

Sicherheitsanforderung

Mobile Endgeräte

Deutsche Telekom Gruppe

Version	6.3
Datum	01.07.2025
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 3.44	Dokumententyp Sicherheitsanforderung
Version 6.3	Stand 01.07.2025	Status Freigegeben
Fachlicher Ansprechpartner Telekom Security psa.telekom.de	Gültigkeitsdauer 01.07.2025 - 30.06.2030	Freigegeben von Stefan Pütz, Leiter SEC-T-TST

Zusammenfassung
Mobile Endgeräte

Copyright © 2025 by Deutsche Telekom AG.

Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Inhaltsverzeichnis

1.	Einleitung	4
2.	Benutzer-Interaktion	5
3.	Systemhärtung	11
4.	Hardware	13
5.	Bootloader- und Software-Updates	15
6.	Firmware	22
7.	Betriebssystem, Web Browser, Application Execution Environments	23
7.1.	Betriebssystem	23
7.2.	Web-Browser	25
7.3.	Application Execution Environments (AEE)	28
8.	Besondere Gerätefunktionen	34
8.1.	Firewall	34
8.2.	Wireless LAN (WLAN / WiFi)	36
8.2.1.	Wireless LAN Zugangspunkt-Funktionalität	36
8.2.2.	Wireless LAN (WLAN) Client-Funktionalität	37
8.3.	Bluetooth-Funktionalität	38
8.4.	Web-Administrations-Oberfläche	40
8.5.	Passwörter	41
8.6.	Mobilfunk-Endgeräte	42
8.7.	Einsatz bei Geschäftskunden	47

1. Einleitung

Dieses Dokument wurde auf Basis der Vorgaben aus den im Konzern gültigen Sicherheitsrichtlinien erstellt.

Die Sicherheitsanforderung dient u. a. als Grundlage zur Freigabe im PSA-Prozess. Sie dient darüber hinaus als Umsetzungsempfehlung für Einheiten, die nicht am PSA-Verfahren teilnehmen. Diese Anforderungen müssen bereits während der Planungs- und Entscheidungsprozesse berücksichtigt werden.

Bei der Umsetzung der Sicherheitsanforderung ist das jeweils vorrangige nationale, internationale und supranationale Recht zu beachten.

2. Benutzer-Interaktion

Req 1 Das Gerät muss den Benutzer über den sicherheitsrelevanten Zustand informieren.

Das Gerät muss sicherstellen, dass Benutzer über den sicherheitsrelevanten Zustand und Zustandsänderungen informiert werden, einschließlich der relevanten Fehlermeldungen und Hinweise, insbesondere bevor ein Benutzer nach einer Entscheidung gefragt wird (prompting). Die Integrität und Authentizität dieser Informationen muss durch das Gerät sichergestellt werden. Falls erforderlich, kann das Gerät dazu sicherheitsrelevante Ereignisse protokollieren.

Motivation: Der Benutzer muss wissen, in welchem Zustand sich sein Gerät befindet, wenn dieser Zustand Einfluss auf die Sicherheit hat oder Kosten generieren kann.

Umsetzungsbeispiel: Man beachte, dass nicht alle im Folgenden aufgeführten Beispiele von allen Endgeräten umgesetzt werden müssen!

- Hinweis auf unverschlüsselte oder nur einseitig authentifizierte Verbindungen (z. B. offenes WLAN, GSM statt 3G und aufwärts)
- Hinweis auf aktive Netzwerkverbindungen (Bluetooth, WLAN, Mobilfunk, VPN)
- Anzeige aktiver Applikationen und aktiver spezieller Sensoren (z. B. GPS): Der Zugriff auf GPS wird durch ein Symbol in der Statusleiste angezeigt.
- Die Verwendung von TLS wird durch ein Schloss-Symbol im Browser angezeigt.
- Der Nutzer wird durch den Ciphering Indicator auf unverschlüsselte GSM-Verbindungen hingewiesen.
- Ein Gerät, welches Internet-Verbindungen über verschiedene Träger herstellen kann (z. B. Mobilfunknetz, WLAN, LAN, USB- oder Bluetooth-Tethering, IPSec-VPN-Tunnel, verschiedene Mobilfunkanbieter, verschiedene Techniken wie UMTS oder höher versus GSM, Auslandseinsatz, Dial-up-Networking, Premium-Rufnummer, TLS im Gegensatz zu Klartext-HTTP), die unterschiedliche Sicherheitseigenschaften aufweisen, muss anzeigen, welcher Träger und/oder Anbieter gerade verwendet wird (beispielsweise in der Statuszeile). Dies hilft dem Benutzer bei der Beurteilung, ob sensitive Informationen übertragen werden dürfen, und ermöglicht es ihm, unerwünschte Aktionen abubrechen (bspw. solche, die Kosten erzeugen): Die Statuszeile des Geräts zeigt den Status der Verbindungen über die verschiedenen Träger (Bearer) an.
- Das Gerät fragt den Benutzer, bevor im Ausland (Roaming-Betrieb) Internetverbindungen aufgebaut werden und/oder das Gerät bietet dem Benutzer Einstellungsmöglichkeiten an, Daten-Roaming komplett abzuschalten.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

ID: 3.33-1/5.3

Req 2 Falls das Endgerät sicherheitsrelevante Ereignisse protokolliert oder den Benutzer über solche Ereignisse mit Zeitangabe informiert, dann muss das Endgerät über eine verlässliche Systemzeit (Datum und Uhrzeit) verfügen.

Dazu kann das Endgerät (abhängig von Anwendungsfall und Nutzungsszenario) seine Zeit über Netzverbindungen synchronisieren (z. B. mittels Network Time Protocol, NTP) oder der Nutzer kann Datum und Uhrzeit manuell einstellen. Wenn eine Zeitsynchronisation technisch möglich ist (z. B. Gerät hat Internet-Verbindung), sollte das Gerät sie unterstützen.

Motivation: Eine verlässliche Systemzeit ist eine Voraussetzung dafür, dass aussagekräftige Protokollierungsdaten erzeugt werden können; nur so können Ereignisse in eine zeitliche Reihenfolge gebracht und zugeordnet werden.

Umsetzungsbeispiel: Ein Gerät mit Internet-Verbindung nutzt diese in regelmäßigen Abständen (z. B. einmal pro Woche), um die Systemzeit seiner Echtzeituhr mittels NTP abzugleichen. Außerdem stellt das Gerät dem Benutzer eine Möglichkeit bereits, Datum und Uhrzeit manuell einzugeben, so dass auch ohne Internet-Verbindung die Uhrzeit eingestellt und bei Bedarf korrigiert werden kann. Alternativ kann das Gerät eine Zeitinformation auch über das DCF-77-Funksignal oder über GPS beziehen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.33-2/5.3

Req 3	Dem Benutzer muss Roaming-Betrieb im Display angezeigt werden, wenn das Gerät in einem PL-MN betrieben wird, welches weder das HPLMN noch ein zum HPLMN äquivalentes Netz ist.
-------	--

Die Statusleiste muss einen Text oder ein Symbol anzeigen, welches den Benutzer darüber unterrichtet, dass sein Endgerät sich im Roaming-Betrieb befindet.

Motivation: Für die Kostenabrechnung (Billing) ist es unbedingt notwendig, dass der Kunde über den Roaming- Status seines Geräts unterrichtet wird.

Umsetzungsbeispiel: Die Statusleiste zeigt den Namen des Netzbetreibers an. Im Nicht-Roaming-Betrieb wird z. B. Telekom.de angezeigt, im Roaming-Betrieb ein ausländischer Netzbetreiber. Üblicherweise bieten mobile Betriebssysteme sogar in den Einstellungen zum Mobilfunknetz die Möglichkeit, Roaming zu deaktivieren, was in Grenzregionen nützlich sein kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

ID: 3.44-3/6.3

Req 4	Im Display muss eine Anzeige des Trägers (Bearer) erfolgen, die es dem Benutzer ermöglicht, zwischen Mobilfunk- und WiFi-Verbindungen sowie zwischen den Betriebsmodi GSM (2G), UMTS (3G), LTE (4G) und 5G zu unterscheiden.
-------	--

Die Statusleiste muss einen Text oder ein Symbol anzeigen, die den Benutzer auf den Träger hinweist, den er gerade nutzt.

Motivation: Die verschiedenen Träger besitzen unterschiedliche Sicherheitsniveaus. Der Benutzer muss in der Lage sein zu entscheiden, ob das verfügbare Sicherheitsniveau den zu übertragenen Daten angemessen ist. In einer Wi-Fi-Umgebung kann er zusätzliche Sicherheit gewinnen, indem er einen VPN-Tunnel aktiviert oder seinen E-Mail-Client so konfiguriert, dass dieser TLS (z. B. IMAPS und SMTPS oder STARTTLS) verwendet.

Umsetzungsbeispiel: Die Statusleiste zeigt einen Text oder ein Symbol an, die den Benutzer auf den Träger (Bearer) hinweist, den er gerade nutzt. Wenn das Gerät über WLAN verbunden ist, wird Internet-Verkehr über diese Verbindung geroutet, sonst über mobile Daten.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

- Unbemerkt durchführbare Angriffe

ID: 3.44-4/6.3

Req 5 Der Cipher Indicator gemäß 3GPP TS 22.101 muss angezeigt werden.

Motivation: Dies versetzt Benutzer in die Lage, Gespräche mit schützbedürftigem Inhalt zu vermeiden, wenn die Luft-schnittstelle der Mobilfunk-Verbindung nicht verschlüsselt wird.

Umsetzungsbeispiel: Das mobile Betriebssystem zeigt eine Warnmeldung "Ungesicherter Anruf".

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.44-5/6.3

Req 6 Der Zugang zu Systemressourcen muss dem Nutzer angezeigt werden.

Bei Betriebssystemen, die den Zugriff auf schutzbedürftige Systemressourcen (wie PIM-Daten, Lokationsinformation, Dateisystem, ...) nicht anzeigen und den Nutzer nicht zur Genehmigung auffordern, muss die Applikation den Nutzer über die Tatsache und die Art des Datenzugriffs informieren. Es darf nicht möglich sein, kundenseitige bezahlte Ressourcen zu missbrauchen, z. B. durch das Herstellen von Verbindungen mit dem Internet, mit Premium-Rufnummern oder durch das Durchführen von Kauftransaktionen (z. B. Musik, Applikationen, Online-Inhalte, NFC-Kartenkauf). Es muss je nach Applikation entschieden werden, ob Eingabeaufforderungen oder Benachrichtigungen nur einmal während oder nach der Installation, bei jedem Start der Applikation oder bei jedem Datenzugriff erfolgen sollen. Falls es schwierig erscheint, eine gute Entscheidung über die sinnvolle Häufigkeit solcher Abfragen zu treffen, sollte das Gerät voreingestellte Werte verwenden und dem Benutzer eine Möglichkeit zur Konfiguration dieser Optionen anbieten.

Motivation: Es ist eine gute Sicherheitspraxis, den Nutzer auf Zugriffe auf seine schutzbedürftigen Daten aufmerksam zu machen und diese von ihm genehmigen zu lassen.

Umsetzungsbeispiel:

- Das Gerät fragt Benutzer, bevor Aktionen ausgeführt werden, die automatisch gestartet wurden (durch Applikationsintegration / Automation, im Gegensatz zu direkter Benutzerinteraktion): Vor dem Aufruf interner (= vom Betriebssystem bereitgestellter) Protokoll-Handler (z. B. tel://...) fragt das Betriebssystem nach, ob der Benutzer die Aktion durchführen möchte; vor dem Aufruf extern definierter Protokoll-Handler (z. B. skype://...) fragt ebenfalls das Betriebssystem oder ersatzweise die Applikation. Eine Rückfrage beim Benutzer muss insbesondere dann stattfinden, wenn durch eine Aktion einer App Kosten entstehen können (z. B. Versand einer SMS, ausgehender Telefonanruf).
- Der Benutzer kann für jede App festlegen, auf welche lokalen Ressourcen (GPS, Adressbuch, ...) diese zugreifen darf.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

ID: 3.33-3/5.3

Req 7	Falls auf dem Gerät Anwendungen laufen können sollen, die Zugriffs-Token verwenden, dann muss das Gerät dem Benutzer eine Möglichkeit anbieten, seine Zugriffs-Token zu verwalten (einschließlich einer Möglichkeit, alle Token und deren Gültigkeitsdauer zu betrachten sowie eines oder alle Token zu invalidieren).
-------	--

Falls es keine eingebaute Funktion des mobilen Endgeräts gibt, muss eine andere Funktion implementiert werden, die es dem Benutzer erlaubt, seine Access-Token zu verwalten.

Motivation: Solche eine Benutzerschnittstelle zur Zugriffs-Token-Verwaltung ermöglicht es den Benutzern, Verantwortung für ihre Token zu übernehmen und Token zurückzurufen (zu invalidieren), wenn sie nicht mehr benötigt werden. Falls eine solche Infrastruktur zum Token-Rückruf etabliert ist, kann die Gültigkeitsdauer von Token länger definiert werden – was zu einem besseren Benutzererlebnis führt – bei gleichzeitiger Beibehaltung eines hohen Sicherheitsniveaus.

Umsetzungsbeispiel: Beispiel 1: Der Security Token Service (STS) der Deutschen Telekom Gruppe stellt Zugriffstoken aus – entweder in einem proprietären Format oder gemäß einer Version des OAuth-Standards. Der STS Service bietet eine Schnittstelle (API) zum Management und zur Invalidierung von Token.

Beispiel 2: Eine Web-Applikation bietet die Funktionalität, alle Token eines Benutzers (identifiziert durch MSISDN, netzwerkbasierend authentifiziert) zu verwalten.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

ID: 3.44-7/6.3

Req 8	Das Gerät muss sichere Schnittstellen für sicherheitsrelevante Endbenutzer-Interaktion bieten, welche die Integrität und Vertraulichkeit der übertragenen Daten garantieren (sicherer Kanal zwischen Anzeige / Tastatur / TouchScreen und dem Betriebssystem bzw. einer App).
-------	---

Das Gerät muss eine sichere Eingabemöglichkeit für Geheimnisse (z. B. Eingabe von Passwörtern, Schlüsseln) anbieten und APIs zu ihrer sachgemäßen Verarbeitung bereitstellen. Die genaue Art der Unterstützung hängt vom Gerät (z. B. Smartphone oder Tablet, Verfügbarkeit und Größe einer Tastatur / eines Touchscreens) und seinen Funktionen ab sowie von der Notwendigkeit, auf diesem Gerät Geheimnisse zu verarbeiten. Geheimnisse, die der Benutzer einem Prozess (einer App oder dem Betriebssystem) anvertraut, dürfen nicht von anderen Prozessen mitgelesen oder manipuliert werden können.

Motivation: Mobile Endbenutzer-Geräte führen häufig Benutzerinteraktionen durch, einschließlich sicherheitsrelevanter Interaktionen (z. B. Eingabe von WPA2- oder WPA3-Schlüsseln während der Einrichtung eines WLAN-Zugangs oder Interaktion mit einem Passwort-Tresor). Die operationelle Sicherheit hängt in starkem Maße von der Benutzerfreundlichkeit der Funktionen zum Umgang mit Geheimnissen ab. Benutzer werden nur dann starke Authentisierungsverfahren nutzen (z. B. starke Schlüssel, lange Passwörter), wenn diese einfach zu benutzen sind.

