

Sicherheitsanforderung

Hom gateway

Deutsche Telekom Gruppe

Version	3.6
Datum	01.07.2024
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 3.40	Dokumententyp Sicherheitsanforderung
Version 3.6	Stand 01.07.2024	Status Freigegeben
Fachlicher Ansprechpartner Telekom Security psa.telekom.de	Gültigkeitsdauer 01.07.2024 - 30.06.2029	Freigegeben von Stefan Pütz, Leiter SEC-T-TST

Zusammenfassung
Homegateway

Copyright © 2024 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.	Technical Due Dilligence	5
3.	General System Hardening	8
4.	Bootloader	13
5.	Firmware	14
6.	Betriebssystem	17
6.1.	Firewall	17
6.2.	Firewall / Network Subsystem with IPv6 Support	19
6.3.	Wireless LAN	20
6.4.	USB Subsystem	22
6.5.	DECT / CAT-iq Subsystem	22
7.	Web GUI	24
7.1.	Embedded HTTP Server	24
7.2.	Basic GUI Hardening	24
7.3.	User Authentication	26
7.4.	Session Management	28
7.5.	Transport Security	30
7.6.	Protection of Configuration Data	31
7.7.	System Log	31
8.	Services	33
8.1.	SIP User Agent	33
8.2.	WAN Management Protocol	33
8.3.	LAN Management Protocol	34
8.4.	Home Media Sharing	37
8.5.	Network Attached Storage (SMB/CIFS)	37
8.6.	File Transfer	38
8.7.	DNS Proxy	40
8.8.	WiFi Simple Configuration / WiFi Protected Setup	42

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. Technical Due Dilligence

Req 1 Jede über die Spezifikation hinausgehende Funktionalität muss der Deutschen Telekom Gruppe gegenüber offengelegt und mit ihr abgestimmt werden.

Die Deutsche Telekom Gruppe stellt eine Spezifikation für ein Home Gateway bereit, die alle Anforderungen der Deutsche Telekom Gruppe an das Endgerät umfasst. In der Regel ist es nicht erforderlich, zusätzliche Funktionalitäten in das Home Gateway zu implementieren. Zusätzliche Funktionen sind Funktionalitäten, die nicht explizit im Rahmen Spezifikation gefordert werden.

Ein Home Gateway basiert oftmals auf einem bestehenden Design, und der Lieferant muss Softwarekomponenten von Dritten (einschl. Open Source) verwenden, um die Anforderungen der Deutsche Telekom Gruppe zu erfüllen. Es ist daher nicht immer möglich, alle Softwarekomponenten des Geräts soweit anzupassen, dass ausschließlich die von der Deutsche Telekom Gruppe geforderte Funktionalität bereitgestellt wird. In diesem Fall muss die Deutsche Telekom Gruppe über zusätzliche Funktionalitäten unterrichtet werden und der Implementierung dieser Funktionen zustimmen.

Beispiele für zusätzliche Funktionalitäten in Sinne der Anforderung sind:

- Eine versteckte Seite in der Web-GUI Anwendung, die beispielsweise den Download von Diagnosedaten ermöglicht.
- Wiederherstellungsfunktionen nach kritischen Ausfällen: z. B. die Möglichkeit, den Boot- Vorgang zu unterbrechen, um den Flash Speicher über TFTP mit einem neuen Firmware- Image wiederherzustellen. D.h. im Rahmen der Abstimmung werden im Wesentlichen solche Funktionen betrachtet, die über ein Netzwerkinterface oder lokal über Zugang zur Gerätehardware des Home Gateways genutzt werden können.

Motivation: Wenn im Gerät Funktionen implementiert werden, die nicht von der Spezifikation der Deutschen Telekom Gruppe gefordert werden, dann ist die Sicherheitsanalyse der Deutsche Telekom Gruppe für das Gerät unvollständig und muss überarbeitet werden. Daher ist es unerlässlich, dass die Deutsche Telekom Gruppe von jeder zusätzlichen Funktionalität in Kenntnis gesetzt wird und dieser zustimmt.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-1/3.6

Req 2 Eine Übersicht der Netzwerkdienste muss der Deutschen Telekom Gruppe zur Verfügung gestellt und mit ihr abgestimmt werden.

Die Übersicht der Netzwerkdienste muss alle aktiven Dienste auf jedwedem Netzwerkinterface des Home Gateways umfassen, insbesondere auf allen LAN und WAN Schnittstellen. Dienste, die nur intern verwendet werden und daher lediglich an das localhost Interface gebunden sind, müssen hier nicht betrachtet werden.

Die Übersicht muss jeweils pro Netzwerkdienst das Interface, an das der Dienst gebunden ist, den tcp/udp Port, das verwendete Protokoll sowie eine kurze Beschreibung des Dienstes enthalten. Zusätzlich muss angegeben werden, in welchem Betriebszustand des Home Gateways ein Dienst aktiv ist.

Motivation: Jeder aktive Netzwerkdienst stellt ein potenzielles Sicherheitsrisiko dar. Die Deutsche Telekom Gruppe muss daher Kenntnis über alle aktiven Netzwerkdienste des Home Gateways besitzen.

Umsetzungsbeispiel: Die folgende Tabelle zeigt beispielhaft, wie eine Übersicht der aktiven Netzwerkdienste aussehen kann:

Interface	Port	Protokoll	Erläuterung
-----------	------	-----------	-------------

WAN (PPPoE via VLAN 7)	5060/tcp	SIP	SIP User Agent für IP-Telefonie. Offen, sofern IP Telefonie aktiviert. IP-ACL auf Call Control gesetzt.
WAN (PPPoE via VLAN 7)	7547/tcp	HTTP	HTTP Server für Connection Request. Offen, sofern TR-069 aktiv. IP-ACL auf ACS gesetzt.
LAN / WLAN	80/tcp	HTTP	Web GUI zur Administration des Home Gateways
LAN / WLAN	53/udp	DNS	DNS Proxy
LAN / WLAN	67/udp	DHCPs	DHCP Server für das Heimnetzwerk. Offen, sofern der DHCP Dienst aktiviert ist.
LAN / WLAN	1900/udp	SSDP	Simple Service Discovery Protocol für TR-064
LAN / WLAN	49000/tcp	SOAP	TR-064 SOAP API via HTTP
LAN / WLAN	49443/tcp	SOAP	TR-064 SOAP API via HTTPS

Die konkrete Ausgestaltung der Übersicht hängt sehr von der Netzwerkarchitektur des Home Gateways ab. Jedes Netzwerkinterface des Home Gateways muss hier betrachtet werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-2/3.6

Req 3 Sicherheitsfunktionen müssen der Deutschen Telekom Gruppe gegenüber offen gelegt und mit ihr abgestimmt werden.

Der Hersteller muss ein Sicherheitskonzept erstellen, welches die Umsetzung der Sicherheitsfunktionen für die Produktion sowie in der Hardware und Firmware des Home Gateway dokumentiert. Insbesondere folgende Punkte müssen im Sicherheitskonzept dargestellt werden:

- Der Algorithmus zur Erzeugung der vorkonfigurierten Gerätepassworte
- Der Algorithmus zur Erzeugung der vorkonfigurierten WLAN Passworte
- Der Algorithmus zum Schutz von vertraulichen Daten innerhalb einer Firmware Image Datei
- Der Algorithmus zum Schutz von vertraulichen Daten bei der Speicherung im Home Gateway (lokale Speicherung und Backup Datei)
- Der Algorithmus zum Schutz der Integrität der Firmware Image Datei und zur Prüfung der Integrität des Bootloaders, des Kernels und der Anwendungen beim Startvorgang
- Die Umsetzung der Nutzung von Sicherheitsfunktionen der Hardware (des Chipsatzes)
- Die Maßnahmen zur sicherheitstechnischen "Härtung" des Betriebssystems und der Anwendungen des Home Gateways

Der Hersteller muss eine Dokumentation liefern, und mit der Deutschen Telekom Gruppe abstimmen. Auf Anfrage der Deutsche Telekom Gruppe muss der Hersteller Beispieldatensätze von durch die genannten Algorithmen generierten Daten liefern, beispielsweise Geräte- und WLAN Passworte.

Motivation: Im Rahmen der technischen Abnahmeprüfung eines Endgerätes wird die Deutsche Telekom Gruppe auch Algorithmen für Sicherheitsfunktionen prüfen. Daher sind eine Dokumentation sowie - auf Nachfrage - auch Beispieldatensätze zu liefern.

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: 3.40-3/3.6

Req 4	Für jede Firmware muss der Hersteller Release Notes bereitstellen, die auch eine Liste der in der Firmware verwendeten Softwarekomponenten enthält. Die Versionsinformationen und enthaltene Sicherheits-Updates der Komponenten muss ersichtlich sein.
-------	---

Die Release Notes müssen Bestandteil jeder Firmware Lieferung sein.

Motivation: Im Rahmen der technischen Abnahmeprüfung möchte die Deutsche Telekom Gruppe evaluieren, ob lediglich aktuellste Software mit allen erforderlichen Sicherheitsupdates verwendet wird.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.40-4/3.6

Req 5	Der Hersteller muss eine separate Entwickler-Version zu jeder Firmware bereitstellen, die einen Root Konsolenzugang über eine lokale Netzwerkschnittstelle (LAN/WLAN) ermöglicht.
-------	---

Der Administrator (root) Konsolenzugang muss mittels des SSH oder des Telnet Protokolls realisiert werden. Der Zugang muss durch Verifikation eines Passwortes abgesichert werden, und die Zugangsdaten müssen der Deutschen Telekom Grupper zur Verfügung gestellt werden. Gerätespezifische Passworte sind hierbei einem statischen Passwort zu bevorzugen.

Es ist zu beachten, dass der Konsolenzugang ausschließlich in der separaten Entwickler-Version zu einer Firmware Version enthalten sein darf. In der zugehörigen Produktions Version der Firmware darf kein Konsolenzugang implementiert und auch die dafür notwendigen Softwarekomponenten müssen entfernt werden.

Motivation: Im Rahmen der technischen Abnahmeprüfung will die Deutsche Telekom Gruppe die Umsetzung von Anforderung verifizieren, die nur mittels einer Root Shell auf dem Router überprüft werden können.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-5/3.6

3. General System Hardening

Req 6	Als Betriebssystem für das Home Gateway muss Linux verwendet werden, und eine aktuelle, stabile Kernel Version mit erweitertem Supportzeitraum (LTS) muss verwendet werden.
-------	---

Alle Funktionen zur Verhinderung von Buffer-Overflow-Angriffen wie ASLR (address space layout randomisation) müssen im Kernel aktiviert werden, und die aktuellsten Sicherheitsupdates müssen implementiert sein. Ggfs. kann es notwendig sein, dass ein Sicherheitsupdate auf eine frühere Version einer Softwarekomponente rückportiert wird.

Motivation: Das Linux Betriebssystem ist ein robustes OS für eingebettete Geräte, es implementiert einen starken Speicherschutz, bietet Techniken zur Verhinderung von Buffer Overflow Angriffen, und es implementiert POSIX-konforme Berechtigungen für Dateisysteme. Durch eine angemessene Härtung des Betriebssystems kann ein sicheres Home Gateway implementiert werden. Ein Home Gateway wird über viele Jahre hinweg von Kunden genutzt, so dass eine aktuelle LTS Version einen langjährige Softwarepflege erleichtert.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- 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: 3.40-6/3.6

Req 7	Die Produktionsversion einer Firmware darf keinen Shell-Zugang oder jedwede andere Form einer Konsolenschnittstelle implementieren.
-------	---

Diese Anforderung betrifft den Konsolenzugang zum Linux Betriebssystem über eine Netzwerkschnittstelle sowie über eine serielle Schnittstelle, die bspw. auf der Leiterplatte des Home Gateways zugänglich ist: es darf kein Konsolenzugang zum Linux Betriebssystem in der Produktionsversion einer Firmware implementiert werden.

