Bundesamt
für Sicherheit in der
Informationstechnik

Testkonzept für Breitband-Router

(DSL-, Kabel-, SOHO-, CE-, CPE-Router, IADs) Stand: Mai 2016

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: routertestkonzept@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Management-Summary

In Deutschland lag die Versorgung mit Breitbandanschlüssen (> 144 kbit/s) im Jahre 2015 bei 99,9%. Dies entspricht ca. 30,1 Millionen Breitbandanschlüssen[1]. Der Netzabschluss dieser Anschlüsse erfolgt überwiegend durch Router.

Häufig bildet ein solcher Router die einzige zentrale und wesentliche Sicherheitskomponente zum Schutz des internen Netzes. Neben der Grundfunktion des Netzabschlusses stellt ein solches Gerät heute regelmäßig weitere Funktionen wie beispielsweise WLAN und VPN-Dienste bereit und bietet die Funktionalität eines zentralen Datenspeichers (NAS). Darüber hinaus wird inzwischen häufig auch die Telefonie über diese Komponenten zur Verfügung gestellt.

Der Absicherung des Routers kommt daher eine herausragende Bedeutung zu. Wird der Router durch einen Angreifer übernommen, kann dieser Kommunikationsdaten des Kunden ausspähen, die Infrastruktur des Kunden Teil eines Botnetzes werden lassen, auf Kosten des Kunden hochpreisige Gespräche führen, SPAM-E-Mails versenden oder den Zugang des Kunden zum Internet unterbinden. Leider sind in der Vergangenheit fortlaufend Schwachstellen in dieser Gerätekategorie herstellerübergreifend bekannt geworden.

Mit dem vorliegenden Dokument möchte das BSI die Grundlage für ein offenes Testkonzept schaffen, mit dessen Hilfe Breitband-Router auf die Einhaltung relevanter Sicherheitseigenschaften überprüft werden können. Hierbei richtet sich der Fokus auf Breitband-Router, die im Privatkunden-Bereich eingesetzt werden. Das Testkonzept erstreckt sich über die Bereiche

- Grundlegende sicherheitsrelevante Funktionen,
- Unterstützung und Einhaltung etablierter Sicherheitsstandards,
- Immunität gegenüber bekannten Sicherheitsrisiken und Angriffsszenarien,
- Kundensupport / Usability sowie
- Sonstige Funktionen.

Das BSI möchte hiermit einen Impuls zur Verbesserung der Sicherheit entsprechender Geräte setzen und ist fortlaufend interessiert an Feedback und Ergänzungsvorschlägen von Herstellern, Providern und der Sicherheitscommunity. Mit der Veröffentlichung wird einerseits ein Beitrag zur Orientierung für Hersteller entsprechender Produkte geliefert und andererseits Providern und Endkunden eine Entscheidungshilfe für die Auswahl für sie geeigneter Geräte bereitgestellt.

1 https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2015/TB_TK_2015.pdf?__blob=publicationFile&v=3

2 Einleitung

Anhand des vorliegenden Testkonzepts können Breitband-Router auf die Einhaltung relevanter Sicherheitseigenschaften geprüft werden.

2.1 Motivation

Die im Rahmen dieses Testkonzepts im Fokus stehenden Breitband-Router bilden häufig die einzige zentrale und wesentliche Sicherheitskomponente zum Schutz eines internen Netzes. Der Absicherung des Routers kommt daher eine herausragende Bedeutung zu. Neben der möglichen individuellen Schädigung eines Opfers besteht auch das Risiko, dass das kompromittierte System als Teil eines Botnetzes zu verteilten Angriffen missbraucht wird.

Das BSI möchte daher mit dem vorliegenden Testkonzept einen Beitrag leisten, um das Schutzniveau an dieser entscheidenden Stelle des Internets zu verbessern.

2.2 Zielsetzung und Adressatenkreis

Um die allgemeine Sicherheit der Breitband-Router zu verbessern, wurde das vorliegende Testkonzept für Breitband-Router entwickelt. Mit Hilfe des Testkonzepts können das Vorhandensein von **sicherheitsrelevanten Funktionen** in Routern überprüft und ausgewählte **Verhaltensweisen** dieser Funktionen untersucht werden. Außerdem werden **Sicherheitsrisiken** und einige **bekannte Schwachstellen** betrachtet, deren Existenz die Angriffsfläche auf Router erhöhen können. Zuletzt werden **Ausschlusskriterien** definiert, bei deren Erfüllung ein Router nicht empfohlen werden kann. Das Testkonzept ist darauf ausgelegt, zu einem späteren Zeitpunkt ggf. als Basis für die Definition von Mindestanforderungen im Hinblick auf die IT-Sicherheit von Routern zu dienen.

Das Testkonzept richtet sich sowohl an Internet Service Provider (ISP) als auch an Router-Hersteller. Ein ISP könnte das Testkonzept u. a. bei Router-Ausschreibungen berücksichtigen, da das Testkonzept u. a. Anforderungen für Router enthält. Die Hersteller hingegen könnten das Testkonzept bei der Entwicklung ihrer Firmware miteinbeziehen. Mit entsprechendem Equipment eignet sich das gesamte Testkonzept ebenfalls für die Überprüfung von Routern durch einen versierten Anwender, wohingegen der durchschnittliche Anwender lediglich die Existenz einiger Funktionen überprüfen kann.

2.3 Aufbau des Testkonzepts

Kapitel 3 befasst sich zunächst mit grundlegenden funktionalen Eigenschaften, deren Existenz mittels Sichtprüfung ohne tiefgehende technische Kenntnisse untersucht werden kann. Dazu zählen grundlegende Funktionen, die beispielsweise bei der Durchführung eines Firmware-Updates unterstützen bzw. über ein Firmware-Update informieren. Zudem werden Funktionen zur sicheren WLAN- und Firewall-Konfiguration behandelt sowie Aspekte der Transparenz in Bezug auf die Darstellung der aktiven Dienste eines Routers betrachtet. Weitere Punkte betreffen die Absicherung der Weboberfläche und die Bereitstellung von Ereignisprotokollen. Darüber hinaus werden Funktionen im Zusammenhang mit VPN, VLAN sowie einem Management-Informationssystem betrachtet.

Während in Kapitel 3 die Sichtprüfung von sicherheitsrelevanten Funktionen behandelt wird, werden in Kapitel 4 die sicherheitsrelevanten Funktionen aus technischer Sicht betrachtet. Es werden Methoden beschrieben, mit denen einige Verhaltensweisen von Routerfunktionen im Labor untersucht werden können, wie beispielsweise die Konformität der Router mit den aktuellen DNS-RFCs. Es wird eine Liste von Diensten definiert, die ein Router in der Standardkonfiguration besitzen und zudem nicht überschreiten sollte, um unnötige Angriffsflächen zu vermeiden. Außerdem werden Einstellmöglichkeiten und das Verhalten des DHCP-Servers untersucht. Des Weiteren werden die Unterstützung von IPv6 sowie

dazugehörigen Privacy-Funktionen geprüft. Inwieweit Gast-Netzwerke bereitgestellt werden, ist ebenfalls Gegenstand der Untersuchungen.

Prüfungsmethoden bezüglich in der Vergangenheit bekannt gewordener Schwachstellen (z. B. Cross-Site-Request-Forgery) werden in Kapitel 5 beschrieben. Der Fokus richtet sich hierbei insbesondere auf Sicherheitsrisiken bzw. Schwachstellen, die aus dem Internet ausgenutzt werden können.

In Kapitel 6 werden abschließend weitere Support- und Usability-Eigenschaften von Breitband-Routern behandelt. Diese Eigenschaften erhöhen nicht unmittelbar die Sicherheit, leisten aber dennoch einen Beitrag dazu.

Jeder Testfrage in den Kapiteln 3, 4, 5 und 6 wurden Punktwerte zugeordnet, die ein zu testendes Gerät bei Erfüllung der jeweiligen Eigenschaft erhalten kann. Das Punktesystem wird in Kapitel 2.4 beschrieben und erlaubt eine differenzierte Betrachtung der Testfragen. Mithilfe des Punktesystems können Router in den einzelnen Kategorien Anforderung, Empfehlung und Option miteinander verglichen werden. Das Testkonzept kann daher auch als Basis für eine Produktempfehlung herangezogen werden.

Das BSI hält einige Sicherheitseigenschaften für zwingend, so dass die Nichterfüllung einer solchen Eigenschaft zum Ausschluss des Geräts führen sollte, sofern dieses Gerät als Perimeter den Internetzugang absichern soll. Diese zwingenden Sicherheitseigenschaften werden in Kapitel 7 zusammengefasst.

Im Anhang befinden sich grafische Darstellungen der unterschiedlichen Testaufbauten und eine Liste der verwendeten Hilfsmittel (Geräte).

2.4 Umgang mit dem Testkonzept

Die überwiegenden Kapitel des Testkonzepts befassen sich mit mehreren Themenbereichen, die ihrerseits aus einem textuellen und einem tabellarischen Teil bestehen. Der textuelle Teil erläutert die einzelnen Testinhalte eines Themenbereichs sowie die jeweils erforderlichen Testschritte zur Ermittlung des Testergebnisses. Der tabellarische Teil verschafft einen Überblick über den dazugehörigen Themenbereich und ergänzt den textuellen Teil um weitere Angaben. Die Spaltenüberschriften einer Tabelle werden wie folgt bezeichnet:

- Nr.
- Testinhalt
- Erwartung
- Relevanz
- Testdurchführung
- Testaufbau
- Punkte

Die **Testinhalte** werden durchnummeriert und fassen in der Regel mehrere Erwartungen unter einem Oberbegriff zusammen. Eine **Erwartung** wird definiert als ein beobachtbares Ergebnis, das im Sinne der Sicherheit dienlich ist. Zudem werden alle Erwartungen nach ihrer **Relevanz** klassifiziert. Hierzu werden die folgenden Klassen bestimmt:

1. Anforderung (Muss)
2. Empfehlung (Soll)
3. Option (Kann)

Die Relevanz bestimmt außerdem den Rahmen bzw. den Wertebereich für die **Punkte**, d. h. für jede Erwartung werden Punkte vergeben, die wiederum von der dazugehörigen Relevanz abhängig sind. Ab Kapitel 4 werden für bestimmte Erwartungen keine Punkte vergeben, da sie in Kapitel 3 bereits in Form

einer Sichtprüfung überprüft werden. Somit wird die doppelte Bewertung eines Sachverhalts vermieden. Gleichwohl führt ein Widerspruch zwischen der Sichtprüfung und der technischen Prüfung zur Abwertung oder zum Ausschluss. Des Weiteren wird auf eine Gesamtpunktzahl verzichtet. Stattdessen wird ein getrenntes Punktesystem eingeführt, sodass jede Kategorie (Anforderung, Empfehlung, Option) eine eigene Maximalpunktzahl besitzt. Dadurch soll verhindert werden, dass das Fehlen einer Anforderung durch viele Optionen kompensiert werden kann.

