeauftragter (ISB)
Weitere Verantwortliche	Benutzer, Haustechnik, Leiter IT, Leiter Personal, Mitarbeiter, Personalabteilung, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

INF.9.A1 Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes [Vorgesetzte, Benutzer]

Die Institution MUSS ihren Mitarbeitern vorschreiben, wie mobile Arbeitsplätze geeignet ausgewählt und benutzt werden sollen. Es MÜSSEN Eigenschaften definiert werden, die für einen mobilen Arbeitsplatz wünschenswert sind, aber auch Ausschlusskriterien, die gegen einen mobilen Arbeitsplatz sprechen. Mindestens MUSS geregelt werden:

- unter welchen Arbeitsplatzbedingungen schützenswerte Informationen bearbeitet werden dürfen,
- wie sich Mitarbeiter am mobilen Arbeitsplatz vor ungewollten Einsichtnahmen von Dritten schützen,
- ob eine permanente Netz- und Stromversorgung gegeben sein muss und
- welche Arbeitsplatzumgebungen komplett verboten sind.

INF.9.A2 Regelungen für mobile Arbeitsplätze [Leiter IT, Benutzer]

Für alle Arbeiten unterwegs MUSS geregelt werden, welche Informationen außerhalb des Unternehmens bzw. der Behörde transportiert und bearbeitet werden dürfen und welche Schutzvorkehrungen dabei zu treffen sind. Dabei MUSS auch geklärt werden, unter welchen Rahmenbedingungen Mitarbeiter mit mobilen IT-Systemen auf interne Informationen ihrer Institution zugreifen dürfen.

Darüber hinaus MUSS die Mitnahme von IT-Komponenten und Datenträgern klar geregelt werden. So MUSS festgelegt werden, welche IT-Systeme und Datenträger mitgenommen werden dürfen, wer diese mitnehmen darf und welche grundlegenden Sicherheitsanforderungen beachtet werden müssen. Es MUSS zudem protokolliert werden, wann und von wem, welche mobile Endgeräte außer Haus eingesetzt wurden.

Die Benutzer von mobilen Endgeräten MÜSSEN für den Wert mobiler IT-Systeme und den Wert der darauf gespeicherten Informationen sensibilisiert werden. Sie MÜSSEN über die spezifischen Gefährdungen und Maßnahmen der von ihnen benutzten Geräte aufgeklärt werden. Außerdem MÜSSEN sie darüber informiert werden, welche Art von Informationen auf mobilen IT-Systemen verarbeitet werden dürfen. Alle Benutzer MÜSSEN auf die geltenden Regelungen hingewiesen werden, die von ihnen einzuhalten sind und entsprechend geschult werden.

INF.9.A3 Zutritts- und Zugriffsschutz [Mitarbeiter]

Den Mitarbeitern MUSS bekanntgegeben werden, welche Regelungen und Maßnahmen zum Einbruchs- und Zutrittsschutz am mobilen Arbeitsplatz zu beachten sind. So MUSS darauf hingewiesen werden, Fenster zu schließen und Türen abzuschließen, wenn der mobile Arbeitsplatz nicht besetzt ist (dies ist z. B. bei Hotelzimmern möglich). Ist dies nicht möglich (z. B. im Zug), MÜSSEN die Mitarbeiter alle Unterlagen und IT-Systeme an sicherer Stelle verwahren, wenn sie abwesend sind. Es MUSS sichergestellt werden, dass Unbefugte zu keiner Zeit auf dienstliche IT und Unterlagen zugreifen können.

Werden Räume nur kurz verlassen, MÜSSEN die eingesetzten Clients gesperrt oder heruntergefahren werden, sodass sie nur nach erfolgreicher Authentisierung wieder benutzt werden können.

INF.9.A4 Arbeiten mit fremden IT-Systemen [Vorgesetzte, Benutzer]

Die Institution MUSS regeln, wie Mitarbeiter mit fremden IT-Systemen arbeiten sollen. Da sich das Schutzniveau solcher IT-Systeme von dem der eigenen Institution stark unterscheiden kann, MUSS jeder mobile Mitarbeiter über die Gefahren unterrichtet sein, die bestehen, wenn fremde IT-Systeme genutzt werden. Die Regelungen MÜSSEN vorgeben, ob und wie schützenswerte Informationen an fremden IT-Systemen bearbeitet werden dürfen und wie verhindert wird, das nicht autorisierte Personen die Informationen einsehen können. Wenn Mitarbeiter mit fremden IT-Systemen arbeiten, MUSS grundsätzlich sichergestellt sein, dass alle währenddessen entstandenen temporären Daten gelöscht werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Mobiler Arbeitsplatz. Sie SOLLTEN grundsätzlich umgesetzt werden.

