



SYS.3.2: Tablet und Smartphone

SYS.3.2.1: Allgemeine Smartphones und Tablets

1 Beschreibung

1.1 Einleitung

Smartphones sind Mobiltelefone, die mit einem großen, üblicherweise berührungsempfindlichen Bildschirm (Touch-Display) ausgestattet sind. Smartphones vereinen neben der Telefonie beispielsweise Media-Player, Personal Information Manager und Digitalkamera in einem Gerät und bieten den Benutzern darüber hinaus viele weitere Anwendungen und Funktionen, wie Web-Browser, E-Mail-Client oder GPS. Zudem sind sie mit Mobilfunk-, WLAN- und Bluetooth-Schnittstellen ausgestattet. Tablets sind, vereinfacht gesagt, Smartphones mit großem Formfaktor, mit denen in der Regel nicht über das Mobilfunknetz telefoniert werden kann. Als Phablets werden Hybridgeräte aus Smartphone und Tablet bezeichnet. Sie werden in diesem Baustein nicht gesondert hervorgehoben.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, den Verantwortlichen des Sicherheitsmanagements und des IT-Betriebs Informationen zu den typischen Gefährdungen für Smartphones und Tablets zu geben sowie ihnen Anforderungen zu vermitteln, wie diese vermieden bzw. beseitigt werden können. Außerdem sollen den Verantwortlichen Ansätze aufgezeigt werden, um schutzbedarfsgerechte Konfigurationsprofile zu erstellen. Diese Konfigurationsprofile können über eine zentrale Infrastruktur zum Mobile Device Management (MDM) verteilt und verwaltet werden. Es kann jedoch bei der Vielzahl von unterschiedlichen Betriebssystemen nicht grundsätzlich vorausgesetzt werden, dass die Geräte in ein solches MDM eingebunden sind.

1.3 Abgrenzung und Modellierung

Der Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* ist für alle Smartphones und Tablets anzuwenden, die für dienstliche Zwecke eingesetzt werden.

Dieser Baustein geht nicht darauf ein, wie spezifische Betriebssysteme von Smartphones und Tablets abgesichert werden, da dies detailliert in den Bausteinen für die jeweiligen Systeme beschrieben wird, z. B. in SYS.3.2.3 *iOS (for Enterprise)* oder SYS.3.2.4 *Android*. Sicherheitsanforderungen für den Betrieb eines MDM werden in SYS.3.2.2 *Mobile Device Management (MDM)* beschrieben. Diese Bausteine sind entsprechend zusätzlich anzuwenden, wenn Smartphones und Tablets in Institutionen eingesetzt werden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* von besonderer Bedeutung:

2.1 Verlust von Smartphones und Tablets

Da Smartphones und Tablets in der Regel klein sind und ständig transportiert werden, können sie leicht vergessen, verloren oder gestohlen werden. Neben dem wirtschaftlichen Schaden wiegt der Verlust der Vertraulichkeit und Integrität der enthaltenen Daten besonders schwer. Über ein entwendetes mobiles Endgerät könnte ein Angreifer auf vertrauliche Informationen oder IT-Ressourcen der Institution zugreifen.

2.2 Fehlende Betriebssystem-Updates

Es erscheinen regelmäßig neue Versionen und Updates von mobilen Betriebssystemen. Diese müssen bei Geräten, die herstellerspezifische Erweiterungen des Betriebssystems haben, erst von den Herstellern in ihre Version integriert und anschließend verteilt werden. Updates werden in der Regel für die neueste Gerätegeneration und für eine Reihe von älteren Gerätegenerationen bereitgestellt. Allerdings werden nicht alle zurückliegenden Betriebssystem-Versionen im gleichen Umfang mit (Sicherheits-) Updates versorgt. Teilweise werden Betriebssysteme auch aus wirtschaftlichen Gründen nicht weiterentwickelt. Nachträglich bekannt gewordene Schwachstellen im Betriebssystem einer bereits abgekündigten Gerätegeneration können dann nicht mehr durch Updates geschlossen und von Angreifern besonders leicht ausgenutzt werden.

2.3 Software-Schwachstellen in Anwendungen (Apps)

Auch bereits vorinstallierte Apps können Schwachstellen enthalten, die für lokale Angriffe oder für Angriffe über Netzverbindungen ausgenutzt werden können. Außerdem werden viele Apps von Drittentwicklern nach einiger Zeit nicht mehr weiter gepflegt. Folglich können erkannte Sicherheitsmängel dann nicht mehr durch entsprechende Updates behoben werden.

2.4 Manipulation von Smartphones und Tablets

Ein Angreifer kann sich Zugang zu Smartphones oder Tablets verschaffen, um gezielt Daten zu manipulieren. So könnte er beispielsweise die Konfiguration ändern, zusätzliche Dienste starten oder Schadsoftware installieren. Dadurch kann er auf dem manipulierten System beispielsweise die Kommunikationsverbindungen mitschneiden (ungewollter Datenabfluss) oder die Regeln nach seinen Bedürfnissen ändern (z. B. Zugriffe aus dem Internet auf das Endgerät erlauben).

2.5 Schadprogramme für Smartphones und Tablets

Wie jedes mit dem Internet verbundene Gerät, sind auch mobile Endgeräte von Schadsoftware bedroht. Das Infektionsrisiko ist verglichen mit Client-Betriebssystemen wie Microsoft Windows zwar noch geringer, jedoch konzentrieren sich Angreifer immer mehr auf mobile Geräte. Insbesondere wenn Apps aus unzuverlässigen Quellen bezogen werden oder keine Updates für bekannte Schwachstellen verfügbar sind, ist die Gefahr einer Infektion hoch. Wird ein Gerät infiziert, können Angreifer beispielsweise Daten auslesen, verändern, löschen oder auf interne IT-Ressourcen der Institution zugreifen.

2.6 Webbasierte Angriffe auf mobile Browser

Mobile Browser, aber auch viele andere Apps, können Webseiten und Webinhalte anzeigen. Dadurch können die Geräte von Phishing-Angriffen, Drive-by-Exploits und anderen webbasierten Angriffsformen betroffen sein.

2.7 Missbrauch von Gesundheits-, Fitness- und Ortungsdaten

Das Betriebssystem vieler Smartphones und Tablets enthält meist spezielle Funktionen, um Gesundheits-, Fitness- und Ortungsdaten zu verwalten. Diese oft personenbezogenen Daten sind besonders schützenswert und stellen ein attraktives Angriffsziel dar, insbesondere wenn sie über einen längeren Zeitraum gesammelt und gespeichert werden. Voraussetzung ist, dass diese Funktionen durch den Benutzer aktiviert wurden.

So kann z. B. der Standort des Mitarbeiters durch einen Angriff auf das Gerät selbst oder auf damit verbundene Cloud-Dienste erkennbar sein. Das kann neben den datenschutzrechtlichen Auswirkungen unter Umständen auch zu weiteren Angriffen führen. So sind beispielsweise Einbrüche bei Mitarbeitern denkbar, die sich laut Standort auf Reisen befinden.

2.8 Missbrauch schutzbedürftiger Daten im Sperrbildschirm

Viele mobile Betriebssysteme verfügen über eine Funktion, die es ermöglicht, Mitteilungen von aktivierten Widgets und Push-Nachrichten auf dem Sperrbildschirm anzeigen zu lassen. Hierdurch können vertrauliche Informationen des Benutzers unberechtigten Dritten preisgegeben und durch diese ausgenutzt werden. Über Sprachassistenten besteht zudem oft auch im gesperrten Zustand die Möglichkeit, auf Telefonfunktionen und Kontaktdaten zuzugreifen. Auch dies kann dazu führen, dass unberechtigte Dritte an vertrauliche Informationen gelangen können.

2.9 Gefahren durch private Nutzung dienstlicher Smartphones und Tablets

Wenn Mitarbeitern firmeneigene Smartphones und Tablets ausgehändigt werden, könnten sie die Geräte auch unerlaubt privat benutzen. Dadurch entstehen gleich mehrere Probleme für die Informationssicherheit der Institution. So könnte ein Benutzer etwa selbstständig Apps installieren, die Schadfunktionen enthalten, oder er besucht eine Webseite, die das Gerät mit Malware infiziert. Ebenso sind viele vom Benutzer privat installierte Apps ein Risiko für die auf dem Gerät gespeicherten Informationen der Institution, da sie z. B. Adressbücher zu unbekanntem Servern übertragen oder direkt auf E-Mails oder Dokumente zugreifen. So können Daten abfließen oder umgekehrt unkontrolliert in die Institution gelangen. Typische Beispiele für Apps mit solchen Risiken sind Social-Media- und Instant-Messaging-Apps.

2.10 Gefahren durch Bring Your Own Device (BYOD)

Werden private Endgeräte dienstlich genutzt, ergeben sich dadurch verschiedene Gefährdungspotentiale. Beispielsweise kann es bezüglich der Software-Lizenzen zu rechtlichen Problemen kommen. Wenn im Notfall dienstliche Daten durch das MDM auf dem Gerät gelöscht werden müssen, kann dies auch Auswirkungen auf die privaten Daten des Benutzers haben.

Zudem können die IT-Verantwortlichen nicht jedes einzelne private Gerät daraufhin prüfen, ob es den dienstlichen Anforderungen genügt. Dadurch können ungeeignete Geräte verwendet werden, mit denen die Benutzer gegen Datenschutz- und Sicherheitsanforderungen verstoßen. Zudem sind die Benutzer oft selbst dafür verantwortlich, ihre Geräte zu warten und reparieren zu lassen. Bei einer solchen Reparatur könnten beispielsweise Firmendaten unbefugt eingesehen werden. Die gleiche Gefahr besteht, falls nicht geregelt ist, was mit den Daten auf dem Gerät geschehen soll, wenn der Mitarbeiter aus der Institution ausscheidet.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.3.2.1 *Allgemeine Smartphones und Tablets* 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.

Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche, Benutzer

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* vorrangig umgesetzt werden:

SYS.3.2.1.A1 Festlegung einer Richtlinie für den Einsatz von Smartphones und Tablets (B)

Bevor eine Institution Smartphones oder Tablets bereitstellt, betreibt oder einsetzt, MUSS eine generelle Richtlinie im Hinblick auf die Nutzung und Kontrolle der Geräte festgelegt werden. Hierbei MUSS unter anderem festgelegt werden, wer auf welche Informationen der Institution zugreifen darf.

SYS.3.2.1.A2 Festlegung einer Strategie für die Cloud-Nutzung (B)

Die Institution MUSS im Zusammenhang mit Smartphones und Tablets eine generelle Strategie für die damit verbundene Cloud-Nutzung sowie für den Schutz und die Kontrolle der Informationen festlegen. Die erlaubte Nutzung von Cloud-Diensten für Informationen der Institution MUSS geklärt und festgelegt werden. Die Benutzer MÜSSEN regelmäßig bezüglich der Nutzung solcher Cloud-Dienste geschult werden.

SYS.3.2.1.A3 Sichere Grundkonfiguration für mobile Geräte (B)

Alle mobilen Endgeräte MÜSSEN so konfiguriert sein, dass sie das erforderliche Schutzniveau angemessen erfüllen. Dafür MUSS eine passende Grundkonfiguration der Sicherheitsmechanismen und -einstellungen zusammengestellt und dokumentiert werden. Nicht benötigte Funktionen SOLLTEN deaktiviert werden. Die Freischaltung von Kommunikationsschnittstellen MUSS geregelt und auf das dienstlich notwendige Maß reduziert werden. Nicht benutzte Schnittstellen SOLLTEN deaktiviert werden. Wenn eine Institution ein MDM einsetzt, MUSS bei der Übergabe des mobilen Endgerätes bereits der MDM-Client installiert sein.

SYS.3.2.1.A4 Verwendung eines Zugriffsschutzes [Benutzer] (B)

Smartphones und Tablets MÜSSEN mit einem angemessen komplexen Gerätesperrcode geschützt werden. Die Nutzung der Bildschirmsperre MUSS vorgeschrieben werden. Die Anzeige von vertraulichen Informationen auf dem Sperrbildschirm MUSS deaktiviert sein. Alle mobilen Geräte MÜSSEN nach einer angemessen kurzen Zeitspanne selbsttätig die Bildschirmsperre aktivieren. Diese Zeitspanne MUSS in Abhängigkeit zum angestrebten Schutzniveau stehen.

Nach mehreren fehlgeschlagenen Versuchen, den Bildschirm zu entsperren, SOLLTE sich das mobile Gerät in den Werkzustand zurücksetzen. Es SOLLTEN dabei die Daten oder die Verschlüsselungsschlüssel sicher vernichtet werden. Es SOLLTE vermieden werden, dass die Benutzer bei einem Passwortwechsel Kennworte nutzen, die erst vor Kurzem verwendet wurden. Die Anzahl der Kennworte, nach der sich ein Passwort wiederholen darf, SOLLTE festgelegt werden.

SYS.3.2.1.A5 Updates von Betriebssystem und Apps (B)

Es MUSS ein Prozess für Updates des Betriebssystems und der eingesetzten Apps etabliert werden. Die Aktualisierungen MÜSSEN getestet werden. Dabei SOLLTEN insbesondere bisher benötigte Funktionen, Sicherheitsmechanismen und die Durchsetzung von Compliance-Anforderungen geprüft werden. Nach der Freigabe MÜSSEN die Aktualisierungen zeitnah ausgerollt werden. Bereits bei der Auswahl von zu beschaffenden mobilen Geräten MUSS die Institution darauf achten, dass der Hersteller über den geplanten Nutzungszeitraum Sicherheitsaktualisierungen für die Geräte bereitstellt. Ältere Geräte, für die keine Aktualisierungen mehr bereitgestellt werden, MÜSSEN

ausgesondert und durch vom Hersteller unterstützte Geräte ersetzt werden. Apps SOLLTEN unter Berücksichtigung von Sicherheitsaspekten ebenfalls NICHT mehr eingesetzt werden, wenn sie nicht mehr durch den Hersteller unterstützt werden.

SYS.3.2.1.A6 Datenschutzzeinstellungen (B)

Der Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen MUSS angemessen eingeschränkt werden. Die Datenschutzeinstellungen MÜSSEN so restriktiv wie möglich konfiguriert werden. Insbesondere der Zugriff auf Kamera, Mikrophon sowie Ortungs- und Gesundheits- bzw. Fitnessdaten MUSS auf Konformität mit den organisationsinternen Datenschutz- und Sicherheitsvorgaben überprüft und restriktiv konfiguriert bzw. deaktiviert werden.

SYS.3.2.1.A7 Verhaltensregeln bei Sicherheitsvorfällen [Fachverantwortliche, Benutzer] (B)

Generell MÜSSEN alle Sicherheitsvorfälle gemeldet und behandelt werden. Gehen Geräte verloren oder werden unberechtigte Änderungen an Gerät und Software festgestellt, MÜSSEN die Verantwortlichen sofort geeignete Gegenmaßnahmen einleiten.

Die möglichen Konsequenzen sicherheitskritischer Ereignisse MÜSSEN untersucht werden. Letztlich MÜSSEN alle erforderlichen Maßnahmen ergriffen werden, um auszuschließen, dass auf vertrauliche und geschäftskritische Informationen der Institution zugegriffen werden kann.

SYS.3.2.1.A8 Keine Installation von Apps aus unsicheren Quellen (B)

Es MUSS unterbunden werden, dass sich Apps aus alternativen Märkten oder aus dem Dateisystem installieren lassen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets*. Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.3.2.1.A9 Restriktive Nutzung von funktionalen Erweiterungen (S)

Funktionale Erweiterungen SOLLTEN nur restriktiv genutzt werden. Wenn möglich, SOLLTE auf funktionale Erweiterungen verzichtet werden. Die funktionalen Erweiterungen SOLLTEN keinen automatischen Zugriff auf schützenswerte Informationen haben. Sie SOLLTEN die festgelegte Grundkonfiguration nicht umgehen oder ändern können.

SYS.3.2.1.A10 Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten [Benutzer] (S)

Es SOLLTE eine verbindliche Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten erstellt werden. Diese SOLLTE festlegen, wie mobile Geräte genutzt und gepflegt werden sollen. Darin SOLLTEN die Themen Aufbewahrung und Verlustmeldung behandelt werden. Außerdem SOLLTE verboten werden, Verwaltungssoftware zu deinstallieren oder das Gerät zu rooten.

SYS.3.2.1.A11 Verschlüsselung des Speichers (S)

Der nichtflüchtige Speicher des mobilen Geräts SOLLTE verschlüsselt werden. Schützenswerte Daten auf zusätzlich verwendeten Speichermedien wie SD-Karten SOLLTEN verschlüsselt werden.

SYS.3.2.1.A12 Verwendung nicht personalisierter Gerätenamen (S)

Der Gerätenamen SOLLTE keine Hinweise auf die Institution oder den Benutzer enthalten.

SYS.3.2.1.A13 Regelungen zum Screensharing und Casting (S)

Es SOLLTE entschieden werden, ob Funktionen zur Übertragung von Bildschirmhalten, Audio oder Video (Screensharing oder Casting) eingesetzt werden sollen. Die Funktionen SOLLTEN organisatorisch oder technisch geregelt werden. Hierzu SOLLTE eine entsprechende Vereinbarung mit den Benutzern getroffen werden.

SYS.3.2.1.A14 Schutz vor Phishing und Schadprogrammen im Browser (S)

Alle mobilen Endgeräte SOLLTEN vor Schadprogrammen geschützt werden. Im verwendeten Browser SOLLTE die Funktion „Safe Browsing“ bzw. die Funktion zur Warnung vor schädlichen Inhalten aktiviert werden.

SYS.3.2.1.A15 Deaktivierung von Download-Boostern (S)

Download-Booster, die Daten über die Server des Herstellers leiten, SOLLTEN deaktiviert werden.

SYS.3.2.1.A16 Deaktivierung nicht benutzter Kommunikationsschnittstellen [Benutzer] (S)

Kommunikationsschnittstellen SOLLTEN nur bei Bedarf und nur in geeigneten Umgebungen aktiviert werden. Wird ein MDM verwendet, SOLLTEN die Schnittstellen zentral über das MDM verwaltet werden.

SYS.3.2.1.A17 Verwendung der SIM-Karten-PIN (S)

Die Nutzung der SIM-Karte der Institution SOLLTE durch eine PIN geschützt werden. Die Super-PIN/PUK SOLLTE nur im Rahmen der definierten Prozesse von den Verantwortlichen benutzt werden.

SYS.3.2.1.A18 Verwendung biometrischer Authentisierung (S)

Wenn biometrische Verfahren zur Authentisierung (z. B. ein Fingerabdrucksensor) genutzt werden sollen, SOLLTE geprüft werden, ob dadurch ein ähnlich hoher oder höherer Schutz im Vergleich zu einem Gerätepasswort erzielt werden kann. Im Zweifelsfall oder bei einem schlechteren Schutz SOLLTEN biometrische Verfahren NICHT genutzt werden. Die Benutzer SOLLTEN für die Fälschbarkeit von biometrischen Merkmalen sensibilisiert werden.

SYS.3.2.1.A19 Verwendung von Sprachassistenten (S)

Sprachassistenten SOLLTEN nur eingesetzt werden, wenn sie zwingend notwendig sind. Andernfalls SOLLTEN sie deaktiviert werden. Generell SOLLTE ein Sprachassistent nicht genutzt werden können, wenn das Gerät gesperrt ist.

SYS.3.2.1.A20 Auswahl und Freigabe von Apps (S)

Apps aus öffentlichen App-Stores SOLLTEN durch die Verantwortlichen geprüft und freigegeben werden. Dazu SOLLTE ein Freigabeprozess entwickelt werden, in dem auch geeignete Bewertungskriterien definiert sind. Alle freigegebenen Apps SOLLTEN intern in einem Standardkatalog veröffentlicht werden.

SYS.3.2.1.A21 Definition der erlaubten Informationen und Applikationen auf mobilen Geräten [Fachverantwortliche, Benutzer] (S)

Die Institution SOLLTE festlegen, welche Informationen auf den mobilen Endgeräten verarbeitet werden dürfen. Grundlage für die Regelung SOLLTEN einerseits die Klassifikation der Institutionsdaten sein und andererseits die Bedingungen, unter denen die Daten auf den Geräten verarbeitet werden.

Die Benutzer der mobilen Endgeräte SOLLTEN nur freigegebene und geprüfte Apps aus als sicher klassifizierten Quellen installieren dürfen.

SYS.3.2.1.A22 Einbindung mobiler Geräte in die interne Infrastruktur via VPN (S)

Mobile Endgeräte SOLLTEN nur mittels eines VPN in die Infrastruktur der Institution integriert werden. Hierzu SOLLTE ein geeignetes Verfahren ausgewählt und eingesetzt werden. Die Authentisierung SOLLTE bevorzugt durch Zertifikate statt durch den Einsatz klassischer Passwörter implementiert und betrieben werden.

SYS.3.2.1.A28 Verwendung der Filteroption für Webseiten (S)

Wird in der Institution bereits ein Reputationsdienst oder ein entsprechender Proxy-Server verwendet, SOLLTE dieser als globaler HTTP-Proxy für alle installierten Browser hinterlegt werden. Ist der Proxy nur im internen Netz erreichbar, SOLLTEN die Endgeräte über eine VPN-Verbindung wahlweise

permanent oder basierend auf den verwendeten Apps geeignet eingebunden werden.

Sind die mobilen Endgeräte nicht in eine vorhandene Proxy- oder Reputations-Infrastruktur der Institution eingebunden, SOLLTEN für Web-Browser Filteroptionen auf Basis von Whitelists oder Blacklists oder Inhaltsfilter Dritter verwendet werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* 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. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.3.2.1.A23 Zusätzliche Authentisierung für vertrauliche Anwendungen (H)

Alle Anwendungen mit vertraulichen Daten SOLLTEN durch einen zusätzlichen Mechanismus zur Authentisierung geschützt werden.

SYS.3.2.1.A24 Einsatz einer geschlossenen Benutzergruppe (H)

Das Passwort für den Zugangspunkt (Access Point Name, APN) einer geschlossenen Benutzergruppe SOLLTE komplex sein. Die Authentisierung SOLLTE das CHAP-Protokoll nutzen.

SYS.3.2.1.A25 Nutzung von getrennten Arbeitsumgebungen (H)

Ist es den Mitarbeitern erlaubt, dienstliche Geräte auch privat zu nutzen, SOLLTEN Lösungen für getrennte Arbeitsumgebungen auf dem Endgerät eingesetzt werden. Wenn möglich, SOLLTEN dafür nur zertifizierte Produkte (z. B. nach Common Criteria) beschafft werden. Dienstliche Daten SOLLTEN ausschließlich in der dienstlichen Umgebung verbleiben.

SYS.3.2.1.A26 Nutzung von PIM-Containern (H)

Informationen auf den mobilen Endgeräten SOLLTEN gekapselt werden, zum Beispiel in einem PIM-Container. Zusätzlich SOLLTEN die Daten durch eine separate Authentisierung und eine vom Betriebssystem unabhängige Daten- und Transportverschlüsselung abgesichert werden.

SYS.3.2.1.A27 Einsatz besonders abgesicherter Endgeräte (H)

Institutionen SOLLTEN abhängig vom Schutzbedarf besonders abgesicherte mobile Endgeräte einsetzen, die für die Verarbeitung von Informationen nach gesetzlichen Informationsschutz-Klassifizierungen zertifiziert sind.

SYS.3.2.1.A29 Verwendung eines institutionsbezogenen APN (H)

Es SOLLTE geprüft werden, ob ein institutionsbezogener Zugangspunkt zum Mobilfunknetz (APN, Access Point Name) zur Eingrenzung des erlaubten Geräte-Pools verwendet werden kann. Alle Geräte, die diesen APN verwenden, erhalten vom Mobilfunk-Provider einen mit der Institution abgestimmten IP-Adressbereich. Für die Authentisierung SOLLTE ein komplexes Passwort mit maximal 64 Stellen mit dem Mobilfunk-Provider vereinbart werden. Beim Einsatz eines institutionsbezogenen APN SOLLTE die Authentisierung auf Basis des Protokolls CHAP realisiert werden.

SYS.3.2.1.A30 Einschränkung der App-Installation mittels Whitelist (H)

Bei erhöhtem Schutzbedarf SOLLTEN die Benutzer der mobilen Endgeräte nur freigegebene und geprüfte Apps installieren dürfen. Wird ein MDM eingesetzt, SOLLTE es verhindern, dass andere Apps installiert werden oder alternativ unbefugt installierte Apps sofort wieder entfernen.

4 Weiterführende Informationen

4.1 Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013, insbesondere in Annex A, A.6.2 „Mobile devices and teleworking“, Vorgaben für den Einsatz von mobilen Endgeräten.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“, insbesondere in Area PA2 Mobile Computing, Vorgaben für den Einsatz von mobilen Endgeräten.

Das National Institute of Standards and Technology (NIST) stellt folgende Dokumente im Bereich mobile Endgeräte bereit:

- „Guidelines for Managing the Security of Mobile Devices in the Enterprise: NIST Special Publication 800-124“, Revision 1, Juni 2013
- „Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53“, Revision 4, April 2013
- „Securing Electronic Health Record on Mobile Devices: NIST Special Publication 1800-1d“, Draft, Juli 2015

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.3.2.1 *Allgemeine Smartphones und Tablets* von Bedeutung.

G 0.14	Ausspähen von Informationen (Spionage)
G 0.15	Abhören
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten
G 0.17	Verlust von Geräten, Datenträgern oder Dokumenten
G 0.18	Fehlplanung oder fehlende Anpassung
G 0.19	Offenlegung schützenswerter Informationen
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle
G 0.21	Manipulation von Hard- oder Software
G 0.22	Manipulation von Informationen
G 0.23	Unbefugtes Eindringen in IT-Systeme
G 0.24	Zerstörung von Geräten oder Datenträgern
G 0.25	Ausfall von Geräten oder Systemen
G 0.26	Fehlfunktion von Geräten oder Systemen
G 0.28	Software-Schwachstellen oder -Fehler

- G 0.29 Verstoß gegen Gesetze oder Regelungen
- G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
- G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen
- G 0.32 Missbrauch von Berechtigungen
- G 0.36 Identitätsdiebstahl
- G 0.37 Abstreiten von Handlungen
- G 0.38 Missbrauch personenbezogener Daten
- G 0.39 Schadprogramme
- G 0.42 Social Engineering
- G 0.43 Einspielen von Nachrichten
- G 0.45 Datenverlust
- G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen	CIA	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G						
		0.15	0.16	0.17	0.18	0.19	0.20	0.21	0.22	0.23	0.24	0.25	0.26	0.28	0.29	0.30	0.31	0.32	0.33	0.34	0.35	0.36	0.37	0.38	0.39	0.40	0.41	0.42	0.43	0.44	0.45
SYS.3.2.1.A1		X			X	X						X	X			X	X												X	X	
SYS.3.2.1.A2					X	X			X	X	X					X	X	X	X	X	X		X					X	X	X	
SYS.3.2.1.A3		X	X	X		X		X	X	X	X					X	X					X	X				X	X	X	X	
SYS.3.2.1.A4			X	X		X				X	X					X	X	X	X	X	X		X				X		X	X	
SYS.3.2.1.A5		X	X	X		X	X	X	X	X	X	X		X								X					X		X	X	
SYS.3.2.1.A6		X				X			X	X	X											X	X				X	X	X	X	
SYS.3.2.1.A7		X	X	X	X				X																			X	X	X	
SYS.3.2.1.A8																						X									
SYS.3.2.1.A9		X				X			X	X	X		X																X	X	
SYS.3.2.1.A10			X													X															
SYS.3.2.1.A11		X						X								X														X	
SYS.3.2.1.A12																														X	
SYS.3.2.1.A13													X																	X	
SYS.3.2.1.A14					X		X	X		X						X						X									
SYS.3.2.1.A15						X			X							X														X	
SYS.3.2.1.A16		X				X				X						X	X														
SYS.3.2.1.A17			X	X												X															
SYS.3.2.1.A18			X	X	X	X				X						X				X										X	
SYS.3.2.1.A19			X	X		X										X	X	X	X	X	X	X								X	
SYS.3.2.1.A20		X				X		X	X	X	X					X	X	X	X	X	X		X				X		X	X	
SYS.3.2.1.A21		X				X	X	X	X	X	X	X		X									X				X		X	X	X
SYS.3.2.1.A22		X	X	X		X			X																				X	X	

SYS.3.2.1.A23	CI	X			X		X	X	X									X	X	X	X
SYS.3.2.1.A24	CI																				X
SYS.3.2.1.A25	CI	X	X	X	X		X	X	X	X								X	X	X	X
SYS.3.2.1.A26	CIA	X	X	X	X			X	X	X								X	X	X	X
SYS.3.2.1.A27	CIA	X	X	X	X		X	X	X	X			X	X				X	X	X	X
SYS.3.2.1.A28																					
SYS.3.2.1.A29	CA																X	X			
SYS.3.2.1.A30	CIA		X		X		X	X			X	X		X		X					