Der Zusammenhang zwischen Relevanz und Punkten wird wie folgt definiert:

- Anforderung → 8 bis 10 Punkte
- Empfehlung → 4 bis 7 Punkte
- Option → 1 bis 3 Punkte

In wenigen Fällen, wie beispielsweise im DNS-Kapitel, werden mehrere Erwartungen dahingehend zusammenfasst, dass sie nur einmalig bewertet werden. Optionale Erwartungen müssen nicht standardmäßig aktiviert sein. Außerdem sind optionale Erwartungen in der Regel nicht oder nur selten in einem Router implementiert. Dennoch werden diese Erwartungen aufgeführt, damit sie als Impuls für die nächsten Router-Generationen dienen und somit einen Mehrwert für den Nutzer bieten. Die Erwartungen können mithilfe der **Testdurchführung** verifiziert werden, wobei der referenzierte **Testaufbau** zu berücksichtigen ist. Eine detaillierte Beschreibung der Testaufbauten befindet sich im Anhang.

2.5 Rahmenbedingungen und verwendete Programme/Skripte

Das Testkonzept für Breitband-Router ist, insbesondere im Hinblick auf den geltenden gesetzlichen Rahmen (z.B. Datenschutz), nur unter bestimmten Voraussetzungen anzuwenden. Daher ist es empfehlenswert, die Tests in einer Laborumgebung durchzuführen.

Die Beschreibungen der Testdurchführung in diesem Testkonzept enthalten die einzelnen Schritte, um ein erwartetes Ergebnis (Erwartung) zu erzielen. Um eine möglichst weitgehende Transparenz bei der Punktevergabe und die Vergleichbarkeit der Testergebnisse zu gewährleisten, werden konkrete Programme bzw. Skripte zur Testdurchführung benannt. Dessen ungeachtet sind Alternativen zu den benannten Programmen vorhanden und können bei Bedarf verwendet werden.

3 Funktionen – Sichtprüfung

In diesem Kapitel wird der Umfang von sicherheitsrelevanten Funktionen (Existenz & Status) in einem Router überprüft. Diese Überprüfung kann in der Regel auch ein technisch versierter Besitzer eines Routers durchführen, da hierfür keine besonderen technischen Hilfsmittel benötigt werden. Vielmehr wird die Überprüfung mithilfe der Weboberfläche und des Benutzerhandbuches durchgeführt.

3.1 Firmware-Update

Eine aktuelle Firmware sorgt für ein relativ sicheres System. Um eine zeitnahe Aktualisierung der Firmware zu gewährleisten, müssen sowohl informative als auch operative Funktionen zur Verfügung gestellt werden. Das Thema "Firmware-Update" wird als Erstes abgehandelt, damit die folgenden Tests mit der aktuellsten Firmware durchgeführt werden.

3.1.1 Aktualität der Firmware

Beschreibung des Testinhalts

Nach dem Aufrufen der Weboberfläche sollte automatisch ein Hinweis auf der Startseite erscheinen, ob ein Firmware-Update zur Verfügung steht (3.1.1.1). Beispieltexte hierfür sind "Firmware ist aktuell" oder "Firmware-Update verfügbar". Der Router ist damit in der Lage, automatisch nach Firmware-Updates zu suchen und zu informieren. Um diesen Hinweis zu bekräftigen, sollte der Zeitpunkt für die letzte automatische Firmware-Update-Suche ersichtlich sein (3.1.1.2). Diese und die folgenden Informationen müssen nicht direkt auf der Startseite bereitgestellt werden. Ebenso muss die verwendete Firmware-Version abrufbar sein (3.1.1.3). Außerdem sollten der Installationszeitpunkt (3.1.1.4) der verwendeten Firmware erkennbar sein.

Beschreibung der Testdurchführung zu 3.1.1.1 - 3.1.1.4

1. Die Weboberfläche des Routers wird aufgerufen und es erfolgt ggf. eine Anmeldung.
2. Es wird überprüft, ob die Informationen unter 3.1.1.1- 3.1.1.4 auf der Startseite bzw. im System-Bereich der Weboberfläche enthalten sind.

3.1.2 Manuelles Update

Beschreibung des Testinhalts

Zur Durchführung eines Firmware-Updates gibt es verschiedene Möglichkeiten. Bei der herkömmlichen Variante kann eine Firmware-Datei manuell heruntergeladen werden, um sie anschließend mithilfe der Weboberfläche zu installieren (3.1.2.1). Bevor eine manuell heruntergeladene Firmware-Datei installiert wird, sollte mithilfe des Routers (Weboberfläche) verifiziert werden, ob die Datei vom originären Router-Hersteller herausgegeben wurde (3.1.2.2). Ein Beispieltext wäre "Die Firmware wurde von x herausgegeben. Möchten Sie mit dem Update fortfahren?". Um das Firmware-Update zu erleichtern, sollte die Weboberfläche ein Online-Update unterstützen (3.1.2.3). Bei einem Online-Update kann, beispielsweise durch das Betätigen eines Buttons, nach einem verfügbaren Firmware-Update gesucht und das Update durchgeführt werden.

Beschreibung der Testdurchführung zu 3.1.2.1

1. Auf der Webseite des Herstellers wird nach einem aktuellen Benutzerhandbuch recherchiert und dieses für die weiteren Tests verwendet.
2. Es wird recherchiert, ob im Benutzerhandbuch eine Funktion erwähnt wird, die die Erwartung von 3.1.2.1 erfüllt.

3. Etwaige Hinweise auf diese Funktion werden auf der Weboberfläche verifiziert bzw. falsifiziert.
4. Sofern das Benutzerhandbuch keine Hinweise enthält, wird die Existenz der Funktionalität an naheliegenden Stellen auf der Weboberfläche untersucht.

Beschreibung der Testdurchführung zu 3.1.2.2

1. Auf der Webseite des Herstellers wird nach einer Firmware-Datei (Update) recherchiert.
2. Der Download der Firmware-Datei (Update) wird ggf. durchgeführt.
3. Die Weboberfläche des Routers wird aufgerufen und es erfolgt ggf. eine Anmeldung.
4. Ein manuelles Firmware-Update wird durchgeführt.

Beschreibung der Testdurchführung zu 3.1.2.3

Der Test wird analog zu 3.1.2.1 durchgeführt.

3.1.3 Auto-Update

Beschreibung des Testinhalts

Eine weitere Möglichkeit zur Durchführung eines Firmware-Updates ist eine Auto-Update-Funktion. Diese Funktion sucht automatisch nach einem Firmware-Update und führt dieses ggf. durch.

Beschreibung der Testdurchführung zu 3.1.3.1

Der Test wird analog zu 3.1.2.1 durchgeführt.

3.1.4 Redundanter Firmware-Speicher

Beschreibung des Testinhalts

Es soll sichergestellt werden, dass der Router im Notfall auf eine funktionierende Firmware zurückgreifen kann. Hierfür sollte zusätzlich zu der aktiven Firmware eine inaktive Firmware in einem redundanten Firmware-Speicher bereitgestellt werden, die im Fehlerfalle verwendet wird (3.1.4). Falls der Router beispielsweise aufgrund eines fehlerhaften Firmware-Updates nicht ordnungsgemäß startet, kann auf die bis dahin inaktive Firmware zurückgriffen werden.

Beschreibung der Testdurchführung zu 3.1.4

Der Test wird analog zu 3.1.2.1 durchgeführt.

3.1.5 Quelloffen (Open Source)

Beschreibung des Testinhalts

Es soll sichergestellt werden, dass der Quelltext (source code) der Firmware frei verfügbar ist (3.1.5). Dadurch kann die Firmware ebenfalls von unabhängiger Stelle überprüft werden.

Beschreibung der Testdurchführung zu 3.1.5

Sofern das Benutzerhandbuch keine Hinweise enthält, werden die Informationen auf der Hersteller-Webseite recherchiert.