Motivation: Ein Shellzugang in der Produktionsversion einer Firmware wird von der Deutschen Telekom Gruppe nicht gefordert, da ein solcher Zugang schwerwiegende Angriffe ermöglicht sowie die Aufklärung der Implementierung des Home Gateways erleichtert.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System

ID: 3.40-7/3.6

Req 8	Systemmeldungen dürfen keine vertraulichen Daten wie kryptographische Schlüssel oder Passwörter enthalten.
-------	--

Diese Anforderung betrifft die Systemmeldungen des Linux Kernels und die Meldungen von beliebigen Anwendungen auf dem Home Gateway. Systemmeldungen können über eine serielle Konsole auf der Leiterplatte, über einen Konsolenzugang zum Betriebssystem oder über die entsprechende Funktion der Web GUI eingesehen werden. In keinem Fall dürfen die Meldungen vertrauliche Daten wie Passwörter, Sitzungsschlüssel oder andere vertrauliche Daten enthalten.

Motivation: Vertrauliche Daten im Home Gateway müssen auch dann geschützt werden, wenn ein Angreifer Zugang zum Home Gateway oder zum Betriebssystem des Home Gateways erhält.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

Req 9	Das Home Gateway muss einen Hardware-Taster besitzen, über den ein Kunde das Gerät in den „werksseitigen Zustand“ zurückversetzen kann (Factory Reset).
-------	---

Bei einem solchen Factory Reset müssen alle kundenspezifischen Konfigurationsdaten gelöscht, und der Auslieferungszustand aller Konfigurationsdateien muss wiederhergestellt werden.

Motivation: Ein Kunde möchte das Gerät möglicherweise an einen Dritten weitergeben. Er muss in der Lage sein, seine personenbezogenen Daten auf dem Home Gateway zu löschen, auch wenn er nur Zugang zur Hardware hat und sich nicht mehr an das Gerätepasswort erinnern kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Req 10	Im Auslieferungszustand dürfen nur diejenigen Netzwerkdienste aktiv sein, die zur Funktion des Home Gateways benötigt werden.
--------	---

Folgende Netzwerkdienste werden nicht zur Funktion eines Home Gateways benötigt und müssen daher im Auslieferungszustand deaktiviert werden: DLNA/UPnP A/V Mediendistribution, Dateiübertragung (FTP), und Netzwerkspeicher (NAS). Diese Dienste müssen bei Bedarf explizit vom Benutzer aktiviert werden.

Es ist zu beachten, dass insbesondere ein Remote Device Management (TR-069), welches u.a. das automatische Verteilen von Firmware Updates ermöglicht, nicht als optionaler Dienst gesehen wird. Daher muss TR-069 im Auslieferungszustand aktiviert werden.

Motivation: Jeder aktive Netzwerkdienst vergrößert die Angriffsfläche auf das Home Gateway. Daher muss das Gerät im Auslieferungszustand sicher konfiguriert werden. Netzwerkdienste, die nicht gleich benötigt werden, müssen daher deaktiviert sein.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Req 11	Wenn ein Netzwerkdienst in der Konfiguration des Home Gateways deaktiviert wurde, dann müssen auf allen Netzwerkschnittstellen, an die der Dienst gebunden war, alle TCP/UDP Ports des Dienstes geschlossen werden.
--------	---

Der Port eines deaktivierten Netzwerkdienstes kann über die eingebaute Firewall oder einfach durch das Beenden des zugehörigen Prozesses geschlossen werden. Es wird empfohlen, jeweils den Prozess (daemon) zu beenden, wenn ein Netzwerkdienst deaktiviert wird.

Motivation: Die Konnektivität zu einem deaktivierten Dienst auf dem Home Gateway über das Netzwerk muss unterbunden werden, damit dieser Dienst nicht angegriffen werden kann (Minimierung der Angriffsfläche).

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

Req 12 Jedwede Anwendung auf dem Home Gateway, die eine Passwort-basierte Authentifizierung implementiert, muss auch Maßnahmen gegen ein systematisches Raten des Passworts vorsehen.

Eine Maßnahme gegen das systematische Raten eines Passworts ist eine sogenannte "Teergrube", d.h. eine Funktion zum Ausbremsen eines Angreifers: nach jeder fehlgeschlagenen Verifikation eines Passworts werden weitere Authentifizierungsversuche für eine relevante Zeitdauer systemseitig unterbunden (verzögert). Die Verzögerungszeit muss nach jedem weiteren, aufeinanderfolgenden Fehlversuch ansteigen. Dieser Verzögerungsmechanismus muss im Home Gateway implementiert werden, weil clientseitige Maßnahmen umgangen werden können.

Es ist zu beachten, dass insbesondere für die folgenden Dienste die Implementierung einer Teergrube gefordert wird: für die Web GUI, den TR-064 Dienst, den Netzwerkspeicher (NAS) sowie für den Dienst zur Übertragung von Dateien (FTP bzw. FTPS Dienst).

Motivation: Das systematische Raten eines Passworts kann den unauthorisierten Zugang zu einem Dienst nach sich ziehen. Private Daten oder die Konfiguration des Home Gateways könnten kompromittiert bzw. manipuliert werden. Daher muss eine Teergrube implementiert werden, die solche Angriffe verhindert.

Umsetzungsbeispiel: Nach dem ersten fehlgeschlagenen Login ist eine erneute Anmeldung erst nach einer Wartezeit von 1 Sekunde möglich. Mit jeder weiteren fehlgeschlagenen Anmeldung verdoppelt sich diese Wartezeit (1, 2, 4, 8, 16, 32, 64, ... Sekunden).

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

Req 13 Die TLS Implementierung des eingebetteten Linux Betriebssystems muss das Protokoll in der Version 1.2 (TLS v1.2) oder neuer unterstützen.

Ältere TLS Protokollversionen als Version 1.2 gelten als veraltet, da sie Schwachstellen aufweisen. Entsprechend unterstützen von dem Endgerät genutzte Telekom Dienste, wie beispielsweise das TR69-basierte Remote Device Management, nur die stets aktuellen Protokollversionen wie TLS v1.2. Die zu unterstützenden kryptographischen Parameter für TLS v1.2 können dem Technischen Report TR-02102-2 "Kryptographische Verfahren: Empfehlungen und Schlüssellängen" des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) entnommen werden.

Ältere TLS Protokollversionen dürfen nicht mehr unterstützt werden.

Motivation: Einige Dienste des Home Gateway benötigen TLS, beispielsweise das Remote Device Management oder die Email-Benachrichtigung. Das Home Gateway muss hier die derzeit von den Diensten geforderten Sicherheitsstandards unterstützen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Req 14 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: 3.01-10/8.0

Req 15 Das System muss vor Überlastsituationen geschützt werden.

Ein System muss über Schutzmechanismen verfügen, die Überlastsituationen so weit wie möglich verhindern. Insbesondere ist eine partielle oder komplette Beeinträchtigung der Verfügbarkeit des Systems zu vermeiden.

Beispiele für mögliche Schutzmaßnahmen sind:

- Begrenzung des pro Anwendung verfügbaren Arbeitsspeichers (RAM)
- Begrenzung der maximalen Sessions einer Web-Anwendung
- Begrenzung der maximalen Größe eines Datensatzes
- Begrenzung von CPU-Ressourcen pro Prozess
- Priorisieren von Prozessen
- Begrenzung der Anzahl oder der Größe von Transaktionen eines Benutzers oder von einer IP-Adresse in einem bestimmten Zeitraum

Anmerkung:

vor Netzwerk-basierenden Angriffen mit extrem hohen Daten- oder Paketraten, den sogenannten "Distributed Denial of Service" (DDoS) Angriffen, kann ein System sich i. d. R. selbst nicht mehr schützen. Zur Abwehr von DDoS Angriffen wird eine vorgelagerte Lösung in der Netzwerk-Schicht benötigt.

Motivation: Angreifer können mit gezielten ressourcenlastigen oder großvolumigen Anfragen versuchen, die Ressourcen eines Systems aufzubrauchen, so dass das System seine regulären Aufgaben bzw. vorgesehenen Aufgabenvolumen nicht mehr erfüllen kann und die Verfügbarkeit der angebotenen Dienste effektiv gestört ist. Die Begrenzung der Ressourcen, die je gestellter Anfrage an das System maximal in Anspruch genommen werden können, ist eine grundlegende Maßnahme, um die Auswirkungen solcher Denial-of-Service (DoS) Angriffe zu reduzieren.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.01-12/8.0

Req 16 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 selbstständig 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: 3.33-5/5.2

Req 17 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: 3.33-47/5.2

4. Bootloader

Req 18	Der Bootloader muss die Integrität des Linux Kernels und die des Root-Dateisystems überprüfen bevor der Kernel ausgeführt wird.
--------	---

Die Integritätsprüfung des Kernels und des Root Filesystems müssen sicherstellen, dass nur authentische und nicht manipulierte Software ausgeführt werden kann. Die Deutsche Telekom Gruppe fordert diese Integritätsprüfungen, überlässt aber die konkrete Implementierung dem Hersteller. Sofern verfügbar, müssen Hardware-basierte Mechanismen für einen sicheren Bootvorgang umgesetzt werden. Der Hersteller muss hier in Abstimmung mit der Deutschen Telekom Gruppe angemessene und geeignete Algorithmen implementieren. Die Prüfung des Root-Dateisystems kann auch durch den Kernel erfolgen.

Motivation: Der Bootloader muss sicherstellen, dass nur integere Images ausgeführt werden können. D.h. Images, die nicht (nachträglich) verändert/manipuliert wurden, und die keine Fehler in ihrer Datenstruktur aufweisen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten

ID: 3.40-18/3.6

Req 19	Der Bootloader darf nicht das Auslesen von vertraulichen Daten im Klartext ermöglichen.
--------	---

Bootloader geben oftmals Systemmeldungen über eine Konsolenschnittstelle aus, oder sie implementieren eine leichtgeichtige Kommandozeilen-Schnittstelle für einige grundlegende Funktionen. Der Hersteller muss den Bootloader so anpassen, dass vertrauliche Daten, die in der Firmware (beispielsweise im Root-Dateisystem) gespeichert werden, nicht im Klartext ausgelesen werden können. Beispiele für vertrauliche Daten im Sinne der Anforderung sind kryptographische Schlüssel oder Passwörter.

Motivation: Das Home Gateway muss vertrauliche Daten vor unbefugtem Auslesen schützen. Vertrauliche Daten, wie z. B. Passwörter dürfen daher nicht auslesbar sein.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

ID: 3.40-19/3.6

5. Firmware

Req 20	Vertrauliche Daten in der Firmware Image Datei müssen verschlüsselt gespeichert werden, und der Advanced Encryption Standard (AES) muss für die Verschlüsselung dieser Daten verwendet werden.
--------	--

Diese Anforderung ist dann zutreffend, wenn vertrauliche Daten als Bestandteil der Firmware Image Datei ausgeliefert werden müssen. Zugangsdaten (z.B. Passworte) und kryptographische Schlüssel, beispielsweise ein privater Schlüssel zu einem x509v3 Zertifikat für die Client-Authentifizierung, werden hier als vertrauliche Daten betrachtet. Der AES unterstützt Schlüssellängen von 128, 192 und 256 Bits. Die bevorzugte Schlüssellänge ist 256 Bit. Der AES-Verschlüsselungsschlüssel zum Schutz vertraulicher Daten in der Firmware Image Datei wird als „Datenverschlüsselungsschlüssel“ bezeichnet.

Motivation: Analysiert ein Angreifer eine Firmware Image Datei, dann darf er nicht in der Lage sein, vorkonfigurierte vertrauliche Daten wie private kryptographische Schlüssel für TLS offenzulegen. AES wird als sicherer Verschlüsselungsalgorithmus betrachtet.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

ID: 3.40-20/3.6

Req 21	Der Datenverschlüsselungsschlüssel muss zur Laufzeit aus einem Schlüssel-spezifischen Satz von Attributen des Home Gateways abgeleitet werden. Die Attribute werden verschleiert innerhalb der Firmware Image Datei gespeichert, und ein Attribut muss eine Zufallszahl sein.
--------	---

Der Datenverschlüsselungsschlüssel darf nicht als zusammenhängendes Binärobjekt innerhalb der Firmware Image Datei gespeichert werden. Der Schlüssel muss zur Laufzeit abgeleitet werden, d.h. nachdem die Firmware auf dem Endgerät installiert wurde. Die Komplexität des Verschleierungsalgorithmus muss verhindern, dass ein Angreifer den Satz von Attributen oder den Algorithmus selbst einfach aufklären kann, beispielsweise durch den Vergleich von verschiedenen Firmware Versionen oder durch die Dekomprimierung und Analyse einer Firmware Image Datei.

