	Nr.	7
	Hersteller	OpenWRT
	Gerät	TL-WR841N V10.0
	Firmware	05/15/01
Anforderung max:	414	328
Empfehlung max:	356	150
Option max:	47	11
Ausschlusskriterium:		Ja

? Unklares Verhalten, ggf. Hersteller fragen.

Nr.	*Testinhalt*	*Erwartung*	*Relevanz*	*Testdurchführung*	*Test-aufbau*	*Punkte*	*Punkte*	Erwartung erfüllt?
Firmware-Update								
3.1.1	Aktualität der Firmware	1. Nach dem Aufrufen der Weboberfläche erscheint automatisch ein Hinweis auf der Startseite, ob ein Firmware-Update zur Verfügung steht.	Empfehlung	Die Existenz des Hinweises bzw. der Funktionalität wird mittels Weboberfläche untersucht.	2	7	0	Nein
		2. Der Zeitpunkt für die letzte automatische Firmware-Update-Suche lässt sich abrufen.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche untersucht.	2	4	4	Ja
		3. Die verwendete Firmware-Version lässt sich abrufen.	Anforderung	Die Existenz der Funktionalität wird mittels Weboberfläche untersucht.	1	10	10	Ja
		4. Der Installationszeitpunkt der verwendeten Firmware lässt sich abrufen.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche untersucht.	1	4	0	Nein
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	10	Ja
		2. Bevor eine manuell heruntergeladene Firmware-Datei installiert wird, kann mithilfe des Routers (Weboberfläche) verifiziert werden, ob die Datei vom originären Router-Hersteller herausgegeben wurde.	Option	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	2	3	0	Nein
		3. Die Weboberfläche unterstützt ein Online-Update.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	2	7	0	Nein
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	0	Nein
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	0	Nein
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	1	Ja
WLAN								
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	10	Ja
		2. Die SSID bzw. ESSID enthält keine Angabe zur Produktbezeichnung.	Empfehlung	Ermittlung der SSID bzw. ESSID mittels Weboberfläche.	1	4	4	Ja
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	0	Nein
		2. Ein vordefinierter WPA2-Schlüssel enthält mindestens 20 Zeichen.	Empfehlung	Ermittlung der WPA2-Schlüssellänge mittels Weboberfläche.	1	6	0	Nein
		3. Bei Eingabe eines WPA2Schlüssels wird seine Schlüsselstärke (Länge u. Komplexität) angezeigt.	Empfehlung	Es wird versucht, einen neuen WLAN-Schlüssel zu setzen.	1	7	7	Ja
		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	0	Nein
3.2.3	WPS-PIN-Funktion	Die WPS-PIN-Funktion sollte standardmäßig deaktiviert sein und bei jeder Aktivierung eine neue zufällige PIN generieren. Alternativ ist die WPS-PIN-Me thode nicht implementiert.	Anforderung	Die Existenz und der Status der WPS-PIN-Funktion werden mittels Weboberfläche und Benutzerhandbuches untersucht.	1	8	8	Ja
Firewall								
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	10	Ja
		2. Der Firewall-Status ist auf der Weboberfläche deutlich erkennbar.	Empfehlung	Der Status der Funktionalität wird mittels Weboberfläche untersucht.	1	5	5	Ja
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	10	Ja
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	10	Ja
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	8	Ja
		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	4	Ja
		3. Internetseiten können auf Basis von DNS gesperrt werden.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	2	5	0	Nein

Weboberfläche								
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	0	Nein