Umsetzungsbeispiel:

- Das Betriebssystem des Geräts unterstützt Benutzerauthentifikation durch eine benutzerfreundliche PIN-Eingabe oder Eingabe eines Gerätepassworts.
- Wenn ein Endbenutzergerät kryptographische Funktionen unterstützt, wird es häufig eine Möglichkeit zur Eingabe von kryptographischen Schlüsseln (WiFi shared secrets, Software-Aktivierungsschlüssel, etc.) und zum Schlüsselmanagement benötigen. Ein solches Gerät besitzt eine Tastatur, ein Touchpad o.ä. für eine benutzerfreundliche Dateneingabe. Auch beim Pairen von Geräten (z. B. bei der Verwendung von Bluetooth-Verbindungen) sowie beim Verwalten des Zugriffs auf freigegebene Ressourcen (z. B. Personal Hotspot) sind sicherheitsrelevante Endbenutzer-Interaktionen erforderlich.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.44-8/6.3

Req 9	Wenn ein Authentisierungsgeheimnis (etwa PIN oder Passwort) eingegeben wird, dann müssen die eingegebenen Ziffern / Zeichen auf dem Display maskiert angezeigt werden, bspw. indem sie durch Sternchen ("*") ersetzt werden.
-------	--

Motivation: Das eingegebene Authentisierungsgeheimnis nicht anzuzeigen ist eine übliche Methode, um das Ausspähen des Geheimnisses durch Dritte zu verhindern.

Umsetzungsbeispiel:

- Um Authentisierungsgeheimnisse (PIN, Passwort) gegen das Ausspähen beim Über-die-Schulter-Schauen zu schützen, werden die eingegebenen Zeichen durch Sternchen ersetzt. Abhängig von der Größe der Tastatur (und der Wahrscheinlichkeit von vom Benutzer unbemerkten Tippfehlern), können die Zeichen auch für einen kurzen Augenblick angezeigt werden, bevor sie ersetzt werden.
- Wird die Bildschirmausgabe jedoch umgelenkt, z. B. auf einen Beamer oder im Rahmen einer Videokonferenz, dürfen die Zeichen nicht mehr unmaskiert angezeigt werden. Ein guter Kompromiss zwischen Usability und Sicherheit wird auch erreicht, wenn eingegebene Zeichen eines Geheimnisses standardmäßig maskiert dargestellt werden und der Benutzer mittels eines Schalters die Möglichkeit hat, in sicherer Umgebung die eingegebenen Zeichen im Klartext anzuzeigen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

ID: 3.44-9/6.3

Req 10	Gerätekomponenten, welche anstelle der Tastatur oder sonstiger Benutzereingaben verwendet werden, müssen Schutz vor böartigen Links und vor Injection-Angriffen bieten.
--------	---

Anwendungen, welche NFC-Tags oder QR-Barcodes lesen und die darüber übermittelte URL in einem Browser-Fenster öffnen, sind Beispiele solcher Komponenten. Abhängig vom Anwendungsfall muss das Gerät einen Link vor seinem Aufruf lokal (Eingabevalidierung) oder durch einen vertrauenswürdigen entfernten Dienst prüfen und/oder den Aufruf des vollständigen Klartext-Links vom Benutzer bestätigen lassen. Vorinstallierte Anwendungen, welche entfernt gesendete Eingaben interpretieren (z. B. Instant Messaging Clients), müssen resistent gegen Injection-Angriffe sein.

Motivation: Dadurch können Aufrufe potenziell böartiger Links (URIs / URLs) unterbunden werden, insbesondere wenn (z. B. aufgrund der Nutzung kontaktloser Kommunikation) die Benutzerabsicht nicht mehr eindeutig unterstellt werden kann. Erfolgt die Ansteuerung spezieller Gerätekomponenten (z. B. der NFC-Hardware) durch Anwendungen von Drittanbietern (z. B. Wallet-Applikation), kann nicht davon ausgegangen werden, dass diese immer eine geeignete Eingabevalidierung bzw. benutzerkonfigurierbares Prompting in ihre Anwendungen eingebaut haben.

Umsetzungsbeispiel: Reader für NFC-Tags (near-field communication) und QR-Codes (zweidimensionale Barcodes) sollten die Links (URL/URI) auf böartige Ziele überprüfen (Short-URLs auflösen, resultierendes Ziel gegen einen Safe-Browsing-Dienst prüfen) und benutzerkonfigurierbar den resultierenden Link vor dem Aufruf im Browser dem Benutzer vollständig im Klartext anzeigen. – Im September 2011 haben Forscher gezeigt, dass es möglich war, von einem iOS-Gerät, auf dem der Skype-Client lief, das Adressbuch auszulesen, indem eine nicht wohlgeformte Instant Message an das Gerät geschickt wurde.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

3. Systemhärtung

Req 11 Der Benutzer muss nicht benötigte Dienste und Protokolle deaktivieren können.

Es muss für den Benutzer erkennbar sein, welche Dienste und Protokolle aktiviert sind. Der Benutzer muss in der Lage sein, nicht gewünschte Dienste und Protokolle selbständig zu deaktivieren (z. B. in den Einstellungen des Geräts).

Motivation: Moderne Endgeräte bieten eine Vielzahl von Funktionen an, bei denen dem Komfortgewinn häufig Einschränkungen hinsichtlich Datensicherheit oder Datenschutz entgegenstehen. Der Benutzer muss in der Lage sein, die Nutzung solcher Funktionen jederzeit gemäß seinen eigenen Bedürfnissen anzupassen.

Umsetzungsbeispiel: Der Benutzer kann auf Basis guter Benutzerführung, evtl. unter Zuhilfenahme des Handbuchs, folgende Einstellungen selbst seinen Bedürfnissen entsprechend vornehmen: Nutzung von Zwischenspeichern für Geheimnisse (z. B. Passwortspeicher im Browser), Aktivierung von Schnittstellen (Bluetooth, WLAN, NFC, GPS, ...), Nutzung von Cloud-Speicherdiensten einschließlich eventueller Synchronisation von Daten über Geräte hinweg.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.33-5/5.3

Req 12 Das System muss robust gegenüber unerwarteten Eingaben implementiert werden.

An das System übergebene Daten müssen vor der Weiterverarbeitung zunächst validiert werden, um sicherzustellen, dass die Daten dem erwarteten Daten-Typ und -Format entsprechen. Dies soll das Risiko einer Manipulation von Systemabläufen und -Zuständen durch entsprechend konstruierte Dateninhalte eliminieren. Eine Validierung ist für jegliche Daten durchzuführen, die an das System übergeben werden. Beispiele sind Benutzereingaben, Werte in Datenfeldern und Protokollinhalte.

Die folgenden typischen Implementierungsfehler müssen vermieden werden:

- Fehlende Validierung der Länge von übergebenen Daten
- Unzutreffende Annahmen über das Format von Daten
- Fehlende Validierung empfangener Daten auf Konformität mit der Spezifikation
- Unzureichende Behandlung von Protokollabweichungen in empfangenen Daten
- Unzureichende Begrenzung der Rekursion beim Parsing komplexer Datenformate
- Unzureichende Umsetzung von Whitelisting oder Escaping zum Schutz vor Eingaben außerhalb des validen Wertebereiches

Motivation: Ein Angreifer kann mittels gezielt konstruierter Dateninhalte versuchen, ein System, das empfangene Daten vor der internen Weiterverarbeitung nicht ausreichend validiert, in einen instabilen Zustand zu versetzen oder nicht autorisierte Aktionen innerhalb des Systems auszulösen. Das Schadenspotential entsprechender Angriffe ist individuell systemabhängig, besitzt jedoch eine theoretische Bandbreite von unkontrollierten Systemabstürzen bis hin zu einer kontrollierten Ausführung von eigens eingeschleustem Code und der daraus resultierenden vollständigen Kompromittierung eines Systems.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

Req 13	Es dürfen keine Konten mit vordefinierten Authentisierungsmerkmalen auf dem Gerät vorhanden sein.
--------	---

Falls Konten mit vordefinierten Authentisierungsmerkmalen dennoch existieren, muss durch Konfiguration (möglichst vor Auslieferung des Geräts) oder mittels Administration durch den Kunden das Authentisierungsmerkmal auf einen nur dem Kunden bekannten Wert geändert oder alternativ das Konto gelöscht oder deaktiviert werden.

Motivation: Vordefinierte Authentisierungsmerkmale sind Angreifern häufig bekannt und ermöglichen diesen dann unberechtigten Zugriff.

Umsetzungsbeispiel: Der Benutzer wird im Handbuch darauf hingewiesen, dass sein Gerät über ein Konto mit vordefiniertem Passwort verfügt, und das Handbuch beschreibt leicht nachvollziehbar, wie das Passwort geändert werden kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.33-7/5.3

4. Hardware

Req 14	Falls auf dem Gerät Daten oder Schlüssel mit einem so hohen Schutzbedarf verarbeitet werden, dass physische Angriffe für sie eine reale Bedrohung darstellen, dann muss das Gerät Schutz vor Manipulation bereitstellen.
--------	--

Der Schutz kann durch eine Kombination aus physischem Schutz (z. B. Gehäuse, Manipulationserfassung) und algorithmischen Abwehrmaßnahmen (z. B. Prüfsummen, Verifikation der Code-Integrität) erzielt werden. Stellt das Gerät nicht den normalerweise von einem Nutzer erwarteten Schutz bereit, dann muss der Benutzer in der Begleitdokumentation des Produkts über diese Abweichung informiert werden.

Motivation: Es muss vermieden werden, dass die Erwartungen von Endnutzern hinsichtlich des vom Gerät bereitgestellten physischen Schutzes nicht erfüllt werden. Der Benutzer muss entscheiden können, ob er ein Endgerät in öffentlicher Umgebung aufstellen kann (z. B. WLAN-Router in einer Gaststätte) oder ob zusätzliche Schutzmaßnahmen erforderlich sind.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten
- Unbemerkt durchführbare Angriffe

ID: 3.33-8/5.3

Req 15	Falls auf dem Gerät Daten oder Schlüssel mit einem so hohen Schutzbedarf verarbeitet werden, dass physische Angriffe für sie eine reale Bedrohung darstellen, dann muss der integrierte Prozessor oder die Systemplatine des Geräts über ein Hardware-Sicherheitsmodul (HSM) oder eine Schnittstelle zu einem externen HSM verfügen.
--------	--

Für mobile Endgeräte, die eine Verbindung mit einem Mobilfunknetzwerk aufbauen, sollte das HSM eine SIM/USIM-Karte sein, welche die Schlüssel speichert, die den Zugriff auf Dienste des Mobilfunknetzes schützen. Befindet sich keine SIM/USIM-Karte im Gerät (z. B. Embedded USIM), muss die stattdessen verwendete Lösung vergleichbare Sicherheit bereitstellen. Das HSM kann auch ein Teil des integrierten Prozessors oder der Systemplatine des Geräts (z. B. wie ein TPM) sein. Zusätzlich können weitere HSM vorhanden sein, wie etwa Secure Elements für den NFC-Betrieb. Andere Geheimnisse / Berechtigungsnachweise können unter Nutzung anderer Mechanismen gespeichert werden.

Motivation: Ein Hardware-Sicherheitsmodul stellt in der Regel Mechanismen bereit, die eine sichere Speicherung von vertraulichen Daten wie z. B. Schlüssel im Gerät ermöglichen, starke Zufallszahlen für verschiedene Applikationen generieren (z. B. Generierung von Session-IDs) und kryptographische Berechnungen beschleunigen.

Umsetzungsbeispiel: Das Gerät bietet einen Steckplatz für eine SIM-Karte (UICC) und/oder nutzt eine sichere eUICC zur Speicherung von eSIM-Profilen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unbemerkt durchführbare Angriffe

ID: 3.44-15/6.3

Req 16	Die Baseband-Firmware muss den Zugang zur SIM/USIM/ISIM-Karte auf vertrauenswürdige (trusted) Prozesse (etwa Teile des Betriebssystems) beschränken.
--------	--

Motivation: Dies trägt zur Verhinderung des Missbrauchs von SIM/USIM/ISIM-Schlüsseln durch nicht vertrauenswürdige (untrusted) Applikationen oder Malware bei.

Umsetzungsbeispiel: Die Baseband-Firmware beschränkt den Zugriff von Applikationen auf bestimmte SIM-

Anwendungen / SIM-Verzeichnisse (z. B. SIM/USIM(ISIM) oder SIM-Funktionen (z. B. AKA, GBA/GAA).

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.44-16/6.3

Req 17	Falls auf dem Gerät Daten oder Schlüssel mit einem so hohen Schutzbedarf verarbeitet werden, dass physische Angriffe für sie eine reale Bedrohung darstellen, dann müssen für Testzwecke vorgesehene Hardware-Schnittstellen sicher deaktiviert werden.
--------	---

Motivation: Ports für den Testzugang eröffnen signifikante Möglichkeiten zur Gewinnung von Informationen über den internen Aufbau des Geräts (Reverse Engineering) und können die Offenlegung von im Firmware-Image gespeicherten vertraulichen Daten ermöglichen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.33-11/5.3

5. Bootloader- und Software-Updates

Req 18	Die Software und Hardware des Systems muss von einem Sicherheitsschwachstellen-Support seitens des Herstellers abgedeckt sein.
--------	--

In einem System dürfen nur Software- und Hardware-Produkte eingesetzt werden, für die ein Sicherheitsschwachstellen-Support durch den Hersteller besteht.

Ein solcher Support muss umfassen, dass der Hersteller

- das Produkt kontinuierlich auf eine Betroffenheit von Sicherheitsschwachstellen beobachtet und analysiert,
- über Art, Schweregrad und Ausnutzbarkeit von im Produkt entdeckten Schwachstellen umgehend informiert
- zeitnah Produktaktualisierungen oder wirksame Workarounds zur Behebung der Schwachstellen bereitstellt.

Der Sicherheitsschwachstellen-Support muss für die gesamte Dauer gegeben sein, in der das betroffene Produkt im Einsatz verbleibt.

Support-Phasen mit eingeschränktem Leistungsumfang

Viele Hersteller bieten für ihre Produkte als Option einen zeitlich ausgedehnten Support an, welcher über die für den allgemeinen Markt vorgesehene Support-Phase hinausgeht, aber oftmals mit Einschränkungen verbunden ist. Einige Hersteller definieren ihren Support grundlegend in Abstufungen, die Einschränkungen schon während der letzten Phase vor dem absoluten Endtermin des regulären Supports enthalten können.

Wird ein Produkt innerhalb von Support-Phasen eingesetzt, die Einschränkungen unterliegen, muss explizit sichergestellt sein, dass diese Einschränkungen die Verfügbarkeit des Sicherheitsschwachstellen-Support nicht beeinträchtigen.

Open Source Software und Hardware

Open Source Produkte werden häufig von freien Organisationen oder Communities entwickelt; entsprechend ist ein vertraglich vereinbarter Sicherheitsschwachstellen-Support unter Umständen nicht verfügbar. Grundsätzlich muss auch hier sichergestellt sein, dass von der Organisation/Community (oder einem offiziell durch diese eingesetzten Dritten) für das betroffene Produkt ein umfassendes Sicherheitsschwachstellen-Management betrieben wird, welches die oben genannten Kriterien erfüllt und als zuverlässig etabliert gilt.

Motivation: Hardware- und Software-Produkte, für die kein vollumfassender Sicherheitsschwachstellen-Support durch den Hersteller besteht, stellen ein Risiko dar. Dies bedeutet, dass ein Produkt nicht ausreichend auf eine Betroffenheit durch weiterentwickelte Angriffsformen oder neu entdeckte Schwächen technischer Umsetzungen geprüft wird. Analog werden bei vorhandenen Sicherheitsschwachstellen in einem Produkt keine Nachbesserungen (z. B. Updates, Patches) bereitgestellt. Hieraus resultiert ein System, dessen Schwachstellen nicht behoben werden können, so dass sie für einen Angreifer ausnutzbar bleiben, um das System zu kompromittieren oder es negativ zu beeinträchtigen.

Umsetzungsbeispiel: Es wird mit dem Hersteller der Information Security Annex (ISA) abgeschlossen, welcher die Details der Bereitstellung von Software-Updates regelt (Zeit bis zur Bereitstellung eines Fixes abhängig vom CVSS-Score).