Motivation: Die Deutsche Telekom Gruppe will sicherstellen, dass Datenverschlüsselungsschlüssel nicht einfach in der Firmware Image Datei oder im Dateisystem des Home Gateways gespeichert werden. Es soll so verhindert werden, dass ein Angreifer sehr leicht die Schutzmechanismen aufklären und umgehen kann. Die Kompromittierung vertraulicher Daten im Firmware Image muss dem Schutzbedarf der Daten angemessen erschwert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

ID: 3.40-21/3.6

Req 22	Die Firmware Image Datei muss einen hinreichend starken Mechanismus zum Schutz der Integrität enthalten und die Integrität der Image Datei muss erfolgreich validiert werden, bevor sie im Flash Speicher des Home Gateways installiert wird.
--------	---

Eine Hash-Funktion oder eine digitale Signatur des Firmware Image wird als ausreichend starker Mechanismus zur Gewährleistung der Integrität betrachtet. Geeignete Algorithmen für digitale Signaturen sind beispielsweise HMAC-SHA-256, RSA oder DSA.

Motivation: Die Integrität des Firmware-Image muss gewährleistet sein, bevor das Image in den Flash-Speicher installiert wird. Daher muss ein hinreichend starker Mechanismus für den Integritätsschutz Teil der Image Datei sein.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Integrität

ID: 3.40-22/3.6

Req 23	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: 3.33-16/5.2

Req 24	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: 3.33-19/5.2

Req 25	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 Ge-

räts 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: 3.33-20/5.2

6. Betriebssystem

6.1. Firewall

Req 26 Die Firewall muss einen zustandsbehafteten Paketfilter implementieren.

Ein zustandsbehafteter Paketfilter beachtet den Zustand von Verbindungen und diese Art des Paketfilters verwirft ein-
treffende Datenpakete, wenn diese nicht zu einer bekannten Netzwerk-Verbindung gehören.

*Motivation: Nur ein zustandsbehafteter Paketfilter kennt den Status jeder Verbindung und kann eingehende Datenpa-
kete verwerfen, wenn diese nicht zu einer bekannten Verbindung gehören. Dieser Typ einer Firewall erschwert daher
z. B. Spoofing-Angriffe, und es kann ein angemessenes Sicherheitsniveau erreicht werden.*

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-26/3.6

Req 27 Die Firewall bzw. das Netz-Subsystem muss ein starkes Endsystemmodell entsprechend dem Ab-
schnitt 3.3.4.2 multihoming requirements des RFC 1122 implementieren.

Das Home Gateway verfügt über mehrere IP-Adressen, die über mindestens zwei physikalische Schnittstellen (WAN-
und LAN-Schnittstelle) mit verschiedenen Netzwerken (Internet und Heimnetzwerk) verbunden sind. Das Home Gate-
way entspricht daher der Definition eines „multihomed hosts“ in Abschnitt 3.3.4.1 des RFC 1122. Das starke Ends-
systemmodell bedeutet, dass bei einem Multihomed Host abgehende Datagramme über die Schnittstelle mit der Quell-
IP-Adresse gesendet und ankommende Datagramme über die Schnittstelle mit der Ziel-IP-Adresse eingehen müssen.
In diesem Modell ist es beispielsweise nicht möglich, über eine LAN- Schnittstelle eine Verbindung mit der WAN-IP-
Adresse des Home Gateway herzustellen.

Motivation: Das starke Endsystemmodell erschwert sogenannte DNS-Rebinding-Angriffe auf das Home Gateway.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-27/3.6

Req 28 Die Firewall muss immer aktiv sein.

Ein Nutzer des Home Gateways darf nicht in der Lage sein, die Firewall mittels einer entsprechenden Konfigurations-
option bspw. der Web GUI zu deaktivieren. Es darf auch nicht möglich sein, die Firewall über das Remote Device Ma-
nagement zu deaktivieren.

*Motivation: Die Firewall ist die wichtigste Sicherheitsfunktion des Home Gateway's. Dieser Dienst muss daher immer
aktiv sein.*

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-28/3.6

Req 29	Als Standardregel der Firewall müssen alle eingehenden Verbindungen auf WAN-Schnittstellen zurückgewiesen werden.
--------	---

Die Firewall muss eingehende Verkehre abweisen, wenn diese nicht zu einer ausgehenden Verbindung gehören, oder wenn nicht explizite Regel in der Konfiguration bspw. das Weiterleiten von Datenpaketen vorsehen (erlauben).

Motivation: Andernfalls ist das Heimnetzwerk nicht angemessen vor Angriffen aus dem Internet geschützt.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.40-29/3.6

Req 30	Port-Weiterleitungen zu einer IP-Adresse des LAN/WLAN-Interface des Home Gateways dürfen nicht von einer einem Benutzer zugänglichen Konfigurationsoption akzeptiert werden.
--------	--

Ein Benutzer darf nicht in der Lage sein, beispielsweise eine Port-Weiterleitung auf Port 80 einer LAN/WLAN-Schnittstelle zu konfigurieren, denn dann wäre die Web GUI des Home Gateways im Internet exponiert.

Motivation: Wenn solche Regeln angelegt werden könnten, dann könnten LAN-seitige Dienste des Home Gateways aus dem Internet erreichbar sein, z. B. aufgrund einer Fehlkonfiguration des Benutzers.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-30/3.6

Req 31	Verbreitete Angriffsvektoren wie SYN Flooding, ICMP Flooding, UDP Flooding, Ping of Death, Smurf Attack, LAND Attack und auf IP Fragmentierung basierende Angriffe müssen von der Firewall erkannt und verhindert werden.
--------	---

Die folgenden Angriffe müssen von der Firewall oder der Netzwerkimplementierung des Home Gateways erkannt und verhindert werden:

- TCP SYN, ICMP, UDP flooding Angriffe:

In diesen Angriffen werden eine hohe Anzahl von TCP SYN-, ICMP- oder von UDP-Paketen zum Opfer gesendet.

- Ping of Death:

Ein ping of death ist ein Denial-of-service Angriff. In diesem Angriff werden ungültige und auf dem Zielsystem Schaden verursachende ICMP echo request ("ping") an das Opfer gesendet. Diese Datenpakete nutzen Schwachstellen in der Implementierung des ICMP Protokolls im Zielsystem aus.

- Smurf Attack:

Ein Smurf Angriff ist ein verteilter Denial-of-service Angriff, bei dem eine sehr große Anzahl von ICMP Paketen mit der Source-IP-Adresse des Opfers als gefälschte Source-IP an Broadcasted Adressen eines Netzwerks gesendet werden. In betroffenen Netzwerken senden dann alle Hosts des Netzwerks ihre Antworten an die IP-Adresse des Opfers.

- LAND Attack:

Der LAND (local area network denial-of-service) Angriff nutzt gefälschte TCP SYN Pakete zum Einleiten einer Verbindung aus, bei denen die IP-Adresse des Opfers als Quell- und Zieladresse angegeben ist. Als Zielport ist ein offener TCP Port des Opfers genannt.

- Angriffe, die auf IP Fragmentierung beruhen:

Diese Angriffe nutzen IP Fragmentierung aus, um den Algorithmus zur Auflösung der Fragmentierung im Zielsystem anzugreifen (um eine Einschränkung der Verfügbarkeit herbeizuführen), oder um bspw. das Regelwerk einer Firewall zu hintergehen. Ein Beispiel für einen solchen Angriff ist der sogenannte "Teardrop" Angriff, bei dem verschränkte IP Fragmente, d.h. solche mit überlappenden oder einer übergroßen Anzahl von Nutzdaten, an das Opfer gesendet werden.

Man beachte, dass der primäre Fokus hier auf dem Home Gateway selbst liegt. D.h. das HG muss robust gegen die genannten Angriffe sein, soweit dies unter den gegebenen Randbedingungen möglich ist. In Bezug auf die Flooding Angriffe bedeutet es z.B. dass das Home Gateway diese Angriffe ohne gravierende Beeinträchtigungen überstehen muss. D.h. Verkehre entsprechender QoS Klassen wie Voice-over-IP Telefonie dürfen nicht nennenswert beeinträchtigt werden.

Motivation: Der IP-Stack soll nicht für gängige Bedrohungen anfällig sein, damit nicht z. B. Denial-of-Service- Angriffe über das Internet durchgeführt werden können.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.40-31/3.6

Req 32	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: 3.33-52/5.2

6.2. Firewall / Network Subsystem with IPv6 Support

Req 33	Die IPv6-Firewall muss ein vergleichbares Netzwerksicherheitsmodell durchsetzen wie die IPv4 NAT-Firewall.
--------	--

Die folgenden Anforderungen beschreiben einen Entwurf für ein IPv6-Netzwerksicherheitsmodell:

- Alle eingehenden Verbindungen zu IPv6-Hosts im LAN/WLAN werden abgelehnt. Ausnahmen müssen explizit vom Nutzer konfiguriert werden. Es darf allerdings nicht möglich sein, eine Ausnahme für eine IP-Adresse der LAN/WLAN Schnittstelle des Home Gateways zu konfigurieren.
- Jede eingehende Verbindung zu einem beliebigen Port an der WAN-Schnittstelle des Home Gateway wird abgelehnt, wenn diese nicht von einem Dienst benötigt wird.
- ICMPv6 muss so restriktiv wie möglich behandelt werden, z. B.:
 - Die ICMPv6-Nachrichtentypen 133/134 (Router Solicitation/Advertisement) SOLLTEN an allen Netz-

werkschnittstellen verarbeitet werden. Diese Nachrichtentypen DÜRFEN NICHT zwischen WAN und LAN/WLAN-Schnittstellen weitergeleitet werden.

- Die ICMPv6-Nachrichtentypen 135/136 (Neighbour Solicitation/Advertisement) SOLLTEN an allen Netzwerkschnittstellen entgegengenommen werden. Diese Nachrichtentypen DÜRFEN NICHT zwischen WAN und LAN/WLAN-Schnittstellen weitergeleitet werden.
- Die ICMPv6-Nachrichtentypen 128/129 (Echo Request/Reply), 1 (Destination Unreachable), 2 (Packet Too Big) und 3 (Time Exceeded) MÜSSEN an LAN/WLAN- und WAN-Schnittstellen entgegengenommen werden und MÜSSEN zwischen WAN- und LAN/WLAN-Schnittstellen weitergeleitet werden.
- Alle anderen ICMPv6-Nachrichtentypen MÜSSEN verworfen werden.

Die Umsetzung einiger Anforderungen ist stark von der konkreten IPv6 Implementierung im jeweiligen Access Netz abhängig, in dem das Gerät betrieben werden soll.

Motivation: Durch IPv6 darf die Sicherheit des Home Gateway und des Heimnetzwerks nicht kompromittiert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-33/3.6

Req 34	Die IPv6 Firewall muss einen Angriff auf die Verfügbarkeit der Tabelle zur Speicherung des Zustands für das Neighbour Discovery Protocol verhindern.
--------	--

Dieser Angriff auf die Zustands-Tabelle für das Neighbour Discovery Protocol (NDP) ist ein Denial-of-Service Angriff. Ein Angreifer flutet hierbei das Home Gateway mit ICMPv6 Nachrichten des Typs „Neighbour Advertisement“, um eine Vielzahl von benachbarten Netzwerk-Hosts vorzutäuschen. Hierdurch können alle freien Einträge der NDP Tabelle aufgebraucht werden. In diesem Fall muss die ICMPv6 Implementierung des Home Gateway einen definierten Fehlerzustand einnehmen, z. B. Einträge aus der NDP Tabelle löschen. In keinem Fall darf dieser Fehlerzustand zu einer Verringerung der Verfügbarkeit des Home Gateway führen.

