APPVISORY®
by mediaTest digital

PRÜFKRITERIEN KATALOG

Version 1.1

Inhalt

1. Übersicht

In diesem Prüfkriterien-Katalog sind alle von mediaTest digital während eines App Audits geprüften Kriterien aufgelistet. Diese können von jedem Kunden über die Sicherheitskonfiguration hinsichtlich ihrer Relevanz für die Risikobewertung eingestuft werden, sofern das dazu erforderliche Modul zum Leistungsumfang der gebuchten Lösung gehört.

Die Prüfkriterien werden zur besseren Übersichtlichkeit in Kategorien thematisch sortiert. Der Umfang der Prüfkriterien wird dynamisch erweitert und kann entsprechend der technologischen Entwicklung der mobilen Betriebssysteme angepasst werden.

2. Mobile Malware & Viren

In dieser Kategorie wird auf das Vorhandensein von mobile Malware, Viren und ähnlichen Bedrohungen geprüft. APPVISORY verwendet neben der Basisprüfung über das Verhalten der App zur Laufzeit und den aufgezeichneten Datenübertragungen die leistungsstarke SAVAPI des Partners Avira zur Erkennung von mobiler Malware und Viren durch die Avira Anti-Malware-Engine als Teil der statischen Analyse.

3. Datenzugriffe / Datenübertragungen

In diesem Abschnitt sind Datenzugriffe und Datenübertragungen von Daten durch Apps nach Datentyp klassifiziert und in eine Oberkategorie einsortiert. Geprüft wird auf die folgenden Datentypen:

Kategorie	Prüfkriterium	Erklärung
Address Book Content	✔ Adresse (Adressbuch)	Adressdaten eines Kontakts aus dem Adressbuch
	✔ E-Mail-Adresse (Adressbuch)	E-Mail-Adresse eines Kontakts aus dem Adressbuch
	✔ Name (Adressbuch)	Name eines Kontakts aus dem Adressbuch
	✔ Telefonnummer (Adressbuch)	Telefonnummer eines Kontakts aus dem Adressbuch
Communication Data	✔ E-Mail-Absender	Absender einer empfangenen E-Mail
	✔ E-Mail-Betreff	Betreff einer gesendeten oder empfangenen E-Mail
	✔ E-Mail-Inhalte	Inhalt einer gesendeten oder empfangenen E-Mail
	✔ SMS-Absender	Telefonnummer des Absenders einer empfangenen SMS
	✔ SMS-Inhalte	Inhalte gesendeter oder empfangener SMS

Device Account Data	✔ Geräteaccount E-Mail-Adresse	E-Mail-Adresse des geräteeigenen Nutzeraccounts (z.B. Apple-Account, Google Play Account etc.)
	✔ Geräteaccount Name	Zugehöriger Name des geräteeigenen Nutzeraccounts (z.B. Apple-Account, Google Play Account etc.)
	✔ Geräteaccount Passwort	Zugehöriges Passwort des geräte-eigenen Nutzeraccounts (z.B. Apple-Account, Google Play Account etc.)
Device ID (dynamic)	✔ Android Advertising ID	Werbe-ID zur Nutzeridentifikation, durch Nutzer änderbar. Nur gültig für Android-Geräte
	✔ Gerätename	Vom Nutzer vergebener Name für das Endgerät
	✔ IDFA (Identifier for Advertisers)	Werbe-ID zur Nutzeridentifikation, durch Nutzer änderbar. Nur gültig für iOS-Geräte
	✔ IDFV (Identifier for Vendors)	ID zur App-/Nutzeridentifikation, vergeben nur für Apps des gleichen Herstellers. Nur gültig für iOS-Geräte
Device ID (static)	✔ Android ID	Eindeutige Geräte-ID, durch Nutzer nicht änderbar. Nur gültig für Android-Geräte
	✔ Geräte-Seriennummer	Eindeutige Seriennummer des Gerätes, durch Nutzer nicht änderbar
	✔ GSFID (Google Service Framework ID)	Google-eigene ID zur Identifikation eines Gerätes im Google Play Store
	✔ IMEI (International Mobile Equipment Identity)	Eindeutige Geräte-ID, durch Nutzer nicht änderbar
	✔ UDID (Unique Device Identifier)	Eindeutige Gerätekennung, durch Nutzer nicht änderbar. Nur gültig für iOS-Geräte
Device ID (external)	✔ WLAN MAC Adresse (verbundener Access Point)	Eindeutige Kennung des WLAN-Adapters eines verbundenen Access Points, durch Nutzer nicht änderbar
	✔ WLAN SSID (verbundener Access Point)	Name oder Kennung des verbundenen Access Points
Device ID (public)	✔ Bluetooth MAC Adresse	Eindeutige Kennung des Bluetooth-Adapters im Gerät, durch Nutzer nicht änderbar
	✔ WLAN MAC Adresse (Gerät)	Eindeutige Kennung des WLAN-Adapters des Endgeräts, durch Nutzer nicht änderbar
	✔ WLAN MAC Adresse (dummy)	Dummy aus Falschdaten für eine eindeutige Geräte-ID. Nur gültig für iOS-Geräte

