SYS.3.2: Tablet und Smartphone

SYS.3.2.4: Android

1 Beschreibung

1.1 Einleitung

Ein oft genutztes Betriebssystem für Smartphones und Tablets ist Android von Google. 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 Verwaltungsrichtlinien mit jeder Version und es gibt herstellerspezifische Erweiterungen, die zusätzliche Richtlinien erlauben.

1.2 Zielsetzung

Ziel des Bausteins ist es, über typische Gefährdungen im Zusammenhang mit Android zu informieren sowie aufzuzeigen, wie Android-basierte Geräte sicher in Institutionen eingesetzt werden können. Auf Basis der im Baustein aufgeführten Anforderungen können zudem Sicherheitsrichtlinien erstellt werden.

1.3 Abgrenzung und Modellierung

Der Baustein SYS.3.2.4 *Android* ist für alle dienstlich verwendeten Smartphones und Tablets mit dem Betriebssystem Google Android anzuwenden.

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 *Allgemeine Smartphones und Tablets* behandelt und sind ebenfalls umzusetzen, wenn Android-basierte Geräte verwendet werden. Ebenfalls nicht Bestandteil dieses Bausteins sind Anforderungen für den Fall einer zentralen Administration von Android-Geräten über ein MDM. Diese sind im Baustein SYS.3.2.2 *Mobile Device Management (MDM)* aufgeführt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für das im Baustein SYS.3.2.4 *Android* behandelte Zielobjekt von besonderer Bedeutung:

2.1 Deaktivieren von Sicherheitsfunktionen

Der Bootprozess von Android-basierten Geräten wird mit Hilfe eines Herstellerzertifikats abgesichert. Dabei wird jeweils der nächste Ausführungsschritt vor dessen Ausführung überprüft. Damit ist sichergestellt, dass das Betriebssystem Android unverändert startet.

Beim Entsperren des Bootloaders wird diese Vertrauenskette unterbrochen, so dass ein verändertes Betriebssystem starten kann. Solche Veränderungen am Bootprozess werden teilweise vom Hersteller unterstützt, teilweise werden Bootloader auch über Schwachstellen entsperrt.

Das Android-Sicherheitskonzept wird hierbei umgangen oder außer Kraft gesetzt und es entstehen neue Gefährdungen, die anderweitig abgesichert werden müssen.

2.2 Schadsoftware für das Android-Betriebssystem

Aufgrund der hohen Verbreitung und der offenen Architektur sind Geräte mit Android-Betriebssystem ein beliebtes Ziel für Schadsoftware, die oft vom Benutzer selbst installiert wird. Unter Android ist es relativ einfach möglich, Apps nicht nur aus dem Playstore von Google, sondern auch aus alternativen Quellen oder per direktem Download zu installieren. Neben den überwachten App Stores von Google, Geräteherstellern und anderen Anbietern werden Apps auch über eher zweifelhafte Quellen zur Installation angeboten. Da es unter Android nicht zwingend erforderlich ist, Apps aus dem offiziellen Google Playstore zu installieren, könnte ein Angreifer beispielsweise eine beliebte App mit einer Schadsoftware infizieren und anschließend wieder zum Download zur Verfügung stellen.

2.3 Fehlende Updates für das Android-Betriebssystem

Einige Hersteller liefern Smartphones 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 Geräte besonders gefährdet. Als Konsequenz können bekannte Schwachstellen dieser Geräte nicht beseitigt und entsprechend leicht von Angreifern ausgenutzt werden.

2.4 Risiko durch Benutzerkonten (Google-ID) für Google-Dienste

Mit der Google-ID können Benutzer zentral auf alle Google-Dienste zugreifen, z. B. auf die Geräteverwaltung, die aufgezeichneten geographischen Positionen, Chatsoftware, Cloud-Speicher, den Play Store, Musik-, Buch- und Filmangebote, Datensicherung, Bookmarks oder 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 hiermit verbundenen Dienste unter der gestohlenen Identität benutzen. Auch kann er beispielsweise auf alle dort gespeicherten Daten zugreifen und Geräte aus der Ferne lokalisieren oder sie zurücksetzen, also alle Daten auf dem Gerät löschen.

2.5 Vorinstallierte Apps und integrierte Funktionen bei Android-basierten Geräten

Mit dem Betriebssystem liefern die Hersteller von Android-Geräten oft bereits fest integrierte und vorinstallierte Apps sowie eine Anbindung zu Diensten von Drittanbietern (Twitter, Facebook, usw.) aus. Diese Apps kann der Benutzer oft nicht selbst entfernen. Damit vergrößert sich die Angriffsfläche des Android-Betriebssystems. Auch die direkte Anbindung an Drittanbieter-Dienste ist in Institutionen oft nicht erwünscht.

Insgesamt steigt durch die tiefe Integration von Apps und Schnittstellen von Drittanbietern die Gefahr, dass das Gerät mit Schadsoftware infiziert wird oder ein Angreifer unberechtigt auf vertrauliche Informationen zugreifen kann.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.3.2.4 *Android* 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 zuständig, dass alle Anforderungen gemäß dem festgelegten

Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein SYS.3.2.4 *Android* vorrangig erfüllt werden:

SYS.3.2.4.A1 ENTFALLEN (B)
Diese Anforderung ist entfallen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein SYS.3.2.4 *Android*. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.3.2.4.A2 Deaktivieren der Entwickler-Optionen (S)
In allen Android-basierten Geräten SOLLTEN die Entwickleroptionen deaktiviert sein.

SYS.3.2.4.A3 Einsatz des Multi-User- und Gäste-Modus (S)
Es SOLLTE geregelt sein, ob ein Gerät mit anderen Personen geteilt werden darf. Es SOLLTE festgelegt werden, ob dazu der Multi-User- oder Gäste-Modus verwendet werden muss. Ein Benutzer auf einem Android-basierten Gerät SOLLTE eine natürlichen Person sein.

SYS.3.2.4.A4 ENTFALLEN (S)
Diese Anforderung ist entfallen.

SYS.3.2.4.A5 Erweiterte Sicherheitseinstellungen (S)
Es SOLLTEN sich nur freigegebene Sicherheits-Apps als Geräteadministrator oder „Trust Agents“ eintragen lassen. Dies SOLLTE regelmäßig überprüft werden.

Weiterhin SOLLTE es nur erlaubten Apps möglich sein, auf Nutzungsdaten und auf Benachrichtigungen zuzugreifen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein SYS.3.2.4 *Android* 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.

SYS.3.2.4.A6 ENTFALLEN (H)
Diese Anforderung ist entfallen.

SYS.3.2.4.A7 ENTFALLEN (H)
Diese Anforderung ist entfallen.

4 Weiterführende Informationen

4.1 Wissenswertes

Für den Baustein SYS.3.2.4 *Android* gibt es keine weiterführenden Informationen.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein SYS.3.2.4 *Android* von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.21 Manipulation von Hard- oder Software

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.38 Missbrauch personenbezogener Daten

G 0.41 Sabotage

G 0.46 Integritätsverlust schützenswerter Informationen