SYS.3: Mobile Devices

SYS.3.3: Mobiltelefon

1 Beschreibung

1.1 Einleitung

Die in diesem Baustein betrachteten Mobiltelefone, die auch „Feature-Phones“ oder „Dumbphones“ genannt werden, besitzen weniger Eigenschaften als ein Smartphone, bieten aber mehr Funktionen als nur die reine Telefonfunktion. So können diese Mobiltelefone zusätzlich mit einer Kamera für Videos und Fotos, einem Terminplaner, E-Mail-Programmen, Spielen, einem MP3-Player oder einem Radioempfänger ausgestattet sein. „Klassische“ Mobiltelefone verfügen in der Regel nicht über einen Touchscreen und ein Betriebssystem, auf das zusätzliche Apps installiert werden können. Diese fehlenden Funktionen unterscheidet das Mobiltelefon von einem Smartphone.

Mobiltelefone sind durch eine international eindeutige Seriennummer (International Mobile Equipment Identity, IMEI) gekennzeichnet. Die Identifizierung der Benutzer des Mobiltelefons erfolgt durch die SIM-Karte, die bei Vertragsabschluss vom Mobilfunkanbieter zugeteilt wird.

1.2 Zielsetzung

Ziel des Bausteins ist es, typische Gefährdungen aufzuzeigen, die bei der Nutzung von Mobiltelefonen auftreten können, sowie Informationen abzusichern, die auf Mobiltelefonen gespeichert sind oder darüber übermittelt werden.

1.3 Abgrenzung und Modellierung

Der Baustein SYS.3.3 *Mobiltelefon* ist auf alle Mobiltelefone anzuwenden, die für dienstliche Zwecke verwendet werden.

Dieser Baustein beschäftigt sich mit allgemeinen Aspekten von typischen Mobiltelefonen, mit Sicherheitsaspekten zur Telefonie und Nachrichtenübermittlung über das Mobilfunknetz und mit Sicherheitsaspekten zum Umgang mit den Geräten. Damit deckt dieser Baustein ein großes Spektrum unterschiedlicher Geräte ab, die an Mobilfunknetze angeschlossen werden können. Ergänzende Aspekte, die über die Kommunikation über ein Mobilfunknetz und den Umgang mit den Geräten hinausgehen, sind in weiteren Bausteinen des IT-Grundschutz-Kompendiums zu finden. So können Sicherheitsanforderungen zu Smartphones und den darauf genutzten Betriebssystemen ergänzend den Bausteinen der Schicht SYS.3.2 *Tablet und Smartphone* entnommen werden. Aspekte datenbasierter Telefonie werden im Baustein NET.4.2 *VoIP* behandelt. Verwendet das betrachtete Mobiltelefon VPNs, sollte zusätzlich der Baustein NET.3.3 *VPN* berücksichtigt werden. Für Smartphones oder Tablets ist der Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* anzuwenden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein SYS.3.3 *Mobiltelefon* von besonderer Bedeutung:

2.1 Unzureichende Planung bei der Anschaffung von Mobiltelefonen

Werden in der Planungsphase relevante Eigenschaften der anzuschaffenden Mobiltelefone nicht ermittelt, könnten dringend benötigte Funkionen nicht verfügbar sein. Werden bestimmte Mobilfunkstandards nicht unterstützt, können die Geräte in bestimmten Ländern nicht verwendet werden. Im schlimmsten Fall entspricht der Funktionsumfang nicht dem Einsatzzweck, sodass diese Geräte überhaupt nicht eingesetzt werden können. Oft gibt es auch weitere Randbedingungen, die erfüllt werden müssen, damit die Geräte eingesetzt werden können. Hierzu gehören beispielsweise Sicherheitsfunktionen, die oft nicht auf den ersten Blick ersichtlich sind, aber zu Problemen bezüglich der Verfügbarkeit und Vertraulichkeit führen können, wenn sie verwendet werden.

2.2 Verlust des Mobiltelefons

Da Mobiltelefone in der Regel klein sind und ständig transportiert werden, können sie leicht verloren gehen, vergessen oder gestohlen werden. Neben dem wirtschaftlichen Schaden wiegt der Verlust der Vertraulichkeit und Integrität der enthaltenen Daten besonders schwer. Denn über ein entwendetes Mobiltelefon könnte ein Angreifer auf institutionskritische Informationen der Institution zugreifen. Außerdem entstehen Kosten und Aufwände, um einen arbeitsfähigen Zustand wiederherzustellen.