		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	0	Nein
		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	0	Nein
		3. 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	0	Nein
3.4.2	Login-Sperre	Die Weboberfläche verwendet einen Captcha oder nach einer fehlgeschlagenen Anmeldung wird ein erneuter Anmeldeversuch zeitlich verzögert.	Anforderung	Ggf. wird der Passwortschutz für die Weboberfläche aktiviert. Inkorrekte Anmelde-Daten werden 10-mal eingegeben.	1	8	0	Nein
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	0	Nein
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	10	Ja
		2. Der Zugriff auf die Weboberfläche (WAN- Schnittstelle) erfolgt über HTTPS bzw. ist nicht implementiert.	Anforderung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	10	10	Ja
		3. Der TCP-Port für HTTPS lässt sich ändern bzw. HTTPS (WAN-Schnittstelle) ist nicht implementiert.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	5	5	Ja
3.4.5	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	0	Nein
Ereignis-Protokollierung								
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	0	Nein
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	8	Ja
		2. Die WLAN-Protokolldatei lässt sich über die Weboberfläche anzeigen.	Anforderung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	8	0	Nein
		3. Die Firewall-Protokolldatei lässt sich über die Weboberfläche anzeigen.	Anforderung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	8	0	Nein
		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	0	Nein
		5. Die Protokolldatei für den Zugriff auf die Telefonie lässt sich über die Weboberfläche anzeigen.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	6	0	Nein
		6. Die verschiedenen Protokolldateien lassen sich entsprechend ihrer Kategorie getrennt betrachten.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	4	0	Nein
		7. ~~Die Protokollierung kann bei Bedarf im Hinblick auf den Datenschutz deaktiviert werden.~~ Bei Bedenken gegen die Protokollierung soll diese deaktivierbar sein oder der Hersteller stellt einen Modus zur Verfügung, der die Protokollierung personenbeziehbare Daten ausschließt.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	4	0	Nein
3.5.3	Verbrauchtes Datenvolumen	1. Eine übersichtliche Gesamtstatistik 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	0	Nein
		2. Eine clientbasierte Statistik über das verbrauchte Datenvolumen kann angezeigt werden.	Option	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	2	2	0	Nein
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	0	Nein
DNS								
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	4	Ja
		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	4	Ja
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	3	Ja
		2. Ausnahmen für den DNS-Rebinding-Schutz können definiert werden.	Option	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	3	3	Ja
VPN								

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	0	Nein
Aktive Dienste								
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	7	Ja
		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	6	Ja
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	0	Nein
		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	0	Nein
IPv6								
3.9.1	Unterstützung	1. IPv6 ist implementiert.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	3	3	Ja