INF.9.A5 Zeitnahe Verlustmeldung [Mitarbeiter]

Mitarbeiter SOLLTEN ihrer Institution umgehend melden, wenn Informationen, IT-Systeme oder Datenträger verloren oder gestohlen wurden. Hierfür SOLLTE es klare Meldewege und Ansprechpartner innerhalb der Institution geben.

INF.9.A6 Entsorgung von vertraulichen Informationen [Mitarbeiter, Haustechnik]

Vertrauliche Informationen SOLLTEN sicher entsorgt werden, also nicht einfach in den Hausmüll. Bevor ausgediente oder defekte Datenträger und Dokumente entsorgt werden, MUSS überprüft werden, ob diese sensible Informationen enthalten. Ist dies der Fall, MÜSSEN die Datenträger und Dokumente wieder mit zurück transportiert werden und auf institutseigenem Wege entsorgt bzw. vernichtet werden.

INF.9.A7 Rechtliche Rahmenbedingungen für das mobile Arbeiten [Leiter Personal, Personalabteilung]

Für das mobile Arbeiten SOLLTEN arbeitsrechtliche und arbeitsschutzrechtliche Rahmenbedingungen beachtet und geregelt werden. Alle relevanten Punkte SOLLTEN entweder durch Betriebsvereinbarungen oder durch zusätzlich zum Arbeitsvertrag getroffene individuelle Vereinbarungen zwischen dem mobilen Mitarbeiter und Arbeitgeber geregelt werden.

INF.9.A8 Sicherheitsrichtlinie für mobile Arbeitsplätze [Leiter IT]

Alle relevanten Sicherheitsanforderungen für mobile Arbeitsplätze SOLLTEN in einer für die mobilen Mitarbeiter verpflichtenden Sicherheitsrichtlinie dokumentiert werden. Sie SOLLTE zudem mit den bereits vorhandenen Sicherheitsrichtlinien der Institution sowie mit allen relevanten Fachabteilungen abgestimmt werden. Auch SOLLTE die Sicherheitsrichtlinie für mobile Arbeitsplätze regelmäßig aktualisiert werden. Ebenso SOLLTE sie festlegen, dass für jeden mobilen Mitarbeiter ein Vertreter benannt und der Vertretungsprozess regelmäßig geprobt wird. Die Mitarbeiter der Institution SOLLTEN hinsichtlich der aktuellen Sicherheitsrichtlinie sensibilisiert und geschult sein.

INF.9.A9 Verschlüsselung tragbarer IT-Systeme und Datenträger [Benutzer]

Damit schützenswerte Informationen nicht durch unberechtigte Dritte eingesehen werden können, SOLLTE sichergestellt werden, dass diese entsprechend den internen Richtlinien abgesichert sind. Mobile Datenträger und Clients SOLLTEN dabei verschlüsselt werden. Die kryptographischen Schlüssel SOLLTEN getrennt vom verschlüsselten Gerät aufbewahrt werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

INF.9.A10 Einsatz von Diebstahlsicherungen (CIA)

Bietet das verwendete IT-System eine Diebstahlsicherung an, SOLLTE sie benutzt werden. Die Diebstahlsicherungen SOLLTEN stets dort eingesetzt werden, wo ein erhöhter Publikumsverkehr herrscht oder die Fluktuation von Benutzern sehr hoch ist. Dabei SOLLTEN die Mitarbeiter immer beachten, dass der Schutz der auf den IT-Systemen gespeicherten Informationen meist einen höheren Wert besitzt, als die Wiederanschaffungskosten des IT-Systems betragen. Die Beschaffungs- und Einsatzkriterien für Diebstahlsicherungen SOLLTEN an die Prozesse der Institution angepasst und dokumentiert werden.