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
3.1.1	Aktualität der Firmware	1. Nach dem Aufrufen der Weboberfläche erscheint automatisch ein Hinweis, ob ein Firmware-Update zur Verfügung steht.	Empfehlung	Die Existenz des Hinweises bzw. der Funktionalität wird mittels Weboberfläche untersucht.	2	7
		2. Der Zeitpunkt für die letzte automatische Firmware-Update-Suche lässt sich abrufen.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche untersucht.	2	4
		3. Die verwendete Firmware-Version lässt sich abrufen.	Anforderung	Die Existenz der Funktionalität wird mittels Weboberfläche untersucht.	1	10
		4. Der Installationszeitpunkt der verwendeten Firmware lässt sich abrufen.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche untersucht.	1	4
3.1.2	Manuelles Update	1. Eine Firmware-Datei kann manuell heruntergeladen werden, um sie anschließend mithilfe der Weboberfläche zu installieren.	Anforderung	– Das aktuelle Benutzerhandbuch wird heruntergeladen. – Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	2	10
		2. Bevor eine manuell heruntergeladene	Option	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	2	3

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
		Firmware-Datei installiert wird, kann mithilfe des Routers (Weboberfläche) verifiziert werden, ob die Datei vom originären Router-Hersteller herausgegeben wurde.				
		3. Die Weboberfläche unterstützt ein Online-Update.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	2	7
3.1.3	Auto-Update	Eine Funktion, die automatisch nach einem Firmware-Update sucht und durchführt, kann aktiviert werden.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	7
3.1.4	Redundanter Firmware-Speicher	Zusätzlich zu der aktiven Firmware wird eine inaktive Firmware bereitgestellt, die im Fehlerfalle verwendet werden kann.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	4
3.1.5	Quelloffen (Open Source)	Der Quelltext (source code) der Firmware ist frei verfügbar.	Option	Sofern das Benutzerhandbuch keine Hinweise enthält, werden die Informationen auf der Hersteller-Webseite recherchiert.	2	1

Tabelle 1: Übersicht Firmware

3.2 WLAN

Die Bereitstellung eines WLAN gehört zur gängigen Funktion eines marktüblichen Routers. Diese Funktion wird häufig verwendet und ist somit sehr schützenswert. Um die folgenden Tests durchzuführen, wird das WLAN aktiviert, sofern es standardmäßig deaktiviert ist.

3.2.1 SSID

Beschreibung des Testinhalts

Die SSID bzw. ESSID muss sich über die Weboberfläche ändern lassen (3.2.1.1). Außerdem sollte die SSID bzw. ESSID keine Angabe zur Produktbezeichnung enthalten, um die Angriffsfläche auch für einfache Angriffe gering zu halten (3.2.1.2).

Beschreibung der Testdurchführung zu 3.2.1.1

1. Es wird recherchiert, ob im Benutzerhandbuch eine Funktion erwähnt wird, die die Erwartung von 3.2.1.1 erfüllt.
2. Etwaige Hinweise auf diese Funktion werden auf der Weboberfläche verifiziert bzw. falsifiziert.
3. Sofern das Benutzerhandbuch keine Hinweise enthält, wird die Existenz der Funktionalität an naheliegenden Stellen auf der Weboberfläche untersucht.
4. Ggf. wird das WLAN aktiviert.

Beschreibung der Testdurchführung zu 3.2.1.2

1. Die Weboberfläche des Routers wird aufgerufen und es erfolgt ggf. eine Anmeldung.
2. Im WLAN-Bereich wird überprüft, ob die Erwartung von 3.2.1.2 zutrifft.

3.2.2 Verschlüsselung

Beschreibung des Testinhalts

Da nicht ausgeschlossen werden kann, dass sich ein Angreifer in der Funkreichweite des Routers befindet, muss das WLAN verschlüsselt sein. Hierzu muss das WLAN standardmäßig eine WPA2-Verschlüsselung aktiviert haben (3.2.2.1). Eine WLAN-Verschlüsselung mittels WPA2 trägt signifikant zur Sicherheit bei, jedoch bietet allein dieses Kriterium keinen hinreichenden Schutz. Daher sollte neben dem Verschlüsselungsverfahren auch eine geeignete Schlüssellänge vorgegeben sein (ISi-WLAN[2]). Der vordefinierte WPA2-Schlüssel sollte mindestens 20 Zeichen enthalten (3.2.2.2). Bei Eingabe eines neuen WPA2-Schlüssels kann seine Schlüsselstärke (Länge u. Komplexität) angezeigt werden (3.2.2.3). Außerdem kann nach der Eingabe eines neuen WPA2-Schlüssels ein QR-Code generiert werden, um beispielsweise Tablets einzubinden (3.2.2.4).

Beschreibung der Testdurchführung zu 3.2.2.1 - 3.2.2.2

Der Test wird analog zu 3.2.1.1 durchgeführt.

Beschreibung der Testdurchführung zu 3.2.2.3 und 3.2.2.4

1. Die Weboberfläche des Routers wird aufgerufen und es erfolgt ggf. eine Anmeldung.
2. Im WLAN-Bereich wird versucht, einen neuen WLAN-Schlüssel zu setzen.

2 https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/ISi-Reihe/ISi-WLAN/wlan_node.html

3.2.3 WPS-PIN-Funktion

Beschreibung des Testinhalts

WPS erleichtert für Netzwerkgeräte den Zugang in ein WLAN, gleichwohl ist es mit Risiken verbunden, da beispielsweise die WPS-PIN-Funktion anfällig für Brute-Force-Angriffe ist. Dieser Test untersucht die Existenz und den Status von WPS. Die WPS-PIN-Funktion sollte standardmäßig deaktiviert sein und bei jeder Aktivierung eine neue zufällige PIN generieren. Die Alternative dazu wäre, dass die WPS-PIN-Funktion nicht implementiert ist (3.2.3.1).

Beschreibung der Testdurchführung zu 3.2.3.1

1. Es wird recherchiert, ob im Benutzerhandbuch eine Funktion erwähnt wird, die die Erwartung von 3.2.3.1 erfüllt.
2. Etwaige Hinweise auf diese Funktion werden auf der Weboberfläche verifiziert bzw. falsifiziert.
3. Sofern das Benutzerhandbuch keine Hinweise enthält, wird die Existenz sowie der Status der Funktionalität an naheliegenden Stellen auf der Weboberfläche untersucht.

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
3.2.1	SSID	1. Die SSID bzw. ESSID lässt sich über die Weboberfläche ändern.	Anforderung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht. Ggf. wird das WLAN aktiviert.	1	10
		2. Die SSID bzw. ESSID enthält keine Angabe zur Produktbezeichnung.	Empfehlung	Ermittlung der SSID bzw. ESSID mittels Weboberfläche.	1	4
3.2.2	Verschlüsselung	1. Das WLAN hat standardmäßig eine WPA2-Verschlüsselung aktiviert.	Anforderung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	2	10
		2. Ein vordefinierter WPA2-Schlüssel enthält mindestens 20 Zeichen.	Empfehlung	Ermittlung der WPA2-Schlüssellänge mittels Weboberfläche.	1	6
		3. Bei Eingabe eines WPA2-Schlüssels wird seine Schlüsselstärke (Länge u. Komplexität) angezeigt.	Empfehlung	Es wird versucht, einen neuen WLAN-Schlüssel zu setzen.	1	7
		4. Nach der Eingabe eines neuen WPA2-Schlüssels wird ein QR-Code generiert.	Option	Es wird versucht, einen neuen WLAN-Schlüssel zu setzen.	1	1
3.2.3	WPS-PIN-Funktion	Die WPS-PIN-Funktion sollte standardmäßig deaktiviert sein und bei jeder Aktivierung eine neue zu-	Anforderung	Die Existenz und der Status der WPS-PIN-Funktion werden mittels Weboberfläche und Benutzerhandbuches untersucht.	1	8

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
		fällige PIN generieren. Alternativ ist die WPS-PIN-Methode nicht implementiert.				

Tabelle 2: Übersicht WLAN

3.3 Firewall

Ein Router, der an das Internet angeschlossen wird, muss eine Firewall besitzen. Zudem sollte die Firewall für unterschiedliche Bedürfnisse bzw. Schutzbedarfe konfiguriert werden können.

3.3.1 Firewall

Beschreibung des Testinhalts

Eine Firewall ist ein unerlässlicher Sicherheitsbestandteil des Routers. Es soll sichergestellt werden, dass die Firewall in der Grundeinstellung aktiviert ist (3.3.1.1). Außerdem sollte der Firewall-Status auf der Weboberfläche deutlich erkennbar sein (3.3.1.2). Es wird erwartet, dass der Firewall-Status auf der Startseite oder im Firewall-Bereich der Weboberfläche angezeigt wird. Beispieltexte hierfür sind "Firewall: aktiviert" oder "Firewall: ☒ Markierfeld

Beschreibung der Testdurchführung zu 3.3.1.1

1. Es wird recherchiert, ob im Benutzerhandbuch eine Funktion erwähnt wird, die die Erwartung von 3.3.1.1 erfüllt.
2. Etwaige Hinweise auf diese Funktion werden auf der Weboberfläche verifiziert bzw. falsifiziert.
3. Sofern das Benutzerhandbuch keine Hinweise enthält, wird die Existenz sowie der Status der Funktionalität an naheliegenden Stellen auf der Weboberfläche untersucht.

Beschreibung der Testdurchführung zu 3.3.1.2

1. Die Weboberfläche des Routers wird aufgerufen und es erfolgt ggf. eine Anmeldung.
2. Sowohl auf der Startseite als auch im Firewall-Bereich wird nach dem Firewall-Status recherchiert.

3.3.2 Portforwarding (IPv4)

Beschreibung des Testinhalts

Es soll sichergestellt werden, dass der Router in der Standardkonfiguration keine Regeln für Portforwarding (IPv4) enthält (3.3.2).

Beschreibung der Testdurchführung zu 3.3.2

1. Die Weboberfläche des Routers wird aufgerufen und es erfolgt ggf. eine Anmeldung.
2. Im Firewall-Bereich wird nach aktivem Portforwarding recherchiert.

3.3.3 Eingehender Datenverkehr bei IPv6

Beschreibung des Testinhalts

Analog zu IPv4-Portforwarding soll sichergestellt werden, dass der Router in der Standardkonfiguration keine Freigaben (Regeln) für eingehende IPv6-Verbindungen enthält (3.3.3).

Beschreibung der Testdurchführung zu 3.3.3

Der Test wird analog zu 3.3.2 durchgeführt.

3.3.4 Filterfunktionen für ausgehenden Datenverkehr

Beschreibung des Testinhalts

Es soll sichergestellt werden, dass der ausgehende Datenverkehr gefiltert werden kann. Hierzu sollte eine portbasierte Filterfunktion für den ausgehenden Datenverkehr vorhanden sein (3.3.4.1). Darüber hinaus sollte eine vordefinierte Liste an Diensten bereitgestellt werden, um einzelne Dienste für das Netzwerk sperren zu können (3.3.4.2). Weiterhin sollte eine Funktion bereitgestellt werden, um Internetseiten auf Basis von DNS zu sperren, d. h. um den Zugriff auf eine Internetseite zu sperren, wird nicht die IP-Adresse, sondern die dazugehörige Domain eingegeben (3.3.4.3).