Motivation: Ein Angreifer darf nicht in der Lage sein, den Betrieb des Home Gateway durch einen einfachen und nicht-verteilten DoS Angriff wie den beschriebenen zu stören.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.40-34/3.6

6.3. Wireless LAN

Req 35	Die Wireless LAN Schnittstelle muss WPA2 sowie WPA3 unterstützen und standardmäßig mindestens mit WPA2 und dem CCMP-Protokoll verschlüsselt werden.
--------	---

Diese Anforderung betrifft nur ein privates Drahtlosnetzwerk nach den Standards der IEEE802.11 Serie. WPA2 und WPA3 stellen aktuelle Sicherheitsmechanismen zur Absicherung des Netzwerks zur Verfügung. Es wird empfohlen, standardmäßig den WPA2/WPA3 mixed mode zu nutzen, damit WPA3 fähige Endgeräte bereits ohne Neukonfiguration die aktuellste WPA Protokollversion nutzen können.

Motivation: WPA2 CCMP ist die sicherste Verschlüsselungsmethode für drahtlose Netzwerke, sofern WPA3 nicht von allen Netzteilnehmern genutzt werden kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-35/3.6

Req 36	Der werksseitig vorkonfigurierte WPA2/WPA3-Schlüssel (das WLAN-Passwort) muss ein zufälliger und gerätespezifischer Wert sein.
--------	--

Der Begriff „zufällig“ beinhaltet die Anforderung, dass der vorkonfigurierte WPA2/WPA3-Schlüssel nicht aus Attributen der Hardware des Home Gateways gebildet wird, wie MAC-Adressen, der Seriennummer, etc.

Motivation: Ein WLAN-Passwort, das erraten werden kann, oder das für alle Geräte gleich ist, bietet keinen ausreichenden Schutz für das drahtlose Heimnetzwerk des Kunden, da solche schwachen Passwörter durch einen Angreifer ermittelt werden können. Nur ein starkes, zufälliges und gerätespezifisches WLAN-Passwort in den Geräten verhindern den Missbrauch von drahtlosen Netzwerken.

Umsetzungsbeispiel: Eine ausreichende Zufälligkeit der vorkonfigurierten WPA2/WPA3-Schlüssel kann durch Anwendung eines guten (Pseudo-) Zufallszahlengenerators erreicht werden, der gleichverteilte Zufallszahlen erzeugt. Solche Generatoren sind im RFC 4086 beschrieben.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-36/3.6

Req 37	Das vorkonfigurierte WLAN-Passwort muss die folgenden Mindestanforderungen erfüllen: eine Länge von 20 Zeichen, bestehend aus den Zahlen 0-9.
--------	---

Diese Aussage legt die Minimalanforderungen an ein vorkonfiguriertes WLAN Passwort fest. Es wird empfohlen, einen umfangreicheren Zeichenraum zu verwenden, beispielsweise alle Zahlen 0-9 und alle Großbuchstaben A-Z.

Motivation: 20 zufällig gewählte Ziffern bieten ausreichend Schutz, um einfache Brute-Force-Angriffe auf das WLAN-Passwort zu erschweren. Und das Gerätepasswort kann problemlos vom Kunden gelesen werden, d.h. ohne dass der Kunde Zeichen verwechseln kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-37/3.6

Req 38	Es darf nicht möglich sein, ein WLAN Passwort zu setzen, welches kürzer als 8 Zeichen ist.
--------	--

Der Anhang M.4 des Standards IEEE802.11-2012 definiert eine Passphrase (hier: ein WLAN Passwort) als Sequenz von 8-63 ASCII-codierte Zeichen. Da es technisch möglich ist, WLAN Schlüssel auch von kürzeren WLAN Passwörtern abzuleiten, wird hier eine in Bezug auf die Mindestlänge zu Annex M.4 konforme Implementierung eingefordert. Das Home Gateway muss sicherstellen, dass der Benutzer nur ein mindestens aus 8 Zeichen bestehendes WLAN Passwort setzen kann.

Motivation: Diese Anforderung soll lediglich einen Minimalstandard definieren. Insbesondere aus Gründen der Benutzbarkeit soll keine strenge Richtlinie definiert werden, die ausschließlich starke WLAN Passwörter erlaubt.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

6.4. USB Subsystem

Req 39	Das Home Gateway darf keinen Code ausführen, der auf USB-Massenspeichergeräten gespeichert ist.
--------	---

Das Home Gateway muss jede Partition eines externen USB-Massenspeichers nur als „nicht-ausführbar“ in sein Dateisystem einbinden.

Motivation: Die Ausführung von Code auf externen Massenspeichern ist nicht erforderlich und könnte für Angriffe missbraucht werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-39/3.6

Req 40	Nur die benötigten USB Geräteklassen dürfen durch das Linux Betriebssystem des Home Gateways unterstützt werden.
--------	--

Typischerweise unterstützt ein Linux Betriebssystem viele USB Geräteklassen, die nicht für Funktionen des Home Gateways benötigt werden. Die Anzahl der unterstützten Geräteklassen muss daher auf die für den Betrieb notwendigen eingeschränkt werden. Bei einem typischen Home Gateway sind dies Massenspeicher und Drucker. Andere Klassen dürfen dann nicht seitens der Firmware unterstützt werden.

Motivation: Jede zusätzliche Gerätekategorie kann ein Sicherheitsrisiko darstellen, wenn ein Angreifer Zugang zum USB-Port des Home Gateways erhält.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-40/3.6

6.5. DECT / CAT-iq Subsystem

Req 41	Die DECT/CAT-iq-Basisstation im Home Gateway muss eine beidseitige Authentisierung zwischen einem Schnurlostelefon und der Basisstation durchsetzen.
--------	--

Schnurlostelefone, die keine beidseitige Authentisierung unterstützen, müssen aus dem DECT/CAT-iq Netz ausgeschlossen werden. Zudem muss die DECT Basisstation den aktuellen DSSA2 Algorithmus zur Authentifizierung verwenden und der "authentication code" muss mindestens 32 Bit lang sein.

Motivation: Ohne beidseitige Authentisierung kann die DECT-Verbindung nicht als sicher betrachtet werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-41/3.6

Req 42	Die DECT/CAT-iq-Basisstation im Home Gateway muss eine Verschlüsselung der Übertragung von Sprach- und Signalisierungsdaten zum Schnurlostelefon durchsetzen.
--------	---

Schnurlostelefone, die keine verschlüsselte Übertragung unterstützen, müssen aus dem DECT/CAT-iq Netz ausgeschlossen werden. Zudem darf die DECT Basisstation nur sichere Verschlüsselungsalgorithmen neuerer DECT standards wie den LU14 Algorithmus anbieten.

Motivation: Wenn die Datenverschlüsselung nicht vom Home Gateway durchgesetzt wird, dann könnten Sprach- und Signalisierungsdaten in Klartext übermittelt und problemlos abgehört werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

ID: 3.40-42/3.6

Req 43	Die DECT-Basisstation im Home Gateway muss zur Erzeugung von Schlüsselmatrial einen kryptographisch starken Zufallszahlengenerator nutzen.
--------	--

Kryptographisch starke Zufallszahlen können durch Anwendung eines guten (Pseudo-) Zufallszahlengenerators generiert werden, der gleichverteilte Zufallszahlen erzeugt. Solche Generatoren sind im RFC 4086 beschrieben. Hinweis: Auf Embedded-Linux-Systemen gelten die Zufallszahlengeneratoren (RNG), die vom Kernel über die beiden Geräte /dev/random und /dev/urandom bereitgestellt werden, als kryptographisch stark, wenn die Implementierung sicherstellt, dass die Initialisierung des Linux RNG (Seeding) beim Systemstart für genug Entropie sorgt. z. B. ist das Seeding des Linux RNG bei jedem Gerätestart mit demselben konstanten Wert nicht zu empfehlen.

Motivation: Einige DECT-Implementierungen generieren Verschlüsselungsschlüssel mit schwachen Zufallszahlen. Dies ermöglicht Brute-Force-Angriffe auf den Verschlüsselungsschlüssel und Gespräche könnten abgehört werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

ID: 3.40-43/3.6

7. Web GUI

7.1. Embedded HTTP Server

Req 44	Der eingebettete HTTP-Server auf dem Home-Gateway muss in einer absoluten Minimalkonfiguration installiert sein.
--------	--

Funktionen des HTTP-Servers, die nicht für den Betrieb des Home Gateways benötigt werden, müssen z. B. per Konfiguration deaktiviert werden. Dies beinhaltet insbesondere die folgenden Anforderungen:

- Die Erstellung von Verzeichnislisten (Directory Listing) muss deaktiviert werden.
- Nur die benötigten HTTP-Methoden, beispielsweise nur GET und POST, dürfen aktiviert werden.
- Der HTTP-Server darf keine Server Side Includes (SSI) unterstützen.

Motivation: Jede zusätzliche Komponente kann Sicherheitsschwachstellen aufweisen und dann für einen Angriff auf den HTTP-Server ausgenutzt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-44/3.6

Req 45	Das Document-Root-Verzeichnis des Web-Servers muss ein von allen Systemverzeichnissen getrenntes Verzeichnis sein, und es darf keine Dateien mit vertraulichen Informationen enthalten.
--------	---

Motivation: Ein Angreifer kann auf Dateien im Document-Root-Verzeichnis des Web-Servers zugreifen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-45/3.6

Req 46	Das CGI-Verzeichnis darf keine ausführbare Dateien enthalten, die für Angriffe verwendet werden können, z. B. Interpreter und Shells.
--------	---

Systemverzeichnisse wie /bin oder /usr/bin auf UNIX-Systemen dürfen nicht als CGI-Verzeichnis verwendet werden. Es dürfen keinerlei sensible Dateien in das Verzeichnis cgi-bin abgelegt werden, da sie über den Web-Server einfach zugänglich wären. Das CGI-Verzeichnis muss ein separates Verzeichnis innerhalb des Document-Root-Verzeichnisses sein.

Motivation: Ausführbare Systemdateien im CGI-Verzeichnis können für Angriffe verwendet werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System

ID: 3.40-46/3.6

7.2. Basic GUI Hardening

Req 47 Die Web GUI darf nur über private LAN/WLAN-Schnittstellen erreichbar sein.

Das Home Gateway darf keine Konfigurationsoption zur Verfügung stellen, welche die Erreichbarkeit der Web-GUI über eine WAN-Schnittstelle nach sich ziehen würde.

Motivation: Die Web-GUI ermöglicht sicherheitsrelevante Konfigurationen des Home Gateway. Um die GUI- Anwendung vor Angriffen zu schützen, darf sie ausschließlich über das Heimnetzwerk zugänglich sein.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-47/3.6

Req 48 Die Web GUI muss den Browser daran hindern, den Inhalt von Passwort-Formularfeldern zu speichern.

Diese Anforderung gilt für die automatische Vervollständigung (Autocomplete) von Formularfeldern mit dem GUI-Gerätepasswort, der Kennung für den Internet-Zugang, für die VoIP-Telefonie sowie von Formularfeldern mit beliebigen anderen Kennungen. Diese Funktion der Browser erleichtert Schadsoftware das Auslesen der vertraulichen Formulardaten.

Motivation: In einem Web-Browser gespeicherte vertrauliche Formular-Daten können leicht kompromittiert werden.

Umsetzungsbeispiel: Die automatische Vervollständigung wird durch Hinzufügen des Attributs „autocomplete“ mit dem Wert „off“ innerhalb des Formularelements deaktiviert. Dies kann entweder direkt in einem Input-Tag vorgenommen werden

```
<input name = "pass" type= "password" autocomplete = "off"/>
```

oder in einem Form-Tag

```
<form name = "form" action = "" autocomplete ="off"> </form>.
```

Mit der ersten Variante sollte die Speicherung aller genau in dieses Feld eingegebenen Daten verhindert werden, während die zweite Variante sicherstellt, dass die in allen Formularfeldern eingegebenen Daten nicht gespeichert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-48/3.6

Req 49 Jedwede Ausgabe der Web-GUI darf keine vertraulichen Daten enthalten, deren Auslieferung nicht im Rahmen eines validen Use Cases erforderlich ist.

Insbesondere Benutzernamen und Passwörter werden hier als „vertrauliche Daten“ betrachtet. So existiert z. B. kein Anwendungsfall zur Anzeige des konfigurierten Passworts für den Internet-Zugang in der Web-GUI. Daher darf die Web-GUI keine Funktion implementieren, die das Auslesen dieses Passworts ermöglicht.

Motivation: Die Web-GUI darf keine vertraulichen Daten offenlegen, die nicht zur Erbringung eines der erlaubten Anwendungsfälle benötigt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.40-49/3.6

Req 50	Alle vom Client gesendeten Eingabedaten müssen durch die Web GUI Anwendung validiert werden.
--------	--

Die Mindestanforderung hinsichtlich der Validierung ist, dass zumindest die Parameterlänge und der erlaubte Zeichensatz überprüft werden.

Motivation: Auf diese Weise werden ungültige Konfigurationsdaten im Home Gateway verhindert.

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: 3.40-50/3.6

Req 51	Bestandteil jedes Requests zur Web GUI Anwendung, der Daten ausliest oder verändert, muss ein „Anti-CSRF-Token“ als verstecktes Feld enthalten. Ein Ausführen der angeforderten Aktion durch die Web GUI darf erst nach der erfolgreich Validierung des Tokens erfolgen.
--------	--

Das Anti-CSRF Token ist eine Zufallszahl, d.h. ein Attribut, welches für einen Angreifer nicht vorhersagbar ist. Das Anti-CSRF-Token muss bei jedem Request validiert werden, der bewirken soll, dass Daten auslesen oder geändert werden. Wenn die Web GUI Anwendung ein ungültiges Anti-CSRF Token erhält, dann darf die angefragte Operation nicht ausgeführt werden, und die aktive Session muss beendet werden.

Wenn die Realisierung eines versteckten Felds nicht möglich oder vertretbar ist, beispielsweise bei Nutzung von AJAX, dann kann das Anti-CSRF-Token auch in einem eigenen HTTP-Header (z. B. „X-anti-CSRF-Token“) übertragen werden.

Motivation: Requests, die nicht auf diese Art geschützt werden, sind für Cross-Site Request Forgery Angriffe (XSRF oder CSRF, auch als „Session Riding“ bezeichnet) anfällig. Hier wird das Opfer dazu bewogen, unwissentlich einen vorbereiteten HTTP-Request zu senden, der dann in einer laufenden Sitzung eine Aktion in seinem Namen auslöst. Dies kann zum Beispiel geschehen, wenn eine schädliche Website besucht wird, die einen entsprechenden Link, z. B. als ein img-, script- oder iframe-Tag, zu einer anderen Anwendung enthält. Das Opfer ist sich dieses Links nicht bewusst, aber der Browser folgt dem Link und löst – gewissermaßen im Hintergrund – dann erfolgreich eine Aktion aus, wenn das Opfer gegenwärtig eine gültige Sitzung für diese andere Anwendung besitzt. Die Einbettung des Tokens als verstecktes Feld bedeutet, dass POST-Requests zur Veränderung von Daten verwendet werden müssen. Um einen umfassenden Schutz vor CSRF-Angriffen sicherzustellen, müsste für jede einzelne Anfrage in einer Web-Anwendung, die zu einer Veränderung von Daten führt, ein anderer Anti-CSRF-Token verwendet werden. Dies verhindert, dass abgefangene Anti-CSRF-Token für einen CSRF-Angriff verwendet 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: 3.40-51/3.6

7.3. User Authentication

Req 52	Der Nutzer muss sich vor Nutzung der Web GUI Anwendung mit dem Gerätepasswort authentisieren.
--------	---

Die Web GUI darf hierbei nur einen einzelnen Nutzer unterstützen: den Geräteadministrator. Dieser Nutzer muss sich über sein Gerätepasswort authentifizieren. Diese Authentifizierung muss erforderlich sein, um auf personalisierte Seiten der Web GUI zugreifen zu können. Nur die Login-Seite selbst oder z.B. eine Statusseite, die lediglich nicht-vertrauliche Daten anzeigt, dürfen ohne Authentifizierung zugänglich sein.

Motivation: Das Home Gateway könnte leicht von einem Angreifer missbraucht werden, wenn ein Zugang zu Ressourcen der Web-GUI ohne Authentisierung möglich ist.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-52/3.6

Req 53	Ein Authentifizierungsprotokoll mit einem challenge handshake Mechanismus vergleichbar zu CHAP nach RFC1994 muss implementiert werden, um das Gerätepasswort zu verifizieren.
--------	---

Die wesentlichen Elemente eines zu RFC1994 konformen CHAP Authentifizierungsprotokolls sind:

- Das Home Gateway sendet zu Beginn eines Authentifizierungsvorgangs eine sogenannte challenge zum Client.
- Die Antwort des Clients auf diese challenge (der Login Request) enthält einen Hashwert der challenge und des Gerätepassworts. Es wird kein Klartextpasswort mehr übertragen.
- Als challenge wird eine Zufallszahl verwendet, um Replay und Rateangriffe zu verhindern bzw. zu erschweren.

Die challenge C muss mindestens eine 64-bit lange Zufallszahl sein, die vor jedem Login Vorgang generiert und zum Client gesendet wird. Geeignete Zufallszahlen können mit einem guten Pseudozufallszahlengenerator für gleichverteilte Zufallszahlen erzeugt werden. Solche Generatoren werden beispielsweise im RFC4086 beschrieben. Die Länge der challenge C muss konstant sein. Und C muss so lang gewählt werden, dass die Summe aus der minimalen Passwortlänge (in Bits) und von C (in Bits) der Länge der verwendeten Hashfunktion (in Bits) entspricht. Die minimale Passwortlänge wird als 48 Bits festgelegt. Sofern die Hashfunktion SHA-256 verwendet wird, muss C die Länge von 208 Bits aufweisen. Die challenge sollte als hexadezimalzahl oder base-64 codiert werden.

Die challenge C kann als identifier einer nicht-authentifizierten Sitzung der Web GUI verwendet werden.

Als Hashfunktion muss ein Algorithmus der Secure Hash Algorithm Familie verwendet werden, die in FIPS180-4 beschrieben ist. Es wird empfohlen, SHA-1, SHA-224 oder SHA-256 zu nutzen.

Motivation: Ein challenge handshake Authentifizierungsprotokoll vermeidet die Klartextübertragung des Gerätepassworts. Dieses wird hier lediglich als Hash übertragen. Replay und systematische Rateangriffe werden durch die challenge, eine lange Zufallszahl, verhindert oder zumindest erschwert. Im referenzierten RFC1994 wird MD5 als Hashfunktion festgelegt. MD5 wird hier jedoch nicht empfohlen, da dieser Algorithmus sich sehr performant implementieren lässt. Somit schützt MD5 nicht mehr zuverlässig das Gerätepasswort.

Umsetzungsbeispiel: Die Stanford JavaScript Cryptographic Library "sjcl" implementiert derzeit nur die SHA-256 Hashfunktion. Es wird daher empfohlen, die Funktion "Sjcl.hash.sha-256" zu nutzen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

ID: 3.40-53/3.6

-
- Req 54 Gerätepasswörter, die den folgenden Anforderungen genügen, müssen in jedem Home Gateway vorkonfiguriert werden:
- Das Gerätepasswort besitzt eine Länge von mindestens 12 Zeichen.
 - Ein Passwort wird jeweils nur bei einem einzelnen Gerät verwendet.
 - Das Passwort besteht aus einer zufälligen ASCII-Zeichenfolge bestehend aus Ziffern (0 – 9) und aus Buchstaben.

Motivation: Ein identisches Standardpasswort für alle Geräte ermöglicht Angriffe (unbefugter Zugriff auf das Gerät), wenn der Nutzer das Standardpasswort nicht ändert. Dies wird durch ein individuelles Gerätepasswort verhindert. Dank des begrenzten, nur aus Zahlen bestehenden Zeichensatzes, kann das vorkonfigurierte Gerätepasswort leicht, d.h. ohne dass Zeichen wie z. B. der Großbuchstabe „O“ und die Zahl „0“ verwechselt werden können, vom Kunden abgelesen werden.

Umsetzungsbeispiel: Eine ausreichende Zufälligkeit bei der Generierung der Gerätepasswörter kann durch den Einsatz eines starken Pseudozufallszahlengenerators erreicht werden, der gleichverteilte Zufallszahlen erzeugt. Geeignete Generatoren sind im RFC 4086 beschrieben.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-54/3.6

-
- Req 55 Bei jeder Passwortänderung müssen die folgenden Regeln für das Gerätepasswort durchgesetzt werden:
- Die Länge des Passworts muss im Bereich von 8 bis 32 Zeichen liegen.
 - Das Passwort muss aus zwei verschiedenen Zeichenklassen bestehen.
 - Gültige Zeichenklassen für das Passwort sind Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (z. B. “!”\$%&/()=+*#;,:.”).

Motivation: Ein triviales Passwort könnte von einem Angreifer schnell erraten werden. Diese Regeln stellen lediglich absolute Mindestanforderungen für „sichere“ Passwörter dar. Es obliegt der Verantwortung des Benutzers, hier nicht zu triviale Passwörter zu wählen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-55/3.6

7.4. Session Management

-
- Req 56 Die Web GUI Anwendung des Home Gateways muss Session-Cookies verwenden (Cookies, die eine Session-ID enthalten), um eine sichere Sitzungsverwaltung zu implementieren.

Motivation: Ein sicherer Sitzungsmechanismus schützt den Zugang zur Web-GUI.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

-
- | | |
|--------|---|
| Req 57 | Eine Session-ID (das Session-Cookie) darf nicht erratbar sein, das heißt: <ul style="list-style-type: none">• Die Session-ID muss für jede Sitzung eindeutig sein.• Die Entropie der Session-ID muss mindestens 64 Bit betragen, d. h. > 20 Ziffern [0...9] oder > 10 Zeichen [A-Z, a-z, 0-9].• Session-IDs müssen jedes Mal beim Start einer Sitzung als Zufallszahl generiert werden. |
|--------|---|
-

Motivation: Da die Web-GUI eine Einzelnutzeranwendung ist, definieren diese vergleichsweise schwachen Anforderungen an eine Session-ID ein angemessenes Sicherheitsniveau für diese Anwendung des Home Gateways. Das bedeutet, dass ein Angreifer die jeweils einzige gültige ID der Sitzung eines authentisierten Nutzers nicht erraten kann.

Umsetzungsbeispiel: Zufällige Session-IDs können durch Anwendung eines guten (Pseudo-) Zufallszahlengenerators erreicht werden, der gleichverteilte Zufallszahlen erzeugt. Solche Generatoren sind im RFC 4086 beschrieben.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

-
- | | |
|--------|---|
| Req 58 | Die Web GUI des Home Gateway darf jeweils nur eine aktive authentifizierte Sitzung akzeptieren. |
|--------|---|
-

Der Benutzer sollte darüber informiert werden, dass er sich nicht korrekt abgemeldet hat, wenn er durch erneutes Anmelden am Home Gateway eine bestehende Admin-Sitzung terminiert und eine neue Sitzung etabliert.

Motivation: Das Home Gateway kann nur von einem Administrator verwaltet 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

-
- | | |
|--------|---|
| Req 59 | Die Web GUI des Home Gateways muss eine Funktion zum Abmelden besitzen („Logout-Button“), die dem Benutzer das Beenden seiner bestehenden Sitzung ermöglicht. |
|--------|---|
-

Durch das Abmelden muss die bestehende Session ID sofort invalidiert werden.

Motivation: Der Nutzer muss die Möglichkeit haben, sich explizit abzumelden (Logout).

Für diese Anforderung sind folgende Bedrohungen relevant:

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

-
- | | |
|--------|---|
| Req 60 | Die Web GUI des Home Gateways muss eine authentifizierte Sitzung spätestens nach 20 Minuten Inaktivität invalidieren. |
|--------|---|
-

Motivation: Meldet sich ein Nutzer nicht explizit ab, dann muss die Sitzung nach einem angemessenen Zeitraum beendet werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-60/3.6

7.5. Transport Security

Req 61	Die Web GUI muss Transport Layer Security (TLS) unterstützen.
--------	---

Die Web GUI muss auch über HTTPS erreichbar sein. Diese Einstellung muss im Werkszustand aktiv sein.