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.44-18/6.3

Req 19	Eingesetzte Software muss aus vertrauenswürdigen Quellen bezogen und auf Integrität geprüft werden.
--------	---

Die auf dem System eingesetzte Software muss aus vertrauenswürdigen Quellen bezogen und vor der Installation auf ihre Integrität geprüft werden.

Diese Anforderung bezieht sich auf sämtliche Arten von Software:

- Firmware sowie Microcode für Hardware-Komponenten
- Betriebssysteme
- Software-Bibliotheken
- Applikationen und Anwendungssoftware
- vorintegrierte Anwendungslösungen, wie z. B. Software Appliances oder Container

sowie weitere Software, die ggf. zum Einsatz kommt.

Vertrauenswürdige Quellen

Als vertrauenswürdige Bezugsquellen gelten allgemein:

- die offiziellen Vertriebs- und Bereitstellungs Kanäle des Herstellers
- dritte Distributoren, sofern sie durch den Hersteller autorisiert und legitimer Bestandteil von dessen Bereitstellungs Kanälen sind
- Internet-Downloads, sofern diese von offiziellen Bereitstellungs-Servern des Herstellers oder autorisierter Distributoren erfolgen
 - (1) Bietet der Bereitstellungs-Server verschiedene Formen von Downloads an, müssen durch Verschlüsselung bzw. kryptografische Signaturen geschützte Downloads jenen ohne einen solchen Schutz vorgezogen werden.
 - (2) Sichert der Bereitstellungs-Server die Transport-Schicht mittels kryptografischer Protokolle (z. B. HTTPS, sftp), müssen die zugehörig präsentierten Server-Zertifikate oder Server-Keys/Fingerprints bei jedem Download validiert werden, um die Identität des Bereitstellungs-Servers zu bestätigen; schlägt die Validierung fehl, ist der Download abubrechen und der Bereitstellungs-Server als nicht vertrauenswürdige Quelle zu bewerten.

Integritätsprüfung

Die Integritätsprüfung soll sicherstellen, dass die erhaltene Software frei von Manipulationen und Schadsoftware-Befall ist. Sofern vorhanden, müssen zur Prüfung die vom Hersteller implementierten Mechanismen verwendet werden.

Valide Mechanismen sind:

- physikalische Siegel bzw. fest aufgebrachte Echtheitszertifikate (bei Bereitstellung der Software auf physikalischen Datenträgern)
- Abgleich von kryptografischen Hash Werten (z. B. SHA256, SHA512) der erhaltenen Software gegen Soll-Werte, die der Hersteller separat benennt
- Prüfung von kryptografischen Signaturen (z. B. GPG, Zertifikate), mit denen der Hersteller seine Software versieht

Zusätzlich ist eine Überprüfung der Software mittels eines Anti-Virus- bzw. Anti-Malware Scanners empfohlen (falls der Hersteller keinen der zuvor erwähnten Integritätsschutz-Mechanismen für seine Software implementiert hat, ist diese Überprüfung verpflichtend).

Erweiterte Integritätsprüfung bei Bezug von Software aus öffentlichen Registries

Öffentliche Registries ermöglichen es Entwicklern, beliebige eigene Software-Projekte zur Nutzung bereitzustellen. Die Bandbreite umfasst sowohl Projekte von namhaften Anbietern mit kontrollierten Entwicklungsprozessen als auch von kleineren Anbietern oder Amateur-Entwicklern.

Beispiele für solche Registries sind:

- Code Registries (z. B. GitHub, Bitbucket, SourceForge, Python Package Index)

- Container Registries (z. B. Docker Hub)

Software aus öffentlichen Registries muss vor dem Einsatz einer erweiterten Integritätsprüfung unterzogen werden. Zusätzlich zu den im vorherigen Abschnitt beschriebenen Bestandteilen der Integritätsprüfung soll die erweiterte Prüfung explizit sicherstellen, dass die Software ihre Funktion tatsächlich wie beschrieben erfüllt, keine inhärenten Sicherheits-Risiken wie etwa gezielt implementierte Malware-Funktionen enthält und nicht von bekannten Sicherheits-Schwachstellen betroffen ist. Sofern die Software direkte Abhängigkeiten zu dritten Software-Projekten aufweist (sog. "Dependencies", sehr typisch in Open Source Software), die zum Einsatz der Software ebenfalls bezogen und installiert werden müssen, sind diese in die erweiterte Integritätsprüfung mit einzubeziehen.

Methoden für eine erweiterte Integritätsprüfung können beispielsweise sein:

- strikte Validierung der Projekt-/Paket-Namen (Vermeidung der Verwechslung mit maliziösen, gezielt nachgeahmten Software-Projekten)
- dynamische Code Analyse / strukturierte Funktionsprüfung in einer Test-Umgebung
- statische Code Analyse mittels eines Linters (z. B. Splint, JSLint, Pylint)
- Untersuchung mittels eines Sicherheitsschwachstellen-Scanners (z. B. Qualys, Nessus)
- Untersuchung mittels eines Container Security Scanners (z. B. JFrog Xray, Harbor, Clair, Docker Scan)
- Untersuchung mittels eines SCA (Software Composition Analysis) Tools bzw. Dependency-Scanners (z. B. OWASP Dependency Check, Snyk)

Die Prüfungsmethoden sind passend zur exakten Form der Software-Bereitstellung (Quellcode, Binaries/Artefakte, Container) auszuwählen und angemessen zu kombinieren.

Motivation: Softwarelieferketten enthalten diverse Angriffsvektoren. Ein Angreifer kann an verschiedenen Stellen ansetzen, um Software zu manipulieren oder gezielt eigene Routinen einzubringen und die Zielumgebung, in der die Software anschließend zum Einsatz gebracht wird, zu schädigen oder unter seine Kontrolle zu bringen. Der Angriff kann auf dem Transport- bzw. Übertragungsweg geschehen oder auch auf die Bereitstellungsquelle selbst ausgeübt werden. Entsprechend erleichtert wird ein Angriff, falls Software nicht über offizielle und kontrollierte Quellen bezogen wird oder eine Integritätsprüfung ausgelassen wird.

Besonderes Risiko zeigt sich für Software, die aus öffentlichen Registries bezogen wird, da diese jedermann für die Bereitstellung von Software-Projekten offenstehen. Perfide Angriffsmethoden sind inzwischen bekannt, in denen der Angreifer zunächst eine Zeitlang sicherheitstechnisch völlig unauffällige, funktionale Software bereitstellt und sobald diese sich etabliert und eine gewisse Verbreitung gefunden hat, in zukünftigen Versionen gezielt versteckten Schadcode integriert. Andere Methoden setzen auf ähnlich klingende Projektnamen zu weit verbreiteten Bestandsprojekten oder überstimmende Versionsnummern, um manipulierte Software in darauf aufbauende Lösungen zu injizieren.

Umsetzungsbeispiel: Bezug der Software über die offiziellen Bereitstellungskanäle des Herstellers. Nach Erhalt der Software umgehend Prüfung auf Integrität mittels kryptografischer Checksummen, wie vom Hersteller bereitgestellt, sowie Freiheit von bekannter Schadsoftware mittels Anti-Malware- / Anti-Virus-Scanner. Ablage der geprüften Software auf einer internen, geschützten Dateiablage und weitere Nutzung (z. B. Rollout auf die Zielsysteme) nur noch von dort.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-2/9.0

Req 20	Bekannte Schwachstellen in der Software oder Hardware des Systems müssen behoben oder gegen Missbrauch abgesichert werden.
--------	--

Bekannte Schwachstellen in Software- und Hardware Komponenten müssen mittels Installation von verfügbaren Systemaktualisierungen des Herstellers (z. B. Patches, Updates/Upgrades) behoben werden. Alternativ ist der Einsatz von Workarounds (Akut-Lösungen, welche die Schwachstelle nicht beheben, aber die Ausnutzung wirksam verhindern) zulässig. Workarounds sollten grundlegend nur temporär Verwendung finden und sobald möglich durch eine reguläre Systemaktualisierung ersetzt werden, um die Schwachstellen vollständig zu schließen.

Komponenten, die bekannte, nicht behebbare Schwachstellen enthalten, dürfen in einem System nicht eingesetzt werden.

Die Behandlung von neu bekannt werdenden Schwachstellen muss zudem für die gesamte Einsatzphase des Systems fortlaufend sichergestellt und in den kontinuierlichen Betriebsprozessen eines Security Patch Managements umgesetzt werden.

Motivation: Der Einsatz von Komponenten ohne eine Behebung enthaltener Schwachstellen erhöht deutlich das Risiko einer erfolgreichen Kompromittierung. Der Angreifer wird zusätzlich dadurch begünstigt, dass i. d. R. nicht nur detaillierte Informationen zu bereits bekannt gewordenen Schwachstellen offen verfügbar sind, sondern oft auch bereits angepasste Angriffswerkzeuge, die eine aktive Ausnutzung erleichtern.

Umsetzungsbeispiel: Im Anschluss an die initiale Installation eines Betriebssystems von einem offiziellen Installationsmedium werden alle aktuell verfügbaren Patches und Sicherheits-Updates eingespielt.

Zusätzliche Informationen:

Primäre Quellen für bereits bekannt gewordene Schwachstellen in einer Software/Hardware sind Auflistungen in den Versionshinweisen sowie die Sicherheitshinweise aus den offiziellen Meldekanälen des Herstellers oder unabhängiger CERTs. Insbesondere die Meldekanäle werden sinnvollerweise fest in kontinuierliche Prozesse des Security Patch Managements für ein System eingebunden, damit neu bekanntwerdende Schwachstellen zeitnah registriert und in operative Behebungsmaßnahmen geführt werden können.

Als ergänzende Maßnahme zur Aufdeckung von potenziell noch enthaltenen, grundsätzlich bereits bekannt gewordenen Arten von Schwachstellen können gezielte Schwachstellenuntersuchungen des Systems durchgeführt werden. Zu diesem Zweck eignen sich besonders spezialisierte Werkzeuge wie automatisierte Schwachstellen-Scanner. Beispiele hierfür sind: Tenable Nessus, Qualys Scanner Appliance.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-10/9.0

Req 21	Das Gerät muss einen sicheren Bootloader bereitstellen, der einen sicheren Bootprozess für die Baseband-Firmware und ggf. Teile des Betriebssystems durchsetzt.
--------	---

Der sichere Bootprozess verifiziert die Integrität des sicherheitsrelevanten ausführbaren Programmcodes (Baseband-Firmware und ggf. Teile des Betriebssystems), bevor dieser ausgeführt wird, und stellt somit sicher, dass das System im Rahmen seiner Bestimmung verwendet wird und nicht manipuliert wurde. Der sichere Boot-Prozess sollte allen ausführbaren Code umfassen (einschließlich der Applikationen), vgl. z. B. Apple iOS. Unbedingt erforderlich ist dies jedoch für die Firmware (Baseband) bzw. Software (ggf. Teile des Betriebssystems), da dort Sicherheitsfunktionen umgesetzt werden (u. a. Zugriff auf SIM/USIM-Applikation und deren Schlüssel durch das Baseband; ggf. Kontrolle des Zugriffs von Anwendungen auf die SIM-Karte).

Motivation: Angriffe auf mobile Betriebssysteme haben gezeigt, dass Schutzmaßnahmen des Betriebssystems durch Patching des Bootloaders umgangen werden konnten.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten
- Unbemerkt durchführbare Angriffe

ID: 3.44-21/6.3

Req 22 Das Gerät (z. B. sein Bootloader) muss die Aktualisierung der gesamten Geräte-Firmware zulassen.

Motivation: Dies ermöglicht es Nutzern, die Firmware ihrer Geräte zu aktualisieren, sollten dort Fehler oder Sicherheitschwachstellen entdeckt worden sein.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.33-16/5.3

Req 23 Das Gerät muss Updates/Patches von Teilen der Software zulassen.

Motivation: Feingranulare Updates (z. B. von einzelnen Dateien oder Applikationen) erlauben die Entschärfung/Behebung von Sicherheitslücken in einzelnen Komponenten oder Applikationen, z. B. im Web-Browser des Geräts oder in der PDF-Darstellungskomponente. Das Einspielen kleinerer Updates verbraucht weniger Zeit, Datenvolumen und Strom und birgt geringere Risiken, weshalb die Wahrscheinlichkeit deutlich größer ist, dass Benutzer solche Updates zeitnah einspielen.

Umsetzungsbeispiel: Updates, die über die Luftschnittstelle (over-the-air) verteilt werden, sollten möglichst klein sein.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.33-17/5.3

Req 24 Das Gerät muss die Image-Integrität durch eine Signatur-Verifikation oder ein vergleichbar starkes Verfahren prüfen, bevor ein Firmware-Image vom / im Flash-Speicher ausgeführt/gespeichert wird.

Motivation: Ungeprüfte Firmware-Updates können schädlichen Code in das System einführen. Daher ist eine strenge Integritäts- und Authentizitätsprüfung erforderlich, um den Nutzer vor Schäden aller Art zu schützen (z. B. SMS-Angriffe, unbefugte Offenlegung von Berechtigungsnachweisen, Keylogger).

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten
- Störung der Verfügbarkeit

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Integrität

ID: 3.33-18/5.3

Req 25	Das Gerät muss einen Rollback zur letzten bekannten korrekten Firmware erlauben, wenn das Einspielen eines Updates/Patches fehlschlägt.
--------	---

Motivation: Mit Rollback-Funktionalität wird sichergestellt, dass ein Gerät mit der alten Firmware-Version weiterarbeiten kann, sollte die Integrität der aktualisierten Firmware nicht erfolgreich verifiziert werden können. Kunden wird so die Angst vor dem Einspielen von Updates genommen und mehr Geräte werden mit aktueller Firmware betrieben.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Integrität

ID: 3.33-19/5.3

Req 26	Das Gerät muss eine Möglichkeit zur Benachrichtigung von Nutzern über verfügbare Updates bereitstellen.
--------	---

Bei dem Nutzer, der benachrichtigt wird, kann es sich um einen administrativen Nutzer handeln (z. B. im Fall eines Home Gateways). Falls das Gerät Benachrichtigungen unterstützt, sollte diese Funktion genutzt werden („push“); andernfalls kann die Information in der Administrationsoberfläche erfolgen („pull“).

Motivation: Die Installation von Updates kann Dienstunterbrechungen verursachen. Je nach Gerät müssen verschiedene Voraussetzungen erfüllt sein, damit ein Update problemlos eingespielt werden kann, z. B. Stromversorgung, Speicherplatz, Art (Geschwindigkeit und Kosten) der Verbindung zum Update-Server, etc. Die Übertragung und Installation von Updates auf das Gerät sollte nur dann forciert und durchgesetzt werden, wenn das Update äußerst sicherheitskritisch ist. Wird das Update nicht automatisch installiert, muss der Geräteadministrator über verfügbare Updates informiert werden.

Umsetzungsbeispiel:

- Mobile Betriebssysteme bieten Dienste zur stromsparenden Benachrichtigung an (iOS: Apple Push Notification Service, Android: Google Firebase Cloud Messaging).
- Eine Benachrichtigung kann auch per E-Mail erfolgen. Dazu kann z. B. die E-Mail bei Ersteinrichtung des Geräts abgefragt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.33-20/5.3

Req 27	Das Gerät darf keine Funktionen (Test- oder Diagnosefunktionen, APIs, Menüpunkte, Komfortfunktionen) enthalten, die es unautorisierten Benutzern oder Anwendungen auf dem Gerät ermöglichen, vertrauliche Daten aus nichtflüchtigem (persistentem) Speicher auszulesen.
--------	---

Motivation: Das Endgerät muss vertrauliche Daten vor unbefugter Offenlegung schützen (verlorenes / gestohlenes Gerät, bösartige Anwendung). Bestimmte vertrauliche Daten, wie z. B. Passwörter, sollten niemals vom Gerät abgerufen werden können.

Umsetzungsbeispiel: Vertrauliche Daten können kryptographische Schlüssel oder Nutzerberechtigungsnaehweise (Credentials) sein, aber auch Benutzerdaten wie z. B. Gesundheitsdaten.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsiehtnahme oder Abgriff von Daten

ID: 3.33-23/5.3

6. Firmware

Req 28	Falls das Gerät vertrauliche Daten in seiner Software/Firmware speichert, dann muss das Gerät diese vertraulichen Daten verschlüsselt innerhalb der Software/Firmware speichern.
--------	--

Enthält die Firmware vertrauliche Daten wie z. B. kryptographische Schlüssel oder Passwörter, dann müssen diese Daten vom Gerät (z. B. von der Firmware) unter Verwendung starker Algorithmen in verschlüsselter Form gespeichert werden. Ob solche Daten (z. B. private TLS-Schlüssel zur Unterstützung von TR-069 oder kryptographische Schlüssel zur Entschlüsselung von Software-Updates) in der Firmware vorhanden sind, hängt vom Funktionsumfang des Geräts ab.

Motivation: Es ist sehr wahrscheinlich, dass Angreifer sich Zugang zu Firmware-Images verschaffen können (z. B. Download der Images aus dem Internet oder Abruf von Speicherinhalten nach bestimmten vorbereitenden Maßnahmen, insbesondere wenn das Gerät keine starken physischen Schutzmechanismen bereitstellt). Durch zusätzliche Verschlüsselung wird der Reengineering-Aufwand, der für den Zugriff auf vertrauliche Daten erforderlich ist, erheblich erhöht.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

ID: 3.33-21/5.3

Req 29	Das Gerät muss Mechanismen (z. B. kryptographische Prüfsummen, Signaturen) enthalten, welche die Integrität relevanter Daten schützen.
--------	--

Verwendet das Gerät Mechanismen zur Selbstprüfung, können Übertragungsfehler und einfache Manipulationen erkannt werden. Durch den Einsatz von kryptographischen Prüfsummen kann die Integrität relevanter Daten (z. B. Root-Zertifikate, öffentliche Schlüssel, Gerätekennungen, IMEI) sichergestellt werden.

Motivation: Damit wird das Risiko der Nutzung fehlerhafter Daten oder schädlicher Firmware-Images reduziert.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten
- Störung der Verfügbarkeit

ID: 3.33-22/5.3

7. Betriebssystem, Web Browser, Application Execution Environments

7.1. Betriebssystem

Req 30	Das Betriebssystem des Geräts muss einen starken Speicherschutz durchsetzen. Es darf nicht möglich sein, dass ein Prozess Datenstrukturen im Adressraum eines anderen Prozesses oder innerhalb des Kernel-Adressraums beschädigen kann.
--------	---

Motivation: Starker Speicherschutz ermöglicht einen stabilen, robusten und sicheren Betrieb.

Umsetzungsbeispiel: Die Speicherbereiche von Kernel und Benutzerprozessen sind klar getrennt. Das Betriebssystem stellt jedem Benutzerprozess seinen eigenen virtuellen Speicherbereich bereit. Dabei setzt es auf einem Prozessor auf, der im protected mode betrieben wird.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.33-24/5.3

Req 31	Das Betriebssystem des Endgeräts muss eine Randomisierung des Adressraum-Layouts (ASLR) implementieren.
--------	---

Motivation: ASLR (Address Space Layout Randomization) wehrt einige Angriffsformen ab, bei denen versucht wird, Speicherüberläufe zur Ausführung von Code zu verwenden.

Umsetzungsbeispiel: Aktuelle Version von Android und iOS unterstützen ASLR.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.44-31/6.3

Req 32	Falls er von Kunden nicht explizit gefordert wird, dann darf ein Shell-Zugang oder eine ähnliche befehszeilenorientierte Benutzeroberfläche nicht implementiert werden.
--------	---

Diese Anforderung gilt für alle Netzchnittstellen (z. B. WAN, LAN, WLAN, ...) sowie für serielle Schnittstellen an der Systemplatine des Geräts. Ausnahme: Geschäftskunden fordern einen solchen Zugang explizit.

Motivation: Shell-Zugang ermöglicht Angriffe sowie die Gewinnung von Informationen über den internen Aufbau des Geräts (Reverse Engineering).

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.33-25/5.3

Req 33 Falls das Gerät über eine Konsolenoberfläche und/oder ein GUI verfügt, dann dürfen diese nur für die Ausgabe nicht vertraulicher Status- oder Protokollmeldungen verwendet werden.

Vertrauliche Daten (wie z. B. private kryptographische Schlüssel, Benutzernamen, Passwörter, Berechtigungsnachweise usw.) dürfen nicht über eine solche Oberfläche unbefugt offengelegt werden. Vom Benutzer selbst vergebene Geheimnisse (z. B. selbst gewählter WLAN-Schlüssel) dürfen angezeigt werden, aber nur nach erfolgreicher Authentisierung (z. B. nach Eingabe des Admin-Passworts für das Gerät).

Motivation: In einem Endgerät gespeicherte vertrauliche Daten müssen geschützt sein, auch wenn ein Angreifer Zugang zur Hardware erlangt. Mobile Geräte könnten verloren gehen; Festnetzgeräte könnten eventuell in Bereichen verwendet werden, die keinen optimalen physischen Schutz bereitstellen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.33-26/5.3

Req 34 Der Nutzer muss beim ersten Gebrauch des Geräts aufgefordert werden, ein Gerätepasswort zu wählen.

Motivation: Ein inaktiviertes Passwort oder identische Standardpasswörter könnten zu Angriffen auf das Gerät führen, wenn der Nutzer das Standardpasswort nicht ändert.

Umsetzungsbeispiel: Im Verlauf des Einrichtungsassistenten wird der Nutzer aufgefordert, ein Gerätepasswort zu wählen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.44-34/6.3

Req 35 Unterstützt das Gerät eine Verwendung durch mehrere Nutzer, dann muss das Gerät Applikationen und anderen Identitätskonsumenten gegenüber die Nutzeridentität ordnungsgemäß bereitstellen und sie über alle Prozesse durchsetzen. Außerdem muss das Gerät geeignete Werkzeuge zum Erstellen, Bearbeiten und Löschen von Identitäten / Benutzerprofilen bereitstellen.

In Fällen, in denen ein Einzelnutzer zu identifizieren ist (anstelle eines Endgeräts, PCs oder einer Client- Applikation), müssen geeignete Mechanismen zum Schutz dieser Identität vorhanden sein. Wenn das Betriebssystem (OS) mehrere Nutzer unterstützt, sollte diese OS-Funktionalität zum Schutz individueller Identitäten eingesetzt werden.

Motivation: Die Identifizierung von Hardware- oder Softwarekomponenten reicht häufig in Anwendungsfällen, in denen eine bestimmte Einzelperson (Nutzer) identifiziert werden muss, nicht aus. Dies gilt insbesondere für Anwendungsfälle mit Datenschutzrelevanz.

Umsetzungsbeispiel:

- Bei Mobiltelefonen und Smartphones gibt es typischerweise eine 1:1-Beziehung zwischen Benutzer und Endgerät.
- Tablets können als Familiengeräte angesehen werden, die von verschiedenen Familienmitgliedern und Freunden dieser genutzt werden können sollen. Daher könnten Bookmarks / Favoriten und die Browser- Historie / Verlauf an einzelne Benutzer gebunden werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.44-35/6.3

Req 36	Die administrativen Einstellungen müssen klar und leicht verständlich sowie möglichst selbsterklärend sein.
--------	---

Motivation: Damit wird das Fehlkonfigurationsrisiko reduziert.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.33-30/5.3

Req 37	Das Gerät muss es dem Nutzer ermöglichen, vor Entsorgung oder Verkauf des Geräts alle auf dem Gerät gespeicherten Daten so zu löschen, dass diese Daten nicht mit vertretbarem Aufwand wiederhergestellt werden können.
--------	---

Das Verfahren zur Durchführung eines Factory Reset muss gut dokumentiert sein, so dass der Nutzer in der Lage ist, den Factory Reset auf Wunsch auszuführen, auch wenn er einige oder alle seiner Berechtigungsnachweise vergessen hat. Andererseits muss ein versehentliches Auslösen der Factory-Reset-Funktionalität verhindert werden. - Die zu löschenden Daten schließen persönliche Nutzerdaten, Kontodaten, Berechtigungsnachweise und Konfigurationsdaten mit ein.

Motivation: Der Nutzer muss eine Möglichkeit haben, seine persönliche Konfiguration zu löschen und alle Nutzerdaten unwiederbringlich zu entfernen. Andernfalls könnten diese Daten wiederhergestellt und missbraucht werden.

Umsetzungsbeispiel:

- Die Bedienungsanleitung enthält eine Beschreibung des Verfahrens zur Rücksetzung auf die werksseitigen Einstellungen.
- Die GSMA Terminal Steering Group beschreibt Empfehlungen für Local Data Wiping in einem Best Practices-Dokument.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.33-31/5.3

7.2. Web-Browser

Dieser Unterabschnitt gilt nur für Endgeräte, die über einen Web-Browser verfügen. Eingebettete Browserkontexte in Anwendungen erfüllen möglicherweise nicht alle genannten Anforderungen; Abweichungen sind im Einzelfall mit Group Security abzustimmen.

Req 38	Falls das Gerät über einen Web-Browser verfügt, dann muss dieser TLS (Transport Layer Security) gemäß neuesten Standards unterstützen.
--------	--

Aktuelle Standards sind zurzeit TLS ab Version 1.2.

Motivation: TLS (der Nachfolger von SSL) ist de facto die Standardmethode zur Absicherung von Datenübertragungen auf der Applikationsschicht.

Umsetzungsbeispiel: Aktueller Stand der Technik ist: TLS 1.3 wird unterstützt, es wird bei TLS die Version 1.2 oder höher erzwungen, und innerhalb von TLS 1.2 vorzugsweise nur solche Cipher Suites, die Perfect Forward Secrecy bieten.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.33-32/5.3

Req 39	Falls das Gerät über einen Web-Browser verfügt, dann muss in dem Web-Browser ein aktueller Satz von TLS-Root-Zertifikaten vorinstalliert sein.
--------	--

Motivation: Die Root-Zertifikate bilden die Vertrauensbasis für alle Server-Zertifikate für Websites.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.33-33/5.3

Req 40	Falls das Gerät über einen Web-Browser verfügt, dann muss es möglich sein, den Inhalt des Zertifikatsspeichers für den Web-Browser immer aktuell zu halten.
--------	---

Die Aktualisierung des Zertifikatsspeichers kann durch zeitnahe Bereitstellung von Patches erfolgen (z. B. für Geräte privater Endbenutzer) oder durch eine Möglichkeit, den Inhalt des Zertifikatsspeichers entfernt zu administrieren (z. B. für Geräte, die von Geschäftskunden genutzt / verwaltet werden).

Motivation: Die Root-Zertifikate bilden die Vertrauensbasis für alle Server-Zertifikate für Websites. Falls Zertifikate von Certification Authoritys (CAs) oder von Root-CAs kompromittiert werden (wie in der Vergangenheit bereits schon mehrfach geschehen - Comodo, DigiNotar), muss diese Information im Web-Browser verfügbar gemacht werden können.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.33-34/5.3

Req 41	Falls das Gerät über einen Web-Browser verfügt, dann muss dieser dem Nutzer sicherheitsrelevante Details zu HTTP-Verbindungen eindeutig anzeigen.
--------	---

Der Web-Browser muss dem Nutzer eindeutig anzeigen,

1. ob eine Verbindung abgesichert ist oder nicht,

2. was der Endpunkt der sicheren Verbindung ist,
3. welche Sicherheitsziele die Absicherung umfasst: (a) Vertraulichkeit (Verschlüsselung), (b) Integritätsschutz, (c) Authentifizierung.

Der Web-Browser muss die von ihm empfangenen TLS-Zertifikate dazu vollständig validieren. Im Falle einer fehlgeschlagenen Validierung muss der Browser dem Nutzer eine aussagekräftige und verständliche Warnung ausgeben mit dem Hinweis der nicht gewährleisteten Vertrauenswürdigkeit der Verbindung.

Motivation: Der Nutzer sollte wissen, ob er vertrauliche Daten eingeben und dem angezeigten Inhalt vertrauen kann.

Umsetzungsbeispiel: Anzeige eines Schlosssymbols (weit verbreitet bei Browsern, um auf TLS-Verbindungen hinzuweisen) zusammen mit dem Domännennamen oder allgemeinen Namen (common name) / der Organisation aus dem Zertifikat.

Inzwischen wird die Mehrzahl der Webseiten mit HTTPS (über TLS) ausgeliefert. Der Browser sollte auf eine ungesicherte Verbindung (HTTP ohne TLS) deutlich hinweisen, etwa durch Rotfärbung und den Hinweis "unsicher" oder "unsichere Verbindung".

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.33-35/5.3

Req 42	Falls das Gerät über einen Web-Browser verfügt, dann muss dieser dem Nutzer eindeutig anzeigen, ob eine Verbindung anhand eines Extended-Validation-Zertifikats (EV-TLS) abgesichert ist.
--------	---

Motivation: Die Ausgabe von Extended-Validation-Zertifikaten unterliegt strengeren Kriterien, wie im CA/Browser-Forum (siehe <http://www.cabforum.org/>) genau dargelegt wird. Extended-Validation-Zertifikate werden häufig für sicherheitskritische Applikationen wie Online-Banking verwendet.

Umsetzungsbeispiel: Andersfarbige Anzeige des Domännennamens oder allgemeinen Namens des Zertifikats (vorzugsweise grün). Die Anzeige des Domainnamens wird - auch auf kleinen Bildschirmen - nicht automatisch aus dem sichtbaren Bildschirmbereich gescrollt, damit der Benutzer nicht über den wahren Namen getäuscht werden kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.33-36/5.3

Req 43	Falls das Gerät über einen Web-Browser verfügt, dann muss der Web-Browser dem Nutzer anzeigen, wenn eine gesicherte Verbindung beendet (zu einer ungesicherten Verbindung umgeleitet) wird.
--------	---

Eine gesicherte Verbindung wird beendet, wenn das Protokoll von HTTPS zu HTTP wechselt. Die Information über den Wechsel zu einer unsicheren Verbindung muss für den Benutzer leicht erkennbar sein.

Motivation: Dies gibt dem Nutzer die Möglichkeit, Transaktionen abubrechen, die über unsichere Verbindungen erfolgen.

Umsetzungsbeispiel: Für unerfahrene Benutzer wird eine Dialogbox mit einem Hinweis eingeblendet. Erfahrene Benutzer können die wiederkehrende Anzeige der Dialogbox unterbinden. Eine Farbkodierung der URL-Eingabezeile und/oder von Eingabefeldern sorgt dafür, dass auch erfahrene Benutzer jederzeit erkennen, wenn eine Web-Seite ei-

ne unsichere Verbindung nutzt.

Inzwischen wird die Mehrzahl der Webseiten mit HTTPS (über TLS) ausgeliefert. Der Browser sollte auf eine ungesicherte Verbindung (HTTP ohne TLS) deutlich hinweisen, etwa durch Rotfärbung und den Hinweis "unsicher" oder "unsichere Verbindung".

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.33-37/5.3

7.3. Application Execution Environments (AEE)

Die Anforderungen in diesem Unterabschnitt gelten nur für Geräte, die die Installation zusätzlicher Applikationen erlauben oder aktive Inhalte bzw. einen heruntergeladenen Code ausführen können. Anwendungsausführungsumgebung (Application Execution Environment) kann das Betriebssystem selbst oder eine weitere Schicht oberhalb des Betriebssystems sein (z. B. Java Virtual Machine, Dalvik VM, Widget Runtime).

Hinweis: Für besondere Arten von Endgeräten (z. B. Mobiltelefone / Smartphones) sind in der Vergangenheit verschiedene Ansätze erörtert worden, so z. B. im OMTP-Rahmenmodell (Open Mobile Terminal Platform) für Applikationssicherheit (<http://wacapps.net/omtp>, vom März 2008). Die Mobile Terminal Requirements enthalten ebenfalls Anforderungen an Application Execution Environments.

Req 44	Falls das Gerät eine Ausführungsumgebung für Applikationen bietet, dann muss das Gerät einen Mechanismus bereitstellen, der die Integrität und Authentizität von zusätzlichem ausführbarem Programmcode wirksam verifiziert, bevor dieser Code ausgeführt wird.
--------	---

Motivation: Dies trägt dazu bei, dass die Ausführung schädlichen Codes verhindert wird.

Umsetzungsbeispiel:

- Code wird signiert und die Code-Signatur vor der Ausführung verifiziert (z. B. Microsoft Authenticode).
- Download von signiertem Code aus einem Application Store; das Gerät erzwingt Code-Signaturen (unsigned Code wird zurückgewiesen und kann nicht ausgeführt werden).

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten
- Unbemerkt durchführbare Angriffe

ID: 3.33-38/5.3

Req 45	Falls das Gerät eine Ausführungsumgebung für Applikationen bietet, dann muss es Mechanismen bereitstellen, die es dem Nutzer ermöglichen eine informierte Entscheidung darüber zu treffen, ob heruntergeladener Code ausgeführt werden darf und ob er Zugang zu den eventuell geforderten Daten bzw. lokalen Ressourcen erhält.
--------	---

Motivation: Mit diesen Mechanismen kann der Nutzer den Zugang zu seinen Daten effizient kontrollieren.

Umsetzungsbeispiel:

- Wenn Applikationen in der Regel vor der Veröffentlichung geprüft werden oder Entwickler wohlbekannt sind (z. B. durch App Store Ecosystems, Signing Schemes) und wenn die Applikation signiert ist, dann muss das Gerät diese Signatur verifizieren.
- Android zeigt dem Benutzer die Permissions (manifest.xml) neuer Anwendungen vor deren erstem Start.
- Android und iOS fragen den Benutzer während der Laufzeit, wenn diese App potenziell gefährliche Berechtigungen anfordert.

gungen (z. B. auf das Mikrofon, die Kamera, die Foto-Galerie, den Standort, etc.) nutzen möchte, ob der Benutzer der App diesen Zugriff gewähren möchte.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.33-39/5.3

Req 46	Falls das Gerät eine Ausführungsumgebung für Applikationen bietet und die Installation zusätzlicher Applikationen erlaubt, dann muss das Gerät verhindern, dass eine Applikation ohne Zustimmung des Nutzers installiert wird.
--------	--

Das Gerät kann eine vorherige ausdrückliche Initiierung durch den Nutzer vorschreiben.

Motivation: Jede Applikation enthält ausführbaren Code, der das Gerät potenziell Risiken aussetzt.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.33-40/5.3

Req 47	Falls das Gerät eine Ausführungsumgebung für Applikationen bietet und die Installation zusätzlicher Applikationen erlaubt, dann muss das Gerät einen Rückruf-Mechanismus für (böartige) Applikationen unterstützen.
--------	---

Motivation: Wenn das Ecosystem der Applikation mit gemanagten Netzen arbeitet, dann sollte das Gerät das entsprechende Management unterstützen.

Umsetzungsbeispiel: Stellt sich eine Applikation als „böartig“ heraus, kann der App Store Provider einen Recall (Rückruf) der Applikation durchführen, der das Gerät zur Deinstallation/Entfernung der böartigen Applikation veranlasst.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.33-41/5.3

Req 48	Falls das Gerät eine Ausführungsumgebung für Applikationen bietet, dann muss das Gerät diesen Applikationen geeignete Standardmechanismen (z. B. ein API) für eine sichere Datenübertragung bereitstellen.
--------	--

Motivation: Anhand solcher Mechanismen kann das Gerät übertragene Daten gemäß ihren Schutzanforderungen schützen.

Umsetzungsbeispiel:

- Die WebView / Widget Runtime eines Geräts implementiert eine Programmierschnittstelle (Application Programming Interface, API), mit deren Hilfe Anwendungen sichere TLS-Verbindungen herstellen können.
- Das Betriebssystem eines Geräts unterstützt VPN-Verbindungen nach gängigen Industriestandards.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.33-42/5.3

Req 49	Falls das Gerät eine Ausführungsumgebung für Applikationen bietet, dann muss es Mechanismen für die sichere Datenspeicherung, Zugriffskontrolle, Nutzer-Authentisierung und Autorisierung von Zugriffen auf geschützte Ressourcen bereitstellen.
--------	--

Diese Mechanismen sollten nicht nur sichere Mechanismen umfassen, mit denen erhöhte Sicherheitszustände erreicht werden können (durch erfolgreiche Authentifikation, vergleichbar einem „Login“) und mit denen der Zugriff auf Ressourcen autorisiert wird, sondern auch Mechanismen, mit denen solche Autorisierungen aufgehoben werden können, wenn sie nicht mehr benötigt werden (ähnlich einem „Logout“), z. B. Timeout, Logout-Button.

Motivation: Anhand dieser Mechanismen kann das Gerät den Zugriff auf lokal gespeicherte Daten beliebig kontrollieren.

Umsetzungsbeispiel:

- Betriebssysteme erlauben eine rollenbasierte Definition von Zugriffsrechten auf Ressourcen.
- Mobilfunk-Betriebssysteme (z. B. Android, iOS) bieten ihren Applikationen exklusiven Zugriff auf einen applikationsspezifischen nichtflüchtigen (persistenten) lokalen Speicherbereich. Dies verhindert den lesenden oder schreibenden (manipulierenden / löschenden) Zugriff einer böartigen Applikation auf alle übrigen auf dem Gerät gespeicherten Benutzerdaten. iOS7 erlaubt es dem Benutzer, für jede Applikation einzeln festzulegen, ob sie auf Lokationsinformation, Kontakte (Adressbuch), Kalender, Erinnerungen, Fotos, per Bluetooth freigegebene Daten, das Mikrofon oder Aktivitätsdaten (Schrittzähler etc.) zugreifen darf; der Benutzer kann eine einmal erteilte Zustimmung jederzeit auch wieder entziehen (siehe Einstellungen / Datenschutz).
- Mobile Betriebssysteme (Android, iOS) bieten Apps einen sicheren Speicher für Geheimnisse an (keychain).
- Falls Autorisierung auf Basis von Token implementiert ist, gibt es eine Möglichkeit, diese Token zu invalidieren, z. B. im Kundencenter.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.33-43/5.3

Req 50	Gespeicherte schutzbedürftige Daten müssen vor nicht autorisierter Einsichtnahme, Veränderung und Löschung geschützt werden.
--------	--

Der Schutzbedarf für gespeicherte Daten ist abhängig von deren Einstufung (beispielsweise nach geltenden gesetzlichen Datenschutzvorgaben, regulatorischen Auflagen, vertraglichen Verpflichtungen), dem Schadenspotential bei deren Missbrauch, sowie weiteren relevanten Faktoren (beispielsweise dem Ort der Speicherung). Art und Umfang von Schutzmaßnahmen müssen entsprechend angemessen gewählt werden.

Gespeicherte Authentisierungsmerkmale wie beispielsweise Passwörter, Private Keys, Tokens oder Zertifikate gelten grundsätzlich als schutzbedürftig. Ebenfalls als grundsätzlich schutzbedürftig gelten Daten, die Funktionalität und sicherheitsrelevantes Verhalten eines Systems bestimmen (z. B. System-Konfigurationsdateien, Betriebssysteme und Kernel, Treiber).

Die Einhaltung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit muss für gespeicherte schutzbedürftige Daten durchgängig gewährleistet werden. Dies gilt auch während einer lediglich kurzfristigen Speicherung (z. B. bei der Zwischenspeicherung in einem Web Cache oder in einem temporären Ordner innerhalb einer Datenverarbeitungskette).

Grundlegend muss der Zugriff auf schutzbedürftige Daten in einem System auf Basis von technisch implementierten Berechtigungsvergaben und -kontrollen vollumfassend reglementiert werden.

Reicht eine solche technische Zugriffskontrolle allein nicht mehr aus, um den erforderlichen Schutzbedarf gespeicherter Daten zu gewährleisten, oder kann deren Wirksamkeit nicht durchgängig sichergestellt werden, müssen zusätzlich kryptografische Verfahren (z. B. Verschlüsselung, Signierung, Hashing) implementiert werden. Bei der Speicherung von Daten eingesetzte kryptografische Verfahren müssen für diesen Zweck anerkannt wirksam sein und dürfen keine bekannten Schwachstellen aufweisen.

Motivation: Die Speicherung von Daten auf einem System ohne einen adäquaten Schutz ermöglicht es einem Angreifer, diese unberechtigt einzusehen, zu nutzen, zu verbreiten, zu verändern, oder zu vernichten. Dies eröffnet potenziell zusätzliche Angriffsvektoren auf die unmittelbaren sowie angeschlossene weitere Systeme und kann zu erheblichen Ausfällen, Kontrollverlusten und Schäden sowie resultierenden Strafzahlungsforderungen und Reputationsverlusten gegenüber Kunden und Geschäftspartnern führen.

Umsetzungsbeispiel: [Beispiel 1]

Ein System exportiert Daten für einen Transport auf einen mobilen Datenträger. Da die technische Zugriffskontrolle des Systems auf Dateiberechtigungsebene nicht mehr greift, sobald der mobile Datenträger aus dem System entfernt wird, müssen zusätzliche Maßnahmen zum Schutz der Daten getroffen sein. Bevor das System die Daten auf den mobilen Datenträger schreibt, werden sie entsprechend mit einem passenden Verfahren verschlüsselt. Der zugehörige Schlüssel wird auf einem separaten Kanal ausgetauscht, so dass die Daten im legitimen Zielsystem wieder entschlüsselt und verarbeitet werden können. Ein Angreifer, der den mobilen Datenträger in seinen Besitz bringt, hat hingegen keinen Zugriff auf die Daten.

[Beispiel 2]

In der lokalen Benutzer-Datenbank eines Systems werden nur kryptografische Hashes der Passwörter gespeichert, die mit einem als sicher geltenden Password-Hashing Verfahren erzeugt wurden. Für das System sind diese Hashes ausreichend, um die Benutzer bei einer Anmeldung am System zu authentifizieren. Sollte ein Angreifer die Benutzer-Datenbank kopieren können, gelangt er somit jedoch nicht unmittelbar in den Besitz von Klartext-Passwörtern, mit denen er sich am System im Namen der Benutzer anmelden könnte.

[Beispiel 3]

Auf einem System sind die Konfigurationsdateien des Web-Servers ausschließlich für den legitimen Admin schreibbar, in dem im Dateisystem entsprechende Berechtigungen gesetzt wurden. Die Zugriffskontrolle des Betriebssystem-Kernels verweigert somit allen anderen Benutzern des Systems, Veränderungen an den Konfigurationsdateien des Web-Servers vorzunehmen; einschließlich dem Web-Server Dienste-Konto selbst, was auch die Angriffsfläche von außen bei Schwachstellen im Web-Server verkleinert.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-14/9.0

Req 51	Schutzbedürftige Daten müssen während der Übertragung vor nicht autorisierter Einsichtnahme und Veränderung geschützt werden.
--------	---

Der Schutzbedarf von zu übertragenden Daten ist abhängig von deren Einstufung (beispielsweise nach geltenden gesetzlichen Datenschutzvorgaben, regulatorischen Auflagen, vertraglichen Verpflichtungen), dem Schadenspotential bei deren Missbrauch, sowie weiteren relevanten Faktoren (beispielsweise der Übertragung über öffentliche Netze). Art und Umfang der Schutzmaßnahmen müssen entsprechend angemessen gewählt werden.

Authentisierungsmerkmale wie beispielsweise Passwörter oder Tokens gelten grundsätzlich als schutzbedürftige Daten. Ebenfalls grundsätzlich als schutzbedürftig gelten Daten, die Funktionalität und sicherheitsrelevantes Verhalten eines Systems bestimmen (z. B. Updates & Patches, Konfigurationsparameter, Fernwartungen, Steuerung über APIs).

Die Einhaltung der Schutzziele Vertraulichkeit und Integrität muss während der Übertragung von schutzbedürftigen Daten durchgängig gewährleistet werden.

I.d.R. erfordert dies eine Implementation von kryptografischen Verfahren (z. B. Verschlüsselung, Signaturen, Hashes). Kryptografische Verfahren können

- vor der Übertragung direkt auf die Daten angewendet werden, was eine anschließende Übertragung der Daten auch über unsichere Kanäle vertretbar machen kann
- auf dem Übertragungs-Kanal eingesetzt sein, um einen sicheren Kanal zu schaffen und beliebige Daten, die durch diesen geleitet werden, zu schützen
- oder auch als Kombination aus beidem umgesetzt sein.

Bei der Übertragung von Daten eingesetzte kryptografische Verfahren müssen für diesen Zweck anerkannt wirksam sein und dürfen keine bekannten Schwachstellen aufweisen.

Motivation: Die Übertragung von Daten ohne einen adäquaten Schutz ermöglicht es einem Angreifer, diese unberechtigt abzufangen, zu nutzen, zu verbreiten, zu verändern oder aus der Übertragung zu entfernen. Dies eröffnet potenziell weitere Angriffsvektoren auf die unmittelbaren Zielsysteme sowie angeschlossene weitere Systeme und kann zu erheblichen Ausfällen, Kontrollverlusten und Schäden sowie resultierenden Strafzahlungsforderungen und Reputationsverlusten gegenüber Kunden und Geschäftspartnern führen.

Umsetzungsbeispiel: [Beispiel 1]

Vertrauliche Dokumente werden vor dem Versand per E-Mail an den Kunden verschlüsselt.

[Beispiel 2]

Ein Administrator konfiguriert eine neue Cloud-Anwendung über das Internet. Der Zugriff erfolgt über eine TLS-verschlüsselte Verbindung ("https").

[Beispiel 3]

Ein System bezieht automatische Software-Updates von einem Update-Server. Der Update-Server liefert die Software Updates kryptografisch signiert aus. Das System kann die empfangenen Software-Updates somit validieren und sicher ausschließen, dass diese während der Übertragung manipuliert wurden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-15/9.0

Req 52	Falls das Gerät eine Ausführungsumgebung für Applikationen bietet, dann muss das Gerät Applikationen in dedizierten Ausführungsumgebungen ausführen (Sandbox-Verfahren) und ihnen klare Schnittstellen für den Zugriff auf Nutzerdaten und Gerätefunktionen außerhalb des Applikationszusammenhangs bereitstellen mit der Möglichkeit, diesen Zugang zu beschränken.
--------	--

Weitergehende Zugriffe (über die durch die Sandbox auferlegten Grenzen hinweg) dürfen entweder gar nicht oder nur nach Bestätigung durch den Benutzer möglich sein. Zugriffe auf Geheimnisse dürfen nur im Rahmen wohldefinierter Protokolle möglich sein.

Motivation: Es muss möglich sein, solche Zugriffe (auf Daten oder lokale Ressourcen) zu kontrollieren, entweder durch vorkonfigurierte Regeln des Geräts oder durch Nutzerinteraktion (z. B. Eingabeaufforderungen).

Umsetzungsbeispiel: Das Betriebssystem des Geräts bietet wohldefinierte Schnittstellen (API) an, welche die oben genannten Einschränkungen durchsetzen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.33-46/5.3

8. Besondere Gerätefunktionen

Die Anforderungen in den nachstehenden Unterabschnitten gelten nur für das Endgerät, wenn es die entsprechende Funktionalität aufweist.

Req 53 Auf dem Gerät verfügbare Protokoll-Stacks müssen robust implementiert sein.

Motivation: Sind Protokoll-Stacks wie der IP-Stack oder SIP-Stack anfällig für gängige Bedrohungen, können möglicherweise entfernte (d. h. vom WAN-Netz initiierte) Denial-of-Service-Angriffe durchgeführt werden, oder ein entfernter Angreifer kann die Kontrolle über das Gerät übernehmen.

Umsetzungsbeispiel: Wohlbekannte Angriffe auf den IP-Protokoll-Stack werden erkannt und entschärft. Zum Nachweis seiner Robustheits-Eigenschaften wurden Fuzzing-Tests gegen das Gerät durchgeführt. An jeder aktiven Netzschchnittstelle ist ein Denial-of-Service (DoS)-Schutz aktiviert. - Informationen über wohlbekannte Angriffe findet man u.a. bei Organisationen wie www.sans.org.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Störung der Verfügbarkeit
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.33-47/5.3

8.1. Firewall

Req 54 Falls das Gerät über Firewall-Funktionalität verfügt und als mehrfach vernetzter (multi-homed) host agiert, dann muss die Firewall-Funktionalität ein starkes Endsystem-Modell gemäß [RFC1122](#) implementieren.

Eine Definition des Begriffs "multi-homed host" findet sich in Abschnitt 3.3.4.1 des [RFC1122](#).

Motivation: Dies trägt zum Schutz vor DNS-Rebinding-Angriffen bei, welche die Same-Origin-Policy umgehen.

Umsetzungsbeispiel: Ein Home Gateway übernimmt die Funktion eines mehrfach vernetzten Hosts (Netzwerke: LAN und Internet). Ein Smartphone kann als mehrfach vernetzter Host agieren, wenn es anderen Geräten über WiFi (Personal HotSpot) oder Bluetooth oder USB-Kabel Zugriff auf seine Mobilfunk-Internetverbindung gewährt (auch bekannt unter dem Namen "Tethering").

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.33-48/5.3

Req 55 Falls das Gerät über Firewall-Funktionalität verfügt, dann muss diese Funktionalität immer aktiv sein. Die Firewall-Funktionalität darf nicht durch einen Fehlerzustand, die Fehlbedienung eines Benutzers oder eine für den Benutzer zugängliche Konfigurationsoption deaktiviert werden können.

Diese Anforderung hindert das Gerät nicht daran, seinen administrativen Nutzern die Möglichkeit zur Konfiguration des Firewall-Regelsatzes zu geben, um Port Forwarding zuzulassen.

Motivation: Die Firewall ist eine sehr wichtige Sicherheitsfunktion des Geräts. Dieser Dienst muss immer aktiviert, stabil und fehlertolerant sein.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.33-49/5.3

Req 56	Falls das Gerät über eine Firewall-Funktionalität verfügt, dann dürfen an den Netzschnittstellen des Endgeräts im Auslieferungszustand nur die erforderlichen TCP-/UDP-Ports offen sein.
--------	--

Alle Ports, die nicht erforderlich sind, müssen dem Kunden im Auslieferungszustand des Geräts im Zustand „geschlossen“ bereitgestellt werden.

Motivation: Jeder offene Port stellt ein potenzielles Sicherheitsrisiko dar.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.33-50/5.3

Req 57	Falls das Gerät über Firewall-Funktionalität verfügt, dann muss die Firewall-Funktionalität ihren Regelsatz dynamisch an die Nutzung des Endgeräts anpassen.
--------	--

Die Firewall muss bei der Aktivierung/Deaktivierung von Diensten auf dem Gerät deren zugehörige Ports automatisch öffnen/schließen.

Motivation: Jeder offene Port stellt ein potenzielles Sicherheitsrisiko dar. Ist ein Dienst nicht konfiguriert und damit nicht funktionsfähig, darf auf ihn nicht über das Netz zugegriffen werden können. Nur bei den wenigsten Endnutzern wird es sich um qualifizierte Firewall-Administratoren handeln. Daher muss jede sinnvolle Methode zur automatischen Konfiguration einer sicheren Firewall implementiert werden.

Umsetzungsbeispiel: Wird ein Netzdienst (z. B. SIP-Client) aufgrund der Konfiguration des Endgeräts deaktiviert, schließt die Firewall automatisch alle mit dem Dienst verbundenen TCP/UDP-Ports (z. B. Port 5060/tcp) an allen Netzschnittstellen, an die der Dienst gebunden ist.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.33-51/5.3

Req 58	Falls das Gerät Firewall-Funktionalität, einen IPv4-Stack und NAT-Funktionalität (Network Address Translation) enthält, dann muss die Firewall eine NAT vom Typ „Port-restricted Cone“ implementieren.
--------	--

Eine Definition des „Port-restricted Cone NAT“-Szenarios findet sich in [RFC3489](#): Ein externer Host mit Source-IP-Adresse X und Source-Port P kann nur dann ein Paket an einen Port eines internen Hosts senden, wenn der interne Host zuvor ein Paket an Port P der IP-Adresse X gesendet hat.

Motivation: Damit wird sichergestellt, dass nur Antworten auf vom Endgerät gesendete Anforderungen weiter verarbeitet werden. Alle nicht angeforderten Pakete werden fallen gelassen.

Umsetzungsbeispiel: Ein Smartphone mit der Funktionalität Tethering bzw. Personal HotSpot muss "Port-restricted Cone" implementieren.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.33-52/5.3

8.2. Wireless LAN (WLAN / WiFi)

8.2.1. Wireless LAN Zugangspunkt-Funktionalität

Die nachstehenden Anforderungen gelten nur, wenn das Endgerät Zugang über Wireless LAN (WLAN / WiFi) bereitstellt, d. h., wenn es die Funktionalität eines WLAN Access Points (WLAN-Zugangspunkts) anbietet. Geräte mit WLAN Access Point-Funktionalität sind z. B. Home Gateways, WLAN-Brücken (Bridges), WLAN-Verstärker (Repeater) usw.

Req 59	Falls das Gerät über WLAN Access Point-Funktionalität verfügt, muss diese in der Voreinstellung Verschlüsselung mit WPA2 oder WPA3 und das CCMP-Protokoll nutzen.
--------	---

Motivation: Nutzer von Endgeräten verwenden ihre Geräte häufig in der Standardkonfiguration. Daher muss WLAN bereits in der Voreinstellung sicher konfiguriert sein. Angriffe gegen WPA2 (basierend auf AES und CCMP) sind seit 2017 möglich (sog. KRACK-Angriffe, siehe <https://www.krackattacks.com/>). WPA3 ist gegenwärtig Stand der Technik (seit 2018) und verhindert einige Angriffe gegen WPA2, aber nicht alle. Endgültige Abhilfe gegen KRACK-Angriffe wird voraussichtlich erst WPA3.1 schaffen. Bis dahin ist WPA2 immer noch weit verbreitet und als leidlich sicher anzusehen. - Die noch älteren Verfahren WPA (basierend auf RC4 und TKIP) sowie WEP sind unsicher und dürfen nicht verwendet werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.33-53/5.3

Req 60	Falls das Gerät über WLAN Access Point-Funktionalität verfügt, diese bei dem Gerät aktiviert ist und ein WPA2-Schlüssel (bzw. WPA3-Schlüssel) vorkonfiguriert ist, dann muss dieser Schlüssel ein zufälliger und geräteindividueller Wert von angemessener Länge und Komplexität sein, der keinen Bezug zu anderen Gerätedaten hat (d. h.: sich nicht von anderen öffentlich auslesbaren oder herleitbaren Daten ableiten lässt).
--------	---

Die für einen vorkonfigurierten Schlüssel erforderliche Komplexität muss mindestens der Komplexität entsprechen, die für einen vom Nutzer gewählten Schlüssel durchgesetzt wird.

Motivation: Ein erratbares oder standardmäßiges WLAN-Passwort ermöglicht Angriffe auf die WLAN-Schnittstelle. Im Internet verfügbare Tools erlauben sogenanntes „Wardriving“ (gezieltes Suchen schwach abgesicherter WLAN-Netze). Abhängigkeiten von anderen Gerätedaten lassen sich durch Reverse Engineering ermitteln, was zur Folge hat, dass Angreifer voreingestellte Schlüssel errechnen und durchprobieren können.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.33-54/5.3

Req 61	Falls das Gerät über WLAN Access Point-Funktionalität verfügt, diese bei dem Gerät aktiviert ist und kein WPA2-Schlüssel vorkonfiguriert ist, dann muss der Nutzer zur Eingabe eines Schlüsselwerts aufgefordert werden und das Endgerät muss eine Mindestschlüsselstärke durchsetzen.
--------	--

Die Anforderungen an die Komplexität (z. B. Mindestlänge, Zeichensatz) des WPA2/WPA3-Passworts hängen vom Endgerät, von seinen Möglichkeiten zur Passwordeingabe, vom Anwendungsfall und von anderen Faktoren, wie z. B. der Lesbarkeit von Zeichen, die auf einem Schild an der Rückseite des Geräts aufgedruckt sind, ab.

Motivation: Nur ein hinreichend starkes WPA2-Passwort kann garantieren, dass nur berechnete Personen Zugriff auf Ressourcen im WLAN erhalten. - Das von einem Home Gateway bereitgestellte WLAN bleibt in der Regel für lange Zeiträume sichtbar (Monate oder sogar Jahre), wird regelmäßig genutzt und ist stationär. Alle diese Aspekte machen es für einen Angreifer zu einem lohnenderen Ziel als einen Ad-hoc-Personal HotSpot, der von einem Smartphone z. B. im Zug bereitgestellt wird und nur ein paar Minuten (oder Stunden) lang sichtbar bleibt. Außerdem ist es möglicherweise schwieriger, Sonderzeichen über ein Smartphone einzugeben als über die PC-Tastatur, die für die Administration eines Home Gateways verwendet wird. Alle diese Faktoren sind bei der Festlegung der Passwortkomplexität zu berücksichtigen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.33-55/5.3

Req 62	Wenn das mobile Endgerät seine Internet-Verbindung freigeben kann (Tethering / Personal Hotspot), muss das Gerät jeglichen anderen Zugriff auf Geräte-Ressourcen (etwa auf dem mobilen Gerät gespeicherte Daten) durch Clients, welche diese Tethering-Funktionalität nutzen, verbieten, solange der Benutzer den Zugriff nicht explizit erlaubt hat.
--------	---

Motivation: Es wird angenommen, dass viele Benutzer ihre Internet-Verbindung für weitere Geräte oder gar für Freunde freigeben wollen – aber typischerweise wollen sie nicht den Zugriff auf alle Daten auf ihrem Gerät freigeben.

Umsetzungsbeispiel: Sofern über die Nutzung der Internet-Verbindung hinaus weitere Zugriffe auf Daten auf dem mobilen Endgerät ermöglicht werden sollen, müssen diese zuvor dem Geräteinhaber unmissverständlich angezeigt und von ihm bestätigt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.44-62/6.3

8.2.2. Wireless LAN (WLAN) Client-Funktionalität

Die nachstehenden Anforderungen gelten nur, wenn das Endgerät die Anbindung an ein Netz (z. B. das Internet) über WLAN ermöglicht.

Req 63	Falls das Gerät über WLAN-Client-Funktionalität verfügt, dann muss diese in der Voreinstellung Verschlüsselung mit WPA2 oder WPA3 und das CCMP-Protokoll nutzen.
--------	--

Motivation: Angriffe gegen WPA2 (basierend auf AES und CCMP) sind seit 2017 möglich (sog. KRACK-Angriffe, siehe <https://www.krackattacks.com/>). WPA3 ist gegenwärtig Stand der Technik (seit 2018) und verhindert einige Angriffe gegen WPA2, aber nicht alle. Endgültige Abhilfe gegen KRACK-Angriffe wird voraussichtlich erst WPA3.1 schaffen. Bis dahin ist WPA2 immer noch weit verbreitet und als leidlich sicher anzusehen. - Die noch älteren Verfahren WPA (basierend auf RC4 und TKIP) sowie WEP sind unsicher und dürfen nicht verwendet werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.33-56/5.3

Req 64	Falls das Gerät neben einem WLAN-Client auch Mobilfunkverbindungen unterstützt und über eine SIM/USIM/ISIM-Karte verfügt, muss es EAP-SIM (RFC4186) in Verbindung mit WLAN unterstützen.
--------	--

Motivation: EAP-SIM erlaubt eine Authentisierung im WLAN mittels SIM-Karte (GSM/2G).

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.44-64/6.3

Req 65	Falls das Gerät neben einem WLAN-Client auch Mobilfunkverbindungen unterstützt und über eine USIM/ISIM-Karte verfügt, muss es EAP-AKA (RFC 4187) in Verbindung mit WLAN unterstützen.
--------	---

Motivation: EAP-AKA erlaubt eine Authentisierung im WLAN mittels USIM-Karte (UMTS/3G und aufwärts).

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.44-65/6.3

8.3. Bluetooth-Funktionalität

Die nachstehenden Anforderungen gelten nur, wenn das Endgerät über einen Bluetooth-Stack verfügt.

Req 66	Falls das Gerät über Bluetooth-Funktionalität verfügt, dann muss das Gerät bei jeder eingehenden Pairing-Verbindungsanfrage eine Benutzerinteraktion erzwingen.
--------	---

Das Gerät darf keine Verbindungen, Dateien oder andere Objekte von unbekannten, nicht vertrauenswürdigen Quellen akzeptieren. Abhängig vom Endgerätetyp sollte Bluetooth außerdem standardmäßig deaktiviert sein und auch die Sichtbarkeit des Gerätes vom Benutzer gesteuert werden können.

Motivation: Der Benutzer muss stets die Kontrolle darüber behalten, welche anderen Bluetooth-Geräte sich mit seinem Endgerät verbinden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.33-57/5.3

Req 67	Falls das Gerät über Bluetooth-Funktionalität verfügt, dann müssen Bluetooth-Applikationen bzw. -Profile Konfigurations- oder Verbindungsaktivitätsanzeigen wie LEDs oder Desktop-Symbole verwenden.
--------	--

Motivation: Es muss für den Benutzer ersichtlich sein, welche Verbindungen bzw. Profile gerade aktiv sind.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unbemerkt durchführbare Angriffe

ID: 3.33-58/5.3

Req 68	Falls das Gerät über Bluetooth-Funktionalität verfügt, dann muss es alle Bluetooth-Geräte eindeutig identifizieren.
--------	---

Motivation: Der Benutzer muss eindeutig entscheiden können, mit welchem Gerät er eine Verbindung (Pairing) herstellen will. Bereits bei einmalig versehentlich falscher Paarung werden häufig schutzbedürftige Daten übertragen, z. B. das Mobiltelefon-Adressbuch an die falsche Freisprecheinrichtung im benachbarten PKW.

Umsetzungsbeispiel: Beispiel 1: Ein Bluetooth-Gerät zeigt als Gerätenamen seinen Produkt- und Modellnamen an, ggf. ergänzt um einen Teil der MAC-Adresse des Geräts.
Beispiel 2: Die Freisprecheinrichtung eines PKWs zeigt als Gerätenamen den Namen des PKW-Herstellers ergänzt um einen Teil der Fahrgestellnummer.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

ID: 3.33-59/5.3

Req 69	Falls das Gerät über Bluetooth-Funktionalität verfügt, dann muss das Gerät die verfügbaren Bluetooth-Sicherheitsmechanismen (Authentisierung, Verschlüsselung) nutzen.
--------	--

Abhängig vom Gerätetyp und den über Bluetooth übertragenen Daten muss das Gerät unverzüglich nach Herstellung der Bluetooth-Verbindung eine Bluetooth-Authentisierung einleiten (auch als Security Mode 3, Link Level-Sicherheit bezeichnet) und nach erfolgter gegenseitiger Authentisierung unverzüglich 128-Bit-Bluetooth-Verschlüsselung aktivieren.

