Bundesamt
für Sicherheit in der
Informationstechnik

Herstelleranforderungen zur Sicherheit von Smartphones

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 95820
E-Mail: referat-tk12@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Dieser Forderungskatalog richtet sich an Erstausrüster, sogenannte Original Equipment Manufacturer (OEM) von Smartphones. Er beschreibt die geforderte Grundausstattung der Geräte aus IT-Sicherheitsperspektive bei der Auslieferung sowie Maßnahmen für den sicheren Betrieb.

Die Umsetzung der Forderungen, die in den einzelnen Kapiteln allgemein beschrieben werden, muss nach dem jeweiligen Stand der Technik erfolgen. Darüber hinaus sind die referenzierten technischen Richtlinien[1] des BSI zu berücksichtigen.

1 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html

2 Forderungskatalog

2.1 Konformität zu EU-Recht und nationalem Recht

Jedes neue Gerät bzw. die darauf vom Hersteller vorinstallierten Apps sowie die verbundenen Dienste müssen den Anforderungen der Datenschutz-Grundverordnung der Europäischen Union (EU-DSVGO) sowie den nationalen Datenschutzregelungen in Deutschland entsprechen. Eine entsprechende Erklärung muss durch den Hersteller abgegeben werden.

Um die Bedeutung dieser Forderung zu unterstreichen, wird sie in den folgenden Kapiteln teilweise wiederholt.

2.2 Aktualität

2.2.1 Aktualität der OS-Version

Zu jedem Gerätetyp muss eine Aussage über die Versorgung mit Betriebssystem-Updates (Hauptversionen) gemacht werden. Diese Erklärung muss die Zeitdauer der Unterstützung in Jahren nach der Veröffentlichung sowie die Mindestanzahl der geplanten Hauptversionen enthalten. (Hierbei wird vorausgesetzt, dass mobile Betriebssysteme jährlich in einer neuen Hauptversion veröffentlicht werden.)

Neugeräte müssen mit dem letzten (neusten) Betriebssystem, das zum Zeitpunkt der Geräteveröffentlichung verfügbar ist, ausgestattet sein. Steht zum Zeitpunkt der Geräteinbetriebnahme ein neueres Betriebssystem zur Verfügung, muss dieses zur Installation angeboten werden.

2.2.2 Unterstützung mit Sicherheits-Updates

Geräte müssen über die Dauer von 5 Jahren nach Geräteveröffentlichung mit Sicherheits-Updates versorgt werden. Aus der Gerätebeschreibung muss klar ersichtlich sein, ab wann ein Gerät aus der Versorgung mit Sicherheits-Updates herausfällt.

Die Sicherheits-Updates müssen alle bekannt gewordenen Sicherheitslücken sämtlicher Softwarekomponenten (Treiber, Betriebssystem sowie customisierte Softwareschicht und vorinstallierte Apps) schließen. Dies muss in einem Bulletin vollständig und transparent dargelegt werden.

2.2.3 Dauer bis Sicherheits-Updates ausgerollt wird

Sicherheits-Updates müssen innerhalb eines Monats nach Veröffentlichung zur Installation bereitgestellt werden.

2.3 Schutz vor unbefugtem Zugriff auf Endgerät

2.3.1 Lock Mechanismus

Mindestens einer der folgenden Mechanismen zur Entsperrung des Geräts muss vorhanden und sicher implementiert sein

- Alphanumeric password
- Fingerprint
- Face recognition / 3D face recognition
- High secure biometric scan

2.3.2 Geräteverschlüsselung

Geräte müssen mit einer Vollverschlüsselung (full disk encryption) für den internen, fest verbauten Speicher ausgerüstet sein. Das für die Verschlüsselung verwendete Schlüsselmaterial muss neben dem Nutzerkennwort auf einem gerätespezifischen, individuellen Merkmal aufbauen. Das Schlüsselmaterial muss sicher gespeichert sein, siehe Kapitel „Sichere Ablaufumgebung/HSE“.

2.3.3 Verschlüsselung der SD-Karte

Bei Geräten mit externer Speicherkarte muss die Möglichkeit einer sicheren Verschlüsselung gegeben sein.

2.3.4 Sichere Ablaufumgebung / HSE

Das Gerät muss eine vom normalen Betriebssystem abgetrennte sichere Ablaufumgebung enthalten (Trusted Execution Environment, TEE). Diese muss auf einem Hardware Secure Element (HSE) aufbauen. Das HSE muss auch zum Schutz kritischer Daten verwendet werden. Siehe dazu auch Kapitel „Dedizierte Hardware für kryptografische Funktionen“.

2.3.5 Sicherer Bootprozess

Bei einem abgesicherten Bootprozess prüft jede ausgeführte Stufe die nächstfolgende auf Integrität und Authentizität, bevor sie ihr die Kontrolle übergibt. Außerdem wird mit der ersten Stufe des Prozesses, dem Bootloader, die Integrität und Authentizität von Updates geprüft. Veränderungen müssen protokolliert und der Bootprozess muss abgebrochen werden. Dem Anwender muss eine Wiederherstellungsmöglichkeit des ausgelieferten Systemzustandes angeboten werden. Darüber hinaus sollte die Möglichkeit angeboten werden das Gerät auszuschalten.

2.3.6 Entsperren des Bootloader

Es muss ein Prozess zum Entsperren des Bootloader angeboten werden. Dieser Prozess muss transparent sein, d.h. der Hersteller muss ein Tool dazu anbieten und/oder eine leicht verständliche Handlungsanweisung bereitstellen.

Während des Entsperrprozesses müssen alle bis dato angefallenen Nutzerdaten sicher gelöscht werden.

Darüber hinaus muss dem Nutzer nach Abschluss des Bootprozesses ein verständlicher Hinweis bzgl. des entsperrten Bootloaders angezeigt werden, der auf die potenziellen Risiken hinweist.

2.3.7 Cyphering

Die Nutzung der neuesten Radio Kanal Cyphering Algorithmen der Telefone hat aus Netzwerksicht sehr hohe Priorität. Geräte die die neuesten Algorithmen unterstützen sind besser geschützt.

Neugeräte müssen nach dem Stand der Technik ausgerüstet sein, d.h. die neusten Algorithmen unterstützen. Weitere Hinweise dazu: siehe Technische Richtlinie des BSI TR-02102 Kap. 4.7 "Cyphering.

2.4 Datenschutz

2.4.1 Vorinstallierte Apps in der Systempartition

In der Systempartition dürfen nur Apps installiert sein, die spezielle (System-) Berechtigungen benötigen (Beispiel: Signature-Permission bei Android). Demgegenüber dürfen Standard-User-Apps, wie beispielsweise der Hersteller-eigene Browser oder Drittanbieter-Apps, dort nicht installiert sein.

2.4.2 Berechtigungen für (vorinstallierte) Apps

Apps dürfen nur diejenigen Berechtigungen beantragen, die sie für die Erfüllung ihrer Aufgabe unbedingt benötigen. Vor der ersten Nutzung einer kritischen[2] App-Berechtigung in einer Applikation muss der Nutzer dem zustimmen. Einmal gewährte Berechtigungen können widerrufen werden. Abgelehnte Anforderungen können nachträglich gegeben werden. Abgelehnte bzw. widerrufene Berechtigungen dürfen zu nachvollziehbaren Funktionseinschränkungen, jedoch nicht zum Absturz der App führen. Es muss einen Menüpunkt zu den App-Berechtigungen geben, der alle öffentlichen sowie internen Berechtigungen widerspiegelt. Es muss eine vollständige und verständliche Beschreibung der Berechtigungen geben.

Diese Forderung gilt grundsätzlich für alle mobilen Apps. In diesem Forderungskatalog sind die im Auslieferungszustand des Gerätes vorinstallierten Apps im Fokus.

2.4.3 Sicherer Softwareentwicklungsprozess

Im Rahmen eines sicheren Softwareentwicklungsprozesses müssen die Vorgaben des Plattformherstellers umgesetzt werden. Für Android wären dies zum Beispiel „Google Best Practices“. Darüber hinaus sollten zusätzliche Richtlinien für die sichere Softwareentwicklung, wie beispielsweise der „Mobile AppSec Verification Standard“ der OWASP.ORG berücksichtigt werden.

2.4.4 Telemetrie

Unter dem Begriff Telemetriedaten werden alle Daten (Nutzer- und Nutzungsdaten, Systemdaten) zusammengefasst, die ein Hersteller auf einem Gerät erhebt, um seine Produkte weiterzuentwickeln. Der Hersteller darf diese Daten nur nach vorheriger expliziter Zustimmung durch den Nutzer zu diesem Zweck weiterverarbeiten oder weitergeben. Es muss eine ausführliche und verständliche Beschreibung der erhobenen und versendeten Daten geben. Die Erfassung sowie die Ausleitung der Telemetriedaten muss auf ein benötigtes Minimalmaß beschränkt werden.

Der Hersteller muss für das Smartphone, bestehend aus Betriebssystem, Hersteller-Branding sowie vorinstallierte Drittanbieter-Apps eine DSGVO-konforme Erklärung über die Erhebung sowie der Verarbeitung der Telemetriedaten abgeben. Bei Ablehnung durch den Nutzer dürfen keinerlei Telemetriedaten erhoben, verarbeitet oder transferiert werden.

2 Kritische App Berechtigung: Berechtigungen die den Zugriff auf persönliche Daten beziehungsweise personenbezogene Daten erlauben (z. Beispiel Kontakte, Nachrichteninhalte, Geodaten), die Manipulation sicherheitsrelevanter Systemfunktionen erlauben (z. Beispiel Systemdialoge oder Einstellungen visuell überlagern) oder deren Verwendung dem Nutzer Kosten verursachen können.

2.4.5 Secure Software Platform

Für Software-Installationen und –Updates des Herstellers muss eine sichere Plattform bereitstehen, die Geräte- und Nutzerinformationen, die diese Plattform für die Erfüllung ihrer Dienste benötigt, zu keinen anderen Zwecken verwendet und auch nicht an Dritte weitergeben darf. Hierzu muss der Anbieter eine DSGVO-konforme Erklärung abgeben.

2.4.6 Netzwerk-Gateways

Der Datenaustausch eines Gerätes mit dem Internet muss über das vom Netzbetreiber vorgeschlagene oder selbst eingetragene Gateway erfolgen. Es dürfen keine hardcodierten (nicht änderbare) Rückfalloptionen über sonstige Server existieren.

Gleiches gilt für die DNS-Konfiguration.

2.5 Angriffsfläche minimieren

2.5.1 Cloud-Dienste

Die Verwendung von Cloud-Diensten muss dem Nutzer vor der ersten Nutzung angezeigt werden und muss konform zur DSGVO erfolgen. Die Nutzung aller Cloud-Dienste muss übersichtlich dargestellt werden. Neue Geräte dürfen keine vorkonfigurierte Cloud-Dienste enthalten (Beispiele: Google-Konto, Hersteller-Apps). Hierzu zählt auch, dass keine lokalen Dienste aktiviert sind, die mit diesen Cloud-Diensten kommunizieren können. Die Verwendung von Cloud-Diensten kann abgelehnt beziehungsweise widerrufen werden, wobei dann nicht anonymisierte Daten in der Cloud gelöscht werden müssen.

2.5.2 Grundkonfiguration beim Kauf

Im Auslieferungszustand müssen relevante Einstellungen so gewählt werden, dass der Sicherheitsaspekt vor dem Komfort des Nutzers steht. Vor unsicheren Einstellungen muss gewarnt werden. Beispiele: Angebote für die Einrichtung einer Bildschirmsperre und für Datenträgerverschlüsselung.

2.5.3 Schnittstellen

WLAN: Die automatische Verbindung zu bekannten WLANs muss abschaltbar sein. Im Gerät gespeicherte Listen bekannter WLAN-Accesspoints muss einsehbar und editierbar sein. In sog. „WiFi probe requests“ dürfen keine SSIDs versendet werden. Zudem muss die MAC-Adresse während der Netzsuche anonymisiert sein.

Bluetooth: Die Verwendung der Bluetooth-Schnittstelle muss durch den Nutzer konfigurierbar sein. Sie muss jederzeit abschaltbar sein.

NFC: Die verwendete NFC-Schnittstelle muss gem. des NFC Handset Test Books[3] der GSM Association (TS 27) zertifiziert sein. Die Verwendung der NFC-Schnittstelle muss durch den Nutzer konfigurierbar sein. Die Schnittstelle sollte standardmäßig abgeschaltet sein. Bevor Daten über die NFC-Schnittstelle auf das Endgerät geladen werden oder eine Applikation - z.B. ein Payment Service - diese Schnittstelle benutzt, muss die Übertragung bzw. Nutzung durch den Nutzer explizit genehmigt werden. Die NFC Schnittstelle muss im Betriebssystem geeignet separiert werden. Es müssen Schutzmaßnahmen gegen unerlaubte

3 https://www.gsma.com/newsroom/wp-content/uploads//TS27-v15-0.pdf

Kommunikationsversuche bestehen und es darf kein unsignierter Code übertragen werden. Insbesondere sollten nur vertrauenswürdige Verbindungsversuche bzw. zertifizierte Applikationen akzeptiert werde.

2.5.4 Dedizierte Hardware für kryptografische Funktionen

Die wesentlichen kryptographischen Funktionen des Betriebssystems müssen durch dedizierte Hardware unterstützt werden. Insbesondere müssen alle kryptographischen Schlüssel direkt in sicherer Hardware durch einen zertifizierten Cryptographic Service Provider verwaltet werden. Der Export von privaten und geheimen Schlüsseln darf nur in gesicherter Form erfolgen.

Die Hardware-Unterstützung muss für die vom Betriebssystem selbst genutzten Sicherheitsfunktionen Full-Disk-Encryption, Secure Boot, FIDO2, verwendet und auch Anwendungen zur Verfügung gestellt werden. Dabei muss auch die Ausführung von sicherheitskritischen Anwendungen in Form von Applets auf der Hardware selbst unterstützt werden.

Das verwendete Hardware-Element muss gem. des Protection Profiles „Cryptographic Service Provider“ (BSI-CC-PP-0104-2019)[4] oder „Cryptographic Service Provider Light“ (BSI-CC-PP-0111-2019 Commen-Criteria-zertifiziert sein.

Weiterhin ist es erforderlich, dass das verwendete Hardware-Element in der Lage ist, eID-Applets gem. Abschnitt 2.2.4 der BSI-TR 03159-2 „Mobile Identities Part 2: EAC and FIDO based mobile identities“[5] zu verarbeiten.

2.5.5 Sicherheitsfunktionen des Prozessors

Der Prozessor muss mit Hardware-basierten Sicherheitsfunktionen das Betriebssystem bei der Abwehr von Angriffen unterstützen. Dazu zählen Mechanismen zur Mitigation von ROP/JOP Angriffen (Pointer Authentication), Angriffen auf die spekulative Ausführung, Speicherverschlüsselung, sowie Separationsmechanismen (Trusted Execution Environments).

2.6 Fortgeschrittene Anforderungen

2.6.1 Datenmigration für PIM-Daten

Es muss die Möglichkeit bestehen sog. Personal Information Management (PIM) Daten in einem standardisierten Datenformat zu exportieren, so dass diese Daten auf einem anderen Gerät problemlos importiert werden können. Zu PIM-Daten zählen Kontakte, Termine, Aufgaben und Notizen sowie zusätzlich lokale E-Mails.

2.6.2 Lokalisierung zentraler Dienste

Betriebssystemrelevante Dienste sowie Dienste systemintegrierter Apps müssen in deutschen Rechenzentren gehostet und verarbeitet werden. Dazu zählen u. a. Update-Server sowie die externe Verarbeitung von Telemetriedaten.

4 https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0104.html
5 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03159/TR-03159-2.pd

2.6.3 FIDO2 Authentifizierung

Das Gerät muss einen Authentifizierungsmechanismus nach FIDO2 Standard anbieten, mit dem sich der Nutzer einfach gegenüber Web-Diensten authentisieren kann. Der FIDO-Authenticator muss mindestens nach FIDO Level 2 zertifiziert sein.