Bundesamt
für Sicherheit in der
Informationstechnik

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 Benutzenden des Mobiltelefons erfolgt durch die SIM-Karte, die bei Vertragsabschluss vom Mobilfunkanbietenden 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

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.3.3 *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 Funktionen 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 könnten Angreifende 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 Mitarbeitenden 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 können Benutzende versäumt haben, den Akku des Gerätes aufzuladen, oder der Akku kann seine Fähigkeit, Energie zu speichern, verloren haben. Auch ist es möglich, dass Benutzende das Zugangspasswort oder die PIN vergessen haben und das Gerät nicht mehr nutzen können. 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 sind die

Benutzenden anschließend nicht mehr erreichbar und können 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 Kommunikationsgeräte aus technischen Gründen geortet werden, um erreichbar zu sein. Somit können Standort-Informationen durch Netzbetreibende oder Dienstbetreibende 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 Mithörenden aufgebaut werden. Viele Mobiltelefone sind mit einer Freisprecheinrichtung ausgestattet, sodass problemlos Gespräche im gesamten Raum erfasst 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 herstellende Institutionen 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 Drittanbietenden ersetzt, sodass diese Mobiltelefone weiterhin Jahrzehnte nach der Produktion eingesetzt werden können.

Oft sind auf diesen veralteten Mobiltelefonen Betriebssysteme installiert, die nicht mehr weiterentwickelt oder supported werden. Softwareschwachstellen können somit nicht mehr durch Updates beseitigt werden. Häufig gibt es die herstellenden Institutionen der Mobiltelefone nicht mehr, oder sie haben ihr Geschäftsfeld auf andere Märkte verlagert. Originales Zubehör und Ersatzteile können deshalb oft nicht mehr nachgekauft werden. Auch Drittherstellende bieten bei sehr alten Mobiltelefonen oft keine entsprechenden Produkte mehr an. Wenn Drittherstellende 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 Ansprechpersonen, die helfen können.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.3.3 *Mobiltelefon* 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.3.3.A1 Sicherheitsrichtlinien und Regelungen für die Nutzung von Mobiltelefonen (B)

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

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

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 Mitarbeitenden im Umgang mit Mobiltelefonen (B)

Mitarbeitende MÜSSEN für die besonderen Gefährdungen der Informationssicherheit durch Mobiltelefone sensibilisiert werden. Sie MÜSSEN in die Sicherheitsfunktion der Mobiltelefone eingewiesen sein. Den Benutzenden MUSS der Prozess bekannt sein, durch den die Mobiltelefone gesperrt werden können. Die Benutzenden 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 diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

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

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 (S) [Benutzende]

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 Benutzenden darüber informiert werden. Es SOLLTE festgelegt werden, ob die Benutzenden 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 Herstellenden 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 (S) [Benutzende]

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 (S) [Benutzende]

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 (S) [Benutzende]

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 Benutzenden 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 die neuen Besitzenden ausgestattet sind. Zudem SOLLTEN die Benutzenden 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 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.3.3.A9 Sicherstellung der Energieversorgung von Mobiltelefonen (H) [Benutzende]

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 Nutzung von Mobilfunk (H) [Benutzende]

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. Falls 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 Nutzung von Mobiltelefonen (H) [Benutzende]

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.