Beschreibung der Testdurchführung zu 3.3.4.1 - 3.3.4.3

Der Test wird analog zu 3.3.1.1 durchgeführt.

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
3.3.1	Firewall	1. Die Firewall ist aktiv.	Anforderung	Die Existenz und der Status der Firewall werden mittels Weboberfläche und Benutzerhandbuches untersucht.	2	10
		2. Der Firewall-Status ist auf der Weboberfläche deutlich erkennbar.	Empfehlung	Der Status der Funktionalität wird mittels Weboberfläche untersucht.	1	5
3.3.2	Portforwarding (IPv4)	Der Router enthält in der Standardkonfiguration keine Regeln für Portforwarding (IPv4).	Anforderung	Die Existenz einer Regel wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	10
3.3.3	Eingehender Datenverkehr bei IPv6	Der Router enthält in der Standardkonfiguration keine Freigaben (Regeln) für eingehende IPv6-Verbindungen.	Anforderung	Die Existenz einer Regel wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	10
3.3.4	Filterfunktionen für ausgehenden Datenverkehr	1. Eine portbasierte Filterfunktion für den ausgehenden Datenverkehr ist vorhanden.	Anforderung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	2	8
		2. Eine vordefinierte Liste von Diensten wird bereitgestellt, um einzelne Dienste für das Netzwerk sperren zu können.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	2	4

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
		3. Internetseiten können auf Basis von DNS gesperrt werden.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	2	5

Tabelle 3: Übersicht Firewall

3.4 Weboberfläche

Die Weboberfläche ist ein häufiges Angriffsziel, da sie in der Regel zur Konfiguration eines Routers verwendet wird. Demzufolge müssen Maßnahmen umgesetzt werden, die dem Schutz der Weboberfläche dienen.

3.4.1 Passwortschutz

Beschreibung des Testinhalts und Bewertung

Ein Passwortschutz für die Weboberfläche ist unerlässlich (IT-Grundschutz-Katalog M2.11 Regelung des Passwortgebrauchs[3]). Es wird erwartet, dass die Weboberfläche des Routers mit einem Passwort geschützt ist, das individuell ist und aus min. 8 Zeichen besteht (3.4.1.1).Weiterhin wird erwartet, dass das vordefinierte Passwort aus Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen besteht. Alternativ sind mindestens zwei dieser Anforderungen umgesetzt (3.4.1.2). Ein neues Passwort sollte sich nur unter Kenntnis des alten Passwortes ändern lassen (3.4.1.3). Bevor ein Passwort gesetzt werden darf, kann die Passwortstärke (Länge u. Komplexität) angezeigt werden (3.4.1.4).

Beschreibung der Testdurchführung zu 3.4.1.1 und 3.4.1.2

1. Mithilfe des Benutzerhandbuches wird untersucht, ob ein individuelles Passwort für die Weboberfläche vorhanden ist.
2. Mithilfe des Benutzerhandbuches wird das Passwort für die Weboberfläche ermittelt.
3. Es wird untersucht, ob ein etwaiges Passwort die Erwartungen von 3.4.1.1 und 3.4.1.2 erfüllt.

Beschreibung der Testdurchführung zu 3.4.1.3 und 3.4.1.4

1. Sofern der Passwortschutz für die Weboberfläche nicht standardmäßig aktiviert ist, wird dieser aktiviert.
2. Es wird versucht, ein neues Passwort für die Weboberfläche zu setzen.

3.4.2 Login-Sperre

Beschreibung des Testinhalts und Bewertung

Es soll sichergestellt werden, dass das Login der Weboberfläche vor Brute-Force-Angriffen geschützt ist. Daher sollte die Weboberfläche einen Captcha verwenden oder nach einer fehlgeschlagenen Anmeldung an der Weboberfläche ein erneuter Anmeldeversuch zeitlich verzögert werden (3.4.2).

Beschreibung der Testdurchführung zu 3.4.2

1. Sofern der Passwortschutz für die Weboberfläche nicht standardmäßig aktiviert ist, wird dieser aktiviert.
2. Die Weboberfläche des Routers wird geschlossen bzw. es erfolgt eine Abmeldung.
3. Die Weboberfläche des Routers wird erneut aufgerufen und inkorrekte Anmelde-Daten werden 10-mal in schneller Folge eingegeben.

3.4.3 Verschlüsselter Zugriff über die LAN-Schnittstelle

Beschreibung des Testinhalts

3 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html

Es soll sichergestellt werden, dass die Kommunikation zwischen der Weboberfläche (Webserver) und dem Browser (Client im LAN) verschlüsselt wird. Daher sollte der Zugriff auf die Weboberfläche (LAN-Schnittstelle) neben HTTP ebenfalls über HTTPS erfolgen (3.4.3).

Beschreibung der Testdurchführung zu 3.4.3

1. Anstelle von HTTP erfolgt der Zugriff auf die Weboberfläche mit dem URI-Schema bzw. mit dem Protokoll HTTPS.
2. Es ist darauf zu achten, dass keine Weiterleitung (Redirect) auf HTTP erfolgt.

3.4.4 Zugriff über die WAN-Schnittstelle

Beschreibung des Testinhalts

Einige Router gestatten den Zugriff auf ihre Weboberfläche auch über die WAN-Schnittstelle. In der Grundeinstellung muss dieser Zugriff deaktiviert sein, sofern diese Funktion implementiert ist (3.4.4.1). Außerdem muss der Zugriff auf die Weboberfläche (WAN-Schnittstelle) über HTTPS erfolgen (3.4.4.2) und der TCP-Port für HTTPS sollte sich ändern lassen (3.4.4.3).

Beschreibung der Testdurchführung zu 3.4.4.1 und 3.4.4.3

1. Es wird recherchiert, ob im Benutzerhandbuch eine Funktion erwähnt wird, die die Erwartung von 3.4.4.1 erfüllt.
2. Etwaige Hinweise auf diese Funktion werden auf der Weboberfläche verifiziert bzw. falsifiziert.
3. Sofern das Benutzerhandbuch keine Hinweise enthält, wird die Existenz der Funktionalität an naheliegenden Stellen auf der Weboberfläche untersucht.

3.4.5 Rollenbasierte Zugriffskontrolle

Beschreibung des Testinhalts

Für die Nutzung einiger Funktionen auf der Weboberfläche ist kein voller Systemzugriff (root-Rechte) erforderlich. Beispielsweise genügt ein lesender Zugriff auf die Weboberfläche, um sich die Anruferliste anzeigen zu lassen. Ein abgestuftes Rechte-Konzept in Form einer rollenbasierten Zugriffskontrolle sollte in der Weboberfläche implementiert sein (3.4.5).

Beschreibung der Testdurchführung zu 3.4.5

1. Es wird recherchiert, ob im Benutzerhandbuch eine Funktion erwähnt wird, die die Erwartung von 3.4.5 erfüllt.
2. Etwaige Hinweise auf diese Funktion werden auf der Weboberfläche verifiziert bzw. falsifiziert.
3. Sofern das Benutzerhandbuch keine Hinweise enthält, wird die Existenz der Funktionalität an naheliegenden Stellen auf der Weboberfläche untersucht.

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
3.4.1	Passwortschutz	1. Die Weboberfläche des Routers ist mit einem Passwort geschützt, das individuell ist und aus min. 8 Zeichen besteht.	Anforderung	Inwieweit ein Passwortschutz vorhanden ist, wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	10
		2. Das vordefinierte Passwort besteht aus Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen. Alternativ sind mindestens zwei dieser Anforderungen umgesetzt.	Empfehlung	Inwieweit ein Passwortschutz vorhanden ist, wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	7
		3. Das neue Passwort lässt sich nur unter Kenntnis des alten Passwortes ändern.	Empfehlung	– Ggf. wird der Passwortschutz für die Weboberfläche aktiviert. – Ein neues Passwort für die Weboberfläche wird vergeben.	1	5
		4. Beim Setzen eines Passworts wird die Passwortstärke angezeigt.	Empfehlung	– Ggf. wird der Passwortschutz für die Weboberfläche aktiviert. – Ein neues Passwort für die Weboberfläche wird vergeben.	1	7
3.4.2	Login-Sperre	Die Weboberfläche verwendet einen Captcha oder nach einer fehlgeschlagenen Anmeldung wird ein	Anforderung	– Ggf. wird der Passwortschutz für die Weboberfläche aktiviert. – Inkorrekte Anmelde-Daten werden 10-mal eingegeben.	1	8

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
		erneuter Anmeldeversuch zeitlich verzögert.				
3.4.3	Verschlüsselter Zugriff über die LAN-Schnittstelle	Der Zugriff auf die Weboberfläche (LAN-Schnittstelle) erfolgt neben HTTP ebenfalls über HTTPS.	Empfehlung	Die Existenz und der Status des Zugriffs werden mittels Weboberfläche und Benutzerhandbuches untersucht. Es ist darauf zu achten, dass keine Weiterleitung (Redirect) auf HTTP erfolgt.	1	4
3.4.4	Zugriff über die WAN-Schnittstelle	1. Der Zugriff auf die Weboberfläche (WAN-Schnittstelle) ist deaktiviert bzw. nicht implementiert.	Anforderung	Die Existenz und der Status des Zugriffs werden mittels Weboberfläche und Benutzerhandbuches untersucht.	1	10
		2. Der Zugriff auf die Weboberfläche (WAN-Schnittstelle) erfolgt über HTTPS.	Anforderung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	10
		3. Der TCP-Port für HTTPS lässt sich ändern.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	5
3.4.4	Rollenbasierte Zugriffskontrolle	Ein abgestuftes Rechte-Konzept sollte in der Weboberfläche implementiert sein.	Option	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	1

Tabelle 4: Übersicht Weboberfläche

3.5 Ereignis-Protokollierung

Eine aussagekräftige Protokollierung der Ereignisse ist ein wirksames Mittel zur Fehlersuche. Im Zusammenhang mit Routern sollte die Protokollierung zusätzlich Aspekte der Sicherheit berücksichtigen, sodass versuchte oder erfolgreiche Angriffe entdeckt werden können.

3.5.1 Letzte Anmeldung

Beschreibung des Testinhalts

Die Angaben zur letzten "erfolgreichen" und "gescheiterten" Anmeldung an der Weboberfläche (Uhrzeit, IP-Adresse) müssen protokolliert werden und sich bei Bedarf anzeigen lassen (3.5.1).

Beschreibung der Testdurchführung zu 3.5.1

1. Sofern der Passwortschutz für die Weboberfläche nicht standardmäßig aktiviert ist, wird dieser aktiviert.
2. Die Weboberfläche des Routers wird geschlossen bzw. es erfolgt eine Abmeldung.
3. Die Weboberfläche des Routers wird erneut aufgerufen und inkorrekte Anmelde-Daten werden 2-mal eingegeben.
4. Die Weboberfläche des Routers wird aufgerufen und es erfolgt eine erfolgreiche Anmeldung.
5. Im System- bzw. Protokoll-Bereich der Weboberfläche wird nach den Erwartungen von 3.5.1 recherchiert.

3.5.2 Protokolldateien

Beschreibung des Testinhalts

Der Router sollte Protokolldateien anlegen und diese auf der Weboberfläche anzeigen. Die Protokolldateien sollten insbesondere Ereignisse bzw. Aktionen für die folgenden Bereiche des Routers enthalten:

- System (3.5.2.1)
- WLAN (3.5.2.2)
- Firewall (3.5.2.3)
- Weboberfläche (3.5.2.4)
- Telefonie (3.5.2.5)

Die Ereignisse bzw. Aktionen können entsprechend ihrer Kategorie getrennt voneinander auf der Weboberfläche betrachtet werden (3.5.2.6). Außerdem kann die Protokollierung bei Bedarf im Hinblick auf den Datenschutz deaktiviert werden (3.5.2.7). Eine Basis-Protokollierung sollte hingegen nicht deaktivierbar sein.

Beschreibung der Testdurchführung zu 3.5.2.1

1. Es wird recherchiert, ob im Benutzerhandbuch eine Funktion erwähnt wird, die die Erwartung von 3.5.2.1 erfüllt.
2. Etwaige Hinweise auf diese Funktion werden auf der Weboberfläche verifiziert bzw. falsifiziert.
3. Sofern das Benutzerhandbuch keine Hinweise enthält, wird die Existenz der Funktionalität an naheliegenden Stellen auf der Weboberfläche untersucht.

Beschreibung der Testdurchführung zu 3.5.2.2 - 3.5.2.7

Der Test erfolgt analog zu 3.5.2.1.

3.5.3 Verbrauchtes Datenvolumen

Beschreibung des Testinhalts

Eine übersichtliche Statistik über das verbrauchte Datenvolumen, bei der zwischen Up- und Download unterschieden wird, kann angezeigt werden (3.5.3.1). Darüber hinaus kann eine clientbasierte Statistik über das verbrauchte Datenvolumen angezeigt werden (3.5.3.2).

Beschreibung der Testdurchführung zu 3.5.3.1 - 3.5.3.2

Der Test wird analog zu 3.5.2.1 durchgeführt.

3.5.4 Aufzeichnen von Datenverkehr

Beschreibung des Testinhalts

Um den Netzwerkverkehr analysieren zu können, sollte der versierte Benutzer die Möglichkeit haben, diesen aufzuzeichnen. Die Aufzeichnung sollte an der WAN-, LAN- und WLAN-Schnittstelle möglich sein (3.5.4).

Beschreibung der Testdurchführung zu 3.5.4

Der Test wird analog zu 3.5.2.1 durchgeführt.

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
3.5.1	Letzte Anmeldung	Angaben zur letzten "erfolgreichen" und "gescheiterten" Anmeldung an der Weboberfläche (Uhrzeit, IP-Adresse) werden protokolliert und lassen sich anzeigen.	Anforderung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	8
3.5.2	Protokolldateien	1. Die System-Protokolldatei lässt sich über die Weboberfläche anzeigen.	Anforderung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	8
		2. Die WLAN-Protokolldatei lässt sich über die Weboberfläche anzeigen.	Anforderung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	8
		3. Die Firewall-Protokolldatei lässt sich über die Weboberfläche anzeigen.	Anforderung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	8
		4. Die Protokolldatei für den Zugriff auf die Weboberfläche lässt sich über die Weboberfläche anzeigen.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	6
		5. Die Protokolldatei für den Zugriff auf die	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	6

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
		Telefonie lässt sich über die Weboberfläche anzeigen.				
		6. Die verschiedenen Protokolldateien lassen sich entsprechend ihrer Kategorie getrennt betrachten.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	4
		7. Die Protokollierung kann bei Bedarf im Hinblick auf den Datenschutz deaktiviert werden. Eine Basis-Protokollierung sollte hingegen nicht deaktivierbar sein.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	4
3.5.3	Verbrauchtes Datenvolumen	1. Eine übersichtliche Statistik über das verbrauchte Datenvolumen, bei der zwischen Up- und Download unterschieden wird, kann angezeigt werden.	Option	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	2	3
		2. Eine clientbasierte Statistik über das verbrauchte	Option	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	2	2

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
		Datenvolumen kann angezeigt werden.				
3.5.4	Aufzeichnen von Datenverkehr	Der Netzwerkverkehr an der WAN-, LAN- und WLAN-Schnittstelle kann aufgezeichnet werden.	Option	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	2

Tabelle 5: Übersicht Ereignis-Protokollierung

3.6 DNS

Das Domain Name System (DNS) bildet einen grundlegenden Dienst für nahezu jede Internetkommunikation. In diesem Zusammenhang kann der Router einige Funktionen bereitstellen, um die Sicherheit der Endgeräte zu erhöhen.

3.6.1 Verwendeter DNS-Server

Beschreibung des Testinhalts

Sofern im Router ein DNS-Proxy vorhanden ist, verwendet der Router typischerweise die vom ISP übermittelten DNS-Server. Optional sollte auch die Nutzung anderer DNS-Server möglich sein. Es soll sichergestellt werden, dass die vom Router verwendeten DNS-Server mithilfe von IPv4-Adressen (3.6.1.1) und IPv6-Adressen (3.6.1.2) konfiguriert werden können.

Beschreibung der Testdurchführung zu 3.6.1.1

1. Es wird recherchiert, ob im Benutzerhandbuch eine Funktion erwähnt wird, die die Erwartung von 3.6.1.1 erfüllt.
2. Etwaige Hinweise auf diese Funktion werden auf der Weboberfläche verifiziert bzw. falsifiziert.
3. Sofern das Benutzerhandbuch keine Hinweise enthält, wird die Existenz der Funktionalität an naheliegenden Stellen auf der Weboberfläche untersucht.

Beschreibung der Testdurchführung zu 3.6.1.2

Der Test wird analog zu 3.6.1.1 durchgeführt.

3.6.2 DNS-Rebind-Schutz

Beschreibung des Testinhalts

Um DNS-Rebinding-Angriffe zu erschweren, sollte ein DNS-Rebind-Schutz aktiviert sein (3.6.2.1) und zudem Ausnahmen definiert werden können (3.6.2.2).

Beschreibung der Testdurchführung zu 3.6.2.1 und 3.6.2.2

Der Test wird analog zu 3.6.1.1 durchgeführt.

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
3.6.1	Verwendeter DNS-Server	1. Die vom Router verwendeten DNS-Server können mithilfe von IPv4-Adressen konfiguriert werden.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	4
		2. Die vom Router verwendeten DNS-Server können mithilfe von IPv6-Adressen konfiguriert werden.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	4
3.6.2	DNS-Rebind-Schutz	1. Ein DNS-Rebind-Schutz ist implementiert.	Option	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	3
		2. Ausnahmen für den DNS-Rebinding-Schutz können definiert werden.	Option	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	3

Tabelle 6: Übersicht DNS

3.7 VPN

Mithilfe eines VPN kann eine sichere Verbindung in das interne Netzwerk hinter dem Router (LAN) hergestellt werden. Die Konfiguration eines VPN sollte gewisse Wahlmöglichkeiten bieten, damit eine sichere Verbindung nach individuellen Bedürfnissen gestaltet werden kann.

3.7.1 VPN-Verbindung

Beschreibung des Testinhalts

Es soll sichergestellt werden, dass mithilfe des Routers eine VPN-Verbindung realisiert werden kann. Zur Realisierung einer VPN-Verbindung kann

- IPsec
- L2TP over IPsec
- OpenVPN

verwendet werden (3.7.1).

Beschreibung der Testdurchführung zu 3.7.1

1. Es wird recherchiert, ob im Benutzerhandbuch eine Funktion erwähnt wird, die die Erwartung von 3.7.1 erfüllt.
2. Etwaige Hinweise auf diese Funktion werden auf der Weboberfläche verifiziert bzw. falsifiziert.
3. Sofern das Benutzerhandbuch keine Hinweise enthält, wird die Existenz der Funktionalität an naheliegenden Stellen auf der Weboberfläche untersucht.

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
3.7.1	VPN-Verbindung	Mithilfe des Routers kann eine VPN-Verbindung über IPsec, L2TP over IPsec oder OpenVPN aufgebaut werden.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	3

Tabelle 7: Übersicht VPN

3.8 Aktive Dienste

Als Nächstes wird untersucht, ob eine Transparenz im Hinblick auf aktive Dienste gegeben ist.

3.8.1 Übersicht auf der Weboberfläche

Beschreibung des Testinhalts

Es soll sichergestellt werden, dass die Weboberfläche eine Übersicht aller aktiven Dienste an der WAN- (3.8.1.1) und LAN-Schnittstelle (3.8.1.2) enthält. Zu einer übersichtlichen Darstellung gehört die Bezeichnung des Dienstes, der dazugehörige Port, das verwendete Protokoll sowie eine kurze Beschreibung.

Beschreibung der Testdurchführung zu 3.8.1.1 und 3.8.1.2

1. Es wird recherchiert, ob im Benutzerhandbuch eine Funktion erwähnt wird, die die Erwartung von 3.8.1.1 und 3.8.1.2 erfüllt.
2. Etwaige Hinweise auf diese Funktion werden auf der Weboberfläche verifiziert bzw. falsifiziert.
3. Sofern das Benutzerhandbuch keine Hinweise enthält, wird die Existenz der Funktionalität an naheliegenden Stellen auf der Weboberfläche untersucht.

3.8.2 Übersicht im Benutzerhandbuch

Beschreibung des Testinhalts

Es soll sichergestellt werden, dass das Benutzerhandbuch eine Übersicht über alle aktiven Dienste an der WAN- (3.8.2.1) und LAN-Schnittstelle (3.8.2.2) enthält. Zu einer übersichtlichen Darstellung gehört die Bezeichnung des Dienstes, der dazugehörige Port, das verwendete Protokoll sowie eine kurze Beschreibung.

Beschreibung der Testdurchführung zu 3.8.1.1 und 3.8.1.2

Mithilfe des Benutzerhandbuches wird untersucht, ob die Erwartung von 3.8.2.1 und 3.8.2.2 erfüllt werden.

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
3.8.1	Übersicht auf der Weboberfläche	1. Alle aktiven Dienste auf der WAN-Schnittstelle werden übersichtlich auf der Weboberfläche dargestellt.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	2	7
		2. Alle aktiven Dienste auf der LAN-Schnittstelle werden übersichtlich auf der Weboberfläche dargestellt.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	2	6
3.8.2	Übersicht im Benutzerhandbuch	1. Alle aktiven Dienste auf der WAN-Schnittstelle werden übersichtlich im Benutzerhandbuch dargestellt.	Option	Mithilfe des Benutzerhandbuches wird untersucht, ob die Erwartung erfüllt wird.	1	3
		2. Alle aktiven Dienste auf der LAN-Schnittstelle werden übersichtlich im Benutzerhandbuch dargestellt.	Option	Mithilfe des Benutzerhandbuches wird untersucht, ob die Erwartung erfüllt wird.	1	2

Tabelle 8: Übersicht aktive Dienste

3.9 IPv6

Immer mehr Dienste werden über IPv6 angeboten. Aus diesem Grund sollte ein moderner Router über eine IPv6-Implementierung verfügen, die die Aspekte der Sicherheit berücksichtigt.

3.9.1 Unterstützung

Beschreibung des Testinhalts

IPv6 gewinnt zunehmend an Bedeutung. Daher kann IPv6 in den Routern implementiert sein (3.9.1.1). Außerdem sollte die Möglichkeit zur Deaktivierung von IPv6 gegeben sein, wenn der Router nicht für einen IPv6-only Betrieb konzipiert ist. Die Alternative dazu wäre, dass IPv6 nicht implementiert ist (3.9.1.2). Ob der Router für einen IPv6-only Betrieb konzipiert ist, sollte im Benutzerhandbuch erwähnt sein.

Beschreibung der Testdurchführung zu 3.9.1.1 und 3.9.1.2

1. Es wird recherchiert, ob im Benutzerhandbuch eine Funktion erwähnt wird, die die Erwartung von 3.9.1.1 erfüllt.
2. Etwaige Hinweise auf diese Funktion werden auf der Weboberfläche verifiziert bzw. falsifiziert.
3. Sofern das Benutzerhandbuch keine Hinweise enthält, wird die Existenz sowie der Status der Funktionalität an naheliegenden Stellen auf der Weboberfläche untersucht.

Beschreibung der Testdurchführung zu 3.9.1.2

Der Test wird analog zu 3.9.1.1 durchgeführt.

3.9.2 IPv6-Präfix

Beschreibung des Testinhalts

Sobald der Router eine neue Internetverbindung aufbaut, kann er ein neues IPv6-Präfix erhalten. Die regelmäßige Änderung des IPv6-Präfixes erschwert die Identifikation des Routers. Deshalb sollte die Weboberfläche des Routers die Möglichkeit anbieten, eine neues IPv6-Präfix anzufordern, z. B. durch die Betätigung eines Buttons oder zeitgesteuert (3.9.2).

Beschreibung der Testdurchführung zu 3.9.2.

Der Test wird analog zu 3.9.1.1 durchgeführt.

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
3.9.1	Unterstützung	1. IPv6 ist implementiert.	Option	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	3
		2. Die Möglichkeit zur Deaktivierung von IPv6 sollte gegeben sein, wenn der Router nicht für einen IPv6-only Betrieb konzipiert ist. Alternativ ist IPv6 nicht implementiert.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	5
3.9.2	IPv6-Präfix	Die Weboberfläche bietet die Möglichkeit, ein neues IPv6-Präfix für den Router anzufordern, z. B. durch die Betätigung eines Buttons oder zeitgesteuert.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	2	4

Tabelle 9: Übersicht IPv6

3.10 Weitere Sicherheitsfunktionen

Im letzten Abschnitt dieses Kapitels werden unterschiedliche Sicherheitsfunktionen behandelt, die in der Regel optional sind.

3.10.1 VLAN

Beschreibung des Testinhalts

Um das LAN strukturieren zu können, kann der Router eine VLAN-Funktion bereitstellen (3.10.1).

Beschreibung der Testdurchführung zu 3.10.1

1. Es wird recherchiert, ob im Benutzerhandbuch eine Funktion erwähnt wird, die die Erwartung von 3.10.1 erfüllt.
2. Etwaige Hinweise auf diese Funktion werden auf der Weboberfläche verifiziert bzw. falsifiziert.
3. Sofern das Benutzerhandbuch keine Hinweise enthält, wird die Existenz der Funktionalität an naheliegenden Stellen auf der Weboberfläche untersucht.

3.10.2 Management-Informationssystem

Beschreibung des Testinhalts

Um eine zeitnahe Reaktion auf gewisse Aktionen zu ermöglichen, sollte eine E-Mail-Adresse im Router hinterlegt werden können, an der nach bestimmten Regeln bzw. bei Auffälligkeiten eine Nachricht versendet wird (3.10.2.1). Insbesondere nach einer Änderung der Konfiguration (Internetverbindung, VoIP, WLAN) sollte eine E-Mail versendet werden (3.10.2.2). Darüber hinaus sollte eine Funktion bereitgestellt werden, die die Protokolldateien verschlüsselt per E-Mail versendet (3.10.2.3). Weiterhin sollte einer Nachricht versendet werden, nachdem die Verfügbarkeit eines Firmware-Updates festgestellt wird (3.10.2.4). Schließlich kann eine Vorschaltseite (Walled Garden) aktiviert werden, die im Browser vor dem ersten Seitenaufruf angezeigt wird, um den Nutzer über besondere Vorfälle zu informieren (3.10.2.5).

Beschreibung der Testdurchführung zu 3.10.2.1 – 3.10.2.5

Der Test wird analog zu 3.10.1 durchführt.

3.10.3 Konfigurationsdatei

Beschreibung des Testinhalts

Es soll sichergestellt werden, dass sich die Router-Konfiguration in eine Datei abspeichern lässt (3.10.3.1). Zudem sollte die Konfigurationsdatei mit einem Passwort geschützt werden können (3.10.3.2).

Beschreibung der Testdurchführung zu 3.10.3.1 und 3.10.3.2

Der Test wird analog zu 3.10.1 durchführt.

3.10.4 Multifaktor-Authentifizierung

Beschreibung des Testinhalts

Eine Multifaktor-Authentifizierung erhöht den Identitäts- und Zugriffs-Schutz. Daher sollte ein Router über eine Multifaktor-Authentifizierung verfügen (3.10.4). Ein Beispiel für eine Multifaktor-Authentifizierung ist ein Hardware-Schreibschutz neben dem Passwortschutz für die Weboberfläche. Router die einen Hardware-Schreibschutz besitzen, können nur konfiguriert werden, falls der Hardware-Schreibschutz

physisch deaktiviert wird. Das heißt, ein Angreifer aus der Ferne kann den Router bei einem aktiven Hardware-Schreibschutz nicht manipulieren.

Beschreibung der Testdurchführung zu 3.10.4

Die Existenz einer Multifaktor-Authentifizierung wird mithilfe des Benutzerhandbuches und des Routers untersucht.

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
3.10.1	VLAN	Der Router unterstützt VLAN.	Option	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	1
3.10.2	Management-Informationssystem	1. Eine E-Mail-Adresse kann zur Benachrichtigung bei auszuwählenden Ereignissen hinterlegt werden.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	7
		2. Eine E-Mail kann nach einer Änderung der Konfiguration versendet werden.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	7
		3. Die Protokolldateien können regelmäßig per E-Mail versendet werden.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	5
		4. Eine E-Mail wird bei der Bereitstellung eines Firmware-Updates versendet.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	7
		5. Eine Vorschaltseite kann aktiviert werden, die im Browser vor dem ersten Seitenaufruf angezeigt wird, um den Nutzer über besondere Vorfälle zu informieren.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	5

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
3.10.3	Konfigurationsdatei	1. Die Router-Konfiguration lässt sich in eine Datei abspeichern.	Anforderung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	8
		2. Die Konfigurationsdatei kann mit einem Passwort geschützt werden.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	7
3.10.4	Multifaktor-Authentifizierung	Der Router verfügt über eine Multifaktor-Authentifizierung.	Option	Die Existenz einer Multifaktor-Authentifizierung wird mittels Router und Benutzerhandbuches untersucht.	1	3

Tabelle 10: Übersicht weitere Sicherheitsfunktionen

Die Kapitel 4 und 5 sind nach dem Traffic Light Protocol TLP AMBER eingestuft und können nach schriftlicher Anerkennung des Traffic Light Protocols durch Provider und Hersteller angefordert werden. Sonstige Interessenten erhalten diese Kapitel, wenn sie zusätzlich schriftlich zusichern, diese Informationen nicht für unerlaubte Angriffe auf Router zu verwenden.

6 Weitere Eigenschaften

Die Sicherheit eines Routers kann nicht nur durch die Bereitstellung von sicheren Funktionen unterstützt werden, sondern auch durch weitere Eigenschaften, die indirekt das Sicherheitsniveau anheben. Dazu zählen Aspekte des Supports sowie der Benutzerfreundlichkeit (Usability).

6.1 Support

Der technische Support sollte bei Bedarf bei der sicheren Konfiguration des Routers unterstützen. Weiterhin sollte ein detailliertes Benutzerhandbuch bzw. eine Hilfe auf der Weboberfläche des Routers mit Anleitungen für eine sichere Konfiguration des Routers vorhanden sein.

6.1.1 Technischer Support

Beschreibung des Testinhalts

Ein technischer Support sollte in Form einer deutschsprachigen Hotline (6.1.1.1) und eines deutschsprachigen E-Mail-Supports (6.1.1.2) zur Verfügung gestellt werden. Zudem sollte auf der Hersteller-Webseite oder im Benutzerhandbuch eine FAQ zu dem Router (6.1.1.3) sowie Kontaktdaten für die Meldung von Sicherheitsvorfällen (6.1.1.4) bereitgestellt werden.

Beschreibung der Testdurchführung zu 6.1.1.1 – 6.1.1.4

1. Es wird recherchiert, ob im Benutzerhandbuch Informationen enthalten sind, die die Erwartungen von 6.1.1.1 – 6.1.1.3 erfüllen.
2. Sofern das Benutzerhandbuch keine Hinweise enthält, werden die Informationen auf der Hersteller-Webseite recherchiert.

6.1.2 Benutzerhandbuch

Beschreibung des Testinhalts

Ein ausführliches Benutzerhandbuch in analoger oder digitaler Form sollte mit dem Router ausgeliefert werden (6.1.2.1). Ein digitales Benutzerhandbuch kann auf einer CD-ROM gespeichert oder auf der Weboberfläche des Routers hinterlegt werden. Ferner kann eine Kurzanleitung für den Router in der Verpackung beiliegen (6.1.2.2).

Beschreibung der Testdurchführung zu 6.1.2.1 und 6.1.2.2

1. Es wird überprüft, ob eine Kurzanleitung sowie ein Benutzerhandbuch in der Verpackung beiliegen.
2. Sofern das Benutzerhandbuch nicht in analoger Form oder als CD-ROM beiliegt, wird im Anmeldebereich und auf der Startseite der Weboberfläche nach einer digitalen Form des Benutzerhandbuches recherchiert.

6.1.3 Weboberfläche

Beschreibung des Testinhalts

Um die Konfiguration des Routers zu erleichtern, sollte die Weboberfläche eine kontextsensitive Hilfe besitzen (6.1.3.1). Hierbei kann die kontextsensitive Hilfe auf einem gesonderten Bereich der Weboberfläche erscheinen. Als Alternative kann die kontextsensitive Hilfe in Form eines Pop-Up-Feldes erscheinen, solange der Mauszeiger sich über eine Funktion befindet. Außerdem sollte ein Einrichtungsassistent für Internet und VoIP zur Verfügung stehen (6.1.3.2).

Beschreibung der Testdurchführung zu 6.1.3.1

1. Die Weboberfläche des Routers wird aufgerufen und es erfolgt ggf. eine Anmeldung.
2. Verschiedene Funktionen werden aktiviert bzw. der Mauszeiger wird über eine Funktion gehalten.

Beschreibung der Testdurchführung zu 6.1.3.2

1. Es wird recherchiert, ob im Benutzerhandbuch eine Funktion erwähnt wird, die die Erwartung von 6.1.3.2 erfüllt.
2. Etwaige Hinweise auf diese Funktion werden auf der Weboberfläche verifiziert bzw. falsifiziert.
3. Sofern das Benutzerhandbuch keine Hinweise enthält, wird die Existenz der Funktionalität an naheliegenden Stellen auf der Weboberfläche untersucht.

6.1.4 Update Support

Beschreibung des Testinhalts

Die gesicherte Bereitstellung von Firmware-Updates über einen gewissen Zeitraum bietet Planungssicherheit für den Anwender. Daher sollte der Hersteller eine Mindestzeit angeben, in der der Router mit Firmware-Updates versorgt wird (6.1.4).

Beschreibung der Testdurchführung zu 6.1.4

Hinweise auf eine Mindestzeit für Firmware-Updates werden auf der Verpackung, im Benutzerhandbuch und auf der Hersteller-Webseite recherchiert.

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
6.1.1	Technischer Support	1. Eine deutschsprachige Hotline wird zur Verfügung gestellt.	Empfehlung	Mithilfe des Benutzerhandbuches und der Hersteller-Webseite wird untersucht, ob die Erwartung erfüllt wird.	1	4
		2. Ein deutschsprachiger E-Mail-Support wird zur Verfügung gestellt.	Empfehlung	Mithilfe des Benutzerhandbuches und der Hersteller-Webseite wird untersucht, ob die Erwartung erfüllt wird.	1	4
		3. Auf der Hersteller-Webseite oder im Benutzerhandbuch wird eine FAQ zu dem Router bereitgestellt.	Option	Mithilfe des Benutzerhandbuches und der Hersteller-Webseite wird untersucht, ob die Erwartung erfüllt wird.	1	1
		4. Auf der Hersteller-Webseite oder im Benutzerhandbuch werden Kontaktdaten für die Meldung von Sicherheitsvorfällen bereitgestellt.	Empfehlung	Mithilfe des Benutzerhandbuches und der Hersteller-Webseite wird untersucht, ob die Erwartung erfüllt wird .	1	4
6.1.2	Benutzerhandbuch	1. Ein ausführliches Benutzerhandbuch in analoger oder digitaler Form wird mit dem Router ausgeliefert.	Empfehlung	Der Verpackungsinhalt und die Weboberfläche des Routers werden nach einem Benutzerhandbuch durchsucht. Ein digitales Benutzerhandbuch kann auf einer CD-ROM gespeichert oder auf der Weboberfläche des Routers hinterlegt werden.	1	7
		2. Eine Kurzanleitung für den Router ist in der Verpackung enthalten.	Option	Der Verpackungsinhalt wird nach einer Kurzanleitung durchsucht.	1	1

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
6.1.3	Weboberfläche	1. Die Weboberfläche besitzt eine kontextsensitive Hilfe.	Empfehlung	– Die Weboberfläche des Routers wird aufgerufen und es erfolgt ggf. eine Anmeldung. – Verschiedene Funktionen werden aktiviert bzw. der Mauszeiger wird über eine Funktion gehalten.	1	4
		2. Ein Einrichtungsassistent für Internet und VoIP wird bereitstellt.	Option	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	2
6.1.4	Update-Support	Der Hersteller gibt eine Mindestzeit an, in der der Router mit Firmware-Updates versorgt wird.	Empfehlung	Hinweise auf eine Mindestzeit für Firmware-Updates werden auf der Verpackung, im Benutzerhandbuch und auf der Hersteller-Webseite recherchiert.	1	7

Tabelle 31: Übersicht Support

6.2 Usability

Eine gute Benutzerfreundlichkeit kann zur Erhöhung der Sicherheit beitragen, indem die Interaktion zwischen dem Benutzer und dem Router verständlich und ergonomisch gestaltet wird.

6.2.1 Werkseinstellung

Beschreibung des Testinhalts

Um die Werkseinstellungen wiederherzustellen, sollte der Router eine physische Vorrichtung besitzen (6.2.1.1). Zusätzlich können sich die Werkseinstellungen mithilfe der Weboberfläche wiederherstellen lassen (6.2.1.2).

Beschreibung der Testdurchführung zu 6.2.1.1

Die Existenz eines Reset-Knopfes wird mithilfe des Benutzerhandbuches und des Routers untersucht.

Beschreibung der Testdurchführung zu 6.2.1.2

1. Es wird recherchiert, ob im Benutzerhandbuch eine Funktion erwähnt wird, die die Erwartung von 6.2.1.2 erfüllt.
2. Etwaige Hinweise auf diese Funktion werden auf der Weboberfläche verifiziert bzw. falsifiziert.
3. Sofern das Benutzerhandbuch keine Hinweise enthält, wird die Existenz der Funktionalität an naheliegenden Stellen auf der Weboberfläche untersucht.

6.2.2 WLAN

Beschreibung des Testinhalts

Es soll sichergestellt werden, dass ein physischer Knopf zur Deaktivierung des WLAN vorhanden ist (6.2.2.1). Zudem kann eine Funktion für eine zeitgesteuerte Deaktivierung des WLAN vorhanden sein (6.2.2.2). Dadurch wird die Angriffsfläche sowie die Leistungsaufnahme des Routers reduziert.

Beschreibung der Testdurchführung zu 6.2.2.1

Die Existenz eines WLAN-Knopfes wird mithilfe des Benutzerhandbuches und einer Inaugenscheinnahme des Routers untersucht.

Beschreibung der Testdurchführung zu 6.2.2.2

Der Test wird analog zu 6.2.1.2 durchgeführt.

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*
6.2.1	Werkseinstellung	1. Die Werkseinstellungen lassen sich mithilfe einer physischen Vorrichtung wiederherstellen.	Empfehlung	Die Existenz eines Reset-Knopfes wird mithilfe des Benutzerhandbuches und des Routers untersucht.	1	7
		2. Die Werkseinstellungen lassen sich mithilfe der Weboberfläche wiederherstellen.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	7
6.2.2	WLAN	1. Ein physischer Knopf zur Deaktivierung des WLAN ist vorhanden.	Option	Die Existenz eines WLAN-Knopfes wird mithilfe des Benutzerhandbuches und des Routers untersucht.	1	1
		2. Das WLAN lässt sich zeitgesteuert deaktivieren.	Option	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	1

Tabelle 32: Übersicht Usability

7 Ausschlusskriterien

In diesem Kapitel werden Ausschlusskriterien definiert, die unabhängig von der sonstigen Punktwertung zur Nicht-Empfehlung eines Routers führen. Die Ausschlusskriterien werden in den vorangegangenen Kapiteln des Testkonzepts implizit überprüft und in der nachfolgenden Tabelle zusammengefasst.

Nr.	***Ausschlusskriterium***	***Kapitel***
7.1	Ein Firmware-Update ist über die Weboberfläche nicht vorgesehen und der Router unterstützt kein TR-069.	3.1 und 4.4.3
7.2	Die Firewall blockiert keine eingehenden Verbindungen sowie einen Ping auf die Global-Unicast-Adresse eines Clients im LAN bzw. WLAN, sofern es sich nicht um Antwortpakete zu einer ausgehenden Verbindung handelt.	4.5.1
7.3	An der WAN-Schnittstelle existiert ein geöffneter Port, dessen zugehöriger Dienst weder eindeutig im Benutzerhandbuch dokumentiert, noch in der Weboberfläche des Routers erläutert und abschaltbar ist.	4.4.1
7.4	Die WAN-Schnittstelle antwortet auf DNS-Abfragen (Open Resolver).	5.1.1
7.5	Die WAN-Schnittstelle antwortet auf UPnP-Abfragen.	5.4.2
7.6	Der Router verfügt über eine Schwachstelle, wie beispielsweise Heartbleed.	5.5.1
7.7	Die Weboberfläche ist im Auslieferungszustand über die WAN-Schnittstelle erreichbar.	4.2.1
7.8	Die Weboberfläche unterstützt kein HTTPS an der WAN-Schnittstelle, sofern der Zugriff über die WAN-Schnittstelle möglich ist.	4.2.1
7.9	Die VoIP-Implementierung bietet an der WAN-Schnittstelle eine Extension an, für die keine Authentifikation (noauth) erforderlich ist.	4.6.2

Tabelle 33: Übersicht Ausschlusskriterien

Anhang

Testumgebungen

In diesem Abschnitt werden verschiedene Testumgebungen beschrieben, die während der Testdurchführung benötigt werden. Jeder Testaufbau enthält eine Liste der erforderlichen Hilfsmittel (Geräte) und zusätzlich eine Beschreibung der notwendigen Software inklusive Konfiguration. Zudem wird der jeweilige Testaufbau grafisch dargestellt.

Testaufbau 1

Hilfsmittel	*Beschreibung*
Benutzer-PC	Windows 7, Ubuntu 14.04
Router	Standard-Konfiguration

Tabelle 34: Hilfsmittel-Testaufbau 1

Abbildung 1: Testaufbau 1

Testaufbau 2

Hilfsmittel	*Beschreibung*
Benutzer-PC	Windows 7, Ubuntu 14.04
Router	Standard-Konfiguration mit einer Internetverbindung

Tabelle 35: Hilfsmittel-Testaufbau 2

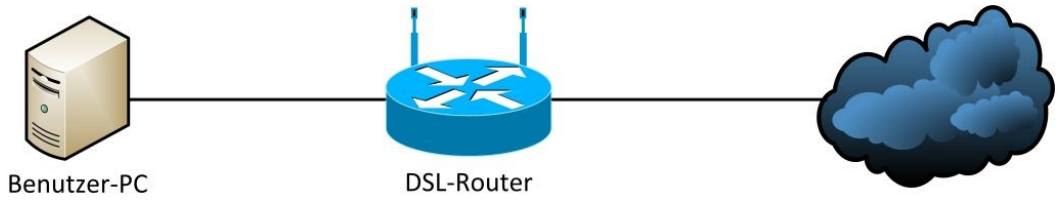

Abbildung 2: Testaufbau 2

Testaufbau 3

Hilfsmittel	*Beschreibung*
Benutzer-PC, Analyse-PC	Windows 7, Ubuntu 14.04
Router	Standard-Konfiguration mit einer Internetverbindung
DSLAM	Keine Restriktionen auf den Netzwerkverkehr
BRAS	Debian oder Ubuntu, PPPoE-Server

Tabelle 36: Hilfsmittel-Testaufbau 3

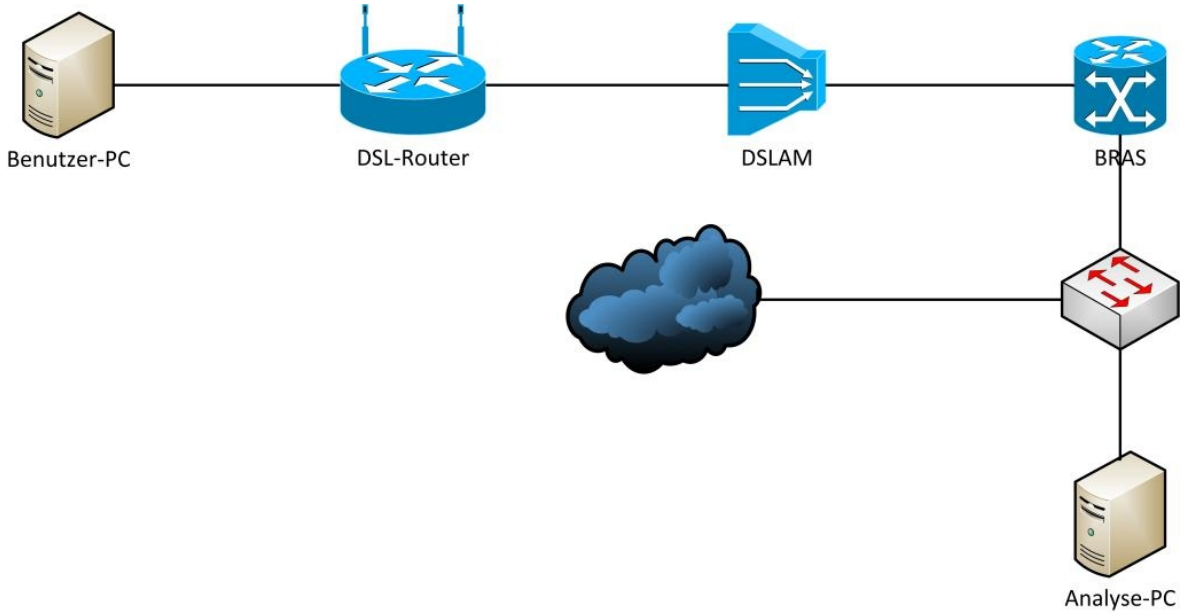

Abbildung 3: Testaufbau 3

Testaufbau 4

Hilfsmittel	*Beschreibung*
Benutzer-PC	Windows 7, Ubuntu 14.04, Wireshark
Router	Standard-Konfiguration mit einer Internetverbindung
DSLAM	Keine Restriktionen auf den Netzwerkverkehr
BRAS	Debian oder Ubuntu, PPPoE-Server
Autoritativer-Nameserver	
Caching-Resolver	

Tabelle 37: Hilfsmittel-Testaufbau 4

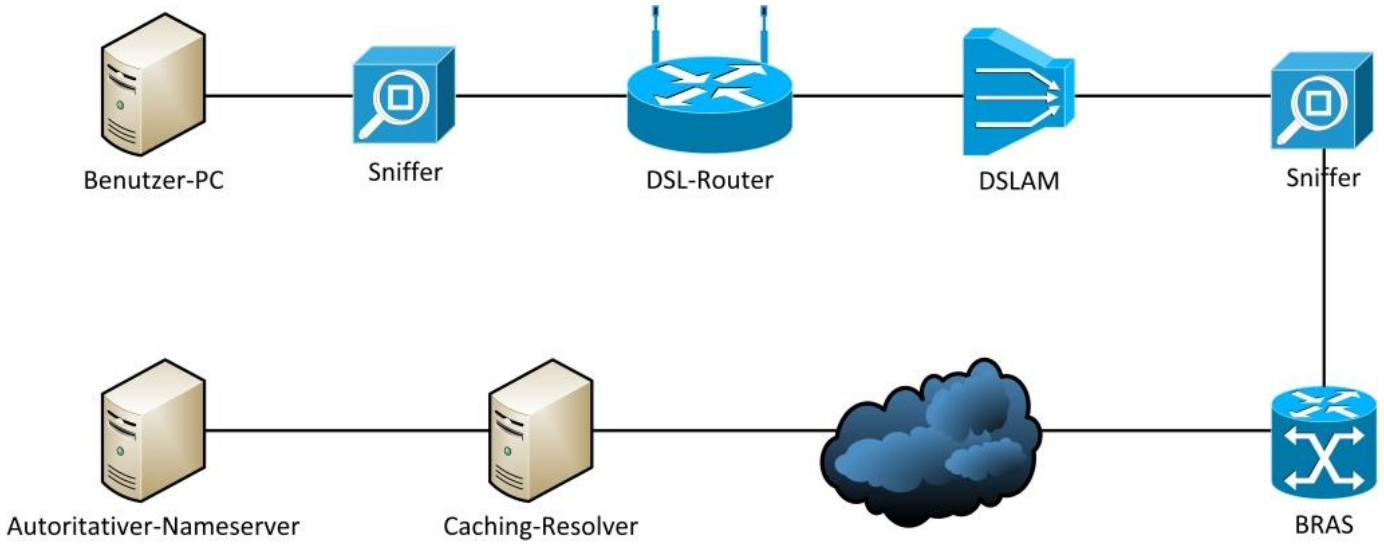

Abbildung 4: Testaufbau 4