Prüfspezifikation

mediaTest digital GmbH
Goseriede 4
30159 Hannover
T | +49 (0) 511-353994-22
F | +49 (0) 511-353994-12
W | www.mediatest-digital.com

Sitz und Registergericht: Hannover | HRB 208916
USt.-ID Nr. DE284516422
Vertretungsberechtigter Geschäftsführer: Sebastian Wolters

Autor	mediaTest digital GmbH
Datum	30.11.2018
Revision	1.3.1

Inhaltsverzeichnis

1. Pre-Testphase: Datenerhebung 3

1.1 Android 3

1.2 iOS 3

2. Analyseverfahren 4

2.1 Statische Analyse 4

2.1.1 Android 4

2.1.2 iOS 4

2.2 Dynamische Analyse 5

3. Auswertungsverfahren 5

3.1 Automatische Auswertung 5

3.2 Manuelle Revision 6

3.2.1 Risikobewertung 6

3.2.2 Plausibilitätsprüfung 6

3.2.3 Erläuterungen 7

4. Reporting & Publikation 7

4.1 Automatische Reporterstellung 7

4.1.1 Report Inhalte 7

4.1.2 Ampelwertung 8

4.1.3 Ampelanpassung 10

4.2 Automatische Publikation 10

4.2.1 Kunden-Interface (ASC/TAD) 10

4.2.2 MDM (Mobile Device Management) via API 10

1. Pre-Testphase: Datenerhebung

Es müssen testvorbereitend Informationen zu jeder einzelnen App-Version aggregiert werden, um eine Basis für den folgenden App-Test zu schaffen. Die Umsetzung entspricht dabei den aktuell zur Verfügung stehenden technischen Möglichkeiten und unterscheidet sich je nach Betriebssystem und den durch den jeweiligen Appstore bereitgestellten Informationen.

1.1 Android

Die Datenerhebung für die testvorbereitende Aufbereitung der Android-Apps erfolgt über einen eigens entwickelten Datenscraper. Über eine inoffizielle Google Play Store API werden die folgenden Informationen gesammelt und aufbereitet.

Version	1.0
Erfasste Daten	**Status der Implementierung**
Versions-ID (entspricht Prüfbericht-ID)	Implementiert
Appname	Implementiert
App-Version	Implementiert
Dateigröße	Implementiert
Hashwert und Hashalgorithmus	Implementiert, je nach Kundenwunsch
App-Hersteller	Implementiert, je nach Kundenwunsch
API-Level minimal (minimale OS-Version)	Implementiert, je nach Kundenwunsch
API-Level optimal	Implementiert, je nach Kundenwunsch
Beschreibungstexte DE/EN & Quellenangabe	Implementiert, je nach Kundenwunsch

1.2 iOS

Die Datenerhebung für die testvorbereitende Aufbereitung der iOS-Apps erfolgt über die von Apple bereitgestellte iTunes App Store API. Es werden die folgenden Informationen gesammelt und aufbereitet.

Version	1.0
Erfasste Daten	**Status der Implementierung**
Versions-ID (entspricht Prüfbericht-ID)	Implementiert
Appname	Implementiert

App-Version	Implementiert
Dateigröße	Implementiert
Hashwert und Hashalgorithmus	Implementiert, je nach Kundenwunsch
App-Hersteller	Implementiert, je nach Kundenwunsch
OS-Version minimal	Implementiert, je nach Kundenwunsch
Beschreibungstexte DE/EN & Quellenangabe	Implementiert, je nach Kundenwunsch

2. Analyseverfahren

2.1 Statische Analyse

2.1.1 Android

Android-Apps durchlaufen in der statischen Analyse die folgenden Schritte: Die manifest.xml wird zur verlässlichen Informationssammlung ausgewertet.

Es findet bei Applikationen, deren Lizenz dies zulässt, ein Berechtigungscheck statt, um bereits im Vorfeld des Tests auf potenziell gefährliche oder als sicherheitskritisch einzustufende Berechtigungen aufmerksam zu werden. Im Zuge des Berechtigungschecks wird auch analysiert, ob eine mögliche Überprivilegierung vorliegt.

Bei Applikationen, deren Lizenz dies zulässt, durchläuft diese eine Methodenanalyse, um zu überprüfen, ob die geforderten Berechtigungen auch aktiv genutzt werden.

Es findet eine Suche nach der Verwendung von bekannten SDKs externer Anbieter von Werbung, Analytics und Tracking statt. Bei Applikationen, deren Lizenz dies zulässt, findet eine Suche nach bekannten Malware-Fingerprints über die virustotal API statt.

2.1.2 iOS

Eine statische Analyse für iOS-Apps befindet sich derzeit in der Test- und Integrationsphase.

Bei Applikationen deren Lizenz dies zulässt, findet eine Suche nach bekannten Malware-Fingerprints über die virustotal API statt.

2.2 Dynamische Analyse

Die App durchläuft einen manuellen Testlauf durch einen IT Security Analysten. Dabei werden alle Kernfunktionen der App ausgeführt. Die möglichen Aktionen umfassen unter anderem das Anlegen von Accounts innerhalb der App, die Ausführung von Kaufaktionen, das Senden von Dateien und Kommentaren und weitere Möglichkeiten der jeweiligen App. Die manuelle Anlage von Daten wird protokolliert und in einer eigens entwickelten Markup Language als Actionlist gespeichert.

Alle in der App festgestellten Möglichkeiten zur externen Datenspeicherung über Cloud-Dienste, alle Möglichkeiten zur externen Anlage von Benutzeraccounts über soziale Netzwerke und alle Möglichkeiten zum Teilen von Inhalten über soziale Netzwerke werden manuell erfasst und protokolliert.

Der während des Tests entstehende Datenverkehr wird mittels einer Man-in-the-Middle-Attacke gesnifft, die SSL-Verschlüsselung aufgebrochen und zur späteren automatischen Auswertung gespeichert.

3. Auswertungsverfahren

3.1 Automatische Auswertung

Nach der dynamischen Analyse durchlaufen die Testergebnisse eine automatische Auswertung. Dabei finden verschiedene Schritte statt.

In der dynamischen Analyse durch den IT Security Analysten angelegten Daten werden in Datengruppen eingeordnet und in Tabellen aufbereitet, um die manuelle Revision vorbereitend zu erleichtern.

Die Mindestzahl der Verarbeitungen der durch den IT Security Analysten angelegten Daten wird anhand der Häufigkeit der manuellen Verarbeitung und der Häufigkeit der Versendung durch die App ermittelt.

Sonderfall Android: Die Zugänglichkeit der angelegten Daten für andere Apps (unverschlüsselte Ablage von Daten auf der internen oder externen SD Karte) wird mittels einer eigens entwickelten Lösung geprüft.

Sonderfall iOS: Die Zugänglichkeit der angelegten Daten für andere Apps (unverschlüsselte Ablage von Daten im App-Speicher) wird mittels einer eigens entwickelten Lösung geprüft

Alle von der App initiierten Verbindungen werden automatisch überprüft und aufgelistet. Es findet eine vollständige Datenverkehrs- und Verbindungsanalyse statt. Diese beinhalten:

- Servername und DNS von gesnifften Paketen und erfassten Verbindungen
- WhoIs-Abfrage aller erfassten IP-Adressen
- IP-Erfassung und Geolokalisierung der IP
- Netzwerkkanalanalyse (Protokoll, Port, Verschlüsselung, Datenmutation)
- Durchsuchung der gesnifften Pakete nach dynamischen & statischen Suchbegriffen
- Auflistung der Suchtreffer
- Vorläufige Einstufung der Datenfunde in Verstoß-Kategorien

Nach Abschluss der automatischen Auswertung werden die aufgezeichneten Verbindungen und Suchtreffer von dynamischen & statischen Suchbegriffen zum Zwecke der manuellen Revision für den IT Security Analyst übersichtlich aufbereitet.

3.2 Manuelle Revision

3.2.1 Risikobewertung

In der manuellen Revision wird die automatische Auswertung durch einen IT Security Analyst manuell ergänzt. Schwachstellen in der Datensicherheit und potenzielle Datenschutzverstöße werden identifiziert und im Testlauf dokumentiert.

Besondere Auffälligkeiten wie Datenübertragung in sehr hoher Frequenz, Übertragung einer Liste von auf dem Gerät installierten Apps etc. werden ebenfalls erfasst und hinsichtlich eines möglichen Datenschutzrisikos bewertet.

Es wird eine Handlungsempfehlung gegeben für den Fall, dass die Man-in-the-Middle-Attacke während des SSL-Sniffings fehlschlägt, bzw. eine Verbindung innerhalb einer aufgebrochenen Sitzung mittels SSL-Pinning verhindert wird. Diese orientiert sich an den Datenübertragungen und Verbindungen, die außerhalb der verschlüsselten Verbindungen protokolliert werden konnten.

3.2.2 Plausibilitätsprüfung

Während der manuellen Revision des Tests findet eine Plausibilitätsprüfung statt, die in mehreren Schritten durchgeführt wird. Die Plausibilitätsprüfung wird mit dem Ziel vorgenommen, die Aussagekraft und Verlässlichkeit der durch den Test zu treffenden Aussagen zu verstärken und potenzielle Gefahren pointierter zu erfassen.

Es wird ein Kernfunktionalitätscheck der aufgebauten Verbindungen und übertragenen Datenpakete vorgenommen, um abzugleichen, welche Verbindungen und aufgezeichneten Datenpaketübertragungen ausschließlich und unmissverständlich der Ausführung der Kernfunktionalität der App dienen.

Die automatisch während der statischen Analyse durchgeführte Rechteprüfung wird hinsichtlich ihres Gefahrenpotenzials eingestuft. Auch an dieser Stelle erfolgt eine Prüfung auf Kernfunktionalität, um eine Aussage über eine eventuell vorliegende Überprivilegierung der App treffen zu können.

Die in den aufgezeichneten Datenpaketübertragungen gefundenen Suchbegriffe werden einer false-positive-Prüfung unterzogen, um eventuell wertungsrelevante Falschtreffer auszusortieren und eine Abstufung der Wertung zu verhindern.

3.2.3 Erläuterungen

Während der Auswertung auftretende Auffälligkeiten oder Besonderheiten werden gesondert erläutert und im Bereich „Erläuterungen“ erfasst.

4. Reporting & Publikation

4.1 Automatische Reporterstellung

4.1.1 Report Inhalte

Nach Abschluss der manuellen Revision wird ein Report automatisch erstellt und intern freigegeben. Dieser enthält folgende Informationen:

- Prüfbericht-ID
- Versionsnummer zugrunde liegender Spezifikation
- Versionsnummer Prüfbericht
- Zeitangaben zum Testabschluss/-ablauf
- Appname und Version
- Releasedatum der App-Version
- App-Hersteller
- Verfügbare Sprachen der App
- Preis der App

- minimale Betriebssystem-Version
- optimale Betriebssystem-Version
- Dateigröße
- Hashwert und Hashalgorithmus
- Bewertung im App-Store
- Beschreibungstexte
- Erläuterungen
- Erfolg oder Misserfolg der Analyse des SSL Verkehrs
- Handlungsempfehlung bei Misserfolg der Analyse des SSL Verkehrs
- Ungetestete Eingabemöglichkeiten/-konfigurationen & Hinweis auf Gültigkeit des Prüfberichtes **nur** für die angegebenen Parameter
- Externe Dienstleister für Datenspeicherung / Login / Social-Network-Sharing
- Externe Dienste für Werbung / Analytics / Tracking
- Verbindungsanalyse
- Datenverkehrsanalyse
- Permissionanalyse
- Ampelwertung
- Ampelmatrix

Die automatischen Reports sind nach der Erstellung zunächst nur intern zugänglich und müssen separat den Kunden freigegeben werden. Dies geschieht über die angebotene Flatrate-Lösung automatisch oder je nach Vereinbarung individuell pro Kunde/Auftraggeber.

Es besteht die Möglichkeit, die Reports als PDF-Datei zu exportieren. Diese Möglichkeit ist intern nicht eingeschränkt, kann aber je nach Kunde individuell aktiviert oder deaktiviert sein.

4.1.2 Ampelwertung

Aus der Ampelmatrix ergibt sich eine Gesamt-Ampelwertung, die als Grundlage für die effektive App-Bewertung genutzt wird. Das schlechteste Ampelergebnis zählt. Die verschiedenen Wertungen ergeben eine Nutzungsempfehlung die sich wie folgt zusammensetzt:

Grün:

Unauffälliges App-Verhalten

Gelb:

Auffälliges App-Verhalten. Geringfügige Verstöße gefunden. Die App ist mit Hinweisen nutzbar, die vom Kunden beachtet werden sollten. Diese Verstöße können im Einzelnen z.B. folgende Punkte beinhalten:

- Geo-Daten werden unverschlüsselt übertragen
- Geräte-IDs werden übertragen
- Benutzernamen werden unverschlüsselt übertragen
- etc.

Rot:

Signifikante Sicherheitsverstöße wurden gefunden. Von der Nutzung der App wird abgeraten. U. U. kann der Kunde unter Beachtung diverser Parameter eine App-Nutzung dennoch veranlassen. Darunter werden z.B. folgende Verstöße zusammengefasst:

- unveränderbare Geräte-IDs werden unverschlüsselt übertragen
- Benutzernamen werden unverschlüsselt an Dritte übertragen
- Nachrichteninhalte werden unverschlüsselt übertragen
- Standortdaten werden unverschlüsselt an Dritte übertragen
- Personen-beziehbare Daten werden unverschlüsselt übertragen
- etc.

Schwarz:

Die Applikation sollte nicht genutzt werden. Hierunter fallen z.B. die folgenden Verstöße:

- Passwörter werden unverschlüsselt übertragen
- Zahlungsinformationen werden unverschlüsselt übertragen
- unveränderbare Geräte IDs (z.B. IMEI) werden unverschlüsselt übertragen
- etc.

4.1.3 Ampelanpassung

Die Ampelwertung kann nach den Wünschen des Kunden, abweichend von der allgemeinen Empfehlung angepasst werden. Dazu wird ein spezielles, auf den Kunden angepasstes Interface zur Verfügung gestellt, sofern der Kunde diese Funktion wünscht. Hierüber können individuelle Regeln erstellt werden, um die Zuordnung zu den Ampelphasen an bestimmte Fälle zu binden. So ist ein individuelles Regelwerk möglich.

4.2 Automatische Publikation

4.2.1 Kunden-Interface (ASC/TAD)

Nach der internen Publikation erfolgt die manuelle initiale Freischaltung für alle Kunden (Flatrate-Lösung) bzw. individuell für einzelne Kunden. Ist die initiale Freischaltung erfolgt, werden fällige Retests automatisch innerhalb des vereinbarten Retest-Zyklus eingestellt und nach erfolgtem Test freigeschaltet.

Es besteht aktuell zudem die Möglichkeit pro Kunde, automatische Modifikationen der abschließenden Wertung vorzunehmen (z.B. automatische Um-Wertung von rot zu schwarz).

4.2.2 MDM (Mobile Device Management) via API

Die folgenden aggregierten & im Test erhobenen Informationen können via API an angebundene MDM-Systeme übertragen oder von diesen angefordert werden:

- Prüfbericht-ID
- Appname und Version
- Versions-ID der App-Version
- Plattform/Betriebssystem
- Preis
- Ampelbewertung
- App-History (Wertung der letzten fünf App-Versionen)
- URL zur App im App-Store
- Bewertung der App im App-Store