INF.9.A11 Verbot der Nutzung unsicherer Umgebungen (CIA)

Es SOLLTEN Kriterien für die Arbeitsumgebung festgelegt werden, die mindestens erfüllt sein müssen, damit Informationen mit erhöhtem Schutzbedarf mobil bearbeitet werden dürfen. Die Kriterien sollten mindestens folgende Themenbereiche abdecken:

- Einsicht und Zugriff durch Dritte,
- geschlossene und falls nötig abschließbare oder bewachte Räume,
- gesicherte Kommunikationsmöglichkeiten und
- eine ausreichende Stromversorgung.

4 Weiterführende Informationen

4.1 Literatur

- [27001A11.2] ISO/ IEC 27001:2013 - Annex A.11.2 Equipment
  Information technology- Security techniques- Information security management systems- Requirements, insbesondere A.11.2 Equipment, ISO, 2013

- [27001A6.2.1] ISO/ IEC 27001: 2013 - Annex A.6.2.1 Mobile device policy
  Information technology- Security techniques- Information security management system - Requirements, insbesondere Annex A, A.6.2.1 Mobile device policy, ISO, 2013

- [ISFPA2] Information Security Forum (ISF), June 2016, insbesondere Area PA2 Mobile Computing
  Information Security Forum, insbesondere Area PA2 Mobile Computing, ISF, 06.2016

- [NIST80046] NIST Special Publication 800-46 Revision 2
  Guide to Enterprise Telework, Remote Access and Bring Your Own Device (BYOD) Security, NIST, 07.2016
  http://dx.doi.org/10.6028/NIST.SP.800-46r2

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Mobiler Arbeitsplatz" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.25 Ausfall von Geräten oder Systemen

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen / Anforderungen	G 0.14	G 0.16	G 0.17	G 0.18	G 0.19	G 0.21	G 0.22	G 0.23	G 0.24	G 0.25	G 0.29	G 0.30	G 0.31	G 0.44	G 0.45	G 0.46
INF.9.A1	x	x		x	x	x	x			x						
INF.9.A2	x	x		x	x	x	x	x	x	x	x	x	x	x	x	
INF.9.A3	x	x			x	x	x		x			x		x		x
INF.9.A4					x		x					x	x			x
INF.9.A5	x				x											
INF.9.A6	x			x	x											x
INF.9.A7											x					
INF.9.A8	x			x	x	x	x	x			x	x	x			x
INF.9.A9	x	x	x		x		x									
INF.9.A10		x						x				x	x		x	
INF.9.A11	x				x					x	x					

INF: Infrastruktur

INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume

1 Beschreibung

1.1 Einleitung

In der Regel hat jede Institution einen oder mehrere Räume, in denen Besprechungen, Schulungen oder sonstige Veranstaltungen durchgeführt werden können. Hierfür sind oft speziell ausgestattete Räume vorgesehen. Besprechungs-, Veranstaltungs- und Schulungsräume zeichnen sich im wesentlichen dadurch aus, dass sie von wechselnden Personen bzw. Personenkreisen und Besuchern sowie in der Regel nur für einen begrenzten Zeitraum genutzt werden. Mitgebrachte IT-Systeme werden dabei häufig gemeinsam mit Geräten der Institution betrieben, wie beispielsweise fremde Laptops an fest verbauten Projektoren. Aus diesen unterschiedlichen Nutzungsszenarien heraus ergibt sich eine Gefährdungslage, die kaum mit denen anderer Räume vergleichbar ist.

1.2 Zielsetzung

Ziel des Bausteins ist der Schutz der Informationen, die in Besprechungs-, Veranstaltungs- und Schulungsräumen bearbeitet werden, sowie der IT-Geräte, die in diesen Räumen betrieben werden. Außerdem wird der richtige Umgang mit Besuchern, die entsprechende Räume nutzen, behandelt.