Motivation: Selbst in einem geschützten Heimnetzwerk kann es einem Angreifer gelingen, Nachrichten zwischen einem Client und der Web GUI des Home Gateways zu belauschen. Auch wenn dieser Fall unwahrscheinlich erscheinen mag, so darf der Angreifer nicht einfach in der Lage sein, in den Nachrichten enthaltene vertrauliche Daten (bspw. Passworte) mitzulesen oder Konfigurationsänderungen zu manipulieren.

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: 3.40-61/3.6

Req 62	Das Home Gateway muss ein gerätespezifisches self-signed Server Zertifikat für TLS besitzen.
--------	--

Das Serverzertifikat für TLS muss auf dem Home Gateway generiert werden, und der private Schlüssel zum Server Zertifikats muss auf dem Home Gateway entsprechend geschützt werden.

Motivation: In einem privaten Heimnetzwerk kann nicht einfach eine kommerzielle CA genutzt werden, die bereits von Betriebssystemen und Browsern als vertrauenswürdig angesehen wird. Daher wird ein auf dem Gerät generiertes self-signed Server Zertifikat verwendet, welches der erfahrene Benutzer in seinem Browser oder Betriebssystem manuell als vertrauenswürdig konfigurieren kann, damit kein Aufruf der Web GUI über TLS keine Zertifikats-Warnmeldungen mehr erscheinen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-62/3.6

Req 63	Wenn das Home Gateway in den Werkszustand zurück gesetzt wird, dann muss ein neues TLS Server Zertifikats generiert werden.
--------	---

Motivation: Das TLS Serverzertifikat wird als ein zur Benutzerkonfiguration zugehöriges Datum angesehen, da ein Nutzer dieses Zertifikat ggf. in seine Endgeräte importiert. Daher wird es wie andere Benutzerdaten auch bei einem Werksreset gelöscht.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unbemerkt durchführbare Angriffe

ID: 3.40-63/3.6

7.6. Protection of Configuration Data

Req 64	Vertrauliche Konfigurationsdaten müssen verschlüsselt gespeichert werden und der Advanced Encryption Standard (AES) muss zur Verschlüsselung geschützt werden.
--------	--

Insbesondere Benutzernamen, Passworte (auch das WLAN Passwort) und geheime kryptographische Schlüssel werden hier als vertrauliche Daten betrachtet. Diese Konfigurationsdaten müssen verschlüsselt gespeichert werden, dies betrifft die Speicherung:

- innerhalb des Home Gateways,
- in der Backup-Datei, die über die Web GUI exportiert werden kann, sowie
- in der Backup-Datei, die über das Remote Device Management (z.B. mittels TR-069) exportiert werden kann.

AES unterstützt die Schlüssellängen 128, 192 und 256 Bits. Die bevorzugte Schlüssellänge ist hier 256 Bits. Der AES Schlüssel zur Verschlüsselung der Konfigurationsdaten wird in diesem Dokument als "backup-key" bezeichnet.

Motivation: Die vertraulichen Konfigurationsdaten müssen angemessen vor der Kompromittierung durch einen Angreifer geschützt werden, d.h. in der Backup-Datei sowie im Filesystem des Routers müssen diese Daten verschlüsselt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

ID: 3.40-64/3.6

Req 65	Der backup-key muss zur Laufzeit von einem Schlüssel-spezifischen Satz von Attributen abgeleitet werden. Eigenschaften der jeweiligen Hardware sowie eine Zufallszahl müssen Bestandteil der Attribute sein.
--------	--

Der backup-key muss zur Laufzeit berechnet werden, beispielsweise während des Startvorgangs des Home Gateways. Der Algorithmus zur Ableitung des Schlüssels muss sicherstellen, dass ein ohne Kenntnis des Algorithmus und der Attribute nicht vorhersagbarer, Geräte-spezifischer Schlüssel erzeugt wird. Daher müssen die Attribute und der Algorithmus zur Ableitung des Schlüssels verschleiert (geschützt) im Flash Speicher abgelegt werden.

Alternativ kann der backup-key auch von einem spezifischen Benutzerpasswort zum Schutz des Backups abgeleitet werden. Dies würde die Übertragung von Backupdateien zwischen verschiedenen Geräten eines Typs ermöglichen.

Motivation: Ein -- ohne die Kenntnis der Attribute oder des Algorithmus zur Schlüsselableitung -- zufällig aussehender AES backup-key verhindert systematische Rateangriffe auf den Schlüssel.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

ID: 3.40-65/3.6

7.7. System Log

Req 66	Die Anwendung muss eine Funktion zur Darstellung von Systemmeldungen besitzen, damit der Benutzer über sicherheitsrelevante Ereignisse informiert werden kann.
--------	--

Die folgenden Ereignisse werden als sicherheitsrelevant betrachtet und für den Benutzer aussagekräftige Systemmeldungen müssen festgelegt werden:

- Erfolgreiche sowie fehlgeschlagene Anmeldevorgänge an:
 - der Web GUI
 - dem TR-064 Interface
 - dem FTP(S) Service
 - dem NAS Service
 - dem WLAN
- Die Aktivierung des WPS/WSC Registrierungsprotokolls sowie der Austausch des WLAN Passworts.
- Das Erreichen des Sperrzustands des WPS/WSC Subsystems. Weitere WPS/WSC Anfragen werden dann abgewiesen.
- Angriffe, die von der Firewall erkannt und verhindert werden. Entsprechend den Firewall Sicherheitsanforderung.
- Erfolgreiche und fehlgeschlagene Verbindungen zum Auto Configuration Server (TR-069).

Treten viele Ereignisse innerhalb eines kurzen Zeitintervalls auf, dann können diese zu einer Meldung zusammengefasst werden.

Motivation: Der Benutzer soll über den Sicherheitszustand seines Home Gateways informiert werden. Er soll in der Lage sein, einige Angriffe zu erkennen, beispielsweise wenn ein Angreifer versucht das Gerätepasswort zu erraten.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unbemerkt durchführbare Angriffe

ID: 3.40-66/3.6

8. Services

8.1. SIP User Agent

Req 67	Die Implementierung des RTP-Protokolls muss gewährleisten, dass keine vertraulichen Informationen über die Quelle des Datenstroms offengelegt werden.
--------	---

RTP beinhaltet das Steuerprotokoll RTCP (Real Time Control Protocol); beide Protokolle sind in RFC3550 definiert. Über die Protokollnachricht SDES (Source Description) des RTCP-Protokolls können Informationen über die Quelle (Source-IP) des RTP-Datenstroms offengelegt werden, die der Kommunikationspartner sonst nicht erhalten würde. Daher gilt die Anforderung: Weder das CNAME Element noch irgendein anderes Feld der SDES-Nachricht darf die WAN-IP-Adresse bzw. den DNS-Namen des Home Gateways oder einen Benutzernamen (bspw. des VoIP-Kontos) enthalten.

Motivation: Damit wird verhindert, dass ein Angreifer über eine VoIP-Verbindung die WAN-IP-/E-Mail-Adresse des Gesprächspartners erfahren kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unbemerkt durchführbare Angriffe

ID: 3.40-67/3.6

Req 68	Der SIP User Agent darf nur SIP-Nachrichten von der Call-Control entgegennehmen und verarbeiten, bei der die Registrierung erfolgt ist.
--------	---

Motivation: Wenn der SIP User Agent SIP-Anfragen von jeder beliebigen Quelle entgegennimmt, dann kann er leicht angegriffen werden. Eine Beschränkung der Konnektivität auf die registrierte Call Control schützt den SIP User Agent vor Angriffen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.40-68/3.6

8.2. WAN Management Protocol

Req 69	Das TR-069 Protokoll des Broadband Forums muss als Protokoll zur Fernwartung des Home Gateways implementiert werden.
--------	--

TR-069 ist ein etabliertes Protokoll zur Fernwartung bei dessen Design notwendige Sicherheitsaspekte beachtet wurden. Die Fernwartung muss im Auslieferungszustand aktiviert sein. Die Implementierung der Fernwartung muss eine automatische Aktualisierung der Firmware des Home Gateways ohne weitere Benutzerinteraktion vorsehen.

Motivation: Die Deutsche Telekom Gruppe setzt auf etablierte und sichere Industriestandards zur Fernwartung ihrer Home Gateways.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-69/3.6

Req 70 Die URL für den HTTP basierten connection request muss für jedes Gerät individuell sein.

Die connection request URL darf nicht identisch für alle Geräte sein. Denn sonst könnte ein Angreifer versuchen, bei einer großen Gerätezahl den connection request auslösen, was zu einem Denial-of-service beim Auto Configuration Server führen würde. Eine gerätespezifische Connection Request URL kann durch Ableitung der URL von einer Zufallszahl oder von geeigneten gerätespezifischen Attributen erreicht werden.

Motivation: Andernfalls könnte ein Angreifer problemlos eine DoS-Attacke auf den Autokonfigurationsserver vornehmen.

Umsetzungsbeispiel: Eine ausreichende Zufälligkeit kann durch die Generierung der connection request URLs mittels eines starken Pseudo-Zufallszahlengenerators erreicht werden. Solche Generatoren sind beispielsweise im RFC 4086 beschrieben.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.40-70/3.6

Req 71 Das Home Gateway muss die Zertifikatkette des TLS-Serverzertifikats des Autokonfigurationsservers entsprechend den Vorgaben des Kapitels 6 des RFC3280 validieren.

Motivation: Nur wenn das Serverzertifikat des ACS gültig ist, kann das Home Gateway der Serverauthentisierung vertrauen und damit gewährleisten, dass es mit dem echten Autokonfigurationsserver kommuniziert.

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: 3.40-71/3.6

Req 72 Die TR-069-Implementierung darf nicht das Auslesen eines Passworts im Klartext ermöglichen.

Weder über die TR-069 Methoden GetParameterValues, GetParameterAttributes noch über die Upload Methode (nutzbar zum Export der Konfiguration) dürfen schützenswerte Passwörter im Klartext auslesbar sein.

Motivation: Die Datenbank des Autokonfigurationsservers darf keine Nutzerpasswörter enthalten. Der Abruf von Passwörtern in Klartext ist kein im Rahmen der Fernwartung benötigter Anwendungsfall. Es kann eventuell erforderlich sein, verschlüsselte Passwörter auszulesen (z. B. als Teil einer Gerätekonfigurationsdatei), um einen Backup- und Restore-Funktion bereit zu stellen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-72/3.6

8.3. LAN Management Protocol

Req 73 Das Protokoll TR-064 des Broadband Forums muss zur maschinellen LAN-seitigen Konfiguration implementiert werden.

Diese Anforderung ist nur zutreffend, wenn Funktionen zur maschinellen LAN-seitigen Konfiguration für das Home Gateway Entwicklungsprojekt relevant sind.

Tr-064 ist vergleichbar zum UPnP IGD Profil (Universal Plug and Play Internet Gateway Device Profil), nur dass das TR-064 Protokoll bei UPnP fehlende Sicherheitsfunktionen vorsieht, beispielsweise zur Authentifizierung oder Autorisierung von Anfragen. Daher darf das unsichere UPnP IGD nicht implementiert werden.

Motivation: Die Gerätekonfiguration über TR-064 muss vergleichbar zur Web GUI abgesichert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-73/3.6

Req 74	Der TR-064-Service einschließlich des für TR-064 erforderlichen UPnP SSDP-Service darf nur über LAN- und private WLAN-Schnittstellen zugänglich sein.
--------	---

Das TR-064 Protokoll benötigt zum Betrieb zwei Dienste: Den SSDP Dienst (SSDP = Simple Service Discovery Protocol) sowie den TR-064 SOAP Web-Service. Beide Dienste sind zum Betrieb in einem geschützten Netzwerk vorgesehen. Daher muss die Verfügbarkeit dieser Dienste auf lokale LAN-Netzwerkschnittstellen beschränkt werden.

Motivation: TR-064 ist ein LAN-seitiger Konfigurationsservice; er ist nicht für WAN-seitige Zugriffe vorgesehen. Der Zugriff aus dem Internet auf diesen Dienst würde daher weitere Angriffe auf das Home Gateway ermöglichen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-74/3.6

Req 75	Alle TR-064-Methoden, mit denen Konfigurationsdaten des Home Gateways verändert und vertrauliche Daten (z. B. Benutzernamen, etc.) abgerufen werden können, dürfen nur nach einer erfolgreichen HTTP-Digest-Authentisierung mit dem Gerätepasswort aufrufbar sein.
--------	--

Das Gerätepasswort muss hier als die Zustandsvariable "ConfigPasswort" verwendet werden, die im TR-064 Standard definiert wird. Da das Gerätepasswort auf das werksseitig vorkonfigurierte Passwort jederzeit zurückgesetzt werden kann, wird dir zusätzlich im TR-064-Standard definierte Variable "ResetPasswort" nicht benötigt, und diese Variable darf nicht implementiert werden.

Die Deutsche Telekom Gruppe stellt eine funktionale TR-064-Spezifikation bereit, die sicherheitsrelevante Methoden entsprechend kennzeichnet. Die Ausführung von sicherheitsrelevanten Methoden darf nur nach einer erfolgreichen Authentifizierung möglich sein. Die HTTP-Digest-Authentisierung muss entsprechend RFC 2617 unter Verwendung der Option „cnonce“ implementiert werden.

Motivation: Einige der SOAP-Methoden von TR-064 lassen die Veränderung oder den Abruf vertraulicher oder sensibler Parameter zu. Diese Methoden müssen durch eine HTTP-Digest-Authentisierung geschützt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-75/3.6

Req 76	Der TR-64 Web Service muss Transport Layer Security (TLS 1.2) für alle Methoden implementieren, die eine Authentifizierung erfordern und die vertrauliche Daten transportieren.
--------	---

Im Rahmen von TLS sind sichere Cipher-Suites zu konfigurieren, d. h. Cipher-Suites haben Serverauthentifizierung und Datenverschlüsselung mit einer Mindest-Schlüssellänge von 128 Bit zu unterstützen.

Motivation: Selbst im LAN sollten in TR-064 SOAP-Nachrichten übertragene vertrauliche Daten verschlüsselt werden, und die Integrität der Kommunikation sollte garantiert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-76/3.6

Req 77	Der TR-064-Webservice muss jeden SOAP-Request validieren, so dass fehlerhafte Anfragen, z. B. solche mit ungültigen Parametern, abgelehnt werden.
--------	---

Motivation: Es soll verhindert werden, dass durch fehlerhafte Requests (z. B. durch zu lange Parameter) Buffer-Overflows auftreten können, die die Stabilität oder die Sicherheit des Home Gateway beeinträchtigen würden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Störung der Verfügbarkeit

ID: 3.40-77/3.6

Req 78	Die TR-064-Methoden "AddPortMapping" und "AddForwardingEntry" dürfen für interne Clients nur IP Adressen aus dem Adressbereich des Heimnetzwerkes (LAN und privates WLAN) akzeptieren. Diese Methode dürfen jedoch nicht eine IP-Adresse einer beliebigen LAN/WLAN-Schnittstelle des Home Gateways selbst akzeptieren.
--------	--

Die TR-064 Implementierung muss das Weiterleiten von Verbindungen auf Systeme im Heimnetzwerk beschränken, wobei das Home Gateway selbst hier ausgenommen werden muss. Insbesondere darf die TR-064 Implementierung nicht das Weiterleiten zu Systemen im Internet gestatten.

Motivation: Es muss verhindert werden, dass LAN-seitige Dienste des Home Gateways im Internet exponiert werden können, oder dass das Home Gateway in einen Proxy verwandelt werden kann, der für Angriffe genutzt 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
- Unbemerkt durchführbare Angriffe

ID: 3.40-78/3.6

Req 79	Die TR-064 Implementierung darf nicht das Auslesen von Passwörtern im Klartext ermöglichen.
--------	---

Jede Zustandsvariable, die ein schützenswertes Passwort enthält, darf nicht im Klartext auslesbar sein. Dies trifft auf nahezu alle Passworte zu; ausgenommen ist lediglich das WLAN Passwort.

Motivation: Passworte werden als vertrauliche Daten betrachtet, und wenn diese einmal im Home Gateway gespeichert wurden, dann dürfen diese nicht mehr auslesbar sein. Ausnahmen von dieser Anforderung müssen mit Bedacht

und unter Berücksichtigung valider Nutzungsszenarien gewählt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-79/3.6

8.4. Home Media Sharing

Req 80	Der UPnP A/V Server darf nur über das Heimnetzwerk (LAN- und private WLAN-Schnittstellen) erreichbar sein.
--------	--

Der UPnP A/V (DLNA) Dienst wurde als Dienst für ein Heimnetzwerk entworfen, denn dieser Dienst verzichtet auf eine Authentifizierung und erlaubt somit einen ungeschützten Zugriff auf die Mediendaten eines angeschlossenen USB-Speichermediums. Daher dürfen alle Dienste des UPnP A/V Servers nur im Heimnetzwerk erreichbar sein. Das Heimnetzwerk ist nur über LAN oder private WLAN Schnittstellen erreichbar.

Motivation: Nur Teilnehmer des Heimnetzwerkes dürfen auf die Mediendaten ohne Authentifizierung zugreifen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-80/3.6

Req 81	Der UPnP A/V Server muss den Zugriff auf das Dateisystem auf Dateisysteme des angeschlossenen USB Speichermediums beschränken.
--------	--

Das interne Dateisystem des Home Gateways darf nicht über den UPnP A/V Server erreichbar sein.

Motivation: Der UPnP A/V Server muss den Zugriff auf Systemdateien im internen Flash Dateisystem des Home Gateways verhindern, um Konfigurations- und Systemdateien zu schützen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-81/3.6

8.5. Network Attached Storage (SMB/CIFS)

Req 82	Der NAS-Server darf nur über das Heimnetzwerk (LAN- und private WLAN-Schnittstellen) zugänglich sein.
--------	---

Motivation: Der NAS-Server ist ein Dienst für das Heimnetzwerk. Einige Nutzer verwenden ggfls. keine Authentisierung zum Zugriff auf ihre Netzlaufwerke. In diesem Fall wären alle Daten im Internet zugänglich, wenn der NAS-Server auch über das WAN-Interface erreichbar ist.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-82/3.6

Req 83	Der NAS Server muss den Zugriff auf das Dateisystem auf Dateisysteme des angeschlossenen USB Speichermediums beschränken.
--------	---

Ein Zugriff auf das interne Dateisystem des Home Gateways über den NAS Dienst muss verhindert werden.

Motivation: Der NAS Server muss den Zugriff auf Systemdateien im internen Flash Dateisystem des Home Gateways verhindern, um Konfigurations- und Systemdateien zu schützen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-83/3.6

Req 84	Der NAS-Server muss Benutzer mit verschiedenen Zugangsberechtigungen zum Dateisystem des angeschlossenen Massenspeichers unterstützen.
--------	--

Es muss möglich sein, Passwörter für Benutzer des NAS Dienstes über die Web-GUI festzulegen.

Motivation: Über Nutzer und Zugangsberechtigungen kann der Kunde vertrauliche Informationen auf dem Dateisystem schützen und den Zugang zu Dateien auf einer Need-to-Know-Basis erlauben. Eine Nutzerauthentisierung ist obligatorisch, sofern der Kunde solche Zugangsberechtigungen durchsetzen möchte.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-84/3.6

Req 85	Beim Setzen der NAS-Benutzerpassworte muss das Home Gateway folgende Richtlinie durchsetzen: • Das Passwort ist 8 bis 32 Zeichen lang. • Das Passwort kann aus den Zeichenklassen Zahlen, Groß-/Kleinbuchstaben sowie Sonderzeichen (z. B. "!"\$%&/()=+*#>.,,") bestehen. • Das Passwort muss aus mindestens zwei Zeichenklassen bestehen.
--------	---

Motivation: Durch Durchsetzung einer Mindestpasswortlänge wird sichergestellt, dass keine extrem einfach zu erratenden Passwörter gesetzt werden können (Mindestschutz).

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-85/3.6

8.6. File Transfer

Req 86	Zur Gewährleistung eines sicheren Dateitransfers über das Internet muss das FTPS-Protokoll unterstützt werden.
--------	--

FTPS verwendet die Sicherheitsfunktionen des TLS Protokolls, um eine Verschlüsselung sowie die Integrität der übertragenen Daten zu gewährleisten. Das FTP Protokoll bietet keine entsprechenden Sicherheitsmechanismen, wenn es über ein unsicheres Netzwerk wie das Internet benutzt wird: alle übertragenen Daten, insbesondere auch die Zu-

gangsdaten (Benutzername/Passwort, werden im Klartext übertragen. Daher kann bei FTP die Kommunikation von einem Angreifer belauscht werden.

Motivation: Die Zugangs- sowie die Nutzerdaten dürfen nicht im Klartext über das Internet übertragen werden, weil sie dann einfach belauscht werden können. Daher muss ein sicheres Protokoll zur Dateiübertragung über unsichere Netzwerke unterstützt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-86/3.6

Req 87	Der FTP(S) Server muss die Benutzer- und Berechtigungsverwaltung des NAS-Servers verwenden.
--------	---

Der NAS Dienst implementiert bereits eine Benutzer und Berechtigungsverwaltung. Das NAS und Dateitransfer ähnliche Dienste darstellen, und der Benutzer des Home Gateways durch eine doppelte Verwaltung nicht unnötig belastet werden soll, ist nur ein System zur Verwaltung der Identitäten notwendig.

Motivation: Es besteht kein Bedarf für eine weitere Benutzerverwaltung auf dem Home Gateway.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unbemerkt durchführbare Angriffe

ID: 3.40-87/3.6

Req 88	Wenn ein FTP(S)-WAN-Zugang ermöglicht werden soll, dann muss der Benutzer des Home Gateways in der Lage sein, diesen WAN-Zugang für jeden NAS-Nutzer individuell zu aktivieren bzw. zu deaktivieren.
--------	--

Wenn ein neuer NAS oder FTP Nutzer angelegt wird, dann muss zunächst der Internet Zugriff (WAN Zugriff) auf den FTP Dienst deaktiviert sein. Der Administrator des Home Gateways muss für jeden Nutzer einzeln festlegen, ob dieser FTP(S) WAN-seitig nutzen kann.

Die Nutzerverwaltung muss auch ermöglichen, das FTPS (TLS) Protokoll WAN-seitig zu aktivieren. Der Administrator des Home Gateways muss gewarnt werden, Der Nutzer des Home Gateway MUSS von der Web-GUI gewarnt werden, wenn er WAN-seitig nur FTP aktiviert, dass nur FTPS über das Internet eine sichere Lösung darstellt.

Man beachte, dass die Ports für den FTP(S) Dienst am WAN-Interface geschlossen werden müssen, wenn kein FTP Benutzer mehr mit einer Internetberechtigung eingerichtet ist.

Motivation: Der Kunde kann so den Internet-Zugang nur für Ressourcen einrichten, auf die er vom Internet aus zugreifen möchte. Zudem kann so der Internet Zugang für den (S)FTP-Server ganz abgeschaltet 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

ID: 3.40-88/3.6

Req 89	Der FTP(S) Server muss den Zugriff auf das Dateisystem auf Dateisysteme des angeschlossenen USB Speichermediums beschränken.
--------	--

Das interne Dateisystem des Home Gateways darf nicht über den FTP(S) Server zugänglich sein.