Motivation: Ohne gegenseitige Authentisierung kann ein Angreifer sich unrechtmäßig als Gegenstelle ausgeben und man-in-the-middle-Angriffe durchführen. Ohne Verschlüsselung kann ein Angreifer die übertragenen Daten mitlesen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.33-60/5.3

Req 70	Falls das Gerät über Bluetooth-Funktionalität verfügt, dann muss das Gerät Bluetooth-Verbindungsschlüssel sicher erzeugen und sicher abspeichern.
--------	---

zur sicheren Erzeugung: Das Schlüsselaushandlungsprotokoll BR/EDR, welches während der Paarung von Bluetooth-Geräten verwendet wird, muss eine Gegenmaßnahme gegen die sog. KNOB-Attack implementieren (vgl. <https://knobattack.com>). Beispielsweise kann eine minimale Entropie von 16 Bytes erzwungen werden. Alternativ kann die Integrität des Schlüsselaushandlungsprotokolls mit dem Link Key geschützt werden. Wenn die Bluetooth Special Interest Group die Spezifikation aktualisiert hat, muss die spezifizierte Gegenmaßnahme implementiert werden.
zur sicheren Speicherung: Es müssen die Möglichkeiten zur sicheren Schlüsselspeicherung genutzt werden, die das Endgerät bietet.

Motivation: zur sicheren Erzeugung: Bei der KNOB-Attack sorgt ein Angreifer im Rahmen der Schlüsselaushandlung

dafür, dass die Entropie für die Schlüsselableitung nur ein Byte lang ist, so dass nur 256 mögliche Schlüssel abgeleitet werden können, die ein Angreifer problemlos alle durchprobieren und so den verwendeten identifizieren kann. zur sicheren Speicherung: Es muss verhindert werden, dass unbefugte Prozesse Zugriff auf die Verbindungsschlüssel erhalten, andernfalls könnte sich ein von einem Angreifer kontrolliertes Gerät fälschlicherweise als authentisierter Bluetooth-Kommunikationspartner ausgeben und auf diese Weise könnten schutzbedürftige Daten abfließen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

ID: 3.33-61/5.3

8.4. Web-Administrations-Oberfläche

Req 71 Sitzungen müssen gegen eine unautorisierte Übernahme ("Session Hijacking") geschützt werden.

In Schnittstellen, die Funktionen für Sitzungen zum System bereitstellen, müssen technische Maßnahmen implementiert werden, die verhindern, dass die Sitzung eines legitimen Benutzers von einem nicht autorisierten Dritten übernommen und weitergeführt werden kann.

Ein derartiger Schutz kann beispielsweise durch die Umsetzung einer für das spezifische System sinnvollen Kombination aus den folgenden Optionen erreicht werden:

- Auf der Transportschicht: Verwendung des TCP-Protokolls (mit dessen Sequenz-Nummern) und entsprechenden Filterlisten
- Auf der Sitzungsschicht: Verwendung des TLS-Protokolls
- Auf der Applikationsschicht: Aushandlung eines zufälligen geheimen Sitzungsschlüssels zwischen Sender und Empfänger zwecks Autorisierung allen Sitzungsverkehrs (z. B. Session-ID, Session Cookie, Session Token)
- Nutzung kryptographischer Verfahren zum Schutz von Sitzungsschlüsseln vor Ausspähung oder Veränderung

Motivation: Ungeschützte Sitzungen können potenziell von einem Angreifer gekapert und weitergeführt werden, um darüber im Kontext des betroffenen Benutzers unberechtigte Zugriffe auf das System auszuüben.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.01-16/9.0

Req 72 Das System muss es Benutzern ermöglichen, sich von ihrer laufenden Sitzung abzumelden.

Das System muss über eine Funktion verfügen, die es dem angemeldeten Benutzer ermöglicht, sich jederzeit abzumelden. Die Wiederaufnahme einer abgemeldeten Sitzung darf nicht ohne erneute und erfolgreiche Authentifizierung des Benutzers möglich sein.

Motivation: Ein Benutzer muss die vollständige Kontrolle über von ihm aufgebaute Sitzungen behalten, um jederzeit situationsgerecht seinen Zugriff auf ein System zu beenden und damit über diesen Zugriff exponierte Daten und Funktionen schützen zu können. Zudem muss der Benutzer davon ausgehen können, dass durch ihn gezielt beendete Sitzungen nicht im Anschluss durch unberechtigte Dritte wieder aufgenommen und weitergeführt werden können.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.01-17/9.0

Req 73	Sitzungen müssen nach einer dem Verwendungszweck angepassten Zeit der Inaktivität automatisch beendet werden.
--------	---

Es ist notwendig, dass Sitzungen auf einem System nach einer vorgegebenen Zeit der Inaktivität automatisch beendet werden.

Aus diesem Grund muss ein Time-Out für Sitzungen gesetzt werden. Der hier zu wählende Zeitraum richtet sich nach der Verwendung des Systems und ggf. nach der physischen Umgebung. So ist beispielsweise der Time-Out für eine Anwendung, die in einer ungesicherten Umgebung genutzt wird, kürzer (wenige Minuten) zu wählen als der Time-Out für eine Anwendung, die von Betriebsmitarbeitern für System-Monitoring-Aufgaben in einem zugangsgeschützten Bereich genutzt wird (60 Minuten und länger).

Motivation: Für eine offene, aber ungenutzte Sitzung besteht ein Risiko, dass ein nicht legitimierter Benutzer diese unbemerkt übernimmt und weiterführt, um im Namen des betroffenen Benutzers einen nicht autorisierten Zugriff auf das System und enthaltene Daten auszuüben.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.01-18/9.0

8.5. Passwörter

Req 74	Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss eine Änderung des eigenen Passwortes jederzeit durch den Benutzer möglich sein.
--------	---

Das System muss eine Funktion bieten, die es einem Benutzer ermöglicht, sein Passwort jederzeit zu ändern.

Bei der Verwendung eines zentralen Systems darf die Funktion auf dieses System weitergereicht oder ausgelagert werden.

Motivation: Nur durch die Möglichkeit, dass ein Benutzer sein Authentisierungsmerkmal jederzeit selbstständig ändern kann, ist ein zeitnahe Änderung möglich, wenn der Benutzer den Verdacht hat, dass dieses in den Besitz Dritter gelangt sein könnte.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-29/9.0

Req 75	Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss ein Schutz gegen Online-Angriffe wie Wörterbuch- und Brute-Force-Attacks vorhanden sein, der das Erraten von Passwörtern stark erschwert.
--------	---

Online Wörterbuch- und Brute-Force Angriffe haben zum Ziel, durch automatisiertes Ausprobieren an einer regulären Zugangsschnittstelle des Systems die Passwörter von Benutzerkonten zu erraten.

Um dies zu verhindern, muss eine der folgenden Maßnahmen oder eine Kombination aus diesen umgesetzt werden:

- mittels technischer Maßnahmen abgebildete Erzwingung einer Wartezeit nach einem fehlgeschlagenen Anmeldeversuch, bevor eine erneute Anmeldung ermöglicht wird. Die Wartezeit sollte sich zudem mit jedem weiteren fehlgeschlagenen Anmeldeversuch automatisch deutlich erhöhen (z. B. durch Verdopplung).
- automatisiertes Sperren des Benutzerkontos nach einer vorgegebenen Anzahl von aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen (typischerweise 5). Allerdings ist bei dieser Lösung zu bedenken, dass diese einen Entsperrungs-Prozess erforderlich macht und ein Angreifer dies gezielt nutzen kann, um Konten zu sperren und somit vorübergehend unbrauchbar zu machen.
- Verwendung von CAPTCHA ("Completely Automated Public Turing test to tell Computers and Humans Apart"), um automatisierte Anmeldeversuche von Maschinen ("Robots" oder "Bots") bestmöglich zu unterbinden. Ein CAPTCHA stellt dazu eine kleine Aufgabe, i. d. R. basierend auf grafischen oder akustischen Elementen, die von einer Maschine nur schwer zu lösen ist. Es ist entsprechend zu berücksichtigen, dass CAPTCHA problematisch bzgl. der Barrierefreiheit sein können.

Um eine höhere Sicherheit zu erreichen, ist es oftmals sinnvoll, zwei oder mehrere der genannten Maßnahmen miteinander zu kombinieren. Dies ist abhängig vom Einzelfall zu prüfen und entsprechend umzusetzen.

Motivation: Ohne entsprechenden Schutz kann ein Angreifer durch bloßes Durchprobieren von Wörterbuchlisten oder automatisch erzeugten Zeichenkombinationen versuchen ein Passwort zu ermitteln, um so das entsprechende Benutzerkonto missbräuchlich zu nutzen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.01-25/9.0

8.6. Mobilfunk-Endgeräte

Req 76	Der Chipsatz des Geräts muss eine Technik zur Abwehr von Buffer Overflow-Angriffen auf den Mobilfunk-Stack implementieren.
--------	--

Motivation: Angreifer könnten einen Aufbau verwenden (z. B. bestehend aus Universal Software Radio Peripheral, USRP, mit Software OpenBTS), der eine Kommunikation ermöglicht, welche nicht konform zu den 3GPP-Protokollen ist, mit dem Ziel einen Pufferüberlauf (Buffer Overflow) des Mobilfunk-Stacks des Gerätes die Ausführung eigenen Codes zu erzwingen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Störung der Verfügbarkeit
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

Req 77 Die IMEI muss manipulationssicher im Gerät gespeichert und verarbeitet werden.

Motivation: In einigen Ländern besteht die gesetzliche Verpflichtung, gestohlene Geräte auf eine schwarze Liste (blacklist) gestohlener Geräte setzen zu können. SIM-Lock-Funktionalität hängt ebenfalls von der Korrektheit der IMEI ab. Schließlich gibt es netzseitige Workarounds für Endgerätefehler, die teilweise auch sicherheitsrelevant sind; auch diese Workarounds hängen von der IMEI ab.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

Req 78 Das Gerät muss den Zugriff auf Geheimnisse des Mobilfunknetzwerks, die vom Baseband verarbeitet werden (wie etwa RAND, SRES, Kc, AUTN, CK und IK), verhindern.

Die Anwendung kann im Kontext der Generic Bootstrapping Architecture (GBA) über wohldefinierte Schnittstellen ein Zugriff auf RAND gewährt werden. Entsprechende Regeln können auf dem Gerät vorkonfiguriert werden.

Motivation: Geheimnisse des Mobilfunknetzwerks müssen geschützt werden.

Umsetzungsbeispiel: Aktuelle Versionen bekannter mobiler Betriebssysteme (Android, iOS) setzen diese Anforderung um.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

Req 79 Dienste des Mobilfunkanbieters dürfen nicht mehr verfügbar sein, nachdem die SIM/USIM/ISIM-Karte aus dem Gerät entfernt wurde. Entsprechende Schlüssel müssen gelöscht werden.

Notrufe bleiben von dieser Anforderung unberührt. Die vom Gerät zu löschenden Schlüssel umfassen Kc, CK und IK. Das gleiche gilt sinngemäß für die Generic Bootstrapping Architecture (GBA).

Motivation: Nachdem die SIM/USIM-Karte entfernt wurde, darf ein mobiles Endgerät gemäß 3GPP nur noch Notrufe absetzen können. Siehe auch 3GPP TS 33.220.

Umsetzungsbeispiel: Aktuelle Versionen bekannter mobiler Betriebssysteme (Android, iOS) setzen diese Anforderung um.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

Req 80 Mobile Endgeräte müssen UICCs unterstützen, welche eine USIM unterstützen.

AKA bezeichnet den Authentication and Key Agreement Algorithmus, USIM eine Universal SIM (UMTS-fähige SIM-Application, mit stärkeren Schlüsseln), und UICC eine Universal Integrated Circuit-Card, also eine SIM-Karte mit installierter USIM-Application. Diese Anforderung ermöglicht es, UMTS AKA oder neuere AKA-Algorithmen (EPS AKA, EAP-AKA) zu verwenden, welche besser Sicherheit bieten als der 2G-Algorithmus GSM AKA. Unterstützung von USIMs war in der Vergangenheit optional (vor Rel-5 für mobile Endgeräte, die nur GERAN unterstützen, siehe Abschnitt 13.1.3 in 3GPP TS 22.101. Einige Gerätehersteller mischen immer noch Features aus verschiedenen Releases.

Motivation: Mobilfunkkunden erwarten Sicherheit auf dem Niveau einer USIM (mit Authentifizierung des Mobilfunknetzes und 128 Bit Schlüssellänge), wenn sie über eine UICC mit USIM-Applikation verfügen. Endgeräte ohne USIM-Unterstützung würden diese Erwartung nicht erfüllen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.44-80/6.3

Req 81 Das Gerät muss 128-Bit lange Verschlüsselungsschlüssel (Kc128) für GSM und GPRS unterstützen.

128-Bit-Schlüssel und Algorithmen dürfen und müssen mit ihren 64-Bit-Varianten koexistieren, solange es noch Kunden mit alten SIM-Karten gibt, auf denen nur 64-Bit-Schlüssel gespeichert sind. Erst eine USIM kann 128-Bit-Schlüssel bereitstellen. Siehe auch 3GPP TS 33.102 (3G Security Architecture), Abschnitt 6.8.1.1.

Motivation: Unterstützung für Kc128 wird benötigt, um die Verschlüsselungsalgorithmen A5/4 und GEA4 zu ermöglichen. A5/4 wird im Mobilfunknetz des Deutschen Telekom Konzerns seit 2021 unterstützt.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.44-81/6.3

Req 82 Wenn das mobile Endgeräte GERAN Mobilfunk unterstützt, muss es Layer 2 Fill Bits Randomization im Uplink und Downlink implementieren.

Die Anforderung wurde mit 3GPP Rel-9 als Standard-Feature eingeführt, siehe 3GPP TS 44.006, Abschnitt 5.2, aber sie muss in jedem neuen mobilen Endgerät, unabhängig vom 3GPP Release, implementiert werden. GERAN (GSM EDGE Radio Access Network, häufig abgekürzt zu EDGE) wird immer noch zur Datenübertragung verwendet (Messaging, E-Mail), wenn nur 2G-Mobilfunkabdeckung verfügbar ist.

Motivation: Diese Funktion entfernt bekannten Klartext aus 2G Radio Frames und erschwert dadurch kryptographische Angriffe.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.44-82/6.3

Req 83	Falls das Gerät 5G unterstützt, muss es Elliptic Curve Integrated Encryption Scheme (ECIES) verwenden, um die SUPI zu verschlüsseln.
--------	--

Aus Datenschutzgründen sollte die SUPI (Subscription Permanent Identifier, entspricht der IMSI bei 2G/3G/4G) von 5G-Endgeräten nicht im Klartext übertragen werden und wird stattdessen in der den Datenschutz wahrenden SUCI (Subscription Concealed Identifier) verschlüsselt. Als Konsequenz wird der Datenschutz der SUPI auf der Luftschnittstelle des 5G-Mobilfunknetzes gewährleistet, indem stattdessen die SUCI genutzt wird. Für SUCIs, welche eine IM-SI-basierende SUPI enthalten, verschleiert das UE (user equipment) im Wesentlichen den MSIN-Teil (Mobile Subscriber Identification Number) der IMSI. Auf 5G-Netzbetreiberseite ist die SIDF-Funktion (Subscription Identifier De-concealing Function) des UDM (Unified Data Management) für die Entschlüsselung der SUCI verantwortlich und leitet die SUPI aus der SUCI basierend auf dem Schutzmechanismus, der beim Generieren der SUCI verwendet wurde, ab. Siehe auch 3GPP TS 33.501 (5G Security Architecture, rel. 17), annex C.3.1.

Motivation: Die Verwendung der Verschlüsselung/Verschleierung schützt die Privatsphäre des Mobilfunkkunden, denn er kann dann nicht durch Mitlauschen auf der Luftschnittstelle identifiziert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

ID: 3.44-83/6.3

Req 84	Das Gerät muss Integritätsschutz der übertragenen Daten unterstützen und erzwingen.
--------	---

- Diese Anforderung bekräftigt die Forderung, dass Integritätsschutz immer verwendet werden muss, auch wenn viele Implementierungen es erlauben, den Integritätsschutz abzuschalten, z. B. für Testzwecke.
- Für UMTS muss das mobile Endgerät Integritätsschutz der übertragenen Daten mit den Algorithmen UIA1 (Kasumi) und UIA2 (SNOW 3G) unterstützen und erzwingen.
- Der 3GPP-Standard 3GPP TS 33.102 (Abschnitte 6.4.2 "1" and 6.5.6) fordert, dass mobile Endgeräte Integritätsschutz verwenden und die Verbindung beenden, falls die andere Seite (Mobilfunknetzwerk) keinen Integritätsschutz unterstützt. Ab Rel-7 aufwärts fordert 3GPP TS 33.102 außerdem die Unterstützung von UIA2 (SNOW 3G) in Mobilfunknetzwerken und mobilen Endgeräten.
- Für LTE/EPC muss das mobile Endgerät Integritätsschutz für die NAS (Non-Access Stratum) und RRC (Radio Resource Control) Signalling Plane erzwingen. RRC Signalling gehört zum Access Stratum (AS). 3GPP TS 33.401 Abschnitt 5.1.4 fordert, dass sowohl Mobilfunknetzwerke als auch mobile Endgeräte Integritätsschutz verwenden und Verbindungsversuche terminieren, falls die andere Seite keinen Integritätsschutz unterstützt.
- Für LTE/EPC muss das mobile Endgerät die Integritätsschutzalgorithmen EIA1 (SNOW 3G) und EIA2 (AES) für NAS und RRC (AS) Signalling Plane unterstützen. 3GPP TS 33.401 Abschnitt 5.1.4.2 fordert und diese Anforderung bekräftigt, dass immer beide Algorithmen (EIA1 und EIA2) unterstützt werden müssen, auch wenn einige Hersteller versuchen, nur einen von beiden zu implementieren. Einer der beiden Algorithmen muss genutzt werden. EIA2 wird im Mobilfunknetzwerk als bevorzugter Algorithmus gesetzt, weil er ausführlicher getestet wurde.
- Für 5GC (5G Core) muss das mobile Endgerät Integritätsschutz für User Plane, NAS und RRC (AS) Signalling Plane erzwingen. Auf der einen Seite wird dies durch User Plane Integrity Protection (UPIP) realisiert. Das Endgerät soll den Integritätsschutz der User Data basierend auf der vom gNB gesendeten Indikation aktivieren (siehe 3GPP TS 33.501 Abschnitt 5.3.3). Auf der anderen Seite fordert 3GPP TS 33.501, dass sowohl Mobilfunknetzwerk (ng-eNB, gNB und AMF) als auch mobile Endgeräte Integritätsschutz verwenden und Verbindungsversuche terminieren, falls die andere Seite keinen Integritätsschutz unterstützt. Falls E-UTRA mit dem 5GC verbunden ist, dann muss das Endgerät anzeigen, dass es UPIP mit einem ng-eNB unterstützt.
- Für 5GC muss das mobile Endgerät die Integritätsschutzalgorithmen NIA0 (Notruef), 128-NIA1 (SNOW 3G) und 128-NIA2 (AES) für NAS und RRC (AS) Signalling Plane unterstützen. NIA2 wird im Mobilfunknetzwerk ak-

tiert und als bevorzugter Algorithmus gesetzt. 3GPP TS 33.501 Abschnitt 5.2.3 fordert und diese Anforderung bekräftigt, dass immer beide Algorithmen (NIA1 und NIA2) unterstützt werden müssen, auch wenn einige Hersteller versuchen, nur einen von beiden zu implementieren. Einer der beiden Algorithmen muss genutzt werden. NIA2 wird im Mobilfunknetzwerk als bevorzugter Algorithmus gesetzt, weil er ausführlicher getestet wurde.

- Der Integritätsschutz von Notrufen hängt von der erfolgreichen Authentifizierung ab (für UMTS siehe 3GPP TS 33.102 Abschnitt 6.4.9, für LTE/EPC siehe 3GPP TS 33.401 Abschnitt 15 und für 5GC siehe 3GPP TS 33.501 Abschnitt 10).

Motivation: Der Schutz der Integrität ist ein wesentlicher Sicherheitsmechanismus. Er unterstützt u.a. die korrekte Abrechnung (Billing) und verhindert Man-in-the-middle-Angriffe und die Veränderung von Nachrichten. LTE/EPC und 5GC wurden von Beginn an mit zwei Sicherheitsalgorithmen entwickelt, um einen schnellen Umstieg zu ermöglichen, falls ein Algorithmus gebrochen werden sollte.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten

ID: 3.44-84/6.3

Req 85	Das Gerät muss den Schutz der Vertraulichkeit der übertragenen Daten unterstützen und erzwingen.
--------	--

Das mobile Endgerät muss Algorithmen gemäß dem International Settings Document (ISD) für Portfolio-Endgeräte unterstützen. Das ISD ist Teil des Portfolio Selection Prozesses (PSP). Der PSP stellt Anforderungen für mobile Endgeräte auf (Mobile Terminal Requirements, MTRs), die als sog. Portfolio Devices vom Deutsche Telekom Konzern ausgewählt werden. Gewisse Anforderungen an das Verhalten der Geräte werden im sog. International Settings Document (ISD) beschrieben, beispielsweise soll GEA4 vom Endgerät unterstützt werden, aber noch so lange im Gerät deaktiviert bleiben, bis GEA4 auch im Live-Mobilfunknetz ausgerollt und die Interoperabilität ausreichend getestet wurde.

Die folgenden Algorithmen müssen unterstützt werden:

- Für GPRS: GEA1 darf vom mobilen Endgerät nicht unterstützt werden. GEA3 muss unterstützt werden. Falls GEA2 auch unterstützt wird, muss GEA3 gegenüber GEA2 bevorzugt werden.
- Für GSM: Das mobile Endgerät muss A5/3 und A5/4 unterstützen und es muss A5/4 gegenüber A5/3 bevorzugen.
- Für UMTS: Das mobile Endgerät muss den Schutz der Vertraulichkeit übertragener Daten mit dem Algorithmus UEA1 (Kasumi) unterstützen und erzwingen.
- Für LTE/EPC: Das mobile Endgerät muss den Schutz der Vertraulichkeit übertragener Daten von User Plane, NAS and RRC (AS) Signalling Plane erzwingen und es muss dazu die Algorithmen EEA1 (SNOW 3G) und EEA2 (AES) unterstützen.
- Für 5GC: Das mobile Endgerät muss den Schutz der Vertraulichkeit übertragender Daten von User Plane, NAS and RRC (AS) Signalling Plane erzwingen und es muss dazu die Algorithmen NEA1 (SNOW 3G) und NEA2 (AES) unterstützen.
- Die Verschlüsselung von Notrufen hängt von der erfolgreichen Authentifizierung ab (für UMTS siehe 3GPP TS 33.102 Abschnitt 6.4.9; für LTE/EPC siehe 3GPP TS 33.401 Abschnitt 15; für 5GC siehe 3GPP TS 33.501 Abschnitt 10).

Motivation: Eine gemeinsame Menge von Algorithmen ist erforderlich um eine sichere Interoperabilität zu ermöglichen. Gewisse Dienste wie SMS Transaktionsnummern (TAN) oder One-Time PIN/Password (OTP) verlassen sich auf eine gesicherte Nachrichtenübertragung.

A5/0 (null encryption) wird typischerweise vom Mobilfunknetz verboten. A5/2 wird als schwach angesehen und selbst

A5/1 wird nicht mehr als sicher genug angesehen. Falls A5/2 im Endgerät nicht entfernt oder dauerhaft abgeschaltet wird, kann eine False Base Station das Endgerät zwingen, A5/2 zu verwenden und dann den Algorithmus brechen und so den GSM-Verschlüsselungsschlüssel Kc berechnen. A5/4 nutzt denselben Basis-Algorithmus wie A5/3 (Kasumi), aber mit einem 128 Bit langen Schlüssel (anstelle der 64 Bit bei A5/3). Bei A5/3 kann der 64-Bit-Schlüssel Kc durch einen Key Recovery-Angriff kompromittiert werden, wenn das Endgerät GEA1 unterstützt (siehe unten). A5/4 ist durch diesen Angriff nicht verwundbar.

Im April 2021 wurde ein Key Recovery-Angriff veröffentlicht, der sich gegen alle mobilen Endgeräte richtet, welche GEA1 unterstützen. Die Veröffentlichung erfolgte im Rahmen des GSMA Coordinated Vulnerability Disclosure (CVD) Programms (GSMA CVD-2020-0041). Mit diesem Angriff kann der 64-Bit-Schlüssel Kc kompromittiert werden; deshalb beeinflusst der Angriff sowohl die Sicherheit von GSM-Anrufen und SMS als auch die von GPRS-Datenverbindungen. Ein Angreifer, der mit Kc verschlüsselte Übertragungen über die Luftschnittstelle aufzeichnen kann, kann diese sogar später entschlüsseln, nachdem er Kc kompromittiert hat. Deshalb stellt bereits die bloße Unterstützung von GEA1 durch das mobile Endgerät eine Schwachstelle dar, die auch die Sicherheit starker Algorithmen wie A5/3 und GEA3 untergräbt, denn diese nutzen den gleichen 64-Bit-Schlüssel Kc. Mobile Endgeräte, die GEA1 nicht unterstützen, sind nicht verwundbar. Datenübertragungen mit GEA4 (mit 128 Bit Schlüssellänge) sind ebenfalls nicht verwundbar - aber GEA4 wird üblicherweise noch nicht auf mobilen Endgeräten unterstützt.

Ab Rel-7 aufwärts fordert der 3GPP standard 3GPP TS 33.102, Abschnitt 6.6.6, auch Unterstützung von UEA2 (SNOW3G) im Mobilfunknetz und in mobilen Endgeräten.

LTE/EPC and 5GC (5G Core) wurden von Beginn an mit zwei Sicherheitsalgorithmen entwickelt, um einen schnellen Umstieg zu ermöglichen, falls ein Algorithmus gebrochen werden sollte.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

ID: 3.44-85/6.3

8.7. Einsatz bei Geschäftskunden

Req 86	Falls das Gerät von Geschäftskunden eingesetzt werden können soll, dann muss das Gerät die hierfür erforderliche Funktionalität durch entsprechende Schnittstellen zusätzlich unterstützen.
--------	---

Falls das Gerät von Geschäftskunden eingesetzt werden können soll, dann muss das Gerät folgende Funktionalität durch entsprechende Schnittstellen zusätzlich unterstützen:

- Zentrale Verwaltung und Provisionierung von Policies,
- Erzwingen der Policy, einschließlich der Möglichkeit, nicht Policy-konforme Geräte vom Zugang zum Firmennetz auszuschließen,
- zentrale Verwaltung und Provisionierung von Anwendungen,
- zentrale Verwaltung und Provisionierung von Patches (Firmware, Betriebssystem, Anwendungen) einschließlich Verfolgung des aktuellen Gerätestatus',
- zentrale Verwaltung und Provisionierung von Zertifikaten und Schlüsselmateriale,
- zentral gesteuerte Passwort-Rücksetzung,
- Schutz gegen Schadsoftware.

Motivation: Der geschäftliche Einsatz einer großen Anzahl von mobilen Endgeräten durch Geschäftskunden erfordert zusätzliche Schnittstellen, um eine dauerhafte Sicherheit und Administrierbarkeit zu gewährleisten.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen

- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.44-86/6.3

Req 87	Falls das Endgerät vollständig von der Deutschen Telekom gemanaged und betrieben wird, müssen für sicherheitsrelevante Protokollierungsdaten, die lokal erfasst werden, geltende Aufbewahrungszeiträume und Löschfristen eingehalten werden.
--------	--

Aus Sicht der IT-Sicherheit wird auf einem System die lokale Erfassung von sicherheitsrelevanten Protokollierungsdaten nicht zwingend gefordert. Da lokal erfasste Protokollierungsdaten bei Systemstörungen beschädigt oder von einem erfolgreichen Angreifer gezielt manipuliert werden können, sind sie für sicherheitstechnische bzw. forensische Analysen nur bedingt belastbar. Entsprechend ist für die IT-Sicherheit relevant, dass Protokollierungsdaten an einen separaten Log Server weitergeleitet werden.

Eine lokale Erfassung kann dennoch erfolgen; beispielsweise falls bei der Erzeugung der Protokollierungsdaten eine lokale Speicherung aufgrund technischer Abläufe zunächst unabdingbar ist oder es begründete betriebliche Interessen gibt, Protokollierungsdaten auch lokal vorzuhalten.

Von der Deutschen Telekom an Endkunden vermietete Endgeräte (z. B. Speedport) gelten nicht als vollständig von der Telekom gemanaged und betrieben. Das gilt sogar dann, wenn Easy Support eingeschaltet ist (automatisches Firmware-Update). Die Verantwortung für den Betrieb und damit auch für Protokollierungsdaten liegt hier beim Endkunden. Ein Beispiel für vollständig von der Telekom verwaltete und betriebene Geräte sind Edge-Router von Geschäftskundenanschlüssen.

Folgende Grundregelung ist bei einer lokalen Erfassung von Protokollierungsdaten zu berücksichtigen:

- sicherheitsrelevante Protokollierungsdaten müssen für einen Zeitraum von 90 Tagen aufbewahrt werden.^[1*]
- nach Ablauf von 90 Tagen muss eine umgehende Löschung von gespeicherten Protokollierungsdaten erfolgen.

^[1*] Diese Anforderung gilt nur, falls auf dem System keine zusätzliche Weiterleitung an einen separaten Log Server umgesetzt ist und Protokollierungsdaten daher ausschliesslich lokal erfasst werden.

Abweichungen

Abweichende Aufbewahrungszeiträume und Löschfristen können durch gesetzliche oder regulatorische Anforderungen (insbesondere im Zusammenhang mit personenbezogenen Daten) bestehen oder durch vertragliche Vereinbarungen definiert sein. In diesen Fällen sind die geltenden Zeiträume individuell mit einem Project Security Manager (PSM) bzw. Datenschutzberater (DSB) abzustimmen oder werden durch diesen vorgegeben.

Motivation: Protokollierungsdaten sind ein immens wichtiges Werkzeug der IT Sicherheit zur Abwendung, Detektierung und Aufklärung von Systemstörungen, Sicherheits- und Datenschutzvorfällen. Auf der anderen Seite unterliegt die Erfassung von Protokollierungsdaten wie jede andere Datenverarbeitung auch gesetzlichen und regulatorischen Auflagen. Entsprechend müssen Richtlinien eingehalten werden, die beides in Einklang bringen.

Umsetzungsbeispiel: Unter Berücksichtigung der gültigen Gesetzeslage und zutreffenden Datenschutz-Regularien werden folgende Löschfristen für lokal erfasste sicherheitsrelevante Protokollierungsdaten auf einem beispielhaften TK-System umgesetzt:

- Standard System Logs: Löschung nach spätestens 90 Tagen
- Protokollierungen von öffentlichen IP-Adressen: Löschung (oder Anonymisierung) nach spätestens 7 Tagen
- Protokollierungen der Vergabe von dynamischen öffentlichen IP Adressen durch die TK-Lösung: Löschung nach spätestens 7 Tagen
- Protokollierungen nicht abrechnungsrelevanter Call Detail Records: Löschung nach spätestens 7 Tagen
- Protokollierungen der Kommunikations-Inhalte von eMail und SMS: Löschung nach spätestens 24 Stunden
- Protokollierungen der behandelten Domain-Abfragen des DNS-Servers der TK-Lösung: Löschung nach spätestens 7 Tagen

stens 24 Stunden

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.33-68/5.3