2.3 Sorglosigkeit im Umgang mit Informationen bei der Mobiltelefonie

Durch Unachtsamkeit und Sorglosigkeit der Mitarbeiter bei der Mobiltelefonie können Dritte an schützenswerte Informationen gelangen. So können beispielsweise Informationen bei Telefongesprächen mitgehört oder aufgenommen sowie Nachrichten beim Verfassen mitgelesen werden.

2.4 Unerlaubte private Nutzung des dienstlichen Mobiltelefons

Firmeneigene Mobiltelefone können unerlaubt für private Zwecke verwendet werden. Durch Unachtsamkeit und sorglosen Umgang können so Probleme bezüglich der Informationssicherheit der Institution entstehen, etwa wenn private und dienstliche Inhalte vermischt werden. Auf diese Weise könnten Unbefugte Kenntnis von Interna der Institution erlangen. Werden dienstliche Mobiltelefone privat genutzt, können außerdem zusätzliche Kosten für die Institution entstehen.

2.5 Ausfall des Mobiltelefons

Der Ausfall eines Mobiltelefons kann mehrere Ursachen haben. So kann ein Benutzer versäumt haben, den Akku des Gerätes aufzuladen, oder der Akku kann seine Fähigkeit, Energie zu speichern, verloren haben. Auch ist es möglich, dass der Benutzer das Zugangspasswort oder die PIN vergessen hat und das Gerät nicht mehr nutzen kann. So kann sich das Gerät bei mehrfach falscher Eingabe des Zugangscodes selbst sperren. Wird mit dem Telefon nicht sorgfältig umgegangen, kann es beschädigt werden, beispielsweise indem es herunterfällt. In allen genannten Fällen ist der Benutzer anschließend nicht mehr erreichbar und kann wiederum selbst niemanden über das Mobiltelefon erreichen.

2.6 Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen

Aufgrund der Eigenschaften von mobiler Kommunikation kann nicht verhindert werden, dass die übertragenen Signale mit entsprechendem Aufwand unbefugt mitgehört und aufgezeichnet werden. Bei den meisten Funkdiensten müssen außerdem die mobilen Kommunikationspartner aus technischen Gründen geortet werden, um erreichbar zu sein. Somit können Standort-Informationen durch den Netzbetreiber oder Dienstbetreiber verwendet werden, um Bewegungsprofile zu erstellen.

2.7 Abhören von Raumgesprächen über Mobiltelefone

Mobiltelefone können dazu verwendet werden, unbemerkt Gespräche aufzuzeichnen oder abzuhören. In Besprechungen können über mitgebrachte Mobiltelefone Verbindungen zu unbefugten Mithörern aufgebaut werden. Viele Mobiltelefone sind mit einer Freisprecheinrichtung ausgestattet, sodass diese problemlos Gespräche im gesamten Raum erfassen können. Bei vielen Geräten ist nicht sichtbar, ob sie eingeschaltet sind oder nicht. Somit kann nicht direkt erkannt werden, ob Gespräche aufgezeichnet oder abgehört werden.

2.8 Einsatz veralteter Mobiltelefone

Da Smartphones vielfältiger als Mobiltelefone genutzt werden können, bieten viele Hersteller inzwischen ausschließlich Smartphones an. Damit übersteigt das Angebot an Smartphones deutlich das Angebot an Mobiltelefonen und es werden kaum noch Mobiltelefone produziert. Aufgrund des geringen Angebots werden zahlreiche Mobiltelefone aus Altbeständen verwendet. Altersschwache Komponenten wie Akkus werden oft durch Nachbauten von Drittherstellern ersetzt, sodass diese Mobiltelefone weiterhin Jahrzehnte nach der Produktion eingesetzt werden können.

Oft sind auf diesen veralteten Mobiltelefonen Betriebssysteme installiert, die nicht mehr weiterentwickelt werden. Softwareschwachstellen können somit nicht mehr durch Updates beseitigt werden. Häufig gibt es den Hersteller der Mobiltelefone nicht mehr, oder er hat sein Geschäftsfeld auf andere Märkte verlagert. Originales Zubehör und Ersatzteile können deshalb oft nicht mehr nachgekauft werden. Auch Dritthersteller bieten bei sehr alten Mobiltelefonen oft keine entsprechenden Produkte mehr an. Wenn Dritthersteller dennoch Ersatzteile anbieten, ist nicht gewährleistet, dass diese Komponenten die gleiche Qualität wie die originalen Teile besitzen. So sind beispielsweise nachgebaute Akkus oft weniger leistungsfähig als die Originale. In der Regel können diese Geräte auch oft nicht mehr repariert werden und bei Problemen gibt es kaum noch geeignete Ansprechpartner, die helfen können.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.3.3 *Mobiltelefon* 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	Benutzer