		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	5	Ja
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. Alternativ ist IPv6 nicht implementiert.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	2	4	0	Nein
Weitere Sicherheitsfunktionen								
3.10.1	VLAN	Der Router unterstützt VLAN innerhalb des integrierten Switch.	Option	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	1	1	Ja
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	0	Nein
		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	0	Nein
		3. Die Protokolldateien können regelmäßig per E-Mail versendet werden.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	5	0	Nein
		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	0	Nein
		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	0	Nein
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	8	Ja
		2. Die Konfigurationsdatei kann mit einem Passwort geschützt werden.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	7	0	Nein
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	0	Nein
WLAN								
4.1.1	SSID	Die SSID bzw. ESSID enthält keine Angabe zur Produktbezeichnung und stimmt zusätzlich mit den Angaben auf der Weboberfläche überein.	Empfehlung		1	Siehe Kap.2.4 e Übereinstimm	0	Ja
4.1.2	Verschlüsselung	Das WLAN hat standardmäßig eine WPA2-Verschlüsselung aktiviert und die Untersuchungsergebnisse stimmen mit den Angaben auf der Weboberfläche überein.	Anforderung		1	Siehe Kap.2.4 e Übereinstimm	ehe Kap.2 bereinstir	Nein
Weboberfläche								
4.2.1	Zugriff über die WAN-Schnittstelle	Der Zugriff auf die Weboberfläche (WAN-Schnittstelle) erfolgt prioritär mithilfe einer Cipher-Suite mit Forward Secrecy (TR-02102-2) oder ein Zugriff über die WAN-Schnittstelle auf die Weboberfläche ist nicht implementiert.	Empfehlung		3	5	5	Ja
DNS-Kompatibilität								
4.3.1	Grundlegende und erweiterte DNS-Kompatibilität	1. Kein Fehler, Rückantwort des abgefragten RR-Sets per UDP.	Anforderung		4	8	8	Ja
		2. Rückantwort des AAAA-Eintrags	Anforderung		4			Ja
		3. Rückantwort des SSHFP Eintrags.	Anforderung		4			Ja
		4. Rückantwort des SRV Eintrags.	Anforderung		4	8	8	Ja
		5. Rückantwort des NAPTR Eintrags.	Anforderung		4			Ja
		6. Kein Fehler, Rückantwort des abgefragten RR-Sets per TCP.	Empfehlung		4			Ja

		7. Unveränderte Rückantwort des WAN-seitigen DNS-Servers (transparentes Verhalten des Routers). Die Anfrage bei 4.3.3.2.1 erfüllt diese Erwartung ebenfalls.	Empfehlung		4	4	4	Ja
		8. Die Abfrage sollte vom Router nicht weitergeleitet werden.	Empfehlung		4	4	4	Ja
		9. TSIG sollte durchgereicht werden. Keine Manipulationen TSIG-signierter Queries.	Empfehlung		4			Ja
4.3.2	Quellport-Randomisierung	1. Source Port Randomness : Great	Anforderung		2	8	8	Ja
		2. Transaction ID Randomness: Great	Anforderung		2			Ja
4.3.3	DNSSEC							
4.3.3.1	EDNS0	1. Kein Fehler, Rückantwort des abgefragten RR-Sets per UDP. TC=0	Anforderung		4	8	0	Ja
		2. Keine Antwort, TC=1	Anforderung		4			Nein
		3. Keine Antwort, TC=1	Anforderung		4			Nein
		4. Kein Fehler, Rückantwort des abgefragten RR-Sets per UDP. TC=0	Anforderung		4			Ja
		5. Kein Fehler, Rückantwort des abgefragten RR-Sets per UDP. TC=0	Anforderung		4			Ja
		6. Keine Antwort, TC=1	Anforderung		4			Nein
		7. Kein Fehler, Rückantwort des abgefragten RR-Sets per UDP. TC=0	Anforderung		4			Ja
		8. Kein Fehler, Rückantwort des abgefragten RR-Sets per UDP. TC=0	Anforderung		4			Ja
		9. Keine Antwort, TC=1	Anforderung		4			Nein
		10. Kein Fehler, Rückantwort des abgefragten RR-Sets per UDP. TC=0	Anforderung		4			Ja
		11. Kein Fehler, Rückantwort des abgefragten RR-Sets per UDP. TC=0	Anforderung		4			Ja
		12. Keine Antwort, TC=1	Anforderung		4			Nein
		13. Kein Fehler, Rückantwort des abgefragten RR-Sets per UDP. TC=0	Anforderung		4			Ja
		14. Kein Fehler, Rückantwort des abgefragten RR-Sets per UDP. TC=0	Anforderung		4			Ja
		15. Kein Fehler, Rückantwort des abgefragten RR-Sets per UDP. TC=0	Anforderung		4			Ja
4.3.3.2	DNS-Abfragen zu unterschiedlichen Zonen	1. Antwort des SOA-Eintrags der unsignierten Zone, keine Flags gesetzt.	Anforderung		4	8	8	Ja
		2. Antwort des SOA-Eintrags der signierten Zone, keine RRSIGS, keine Flags.	Anforderung		4			Ja
		3. Keine Rückantwort, oder SERVFAIL, da Signatur der abgefragten Zone abgelaufen.	Anforderung		4			Ja
4.3.3.3	DNSSEC-Protokollbits	1. Antwort des SOA-Eintrags der unsignierten Zone, keine Flags in Antwort gesetzt.	Anforderung		4	8	0	Ja
		2. Antwort des SOA-Eintrags der unsignierten Zone, CD-Flag bleibt gesetzt.	Anforderung		4			Ja
		3. Antwort des SOA-Eintrags der unsignierten Zone, nur CD-Flag bleibt gesetzt.	Anforderung		4			Ja
		4. Antwort des SOA-Eintrags der signierten Zone, AD-Flag bleibt gesetzt, keine RRSIGS.	Anforderung		4			Nein
		5. Antwort des SOA-Eintrags der signierten Zone, CD-Flag bleibt gesetzt, keine RRSIGS.	Anforderung		4			Ja
		6. Antwort des SOA-Eintrags der signierten Zone, AD-Flag und CD-Flag bleiben gesetzt, keine RRSIGS.	Anforderung		4			Nein
4.3.3.4	DNSSEC-Abfragen	1. Antwort des SOA-Eintrags der unsignierten Zone, DO bleibt gesetzt, sonst keine Flags gesetzt.	Anforderung		4	8	0	Ja
		2. Antwort des SOA-Eintrags der signierten Zone, DO bleibt gesetzt, AD-Flag wird gesetzt, RRSIGS werden geliefert.	Anforderung		4			Nein
		3. Keine Rückantwort, oder SERVFAIL, da Signatur der abgefragten Zone abgelaufen.	Anforderung		4			Ja
		4. Antwort des SOA-Eintrags der unsignierten Zone, DO und CD bleiben gesetzt, sonst keine Flags gesetzt.	Anforderung		4			Ja
		5. Antwort des SOA-Eintrags der signierten Zone, DO und CD bleiben gesetzt, AD-Flag wird gesetzt, RRSIGS werden geliefert.	Anforderung		4			Nein
		6. Antwort des SOA-Eintrags der signierten Zone, DO und CD bleiben gesetzt, AD-Flag wird *nicht* gesetzt, RRSIGS werden geliefert.	Anforderung		4			Ja
4.3.3.5	Kompatibilität eines ggf. vorhandenen DNS-Caches mit DNSSEC	Sofern der Router einen DNS-Proxy-Cache besitzt, sollte dieser zwischen einer Abfrage mit gesetztem bzw. nicht gesetztem DO-Bit unterscheiden. Die Erwartungen sind ebenfalls mit “JA” festzulegen, falls der Router keinen DNS-Proxy-Cache besitzt.	Anforderung		4	8	8	Ja
4.3.3.6	Abfrage-Kompatibilität mit TLSA-Einträgen	Der Router sollte auch Abfragen zu TLSA-Einträgen (RFC6698) korrekt unterstützen.	Anforderung		4	8	8	Ja

Aktive Dienste								
4.4.1	WAN-Schnittstelle	1. An der WAN-Schnittstelle sind bis auf wenige Ausnahmen keine aktiven Dienste (offenen Ports 0-65535) über TCP vorhanden. Ausnahmen: SIP (5060) SIPS (5061) CWMP (7547) Ein zufällig gewählter CWMP-Port ist zulässig, sofern dieser Port auf der Weboberfläche des Routers angezeigt wird.	Anforderung		3	10	10	Ja
		2. An der WAN-Schnittstelle sind bis auf wenige Ausnahmen keine aktiven Dienste im untersuchten Portnummernbereich (0-1023, 5060, 5061, 7547) über UDP vorhanden. Ausnahmen: SIP (5060) SIPS (5061) CWMP (7547) Ein zufällig gewählter CWMP-Port ist zulässig, sofern dieser Port auf der Weboberfläche des Routers angezeigt wird.	Anforderung		3	10	10	Ja
		3. Alle standardmäßig aktiven Dienste, die zuvor mithilfe des Portscans (Nmap) ermittelt wurden, werden auf der Weboberfläche oder im Benutzerhandbuch übersichtlich dargestellt oder es sind keine Ports offen.	Anforderung		2	8	8	Ja
		4. Alle Dienste (WAN-Schnittstelle) lassen sich mithilfe der Weboberfläche deaktivieren, sodass die entsprechenden Ports geschlossen werden oder es sind keine Ports offen.	Anforderung		2	10	10	Ja
4.4.2	LAN-Schnittstelle	1. An der LAN-Schnittstelle sind bis auf wenige Ausnahmen keine aktiven Dienste (offenen Ports 0-65535) über TCP vorhanden. Ausnahmen: DNS (53) HTTP (80) HTTPS (443)	Empfehlung		1	6	0	Nein
		2. An der LAN-Schnittstelle sind bis auf wenige Ausnahmen keine aktiven Dienste (offenen Ports 0-1023) über UDP vorhanden. Ausnahmen: DNS (53) DHCP (67)	Empfehlung		1	6	6	Ja
		3. Alle standardmäßig aktiven Dienste, die zuvor mithilfe des Portscans (Nmap) ermittelt wurden, werden auf der Weboberfläche oder im Benutzerhandbuch übersichtlich dargestellt.	Anforderung		1	8	8	Ja
4.4.3	TR-069	1. Der Router unterstützt TR-069.	Option		1	3	0	Nein
		2. Der Status von TR-069 lässt sich immer auf der Weboberfläche abrufen, sofern TR-069 implementiert ist.	Empfehlung		2	5	5	Ja
		3. TR-069 ist deaktivierbar, wenn der Router über andere Firmware-Update-Mechanismen (Kapitel 3.1) verfügt. Die Erwartungen sind ebenfalls mit “JA” festzulegen, falls der Router lediglich über TR-069 provisioniert wird.	Empfehlung		1	7	7	Ja
IPv6								
4.5.1	Firewall-Bypass	1. Eine IPv6-Firewall ist vorhanden und blockiert alle eingehenden IPv6-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 (siehe Testdurchführung).	Anforderung		3	10	0	Nein
		2. Die Weboberfläche bietet nicht die Möglichkeit an, die IPv6-Firewall zu deaktivieren, wenn der Zugriff auf die Weboberfläche über die WAN-Schnittstelle erfolgt.	Anforderung		3	10	10	Ja
4.5.2	ICMPv6	ICMPv6-Nachrichten des Typ Packet Too Big werden von der IPv6-Firewall blockiert, wenn sie nicht zu einer Verbindung gehören, die aus dem LAN initiiert wurde.	Empfehlung		4	6	0	Nein
VoIP								
4.6.1	Sperrliste ~~für Rufnummern~~	1. Eine Sperrliste für Rufnummern (ankommende und ausgehende Anrufe) kann definiert werden	Empfehlung		1	6	0	Nein
		2. Die Nutzung von VoIP aus dem LAN kann unterbunden werden.	Empfehlung		1	7	0	Nein
4.6.2	SIP User Agent	1. Der SIP User Agent sollte an der WAN-Schnittstelle nicht auf SIP-Requests (Register) antworten, die von einem beliebigen Kommunikationspartner gestellt werden. Alternativ kann der SIP User Agent mit einer Fehlermeldung antworten.	Anforderung		3	8	8	Ja

		2. Extensions, für die keine Authentifikation (noauth) erforderlich sind, existieren nicht an der WAN-Schnittstelle.	Anforderung		3	10	10	Ja
DHCP								
4.7.1	Konfigurationsoption: DNS-Server	1. Die per DHCP übermittelten IPv4-DNS-Server können manuell bestimmt werden.	Empfehlung		1	4	4	Ja
		2. Die per DHCP übermittelten IPv6-DNS-Server können manuell bestimmt werden.	Empfehlung		1	4	4	Ja
4.7.2	Übermittelter DNS-Server (Option 6)	Das DHCP-Optionsfeld 6 enthält entweder die IPv4-Adresse des eingebauten DNS-Proxies oder die IPv4-Adresse eines vom ISP mitgeteilten DNS-Servers.	Empfehlung		2	4	4	Ja