Motivation: Der FTP(S) Server muss den Zugriff auf Systemdateien im internen Flash Dateisystem des Home Gateways verhindern, um Konfigurations- und Systemdateien zu schützen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.40-89/3.6

8.7. DNS Proxy

Req 90	Der DNS-Proxy muss konform zu den Anforderungen aus Kapitel 3 „Transparency Principle“ und Kapitel 4 „Protocol Conformance“ des RFC 5625 implementiert werden.
--------	--

Der DNS-Proxy des Home Gateways muss die Sicherheitserweiterungen des DNS Protokolls unterstützen, d.h. die „Secret Key Transaction Authentication for DNS“ (TSIG) nach RFC 2854 und die „DNS Security Extensions“ (DNSSEC) nach RFC 4033, RFC 4034, RFC 4035, und weitere. RFC 5625 definiert Richtlinien für die Implementierung eines DNS-Proxies. Speziell Kapitel 3 „Transparency Principle“ und Kapitel 4 „Protocol Conformance“ enthalten obligatorische Anforderungen für die Unterstützung von TSIG und DNSSEC.

Motivation: Das Home Gateway muss die Sicherheitserweiterungen des DNS Protokolls unterstützen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten

ID: 3.40-90/3.6

Req 91	Der DNS-Proxy muss die Antworten auf DNS Abfragen entsprechend den im Abschnitt 9.1 „Query Matching Rules“ des RFC 5452 definierten Regeln prüfen.
--------	--

Abschnitt 9.1 des RFC 5452 definiert Regeln, die jeder DNS-Client/-Proxy implementieren muss, um gefälschte Antworten auf DNS Abfragen erkennen zu können. Wenn eine DNS Antwort nicht konform zu diesen Regeln ist, dann muss diese durch den DNS-Proxy als ungültig angesehen und verworfen werden. Wenn der DNS-Proxy gefälschte Antworten identifiziert, dann sollte die Implementierung gemäß Abschnitt 9.3 des RFC 5452 die korrespondierenden Abfragen nicht erneut über UDP, sondern über TCP senden.

Motivation: Die Erkennung von gefälschten Antworten auf DNS Abfragen verhindert DNS-Cache-Poisoning- Angriffe.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten

ID: 3.40-91/3.6

Req 92	Der DNS-Proxy muss eine nicht-vorhersagbare Query-ID für ausgehende DNS Abfragen verwenden, und der gesamte für diese ID zur Verfügung stehende Bereich (0-65535) muss genutzt werden.
--------	--

Die Query-IDs muss mit einem starken (Pseudo-)Zufallszahlengenerators erzeugt werden, der gleichverteilte Zufallszahlen erzeugt.

Motivation: Die Verwendung von nicht-vorhersagbaren Query IDs erschwert einem Angreifer erheblich die Fälschung von Antworten auf DNS Abfragen. Dies verhindert DNS-Cache-Poisoning-Angriffe.

Umsetzungsbeispiel: Geeignete Zufallszahlengeneratoren werden im RFC 4086 beschrieben, z. B. im Abschnitt 7.1.2 werden die beiden Geräte /dev/random und /dev/urandom genannt, die insbesondere unter Linux zur Verfügung stehen.

hen, und die als geeignet angesehen werden können.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten

ID: 3.40-92/3.6

Req 93	Der DNS-Proxy muss den limitierten Bereich der Query-IDs durch die Verwendung von nicht-vorhersagbaren Source-Ports für ausgehende DNS-Abfragen erweitern.
--------	--

Diese Erweiterung des Bereichs der Query-IDs muss konform zu den entsprechenden Anforderungen in Abschnitt 9.2 „Extending the Q-ID Space by Using Ports and Addresses“ des RFC 5452 implementiert werden. Insbesondere muss der DNS-Proxy einen möglichst großen Bereich zur Auswahl eines zufälligen Source-Ports verwenden, und für vielen simultan ausgehende DNS Abfragen müssen verschiedene Source-Ports verwendet werden.

Motivation: Die Erweiterung des Bereichs für Query IDs durch nicht-vorhersagbare Source-Ports erschwert einem Angreifer erheblich die Fälschung von Antworten auf DNS Abfragen. Dies verhindert DNS-Cache-Poisoning- Angriffe.

Umsetzungsbeispiel: Nicht-vorhersagbare Ports können durch Anwendung eines starken (Pseudo-)Zufallszahlengenerators erzeugt werden, der gleichverteilte Zufallszahlen erzeugt. Solche Generatoren werden im RFC 4086 beschrieben, z. B. im Abschnitt 7.1.2 werden die beiden Geräte /dev/random und /dev/urandom genannt, die insbesondere unter Linux zur Verfügung stehen, und die als geeignet angesehen werden können 1.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten

ID: 3.40-93/3.6

Req 94	Der DNS-Proxy darf keine DNS Abfragen über ein WAN-Interface beantworten.
--------	---

Hinweis: Im Abschnitt 6.2 „Interface Binding“ des RFC 5625 wird eine ähnliche Anforderung an die Erreichbarkeit des DNS-Proxys gestellt. Allerdings ist die Anforderung aus RFC 5625 nicht ausreichend, da im RFC die Bindung des DNS-Proxies an ein WAN-Interface nicht strikt ausgeschlossen wird.

Motivation: Offene DNS-Resolver ermöglichen sogenannte DNS-Reflector-Angriffe, wie sie im RFC 5358 beschrieben sind.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.40-94/3.6

Req 95	Der DNS-Proxy muss DNS rebinding Angriffe verhindern.
--------	---

Das Ziel des DNS Rebinding Angriffs ist das Aushebeln der Same-Origin-Policy eines Web-Browsers, um insbesondere unbefugt auf lokale Ressourcen in einem privaten Heimnetzwerk von einer bösartigen Webanwendung aus zugreifen zu können. Dies kann für verschiedene Arten von Angriffen genutzt werden. Im Verlauf eines DNS rebinding Angriffs liefert ein externer DNS-Server auf eine Anfrage hin daher IP-Adressen zurück, die auf das private, lokale Heimnetzwerk verweisen. Der DNS-Proxy muss solche Einträge aus den Antworten eines externen DNS-Servers entfernen.

Motivation: Verhinderung des unbefugten Zugriffs auf lokale Ressourcen im Heimnetzwerk von einer Web-Anwendung aus.

Umsetzungsbeispiel: Der DNS-Proxy muss A/AAAA Einträge aus DNS Antworten externer DNS-Server löschen, die private oder link-lokale IP Adressen enthalten. D.h. die folgenden Adressbereiche müssen gefiltert werden:

- 192.168.0.0/16 as defined in RFC1918

- 172.16.0.0/12 as defined in RFC1918
- 10.0.0.0/8 as defined in RFC1918
- 169.254.0.0/16 as defined in RFC5735
- fe80::/10 IPv6 link local addresses
- fd::/10 IPv6 Unique Local Addresses as defined in RFC4139

Die um diese Einträge bereinigte Antwort des externen DNS-Servers wird an den Client zurückgesendet, um ein Timeout zu verhindern. Des Weiteren bietet der DNS-Proxy dem Benutzer die Möglichkeit an, Ausnahmen (FQDNs) für diesen Filtermechanismus zu definieren.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

ID: 3.40-95/3.6

8.8. WiFi Simple Configuration / WiFi Protected Setup

Req 96	Es muss die Protokollversion 2.0.2 oder neuer des Wi-Fi Simple Configuration Protokolls implementiert werden.
--------	---

Die technische Spezifikation zur Version 2.0.2 wurde am 30. Januar 2012 veröffentlicht, und diese ersetzt die WSC Spezifikation Version 2.0. WSC 2.0.2 fordert die Implementierung von Maßnahmen zur Vermeidung von Brute Force Angriffen auf die Geräte-PIN des WLAN Zugangspunktes (des Home Gateways), sofern ein externer Registrar (external registrar) benutzt wird: nach maximal 10 aufeinanderfolgenden Fehlversuchen bei der PIN Verifikation muss der WLAN Zugangspunkt das WSC Protokoll sperren. Diese Sperre muss unbefristet sein, und es müssen alle Fehlversuche beliebiger Registrare berücksichtigt werden. Im gesperrten Zustand muss der Access Point die Bearbeitung von Nachrichten des WSC Registrierungsprotokolls ablehnen. Das Aufheben des Sperrzustands muss eine gezielte Nutzerinteraktion erfordern. Zusätzlich zur WSC 2.0.2 Spezifikation wird gefordert, dass der WLAN Zugangspunkt die Sperrfunktion auch dann implementieren muss, wenn dieser eine dynamisch generierte zufällige Geräte PIN verwendet.

Motivation: Die aktuelle Protokollspezifikation enthält wichtige Sicherheitsfunktionen, die eine im Design des WSC 2.0 Protokolls begründete Schwachstelle beheben.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.40-96/3.6

Req 97	Ein Benutzer muss in der Lage sein, das WSC (WPS) Protokoll dauerhaft zu deaktivieren.
--------	--

Wenn das WSC Protokoll konfigurativ deaktiviert wurde, dann dürfen keine Informationselemente des WSC Protokolls in den Beacon oder in den Management Nachrichten mehr enthalten sein. D.h. es dürfen keine WSC Nachrichten mehr ausgetauscht werden.

Motivation: WSC erlaubt die einfache Integration neuer Clients in ein bestehendes WLAN. Daher kann das Protokoll grundsätzlich zur Kompromittierung des WLAN Passwortes führen, wenn es unbefugt genutzt wird. Ein erfahrener Nutzer möchte daher ggfls. sein Home Gateway so sicher wie möglich konfigurieren, d.h. WSC deaktivieren. Durch eine Deaktivierung von WSC wäre auch dann die Sicherheit des WLANs gewährleistet, wenn ein kritischer Implementierungsfehler in der WSC Funktion eines Home Gateways bekannt würde.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Req 98	Die Aktivierung des WSC Registrierungsprotokolls muss eine Interaktion mit dem Benutzer am Home Gateway erfordern.
--------	--

Diese Anforderung muss für beliebige WSC Methoden umgesetzt werden. Die „Push Button Configuration“ (PBC) Methode erfordert das Auslösen eines physikalisch oder in Software realisierten Tasters, die PIN Methode mit einem internen Registrator erfordert die Eingabe der Geräte PIN der WLAN Station (des Clients). Diese beiden Methoden erfüllen die Anforderung schon aufgrund des in der Spezifikation definierten Protokollablaufs. Die PIN Methode im Zusammenspiel mit einem externen Registrator könnte zwar ohne Benutzerinteraktion implementiert werden, auch für diese Methode wird gefordert: Die Aktivierung muss auf Basis einer Interaktion mit dem Benutzer z.B. über das Auslösen eines Schalters auf einer geschützten Seite der Web-Konfigurationsoberfläche des Home Gateways erfolgen.

Motivation: WSC Methoden, die eine Nutzer Interaktion erfordern, können von einem Angreifer nicht einfach aus der Ferne (d.h. innerhalb der Reichweite des WLANs) ausgenutzt werden. Denn diese Methoden erfordern dann einen physikalischen Zugang zum Home Gateway bzw. einen Zugriff auf eine geschützte Seite der Web-Konfigurationsoberfläche.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

Req 99	Der WLAN Zugangspunkt des Home Gateways muss die Aktivierung des WSC Registrierungsprotokolls zeitlich begrenzen.
--------	---

Diese Anforderung muss für beliebige WSC Methoden umgesetzt werden. Gemäß der Spezifikation wird für die PBC Methode eine Begrenzung auf 120 Sekunden gefordert. Für jedwede PIN-basierte (d.h. Passwort-basierte) Methode muss die Aktivierung ebenfalls zeitlich begrenzt werden, diese Aktivierungszeit DARF 600 Sekunden nicht überschreiten.

Motivation: Im Rahmen des WSC Registrierungsprotokolls erfolgt der Austausch des WLAN Passworts. Daher ist das Protokoll Ziel von Angriffen zur Kompromittierung des WLAN Passworts. Eine Terminierung des WSC Registrierungsprotokolls nach Ablauf der Aktivierungszeit erhöht wieder die Sicherheit des WLAN Zugangspunkts.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

Req 100	Der WLAN Zugangspunkt muss immer eine neue, zufällige Geräte PIN erzeugen, bevor das WSC Registrierungsprotokoll der external registrar PIN Methode aktiviert wird.
---------	---

Diese Anforderung bedeutet insbesondere, dass der WLAN Zugangspunkt keine statische Geräte-PIN implementieren darf.

Motivation: Eine dynamisch erzeugte zufällige Geräte-PIN verhindert Angriffe mit bekannten Default-PINs.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen