



SYS.3.2.1 Allgemeine Smartphones und Tablets

1. Beschreibung

1.1. Einleitung

Smartphones sind auf den mobilen Einsatz ausgerichtete IT-Systeme mit einer angepassten Oberfläche, die mit einem großen, üblicherweise berührungsempfindlichen Bildschirm (Touch-Display) bedient werden können. Smartphones vereinen neben der Telefonie beispielsweise Media-Player, Personal Information Manager und Digitalkamera in einem Gerät und bieten den Benutzenden darüber hinaus viele weitere Anwendungen und Funktionen, wie Webbrowser, E-Mail-Client oder Ortung (z. B. über GPS). Zudem sind sie mit Mobilfunk-, WLAN-, Bluetooth- sowie NFC-Schnittstellen ausgestattet. Tablets sind, vereinfacht gesagt, Smartphones mit großem Formfaktor, mit denen in der Regel nicht über das Mobilfunknetz telefoniert werden kann.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, den Zuständigen 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 Zuständigen Ansätze aufgezeigt werden, um schutzbedarfsgerechte Konfigurationsprofile zu erstellen. Diese Konfigurationsprofile können über eine zentrale Infrastruktur mit einem Mobile Device Management (MDM) verteilt und verwaltet werden. Es kann jedoch bei der Vielzahl von unterschiedlichen mobilen Betriebssystemen nicht grundsätzlich vorausgesetzt werden, dass die Geräte in ein solches MDM eingebunden werden können.

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.

Smartphones sind, so wie gewöhnliche Clients, durch Schadprogramme gefährdet. Sie müssen im Konzept zum Schutz vor Schadsoftware berücksichtigt werden. Anforderungen zum Schutz vor Schadprogrammen finden sich im Baustein OPS.1.1.4 *Schutz vor Schadprogrammen*.

Smartphones und Tablets bieten in der Regel die Möglichkeit, mobile Anwendungen (Apps) zu installieren. Damit dabei keine unnötigen Sicherheitsrisiken entstehen, sind die Anforderungen des Bausteins APP.1.4 *Mobile Anwendungen (Apps)* zu berücksichtigen. Darüber hinaus können aus der Schicht APP *Anwendungen* auch andere Bausteine, wie APP.1.2 *Webbrowser*, relevant sein.

Da Smartphones in der Regel über Mobilfunkfunktionen verfügen, sind die relevanten Anforderungen des Bausteins SYS.3.3 *Mobiltelefon* zu berücksichtigen.

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.3.2.1 *Allgemeine Smartphones und Tablets* von besonderer Bedeutung.

2.1. Fehlende Betriebssystem-Updates

Es erscheinen regelmäßig neue Versionen und Updates von mobilen Betriebssystemen. Diese müssen bei Geräten, die spezifische Erweiterungen des Betriebssystems der herstellenden Institution haben, erst von diesen 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 bei einem Angriff besonders leicht ausgenutzt werden.

2.2. Software-Schwachstellen in vorinstallierten 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 Drittentwickelnden nach einiger Zeit nicht mehr weiter gepflegt. Folglich können erkannte Sicherheitsmängel dann nicht mehr durch entsprechende Updates behoben werden.

2.3. Manipulation von Smartphones und Tablets

Bei einem Angriff kann sich Zugang zu Smartphones oder Tablets verschafft werden, um gezielt Daten zu manipulieren. So könnte beispielsweise die Konfiguration geändert, zusätzliche Dienste gestartet oder Schadsoftware installiert werden. Dadurch kann auf dem manipulierten System beispielsweise die Kommunikationsverbindungen mitgeschnitten (ungewollter Datenabfluss) oder Sicherheitseinstellungen verändert werden (z. B. Zugriffe aus dem Internet auf das Endgerät erlauben).

2.4. 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 Angreifende immer mehr auf mobile Geräte. Insbesondere wenn Apps aus nicht vertrauenswürdigen Quellen bezogen werden oder keine Updates für bekannte Schwachstellen verfügbar sind, besteht die Gefahr einer Infektion. Wird ein Gerät infiziert, können beispielsweise Daten ausgelesen, verändert, gelöscht oder auf interne IT-Ressourcen der Institution zugegriffen oder im Namen der Institution agiert werden.

2.5. 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.

2.6. Missbrauch von Gesundheits-, Fitness- und Ortungsdaten

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

So kann z. B. der Standort des Gerätes 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 Mitarbeitenden denkbar, die sich laut Standort auf Reisen befinden.

2.7. 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 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.

Zudem besteht im gesperrten Zustand oft die Möglichkeit, Schnittstellen wie WLAN oder Bluetooth zu konfigurieren. So lässt sich beispielsweise ein zusätzlicher Angriffsvektor aktivieren, wenn die Bluetooth-Schnittstelle durch einen Angreifenden mit physischem Zugriff eingeschaltet wird.

2.8. Gefahren durch private Nutzung dienstlicher Smartphones und Tablets

Wenn Mitarbeitende firmeneigene Smartphones und Tablets privat benutzen, entstehen gleich mehrere Probleme für die Informationssicherheit der Institution. So könnten die Benutzenden etwa selbstständig Apps installieren, die Schadfunktionen enthalten, oder sie besuchen eine Webseite, die das Gerät mit Malware infiziert. Ebenso sind viele privat installierte Apps ein Risiko für die auf dem Gerät gespeicherten Informationen der Institution, da sie z. B. Adressbücher auslesen und zu unbekanntem Servern übertragen oder möglicherweise auf E-Mails oder Dokumente zugreifen können. So könnten Daten abfließen oder umgekehrt unkontrolliert in die Institution gelangen. Typische Beispiele für Apps mit solchen Risiken sind Social-Media- und Messenger-Apps.

2.9. Gefahren durch Bring Your Own Device (BYOD)

Werden private Endgeräte dienstlich genutzt, ergeben sich dadurch verschiedene Gefährdungspotentiale. Beispielsweise können bezüglich der Software-Lizenzen rechtliche Probleme

eintreten. Wenn im Notfall dienstliche Daten durch das MDM auf dem Gerät gelöscht werden müssen, kann dies auch Auswirkungen auf die privaten Daten auf dem Gerät haben.

Zudem können die IT-Zuständigen nicht jedes einzelne private Gerät daraufhin prüfen, ob es den dienstlichen Anforderungen genügt. Dadurch können Geräte verwendet werden, mit denen die Benutzenden gegen Datenschutz- und Sicherheitsanforderungen verstoßen. Zudem sind die Benutzenden oft selbst dafür zuständig, 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 Mitarbeitende aus der Institution ausscheiden.

2.10. Rechteerhöhung durch Schwachstellen

In Betriebssysteme von Smartphones und Tablets werden immer wieder Schwachstellen entdeckt, die es ermöglichen, das von den herstellenden Institutionen etablierte Sicherheitskonzepte zu umgehen und somit auf Systemprozesse und geschützte Speicherbereiche zuzugreifen. Dadurch können Programme nicht vorgesehene Berechtigungen erlangen, mit denen sie unerlaubte Aktionen ausführen können. Beispielsweise könnten die Programme so auf Daten des Betriebssystems und anderer Apps zugreifen.

Sogenannte Jailbreaks nutzen diese Schwachstellen aus, um beispielsweise alternative App-Stores oder sonstige Erweiterungen nutzen zu können. Jailbreak-Techniken können im Falle eines Angriffs dafür verwendet werden, um Schadprogramme zu installieren oder andere schädliche Manipulationen auf dem Gerät vorzunehmen.

Schadprogramme können auch Schwachstellen ausnutzen, um sich auf einem Gerät zu installieren oder es zu manipulieren. Hierdurch kann das Betriebssystem anders als vorgesehen genutzt und wichtige Sicherheitsfunktionen können übergangen werden.

Insbesondere betroffen sind Daten, die vom mobilen Betriebssystem in geschützten Bereichen gelagert werden, da eine App mit Superuser-Rechten diese unter Umständen auslesen kann.

Durch beabsichtigte Rechteerhöhung („Rooten“) können ähnliche Gefährdungsszenarien entstehen, wenn der Zugriff auf die privilegierten Rechte nicht geschützt wird.

3. Anforderungen

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

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.3.2.1.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 für die Nutzung und Kontrolle der Geräte festgelegt werden. Hierbei MUSS unter anderem festgelegt werden, wer mit Smartphones 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 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. Es MUSS festgelegt werden, ob und in welchem Umfang Cloud-Dienste bei privater Nutzung der Geräte erlaubt sind. Die Benutzenden MÜSSEN regelmäßig bezüglich der Nutzung solcher Cloud-Dienste sensibilisiert 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.

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

Smartphones und Tablets MÜSSEN mit einem angemessen komplexen Gerätesperrcode geschützt werden. Die Bildschirmsperre MUSS genutzt 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.

Bei jedem fehlgeschlagenen Versuch, das Gerät zu entsperren, SOLLTE sich die Wartezeit zu einem neuen Versuch verlängern. Die Anzahl der Gerätesperrcodes, nach der sich ein Code wiederholen darf, SOLLTE festgelegt werden. 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 Benutzenden bei einem Passwortwechsel Kennworte nutzen, die erst vor Kurzem verwendet wurden.

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

Bereits bei der Auswahl von zu beschaffenden mobilen Geräten MUSS die Institution darauf achten, dass die herstellende Institution angibt, über welchen geplanten Nutzungszeitraum Sicherheitsaktualisierungen für die Geräte bereitgestellt werden. Ältere Geräte, für die keine Aktualisierungen mehr bereitgestellt werden, MÜSSEN ausgesondert und durch von der herstellenden Institution unterstützte Geräte ersetzt werden. Apps SOLLTEN ebenfalls NICHT mehr eingesetzt werden, wenn sie nicht mehr durch die herstellende Institution unterstützt werden.

SYS.3.2.1.A6 Datenschutzeinstellungen und Berechtigungen (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, Mikrofon sowie Ortungs- und Gesundheits- bzw. Fitnessdaten MUSS auf Konformität mit den organisationsinternen Datenschutz- und Sicherheitsvorgaben überprüft werden. Der Zugriff MUSS restriktiv konfiguriert bzw. deaktiviert werden.

Sicherheitsrelevante Berechtigungseinstellungen MÜSSEN so festgelegt werden, dass sie nicht durch Benutzende oder Apps geändert werden können. Wo dies technisch nicht möglich ist, MÜSSEN die Berechtigungseinstellungen regelmäßig geprüft und erneut gesetzt werden. Dies gilt insbesondere auch nach der Installation von Updates.

SYS.3.2.1.A7 Verhaltensregeln bei Sicherheitsvorfällen (B) [Benutzende]

Gehen Geräte verloren oder werden unberechtigte Änderungen an Gerät und Software festgestellt, MÜSSEN die Benutzenden sofort die Zuständigen informieren.

SYS.3.2.1.A8 Installation von Apps (B)

Die Institution MUSS regeln, ob, wie und welche Apps Benutzende selbst auf ihren Geräten installieren dürfen. Sie SOLLTEN nur freigegebene Apps installieren dürfen. Die Institution MUSS festlegen, aus welchen Quellen Apps installiert werden dürfen. Es MUSS unterbunden werden, dass sich Apps aus nicht zugelassenen Quellen installieren lassen.

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.3.2.1.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 Mitarbeitende zur Benutzung von mobilen Geräten (S) [Benutzende]

Eine verbindliche Richtlinie für Mitarbeitende zur Benutzung von mobilen Geräten SOLLTE erstellt werden. Diese SOLLTE festlegen, wie mobile Geräte genutzt und gepflegt werden sollen. Die Themen Aufbewahrung und Verlustmeldung SOLLTEN darin behandelt werden. Außerdem SOLLTE verboten werden, Verwaltungssoftware zu deinstallieren, das Gerät zu rooten oder sicherheitsrelevante Konfigurationen zu ändern.

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 die Benutzenden enthalten.

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

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

SYS.3.2.1.A14 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.1.A15 ENTFALLEN (S)

Diese Anforderung ist entfallen.

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

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 ENTFALLEN (S)

Diese Anforderung ist entfallen.

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 Benutzenden 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 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.1.A21 ENTFALLEN (S)

Diese Anforderung ist entfallen.

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. Statt durch Passwörter SOLLTEN sich die Geräte über Zertifikate gegenüber der internen Infrastruktur authentisieren.

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 Webbrowser Filteroptionen auf Basis von Allowlists oder Blocklists oder Inhaltsfilter Dritter verwendet werden.

SYS.3.2.1.A31 Regelung zu Mobile Payment (S)

Es SOLLTE geregelt werden, ob Mobile Payment mit dienstlichen Smartphones und Tablets erlaubt wird.

SYS.3.2.1.A32 MDM Nutzung (S)

Smartphones und Tablets SOLLTEN durch ein MDM-System verwaltet werden.

SYS.3.2.1.A33 Auswahl und Installation von Sicherheits-Apps (S)

Alle mobilen Endgeräte SOLLTEN vor Schadprogrammen geschützt werden. Falls möglich, SOLLTEN für das Endgerät geeignete Sicherheits-Apps ausgewählt werden. Die Sicherheits-Apps SOLLTEN automatisch, zum Beispiel durch ein MDM, installiert werden.

SYS.3.2.1.A34 Konfiguration des verwendeten DNS-Servers (S)

Standard-Gateway-Einträge, wie beispielsweise DNS-Server der herstellenden oder entwickelnden Institutionen, SOLLTEN durch die des Providers oder durch eigene ersetzt werden.

Sollte der Provider sogenanntes DNS-over-HTTPS (DoH) anbieten, SOLLTE dieses verwendet werden. Bietet er es noch nicht an, SOLLTE es deaktiviert werden.

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.3.2.1.A23 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.3.2.1.A24 ENTFALLEN (H)

Diese Anforderung ist entfallen.

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

Ist es den Mitarbeitenden 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, SOLLTEN vom Mobilfunk-Provider einen mit der Institution abgestimmten IP-Adressbereich erhalten. 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 Allowlist (H)

Bei erhöhtem Schutzbedarf SOLLTEN auf den mobilen Endgeräten nur freigegebene und geprüfte Apps installiert werden dürfen. Wird ein MDM eingesetzt, SOLLTE es verhindern, dass andere Apps installiert werden oder alternativ unbefugt installierte Apps sofort wieder entfernen.

SYS.3.2.1.A35 Verwendung einer Firewall (H)

Auf Smartphones und Tablets SOLLTE eine Firewall installiert und aktiviert sein.

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