4.7.3	Domain Name (Option 15)	Sofern der Router in DHCP-Optionsfeld 15 eine (eigene) Domain übermittelt, muss der Router verhindern, dass DNS-Abfragen an diese Domain an externe DNS-Server über die WAN-Schnittstelle weitergeleitet werden. Die Erwartungen sind ebenfalls mit “JA” festzulegen, falls der Router in DHCP-Optionsfeld 15 keine (eigene) Domain übermittelt.	Empfehlung		4	4	4	Ja
4.7.4	IPv4-Adressbereich im LAN	Der IPv4-Adressbereich (Range), der vom DHCP-Server verwaltet wird, kann geändert werden.	Option		1	2	2	Ja
Weitere Sicherheitsfunktionen								
4.8.1	LAN-Gast-Netzwerk	1. Der integrierte Switch verfügt über einen Port (LAN-Interface), der einen Zugang zu einem Gast-Netzwerk ermöglicht.	Option		1	2	0	Nein
		2. Der LAN-Gast-Interface ist deaktiviert oder es ist kein LAN-Gast-Interface implementiert.	Empfehlung		1	4	4	Ja
		3. Der Zugriff auf die Weboberfläche aus dem LAN-Gast-Netzwerk ist nicht möglich oder es ist kein LAN-Gast-Interface implementiert.	Anforderung		1	8	8	Ja
		4. ICMP-Nachrichten des Typs "Echo-Request" sowie "Echo Reply" werden nicht zwischen den beiden Netzwerken weitergeleitet oder es ist kein LAN-Gast-Interface implementiert.	Anforderung		1			Ja
4.8.2	WLAN-Gast-Netzwerk	1. Ein persönliches WLAN-Gast-Netzwerk ist vorhanden.	Option		1	3	0	Nein
		2. Ein persönliches WLAN-Gast-Netzwerk ist deaktiviert oder nicht implementiert.	Empfehlung		1	7	7	Ja
		3. Der Zugriff auf die Weboberfläche aus dem WLAN-Gast-Netzwerk ist nicht möglich oder es ist kein WLAN-Gast-Netzwerk ist nicht implementiert.	Anforderung		1	8	8	Ja
		4. WPA2- wird zur Verschlüsselung des WLAN-Gast-Netzwerks verwendet und die SSID bzw. ESSID enthält keine Angabe zur Produktbezeichnung. Eine andere Möglichkeit ist, dass ein WLAN-Gast-Netzwerk nicht implementiert ist.	Anforderung		1			Ja
		5. ICMP-Nachrichten des Typs "Echo-Request" sowie "Echo Reply" werden nicht zwischen den beiden Netzwerken weitergeleite. Eine andere Möglichkeit ist, dass ein WLAN-Gast-Netzwerk nicht implementiert ist.	Anforderung		1			Ja
DNS								
5.1.1	DNS-Reflection-Angriffe	DNS-Abfragen werden nicht über die WAN-Schnittstelle beantwortet.	Anforderung		3	10	10	Ja
CSRF								
5.2.1	Schutzmechanismus gegen CSRF-Angriffe	1. CSRF-Angriffe (img-, iframe-, forms-tags) mittels Authentifikation sind erfolglos.	Anforderung		2	10	10	Ja
		2. CSRF-Angriffe (img-, iframe-, forms-tags) bei einer aktiven Session sind erfolglos.	Anforderung		2	8	8	Ja
5.2.2	Ausspähung von Daten	1. Bei der Übermittlung von funktionalen Änderungen sollte der HTTP-Request die POST-Methode verwenden.	Empfehlung		1	7	7	Ja
		2. Ein HTTP-Request sollte das Passwort für die Weboberfläche nicht im Klartext enthalten.	Empfehlung		1	6	0	Nein
Session Management								
5.3.1	Session-Timeout	Eine Session ID verliert standardmäßig nach einer inaktiven Zeit von 10 Minuten ihre Gültigkeit, sodass eine erneute Authentisierung an der Weboberfläche erforderlich ist.	Empfehlung		1	7	0	Nein
5.3.2	Logout-Button	1. Ein Logout-Button wird bereitgestellt.	Empfehlung		1	5	5	Ja
		2. Falls ein Logout-Button zur Verfügung steht und dieser vom Benutzer nicht verwendet wird, sollte der Benutzer nach der nächsten Anmeldung darauf hingewiesen werden, dass die letzte Session nicht ordnungsgemäß mithilfe des Logout-Buttons beendet wurde	Option		1	3	0	Nein
5.3.3	Browserfenster	1. Die Weboberfläche öffnet sich in einem separaten Browserfenster.	Empfehlung		1	7	0	Nein