Device Metadata	✔ Betriebssystemversion	Betriebssystem und Versionsnummer des auf dem Endgerät installierten Betriebssystems
	✔ Telefonmodell	Modellbezeichnung des genutzten Endgeräts
Device Password	✔ Geräte-PIN	Ziffernfolge zum Entsperren des Endgeräts
	✔ SIM-PIN	Entsperr-PIN der aktiven SIM-Karte
Device Password (external)	✔ WLAN Passwort (verbundener Access Point)	Passwort des verbundenen Access Points
Exif Data	✔ Foto-Metadaten	Metadaten auf dem Gerät gespeicherter oder übertragener Mediendateien
IP Address	✔ Lokale IP Adresse (Gerät)	Lokale (interne) IP-Adresse des Endgeräts
	✔ Öffentliche IP Adresse	Persönliche Adresse, zur Weitergabe bestimmt (z.B. an Logistik-Dienstleister)
Location Data	✔ Standortdaten (exakt)	Exakte Standortdaten des Endgerätes, Genauigkeit auf wenige Meter
	✔ Standortdaten (grob)	Grobe Standortdaten des Endgerätes, Genauigkeit ca. 1 km
Payment Data	✔ BIC (Business Identifier Code)	Internationale Bank-Identifikationskennzahl
	✔ IBAN (International Bank Account Number)	Internationale Kontonummer
	✔ Kontoinhaber	Name des Kontoinhabers
	✔ Kreditkarteninhaber	Name des Kreditkarteninhabers
	✔ Kreditkartennummer	Kreditkartennummer
	✔ PayPal E-Mail-Adresse	E-Mail-Adresse des PayPal-Accounts
	✔ PayPal Passwort	Zugehöriges Passwort des PayPal-Accounts

Personal Data	✔ E-Mail-Adresse	E-Mail-Adresse
	✔ Name (Vor-/Nachname)	Vorname und/oder Nachname
	✔ Persönliche Adresse	Persönliche Adresse, nicht öffentlich einsehbar (z.B. in einem Profil gespeichert)
	✔ Telefonnummer	Telefonnummer
	✔ Vertragsdaten (nicht sensitiv)	Nicht-sensible Daten ohne direkten Personenbezug (z.B. Buchungs-nummern, Bestellnummern etc.)
	✔ Vertragsdaten (sensitiv)	Sensible Daten mit direktem Personenbezug (z.B. Steuer-IDs, Versicherungsnummern etc.)
SIM ID (static)	✔ Geräte-Telefonnummer	Telefonnummer der aktiven SIM-Karte
	✔ ICCID (Integrated Circuit Card Identifier)	Seriennummer der aktiven SIM-Karte
	✔ IMSI (International Mobile Subscriber Identity)	Eindeutige Nutzerkennung im Mobilfunknetz
Social Network Data	✔ Facebook Login-Name	Login-Name des Facebook-Accounts
	✔ Facebook Nutzername	Nutzername des Facebook-Accounts
	✔ Facebook Passwort	Zugehöriges Passwort des Facebook-Accounts
	✔ Google+ Nutzername	Nutzername des Google+-Accounts
	✔ Google+ Passwort	Zugehöriges Passwort des Google+-Accounts
	✔ Twitter Login-E-Mail-Adresse	Login-E-Mail-Adresse des Twitter-Accounts
	✔ Twitter Nutzername	Nutzername des Twitter-Accounts
	✔ Twitter Passwort	Zugehöriges Passwort des Twitter-Accounts
User Data	✔ Benutzername	Benutzername
	✔ Bundle Identifier (installed Apps)	Eindeutiges Identifikationsmerkmal jeder App
	✔ Passwort	Passwort
User Generated Data	✔ Feedback und Kommentare	Durch Nutzer abgegebene Kommentare oder gesendetes Feedback
	✔ Nutzer-Inhalte	Sammelkategorie für durch Nutzer erzeugte Daten (z.B. Notizen, gespeicherte Dateien, Texte etc.)
	✔ Suchanfrage	Suchanfrage

4. Drittanbieter

In dieser Kategorie sind Drittanbieter aufgelistet, die in Apps integriert werden können. Einzelne Drittanbieter werden dabei in die folgenden Kategorien sortiert:

- **Werbedienste**: Einblendung von Werbeanzeigen innerhalb der App
- **Analytics-Dienste**: Messung von Nutzerverhalten, Performance-Analyse
- **Tracking**: Identifikation einzelner Nutzer/Geräte als Unterstützung zum Ausspielen von gezielter Werbung
- **Cloud-Dienste**: Online-Datenspeicher für Dateien auf unternehmensfremden Servern
- **Kartendienste**: Darstellung von Kartenmaterial, häufig zusätzlich mit Lokalisierung des Nutzers verbunden
- **Soziale Netzwerke**: Anbindung Sozialer Netzwerke wie Facebook, Xing etc. zum Teilen von Kommentaren, Dateien etc.

5. Serverstandorte

In dieser Kategorie werden alle von einer App während der Nutzung kontaktierten bzw. im automatischen Test potenziell kontaktierten Server gelistet und die Standorte der Server überprüft. Diese können einzeln zugelassen oder abgelehnt werden.

6. Zusatztests

In dieser Kategorie werden zusätzliche Prüfungen abgebildet. Diese umfassen neben App-Eigenschaften auch Prüfungen auf Schwachstellen.

- **App nutzt Jailbreak-Erkennung**: Die App nutzt eine Jailbreak-Erkennung, um zu prüfen, ob auf dem Gerät Administratorzugriff auf das Betriebssystem möglich ist. Dadurch ist es für eine App möglich, zu erkennen, ob sie Aktionen ausführen kann, die nicht zum gewünschten Funktionsumfang der App gehören müssen.
- **App mit iCloud-Implementierung**: Die App greift auf die native iCloud-Implementierung zurück. Dabei werden Daten automatisch auf unternehmensfremde Server übertragen.
- **In-App-Purchases**: In der App sind kostenpflichtige Funktionserweiterungen verfügbar. Dadurch können ungeplante Zusatzkosten entstehen.

- **App kann (kostenpflichtige) SMS versenden**: Die App hat Zugriff auf die SMS-Funktion des Endgerätes und kann kostenpflichtige SMS versenden. Dadurch können ungeplante Zusatzkosten entstehen.

- **App kommuniziert mit anderen installierten Apps**: Die App nutzt die Betriebssystem-Funktion „InterProcessCommunication“, um mit anderen installierten Apps zu kommunizieren. Dabei kann ein unkontrollierter Datenaustausch zwischen den Apps auftreten.

- **App ist XARA-anfällig**: Die App ist anfällig für die iOS-Sicherheitslücke „XARA“. Dabei wird die Sicherheit des Passwortmanagers „Keychain“ kompromittiert, gespeicherte Passwörter können ausgelesen und modifiziert werden.

- **App blendet aktive Werbeanzeigen ein**: Die App nutzt eingebundene Werbe-Netzwerke, um InApp-Werbung einzublenden. Dabei kann es sich sowohl um Grafiken und Banner, als auch um Videowerbung handeln.

7. Zusatzfragen

In dieser Kategorie können zusätzliche Elemente in die Risikobewertung einfließen, die über eine rein technische Prüfung hinausgehen.

- **Soll die History in der Bewertung mit berücksichtigt werden**: Apps erhalten nur dann eine neue Risikobewertung, wenn zwei aufeinander folgende Prüfungen die gleiche Risikobewertung haben. So wird bei Ausreißern eine Eskalation in angebundene MDMs verhindert.

- **Soll die AGB in der Bewertung mit berücksichtigt werden**: Legt fest, ob eine Prüfung der Allgemeinen Geschäftsbedingungen und der Datenschutzerklärung der App in die Risikobewertung einfließen soll. Eine Prüfung erfolgt nur auf individuelle Beauftragung und nur bei ausgewählten Apps. Die Prüfung findet nach deutschem Recht statt.

- **Soll die mediaTest digital Nutzungsempfehlung mit berücksichtigt werden**: In Einzelfällen vergibt mediaTest digital eine Nutzungsempfehlung, die nicht an technische Bedingungen geknüpft ist. Dabei wird u.a. das Geschäftsmodell des App-Herstellers berücksichtigt

8. Support

Wir hoffen, dass dieser Prüfkriterienkatalog Ihnen im Umgang mit APPVISORY eine Hilfe darstellt. Sollten dennoch Fragen auftreten, wenden Sie sich bitte an unseren Professional Service.

Professional Service
+49 (0)172 667 99 76
service@appvisory.com

mediaTest digital GmbH
Goseriede 4
30159 Hannover
+49 (0)511 35 39 94 22
contact@appvisory.com

www.appvisory.com