1.3 Abgrenzung

Dieser Baustein betrachtet alle technischen und nicht-technischen Sicherheitsaspekte zur Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen. Detaillierte Empfehlungen, wie die IT-Systeme in diesen Räumen konfiguriert und abgesichert werden können, werden nicht im Rahmen dieses Bausteins behandelt, diese sind in SYS.2.1 Allgemeiner Client sowie den betriebssystemspezifischen System-Bausteinen zu finden. Weitere für Besprechungsräume typische Aspekte wie z. B. WLAN oder Videokonferenzanlagen werden in den Bausteinen der Schichten NET.2 Funknetze oder NET.4 Telekommunikation betrachtet. Die Verkabelung in diesen Räumen wird in dem Baustein INF. 3 Elektrotechnische Verkabelung und INF.4 IT-Verkabelung gesondert berücksichtigt. Anforderungen zum Brandschutz sind im Baustein INF.1 Allgemeines Gebäude zu finden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Bereich der Besprechungs-, Veranstaltungs- und Schulungsräumen von besonderer Bedeutung:

2.1 Fehlende oder unzureichende Regelungen

Wenn z. B. Mitarbeiter die Fenster und Türen nach Verlassen des Raumes nicht schließen oder vertrauliche Informationen von einem Whiteboard oder Flipchart nicht entfernt werden, können so sensible Informationen von unberechtigten Personen eingesehen werden. Generell sollten daher den Mitarbeitern entsprechende Regelungen an die Hand geben werden, sodass entsprechende Si-

cherheitslücken nicht auftreten können. Regelungen lediglich festzulegen sichert aber noch nicht, dass sie auch beachtet werden und der Betrieb störungsfrei ist. Viele Probleme entstehen auch, wenn die Regelungen vorhanden, aber nicht bekannt sind. Oft wissen z. B. die Mitarbeiter nicht, dass Fenster und Türen nach Besprechungen verschlossen werden müssen und wie mit einem genutzten Flipchart umzugehen ist.

2.2 Inkompatibilität zwischen fremder und eigener IT

IT-Systeme werden immer mobiler und werden zunehmend in unterschiedlichen Umgebungen verwendet. Oft finden die mobilen IT-Benutzer Szenarien vor, in denen die IT-Systeme aufgrund von Inkompatibilität nicht wie geplant genutzt werden können. Beispielsweise verfügen ältere Geräte nicht über die gleichen Anschlüsse und Stecker wie neuere Geräte. Zudem werden Geräte hergestellt, die nicht ohne passenden Adapter mit anderen Geräten kompatibel sind. Liegt also z. B. ein passender Adapter nicht vor, so kann ein Laptop, der mit allen wichtigen Daten für eine Besprechung vorbereitet wurde, nicht an einen Beamer genutzt werden. Darüber hinaus können Versuche, die IT-Systeme doch zu verbinden, zu Schäden an den Geräten oder den gespeicherten Daten führen.

2.3 Gefährdung durch Besucher

Es ist bereits nicht immer ganz einfach, eigene Mitarbeiter ausreichend zum richtigen Umgang mit sensiblen Informationen und mit IT-Systemen zu sensibilisieren und zu schulen. Bei Besuchern kann grundsätzlich nicht vorausgesetzt werden, dass sie mit den ihnen zugänglichen Informationen und der Informationstechnik entsprechend den Vorgaben der besuchten Institution umgehen, vor allem, da sie diese Vorgaben in vielen Fällen nicht kennen. Besucher können generell an vertrauliche Informationen gelangen, indem die eigenen Mitarbeiter unachtsam sind. Ebenso kann dies aus Unwissen geschehen, wenn sich die Besucher beispielsweise auf dem Weg zur Toilette in der Türe irren und ein Mitarbeiterbüro betreten, an dessen Whiteboard vertrauliche Informationen stehen. Besucher könnten auch vorsätzlich Geräte zerstören oder beschädigen, um vertrauliche Informationen zu erhalten.

2.4 Fliegende Verkabelung

In Besprechungs-, Veranstaltungs- und Schulungsräumen wechseln häufig sowohl die Benutzer als auch die Art, wie die Räume genutzt werden. Damit wird mitunter die Geräteausstattung und damit natürlich auch die Verkabelung in solchen Räumen permanent geändert. Kabel können somit, je nach Lage der Anschlusspunkte im Raum (Steckdosen der Stromversorgung und des Datennetzes) übergangsweise quer durch den Raum, auch über Verkehrswege hinweg, verlegt werden. Nicht nur Personen werden durch diese Stolperfallen gefährdet, auch IT-Geräte können beschädigt werden, wenn Personen die "fliegenden" Kabel mit sich reißen.

2.5 Diebstahl

Wenn die in einem Besprechungsraum teils stationär verbauten Datenträger, IT-Systeme, Zubehör, Software oder Daten gestohlen werden, entstehen einerseits Kosten für die Wiederbeschaffung sowie für die Wiederherstellung eines arbeitsfähigen Zustandes. Andererseits kann der Besprechungsraum aufgrund mangelnder Verfügbarkeit der Geräte anschließend nur eingeschränkt genutzt werden. Somit kann es zu Engpässen bezüglich der Belegung von Räumen kommen. Darüber hinaus können vertrauliche Informationen gestohlen, missbraucht oder weitergegeben werden.

Gestohlen werden neben teuren IT-Systemen häufig auch mobile Endgeräte, die unauffällig und leicht zu transportieren sind. Sind die Besprechungs-, Veranstaltungs- und Schulungsräume nicht verschlossen bzw. beaufsichtigt oder die IT-Systeme nicht ausreichend gesichert, kann die Technik dementsprechend schnell und unauffällig entwendet werden. Dies gilt ganz besonders, wenn beispielsweise in Besprechungspausen die Räumlichkeiten nicht verschlossen werden.

2.6 Vertraulichkeitsverlust schützenswerter Informationen

Durch technisches Versagen, Unachtsamkeit, Unwissen auch durch vorsätzliche Handlungen können vertrauliche Informationen offengelegt werden. Dabei können diese vertraulichen Informationen an unterschiedlichen Stellen vorliegen, wie z. B. auf Speichermedien innerhalb von Rechnern (wie Festplatten), auf austauschbaren Speichermedien (wie USB-Sticks oder optische Medien), in gedruckter Form auf Papier sowie auf Whiteboards oder Flipcharts. Werden Informationen unberechtigt gelesen oder preisgegeben, kann das schwerwiegende Folgen für die Institution haben, wie beispielsweise Verstöße gegen Gesetze, Wettbewerbsnachteile oder finanzielle Auswirkungen.

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz d*er Besprechungs-, Veranstaltungs- und Schulungsräume* aufgeführt. Grundsätzlich ist der Leiter Organisation für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	Leiter Organisation
Weitere Verantwortliche	Haustechnik, Leiter IT, Mitarbeiter

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

INF.10.A1 Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen [Leiter IT, Haustechnik]

In den Räumen vorhandene Gerätschaften MÜSSEN angemessen gegen Diebstahl gesichert werden. Zudem MUSS festgelegt werden, wer die in den Räumen dauerhaft vorhandenen IT- und sonstigen Systeme administriert. Es MUSS auch festgelegt werden, ob und unter welchen Bedingungen Besucher mitgebrachte IT-Systeme verwenden dürfen. Weiterhin MUSS festgelegt werden, ob und auf welche Netzzugänge und TK-Schnittstellen Besucher zugreifen dürfen.

INF.10.A2 Beaufsichtigung von Besuchern [Mitarbeiter]

Besucher MÜSSEN außerhalb von Räumen, die ausdrücklich für den Zugang durch Besucher vorgesehen sind, beaufsichtigt werden. Mitarbeiter MÜSSEN dazu angehalten werden, institutionsfremde Personen nicht unbeaufsichtigt zu lassen.

INF.10.A3 Geschlossene Fenster und Türen [Mitarbeiter]

Die Fenster der Besprechungs-, Veranstaltungs- und Schulungsräume MÜSSEN beim Verlassen verschlossen werden. Bei Räumlichkeiten, in denen sich IT-Systeme oder schützenswerte Informationen befinden, MÜSSEN die Türen beim Verlassen abgeschlossen werden. Zusätzlich MUSS regelmäßig geprüft werden, ob die Fenster und Türen nach Verlassen der Räume verschlossen wurden. Ebenso MUSS darauf geachtet werden, dass Brand- und Rauchschutztüren tatsächlich geschlossen werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Besprechungs-, Veranstaltungs- und Schulungsräume. Sie SOLLTEN grundsätzlich umgesetzt werden.

INF.10.A4 Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen

Bei der Planung von Besprechungs-,Veranstaltungs- und Schulungsräumen SOLLTE besonders die Lage der Räume berücksichtigt werden. Insbesondere Räumlichkeiten, die oft mit Besuchern genutzt werden, SOLLTEN NICHT in Gebäudeteilen liegen, in deren Nähe regelmäßig vertrauliche Informationen bearbeitet werden. Es SOLLTE für jeden Raum festgelegt werden, wie vertraulich die Informationen sein dürfen, die in den Räumlichkeiten besprochen oder verarbeitet werden dürfen.

INF.10.A5 Fliegende Verkabelungen

Um fliegende Verkabelung zu vermeiden, SOLLTEN sich die Stromanschlüsse dort befinden, wo Beamer, Laptops oder andere Verbraucher aufgestellt werden. Zudem SOLLTEN Verkabelungen, die über den Boden verlaufen, mit einem Kabelschacht abgedeckt werden.

INF.10.A6 Einrichtung sicherer Netzzugänge [Leiter IT]

Es SOLLTE sichergestellt werden, dass mitgebrachte IT-Systeme nicht über das Datennetz mit internen IT-Systeme verbunden werden können. Ausschließlich dafür vorgesehene IT-Systeme SOLLTEN auf das LAN der Institution zugreifen können. Ein Datennetz für Besucher SOLLTE vom LAN der Institution getrennt werden. Netzzugänge SOLLTEN so eingerichtet sein, dass verhindert wird, dass Dritte den internen Datenaustausch mitlesen können. Netzanschlüsse in Besprechungs-, Veranstaltungs- oder Schulungsräumen SOLLTEN abgesichert werden. Es SOLLTE verhindert werden, dass IT-Systeme in Besprechungs-, Veranstaltungs- und Schulungsräumen gleichzeitig eine Verbindung zum Intranet und zum Internet aufbauen können.

Außerdem SOLLTE die Stromversorgung aus einer Unterverteilung heraus getrennt von anderen Räumen aufgebaut werden.

INF.10.A7 Sichere Konfiguration von Schulungs- und Präsentationsrechnern [Leiter IT]

Dedizierte Schulungs- und Präsentationsrechner SOLLTEN mit einer Minimalkonfiguration versehen werden. Es SOLLTE festgelegt sein, welche Anwendungen auf Schulungs- und Präsentationsrechner in der jeweiligen Veranstaltung genutzt werden können. Die Schulungs- und Präsentationsrechner SOLLTEN nur an ein separates, vom LAN der Institution getrennten Netz angeschlossen werden. Auf andere Netze SOLLTE nur restriktiv zugegriffen werden können.

INF.10.A8 Erstellung eines Nutzungsnachweises für Räume

Je nach Nutzungsart der Besprechungs-, Veranstaltungs- und Schulungsräume SOLLTE ersichtlich sein, wer die Räume zu welchem Zeitpunkt genutzt hat. Für Räumlichkeiten, in denen Schulungen an IT-Systemen oder besonders vertrauliche Besprechungen durchgeführt werden, SOLLTEN ebenfalls Nutzungsnachweise erbracht werden. Es SOLLTE überlegt werden, für Räumlichkeiten, die für jeden Mitarbeiter zugänglich sind, ebenfalls entsprechende Nutzungsnachweis einzuführen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

INF.10.A9 Zurücksetzen von Schulungs- und Präsentationsrechnern [Leiter IT] (CA)

Es SOLLTE ein Verfahren festgelegt werden, um Schulungs- und Präsentationsrechner nach der Nutzung auf einen vorher definierten Zustand zurückzusetzen. Durch Benutzer vorgenommene Änderungen SOLLTEN dabei vollständig entfernt werden.

4 Weiterführende Informationen

4.1 Literatur

- [27001] ISO/IEC 27001:2013
  Information technology- Security techniques- Information security management system- Requirements, ISO, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

- [DIN1627] DIN EN 1627:2011-09
  Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Anforderungen und Klassifizierung, 2011

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein "Besprechungs-, Veranstaltungs- und Schulungsräume" von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.21 Manipulation von Hard- oder Software

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.41 Sabotage

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

G 0.45 Datenverlust

Elementare Gefährdungen / Anforderungen	G 0.14	G 0.15	G 0.16	G 0.18	G 0.21	G 0.24	G 0.41	G 0.44	G 0.45
INF.10.A1			x		x	x		x	
INF.10.A2			x		x	x	x	x	
INF.10.A3					x	x	x	x	
INF.10.A4	x	x					x		
INF.10.A5				x					
INF.10.A6	x	x					x		
INF.10.A7	x			x	x		x		x
INF.10.A8							x	x	
INF.10.A9	x	x					x		