		2. Durch die Betätigung des Logout-Buttons wird das Browserfenster bzw. der Browsertab geschlossen.	Empfehlung		1	4	0	Nein

UPnP								
5.4.1	UPnP	Die Übertragung von Statusinformationen über UPnP und die Steuerung des Routers über UPnP können unabhängig voneinander aktiviert werden.	Empfehlung		1	7	0	Nein
5.4.2	WAN-Schnittstelle	UPnP-Abfragen werden an der WAN-Schnittstelle nicht beantwortet. Außerdem verwendet die UPnP-Implementierung keine Module bzw. Libraries, die bekannte Schwachstellen aufweisen. Identified = 0 Exploitable = 0	Anforderung		3	10	10	Ja
5.4.3	LAN-Schnittstelle	Die UPnP-Implementierung verwendet keine Module bzw. Libraries, die bekannte Schwachstellen aufweisen. Identified = 0 oder 1 Exploitable = 0	Anforderung		1	10	10	Ja
Heartbleed								
5.5.1	Zugriff auf die Weboberfläche	1. Der Zugriff auf die Weboberfläche ist über die WAN-Schnittstelle nicht anfällig für Heartbleed. Identified = 0 oder 1 Exploitable = 0	Anforderung		3	10	10	Ja
		2. Der Zugriff auf die Weboberfläche ist über die LAN-Schnittstelle nicht anfällig für Heartbleed. Identified = 0 oder 1 Exploitable = 0	Anforderung		1	10	10	Ja
Pixie Dust	**Angriff**							
5.6.1	WPS-PIN-Funktion	WPS-PIN-Funktion ist nicht für Pixie Dust Angriffe anfällig.	Anforderung		1	10	10	Ja
Support								
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	4	Ja
		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	0	Nein
		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	1	Ja
		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	4	Ja
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 (gespeichert) werden.	1	7	0	Nein
		2. Eine Kurzanleitung für den Router ist in der Verpackung enthalten.	Option	Der Verpackungsinhalt wird nach einer Kurzanleitung durchsucht.	1	1	0	Nein
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	0	Nein
		2. Ein Einrichtungsassistent für Internet und VoIP wird bereitstellt.	Option	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	2	0	Nein
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	0	Nein
Usability								
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	7	Ja
		2. Die Werkseinstellungen lassen sich mithilfe der Weboberfläche wiederherstellen.	Empfehlung	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	7	7	Ja
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	0	Nein
		2. Das WLAN lässt sich zeitgesteuert deaktivieren.	Option	Die Existenz der Funktionalität wird mittels Weboberfläche und Benutzerhandbuches untersucht.	1	1	0	Nein
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.								

	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			Nein	
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			Ja	
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			Nein	
7.4	Die WAN-Schnittstelle antwortet auf DNS-Abfragen (Open Resolver).			5.1.1			Nein	
7.5	Die WAN-Schnittstelle antwortet auf UPnP-Abfragen.			5.4.2			Nein	
7.6	Der Router verfügt über eine Schwachstelle, wie beispielsweise Heartbleed.			5.5.1 und 5.6.1			Nein	
7.7	Die Weboberfläche ist im Auslieferungszustand über die WAN-Schnittstelle erreichbar.			3.4.4			Nein	
7.8	Die Weboberfläche unterstützt kein HTTPS an der WAN-Schnittstelle und der Zugriff ist standardmäßig aktiviert.			3.4.4			Nein	
7.9	Die VoIP-Implementierung bietet an der WAN-Schnittstelle eine Extension an, für die keine Authentifikation (noauth) erforderlich ist.			4.6.2			Nein	