Bundesamt
für Sicherheit in der
Informationstechnik

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. Zudem ermöglichen spezifische Erweiterungen der herstellenden Institutionen zusätzliche Richtlinien.

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

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.3.2.4 *Android* von besonderer Bedeutung.

2.1. Deaktivieren von Sicherheitsfunktionen

Der Bootprozess von Android-basierten Geräten wird mit Hilfe eines Herstellendenzertifikats 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 von der herstellenden Institution 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 von Benutzenden 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, Geräteherstellenden und anderen Anbietenden 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, könnten Angreifende 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 herstellende Institutionen 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 Angreifenden ausgenutzt werden.

2.4. Risiko durch Konten (Google-ID) für Google-Dienste

Mit der Google-ID können Benutzende 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 Anbietende von Diensten im Internet verwenden die Google-ID, um Benutzende zu authentisieren.

Können sich Angreifende über die Google-ID authentisieren, können alle hiermit verbundenen Dienste unter der gestohlenen Identität benutzt werden. Auch können beispielsweise auf alle dort gespeicherten Daten zugegriffen und Geräte aus der Ferne lokalisiert oder zurückgesetzt, also alle Daten auf dem Gerät gelöscht werden.

2.5. Vorinstallierte Apps und integrierte Funktionen bei Android-basierten Geräten

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

Insgesamt steigt durch die tiefe Integration von Apps und Schnittstellen von Drittanbietenden die Gefahr, dass das Gerät mit Schadsoftware infiziert wird oder Angreifende unberechtigt auf vertrauliche Informationen zugreifen können.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.3.2.4 *Android* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein 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 diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.3.2.4.A2 Deaktivieren des Entwicklermodus (S)

In allen Android-basierten Geräten SOLLTE der Entwicklermodus 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. Benutzende auf einem Android-basierten Gerät SOLLTEN natürliche Personen sein.

SYS.3.2.4.A4 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.4.A5 Erweiterte Sicherheitseinstellungen (S)

Es SOLLTEN nur freigegebene Sicherheits-Apps Rechte zur Geräteadministration bekommen oder sich als „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 diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen 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.