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein SYS.3.3 *Mobiltelefon* vorrangig erfüllt werden:

SYS.3.3.A1 Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung (B)

Im Hinblick auf die Nutzung und Kontrolle der Geräte MUSS eine Sicherheitsrichtlinie erstellt werden. Jedem Benutzer eines Mobiltelefons MUSS ein Exemplar der Sicherheitsrichtlinie ausgehändigt werden. Es MUSS regelmäßig überprüft werden, ob die Sicherheitsrichtlinie eingehalten wird. Die Sicherheitsleitlinie zur dienstlichen Nutzung von Mobiltelefonen SOLLTE Bestandteil der Schulung zu Sicherheitsmaßnahmen sein.

SYS.3.3.A2 Sperrmaßnahmen bei Verlust eines Mobiltelefons [Benutzer] (B)

Bei Verlust eines Mobiltelefons MUSS die darin verwendete SIM-Karte zeitnah gesperrt werden. Falls möglich, SOLLTEN vorhandene Mechanismen zum Diebstahlschutz, wie Fernlöschung oder -sperrung, genutzt werden. Alle notwendigen Informationen zur Sperrung von SIM-Karte und Mobiltelefon MÜSSEN unmittelbar griffbereit sein.

SYS.3.3.A3 Sensibilisierung und Schulung der Mitarbeiter im Umgang mit Mobiltelefonen (B)

Mitarbeiter MÜSSEN für die besonderen Gefährdungen der Informationssicherheit durch Mobiltelefone sensibilisiert werden. Sie MÜSSEN in die Sicherheitsfunktion der Mobiltelefone eingewiesen sein. Den Benutzern MUSS der Prozess bekannt sein, durch den die Mobiltelefone gesperrt werden können. Die Benutzer MÜSSEN darauf hingewiesen werden, wie die Mobiltelefone sicher und korrekt aufbewahrt werden sollten.

SYS.3.3.A4 Aussonderung und ordnungsgemäße Entsorgung von Mobiltelefonen und darin verwendeter Speicherkarten (B)

Mobiltelefone MÜSSEN vor der Entsorgung auf den Werkszustand zurückgesetzt werden. Es MUSS überprüft werden, ob alle Daten gelöscht wurden. Es SOLLTE zudem sichergestellt werden, dass die Mobiltelefone und eventuell darin verwendete Speicherkarten ordnungsgemäß entsorgt werden. Falls die Mobiltelefone und Speicherkarten erst zu einem späteren Zeitpunkt beziehungsweise in größerer Anzahl entsorgt werden, MÜSSEN die gesammelten Mobiltelefone und Speicherkarten vor unberechtigtem Zugriff geschützt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein SYS.3.3 *Mobiltelefon*. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.3.3.A5 Nutzung der Sicherheitsmechanismen von Mobiltelefonen [Benutzer] (S)

Die verfügbaren Sicherheitsmechanismen SOLLTEN auf den Mobiltelefonen genutzt und vorkonfiguriert werden. Die SIM-Karte SOLLTE durch eine sichere PIN geschützt werden. Die Super-PIN/PUK SOLLTE nur im Rahmen der definierten Prozesse von den Zuständigen benutzt werden. Das Mobiltelefon SOLLTE durch einen Geräte-Code geschützt werden. Falls möglich, SOLLTE das Gerät an die SIM-Karte gebunden werden (SIM-Lock).

SYS.3.3.A6 Updates von Mobiltelefonen [Benutzer] (S)

Es SOLLTE regelmäßig geprüft werden, ob es Softwareupdates für die Mobiltelefone gibt. Der Umgang mit Updates SOLLTE geregelt werden. Wenn es neue Softwareupdates gibt, SOLLTE festgelegt werden, wie die Benutzer darüber informiert werden. Es SOLLTE festgelegt werden, ob die Benutzer die Updates selber installieren dürfen, oder ob die Mobiltelefone an einer zentralen Stelle hierfür abgegeben werden sollen.

SYS.3.3.A7 Beschaffung von Mobiltelefonen (S)

Bevor Mobiltelefone beschafft werden, SOLLTE eine Anforderungsliste erstellt werden. Anhand der Anforderungsliste SOLLTEN die am Markt erhältlichen Produkte bewertet werden. Das Produkt SOLLTE danach ausgewählt werden, ob die Hersteller für den geplanten Einsatzzeitraum Updates anbieten. Es SOLLTE gewährleistet werden, dass Ersatzteile wie Akkus und Ladegeräte in ausreichender Qualität nachbeschafft werden können.

SYS.3.3.A8 Nutzung drahtloser Schnittstellen von Mobiltelefonen [Benutzer] (S)

Drahtlose Schnittstellen von Mobiltelefonen wie IrDA, WLAN oder Bluetooth SOLLTEN deaktiviert werden, solange sie nicht benötigt werden.

SYS.3.3.A10 Sichere Datenübertragung über Mobiltelefone [Benutzer] (S)

Es SOLLTE geregelt sein, welche Daten über Mobiltelefone übertragen werden dürfen. Die dafür erlaubten Schnittstellen SOLLTEN festgelegt werden. Außerdem SOLLTE beschlossen werden, wie die

Daten bei Bedarf zu verschlüsseln sind.

SYS.3.3.A11 Ausfallvorsorge bei Mobiltelefonen [Benutzer] (S)

Die auf einem Mobiltelefon gespeicherten Daten SOLLTEN in regelmäßigen Abständen auf einem externen Medium gesichert werden. Muss ein defektes Mobiltelefon repariert werden, SOLLTEN zuvor alle Daten gelöscht und das Gerät auf den Werkszustand zurückgesetzt werden. Es SOLLTEN immer Ersatzgeräte vorhanden sein, um ein ausgefallenes Mobiltelefon kurzfristig ersetzen zu können.

SYS.3.3.A12 Einrichtung eines Mobiltelefon-Pools (S)

Bei häufig wechselnden Benutzern dienstlicher Mobiltelefone SOLLTE eine Sammelaufbewahrung (Pool) eingerichtet werden. Die Ausgabe und Rücknahme von Mobiltelefonen und Zubehör SOLLTE dokumentiert werden. Vor der Ausgabe SOLLTE sichergestellt werden, dass die Mobiltelefone aufgeladen und mit den nötigen Programmen und Daten für den neuen Besitzer ausgestattet sind. Zudem SOLLTEN die Benutzer auf die Einhaltung der Sicherheitsleitlinie hingewiesen werden. Nachdem die Geräte wieder zurückgegeben wurden, SOLLTEN sie auf den Werkszustand zurückgesetzt werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein SYS.3.3 *Mobiltelefon* 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.3.3.A9 Sicherstellung der Energieversorgung von Mobiltelefonen [Benutzer] (H)

Es SOLLTEN angemessene Maßnahmen getroffen werden, um die dauerhafte Energieversorgung von Mobiltelefonen sicherzustellen. Je nach Bedarf SOLLTEN Wechselakkus oder Powerbanks eingesetzt werden.

SYS.3.3.A13 Schutz vor der Erstellung von Bewegungsprofilen bei der Mobilfunk-Nutzung [Benutzer] (H)

Es SOLLTE geklärt werden, ob sich die Erstellung von Bewegungsprofilen durch Dritte negativ auswirken kann oder als Problem angesehen wird. Um eine Ortung über GPS zu verhindern, SOLLTE diese Funktion abgeschaltet werden. Wenn eine Ortung über das Mobilfunknetz verhindert werden soll, SOLLTE das Mobiltelefon abgeschaltet und der Akku entfernt werden.

SYS.3.3.A14 Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung [Benutzer] (H)

Um zu verhindern, dass die verwendeten Rufnummern bestimmten Personen zugeordnet werden können, SOLLTEN Rufnummern für ausgehende Anrufe unterdrückt werden. Außerdem SOLLTEN KEINE SMS- und MMS-Nachrichten versendet werden. Rufnummern von Mobiltelefonen SOLLTEN NICHT veröffentlicht oder an unbefugte Dritte weitergegeben werden.

SYS.3.3.A15 Schutz vor Abhören der Raumgespräche über Mobiltelefone (H)

Damit vertrauliche Informationen nicht abgehört werden können, SOLLTE dafür gesorgt werden, dass keine Mobiltelefone zu vertraulichen Besprechungen und Gesprächen in die entsprechenden Räume mitgenommen werden. Falls erforderlich, SOLLTE das Mitführungsverbot durch Mobilfunk-Detektoren überprüft werden.

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.6.2.1 *Mobile device policy*, Vorgaben für den Einsatz von mobilen Endgeräten.

Das National Institute of Standards and Technology (NIST) stellt das Dokument „Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53, Revision 4, Dezember 2014" zur Verfügung.

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.3.3 *Mobiltelefon* 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 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen