Independent Tests of
Anti-Virus Software

Router Test 2020

Im Auftrag von PC Magazin

TESTZEITRAUM: MÄRZ – APRIL 2020
SPRACHE: DEUTSCH
LETZTE REVISION: 08. APRIL 2020

WWW.AV-COMPARATIVES.ORG

Inhalt

Einleitung

Im Auftrag von PC Magazin sollen fünf ausgewählte Router auf verschiedene Sicherheitsaspekte und ihre verfügbaren Sicherheitsfunktionen (z.B. Schutz vor Phishing-Webseiten) getestet werden. Es sind andere nützliche Funktionen, die zusätzlich vom Router angeboten werden (z.B. Protokollierung von Ereignissen und Datei-/Medienfreigabe), ebenfalls zu überprüfen. Sowohl die Testgeräte, Testmethode als auch die Testkriterien, anhand welcher die Router bewertet werden sollen, sind vom Auftraggeber vorgegeben. Darüber hinaus haben wir nach unserem Ermessen die Testkriterien durch weitere sicherheitsrelevante Eigenschaften ergänzt. In den folgenden Abschnitten werden der Testaufbau und die angewendete Testmethode näher beschrieben sowie die getesteten Produkte aufgelistet.

Testumgebung

Der zu testende Router wird an Stelle des vom Provider zur Verfügung gestellten Routers im Labornetzwerk nach Abbildung 1 platziert. Die Test-Rechner 1 und 2 sind direkt mit dem Test-Router über Ethernet oder WLAN verbunden und erhalten eine private IP-Adresse. Dies ermöglicht den Zugriff auf den Router und die weitere Administration aus dem LAN. Außerdem können die Gast-Netzwerk-Funktion getestet sowie Port-Scans auf der LAN-Seite durchgeführt werden.

Der Test-Router erhält vom ISP eine öffentliche IP-Adresse, über die er mit den Test-Rechnern 3 und 4 über das Internet kommuniziert. Auf Test-Rechner 3 läuft das Greenbone OS mit dem *OpenVAS Vulnerability Scanner*[1]. Test-Rechner 4 stellt einerseits Malware-Dateien über HTTP zur Verfügung und führt andererseits Port-Scans auf der WAN-Seite durch.

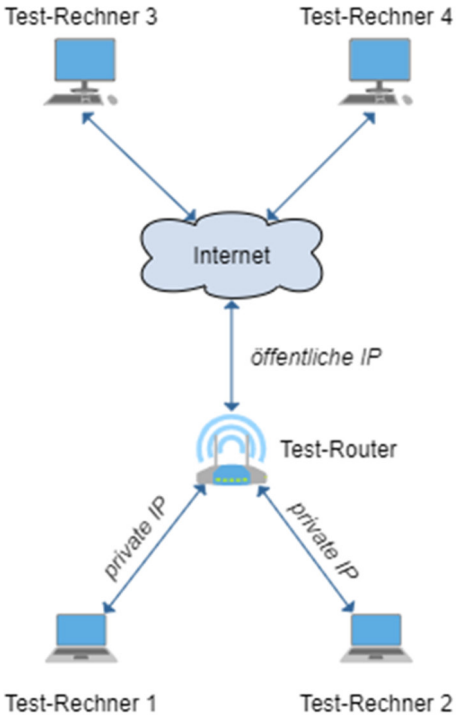

Abbildung 1 Testaufbau

Testmethode

Zur besseren Übersicht wurden die vom Auftraggeber bereits definierten und von uns ergänzten Testkriterien in einer Liste zusammengetragen und anschließend in drei Testkategorien eingeteilt. Diese und die weitere Vorgehensweise beim Testen werden im nächsten Abschnitt näher erläutert. Wir führten Tests in folgenden Kategorien durch:

- *Sicherheitsmerkmale* beinhalten Features, die für die Sicherheit des Routers, der verschiedenen Netzwerke (LAN, WAN, Gast) und der Kommunikation innerhalb und zwischen den einzelnen Netzwerken eine wichtige Rolle spielen. Dazu gehören unter anderem Passwörter, Firmware, Administration, Zugriffsrechte, Wi-Fi, Firewall und Port-Weiterleitungen.

[1] https://www.openvas.org

- *Qualitätsmerkmale* haben nur indirekt mit Sicherheit zu tun. Sie erweitern bestehende Router-Funktionen um nützliche Netzwerkdienste sowie Quality-of-Life Services. Hierzu zählen beispielsweise das Erfassen von Ereignissen („Logging"), Senden von Benachrichtigungen oder die Datei- und Medienfreigabe über ein an den Router angeschlossenes Speichermedium.

- *Schutzfunktionen* stellen zusätzliche Komponenten dar, die Nutzern vor schädlichen Webseiten oder Angriffen aus dem Internet sowie Bedrohungen im Heimnetzwerk (z.B. infizierte Netzwerkgeräte) schützen. Einige Router bieten optionale Schutz-Software von Drittanbietern an. Hierbei unterscheiden wir zwischen folgenden Schutzkomponenten:

    - Schutz vor Phishing-Webseiten (Phishing-Filter)
    - Schutz vor bösartigen Webseiten
    - Schutz vor bösartigen Dateien während des Downloads
    - Schutz vor nicht-jugendfreien Inhalten und Kontrolle des Internetzuganges für Kinder/Jugendliche (Kinderschutz und -sicherung)

Beim Testvorgang liegt der Fokus vorwiegend auf dem Aspekt der Sicherheit. Daher werden die Sicherheitsmerkmale und Schutzfunktionen genauer unter die Lupe genommen und Qualitätsmerkmale nur am Rande erwähnt. Der Großteil der Informationen über vorhandene Features wurde aus dem Webinterface des Routers sowie der Produktdokumentation entnommen.

Um festzustellen, welche Ports auf der LAN- und WAN-Seite standardmäßig geöffnet sind, wurde der Port-Scanner *nmap*[2] auf Test-Rechner 1 und 4 (siehe Abbildung 1) installiert. Wir überprüften die Testprodukte auf weitere Sicherheitslücken und andere Schwachstellen mit Hilfe des *OpenVAS Vulnerability Scanners*, der auf Test-Rechner 3 eingerichtet wurde. Der zu testende Router durchläuft dabei eine Reihe von Netzwerk-Schwachstellen-Tests, welche über das *Greenbone Security Feed*[3] zur Verfügung gestellt und täglich auf die neuesten Schwachstellen aktualisiert werden. Zu guter Letzt testeten wir den Router auf bekannte Schwachstellen im WPS (Wi-Fi Protected Setup), indem wir unter Zuhilfenahme von Kali-Linux und Open-Source-Tools wie *Reaver*[4] mehrere Brute-Force-Attacken starteten.

Für den Test des Phishing-Filters wurden 25 aktuell verfügbare Phishing-Webseiten angesurft. Ebenso versuchten wir beim Testen des Schutzes vor bösartigen Webseiten, 50 Malware-URLs aufzurufen und die dahinter befindliche schädliche Software herunterzuladen. Beim Test des Schutzes vor bösartigen Dateien wurden 100 Malware-Dateien vom Datei-Server (Test-Rechner 4) über HTTP heruntergeladen. Beim Test von Kinderschutz und -sicherung besuchten wir 30 URLs, die auf nicht-jugendfreie sowie pornographische Inhalte verweisen. Alle diese web-basierten Tests wurden mit dem *Google Chrome*[5] Browser durchgeführt.

[2] https://nmap.org/
[3] https://www.greenbone.net/security-feed/
[4] https://github.com/t6x/reaver-wps-fork-t6x
[5] Safe-Browsing wurde vor dem Test deaktiviert

Produkte im Test

Folgende Router mit zum Testzeitpunkt aktuell verfügbarer Firmware-Version wurden geprüft:

Hersteller	Produkt	Firmware
AVM	Fritzbox 7590	07.12
Telekom	Speedport Smart 3	010137.3.0.005.3
TP-Link	AX6000	1.0.7 Build 20200212 rel.7095
Asus	RT-AX88U	3.0.0.4.384_8018
Netgear	Nighthawk RS400	1.5.0.34_10.0.33

Testergebnisse

In diesem Abschnitt werden die Ergebnisse für jede Testkategorie präsentiert. Zum besseren Überblick und Verständnis erfolgt dies sowohl in Form von Tabellen als auch textuellen Beschreibungen am Ende jeder Tabelle, wobei letztere nur die wichtigsten Ergebnisse diskutieren. Zu Beginn ist zu erwähnen, dass alle fünf Router in der jeweiligen getesteten Firmware-Version von keinen bekannten oder schwerwiegenden Schwachstellen (z.B. kr00k) betroffen sind. Sowohl die Tests mit dem OpenVAS Scanner als auch der Brute-Force-Angriff via WPS lieferten keine nennenswerten Ergebnisse.

Der Telekom Speedport Smart 3 konnte aufgrund lokaler und hersteller-spezifischer Einschränkungen nicht im Internet getestet werden. Dieser Router scheint ausdrücklich einen DSL-Anschluss und Vertrag mit Deutsche Telekom zu verlangen, da auch die Versuche, einen der LAN-Ports am Telekom-Router als WAN-Port zu verwenden, erfolglos blieben. Daher konnten die Tests der Sicherheitsmerkmale und Schutzfunktionen in diesem Fall nur eingeschränkt durchgeführt werden.

Symbole

Die für die Bewertung der Testkriterien verwendeten Symbole sind der untenstehenden Tabelle zu entnehmen, wobei ein Symbol mehrere Bedeutungen je nach Testkriterium haben kann.

Symbol	Bedeutung
●	Funktion vorhanden und standardmäßig aktiviert (z.B. automatisch während/nach Setup); Wert veränderbar
◐	Funktion vorhanden, aber standardmäßig deaktiviert; Wert eingeschränkt veränderbar
O	Funktion nicht vorhanden; Wert nicht veränderbar
k.A.	Keine Angaben; Test konnte nicht durchführt werden

Sicherheitsmerkmale

	AVM Fritzbox 7590	Telekom Speedport Smart 3	TP-Link AX6000	ASUS RT-AX88U	Netgear RS400
Passwort					
Standardpasswort vor Setup gesetzt	●	●	0	●	0
Aufforderung (Standard-)Passwort für Wi-Fi zu ändern	0	0	●	●	●
Aufforderung (Standard-)Passwort für Router-Login zu ändern	0	0	●	●	●
Prüfung von Passwortstärke	●	0	0	0	0
Einschränkungen bei Passwort (z.B. Länge, Zeichensatz)	●	●	●	●	●
Firmware					
1-Klick oder manuelles Update	1-Klick, manuelles Update	1-Klick, manuelles Update	1-Klick, manuelles Update	1-Klick, manuelles Update	1-Klick, manuelles Update
Sicherer & valider Download bei manuellem Update	●	●	●	●	●
Update während Setup	0	0	0	●	●
Automatische Updates	●	◐[6]	0	0	●
Benachrichtigungen und/oder Aufforderung zum Update	●	●	●	●	●
Backup von Router-Einstellungen vor Update	●	0	0	0	0
Router-Einstellungen nach Datei exportieren	●[7]	●	●	●	●
Administration					
Hinzufügen von weiteren Nutzern und/oder Nutzergruppen	●	0	0	0	0
Lokaler Zugriff					
Zugriff über Hostname und/oder IP-Adresse	Hostname, IP-Adresse	Hostname, IP-Adresse	Hostname, IP-Adresse	Hostname, IP-Adresse	Hostname, IP-Adresse
HTTPS unterstützt	◐	0	◐	◐	●
UserID/Benutzername ändern	●	0	0	●	0
Passwort ändern	●	●	●	●	●
TCP/IP Port ändern	0	0	0	◐[8]	0

[6] nur bei Anschlüssen von Deutsche Telekom
[7] zusätzlich mit Passwort geschützt
[8] nur HTTPS-Port

Einschränkungen für lokalen Zugriff					
IP-Adresse(n)	0	0	0	0	0
MAC-Adresse(n)	0	0	●	0	0
nur HTTPS	0	0	0	0	0
nur Ethernet	0	0	0	0	0
SSID und/oder VLAN	0	0	0	0	0
kein Zugriff für Nutzer im Gast-Netzwerk	●	●	●	●	●
Remote-Zugriff					
Verfügbar	●	0	●	●	●[9]
Standardmäßig deaktiviert	●	0	●	●	●
Zugriff über Hostname und/oder IP-Adresse	IP-Adresse	0	IP-Adresse	IP-Adresse	Hostname
UserID/Benutzername ändern	●	0	0	●	0
Passwort ändern	●	0	●	●	●
TCP/IP Port ändern	●	0	●	●	0
Einschränkungen für Remote-Zugriff					
IP-Adresse(n)	0	0	●	●	0
nur HTTPS	●	0	0	●	●
Webinterface					
Registrierte oder verbundene Geräte anzeigen	●	●	●	●	●
Session Timeout (Auto-Logout)	●	●	●	●	●
Zeitlimit für Session setzen	0	0	0	●	0
nur eine Session pro UserID	0	0	●	●	●
Login mit CAPTCHA	0	0	0	0	0
Logout von Webinterface möglich	●	●	●	●	●
Lockout nach zu vielen falschen Anmeldeversuchen	●	●	●	●	0[10]

[9] nur über VPN und Hostname (DDNS)
[10] nur Passwort wiederherstellen, aber kein Lockout

Smartphone App					
Verfügbar	●	0	●	●	●
Benutzerkonto beim Hardware-Hersteller notwendig	0	0	0	0	●
Kommunikation über Bluetooth und/oder Wi-Fi	Wi-Fi	0	Bluetooth, Wi-Fi	Wi-Fi	Wi-Fi
Berechtigungen am Smartphone	0	0	Standort	Standort	Standort, Kamera
Logout von App	●	0	●	0	●
Wi-Fi					
Wi-Fi-Netzwerk standardmäßig aktiviert	2,4 GHz, 5 GHz	2,4 GHz, 5 GHz	2,4 GHz, 5 GHz	2,4 GHz, 5 GHz	2,4 GHz, 5 GHz
Name (SSID) ändern	●	●	●	●	●
Passwort ändern	●	●	●	●	●
Per Webinterface ausschalten	●	●	●	●	●
Per On/Off-Taste ausschalten	●	●	●	●	●
Zeitraum für Ausschalten festlegen	●	●	●	0	●
Zugriff einschränken	●	●	●	●	●
Unterstützte Verschlüsselungen	WPA2+CCMP, WPA/WPA2	WPA, WPA2, WPA/WPA2	WEP, WPA/WP2, WPA/WP2-Enterprise	WPA2, WPA3, WPA/WPA2, WPA2/WPA3, WPA2-Enterprise, WPA3-Enterprise, WPA/WPA2-Enterprise	WPA2-PSK, WPA-PSK/WP2-PSK, WPA/WPA2-Enterprise
WPS					
Verfügbar	●	●	●	●	●
Standardmäßig eingeschaltet	●	●	●	●	●
Kann deaktiviert werden	●	●	●	●	●
Anfällig für Brute-Force Attacken (z.B. Reaver, Pixie Dust)	0	k.A.	0	0	0
Gast-Modus/-Netzwerk					
Verfügbar	●	●	●	●	●
Name (SSID) ändern	●	●	●	●	●
Passwort ändern	●	●	●	●	●
Aufforderung (Standard-)Passwort zu ändern	0	0	0	0	0
Gast-Passwort muss anders als LAN-Passwort sein	0	0	0	0	0

Traffic verschlüsselt	●	●	◐[11]	●	◐[11]
Zugriff auf Geräte im privaten LAN (Wi-Fi)	○	◐	◐	◐	◐
Zugriff auf Geräte im selben Gast-Netzwerk	◐	◐	◐	◐	◐
Zugriff auf Geräte im anderen Gast-Netzwerk	○	○	◐	○	◐
Zeitraum/Limit für Gast-Netzwerk	●	●	○	●	○
Zeitlimits pro User	○	○	○	○	○
Maximale Anzahl an Nutzern	unbegrenzt	unbegrenzt	unbegrenzt	unbegrenzt	unbegrenzt
Limit für Bandbreite	○	○	○	●	○
Eigenes, vom privaten LAN unabhängiges Subnetz	●	○	○	○	○
Anmeldung über Dialog im OS	●	●	●	●	●
Anmeldung über gesicherte Login-Seite im Browser	◐[12]	○	○	○	○
UPnP					
Verfügbar	●	○	●	●	●
Standardmäßig auf LAN-Seite aktiviert	●	○	●	●	●
Standardmäßig auf WAN-Seite deaktiviert	●	○	●	●	●
Kann deaktiviert werden	●	○	●	●	●
Firewall					
Ports auf LAN-Seite geöffnet/verfügbar	21, 53, 80, 443, 5060, 8181	53, 80, 443, 5060, 8443	22, 53, 80, 443, 1900	53, 515, 8443, 9100, 49152	53, 80, 443, 631, 4444, 4567, 5000, 20005, 49152
Ports auf WAN-Seite geöffnet/verfügbar	○	k.A.	○	○	○
Regeln für ein-/ausgehende Anfragen	●	●	●	●	●
Port-Weiterleitung					
Verfügbar	●	●	●	●	●
Auf Quell-IP-Adresse und/oder -Subnetzwerk einschränken	●	●	●	●	○
Zeitraum/Limit festlegen	○	○	○	○	○

[11] standardmäßig unverschlüsselt, aber Verschlüsselung vorhanden
[12] Anmeldung über HTTP

VPN					
Verfügbar	●	0	●	●	●
Unterstützte Protokolle	IPSec, IPSec Xauth PSK	0	OpenVPN, PPTP	IPSec, OpenVPN, PPTP	OpenVPN
Weitere Merkmale					
IPv6 unterstützt	●	◐[13]	●	●	●
Dynamic DNS (DDNS) verfügbar	●	●	●	●	●
HNAP verfügbar	0	0	0	0	0
VLAN verfügbar	0	0	0	0	●
Benutzerkonto beim Hardware-Hersteller notwendig	0	0	0	0	●
Auf Werkseinstellungen zurücksetzen	●	●	●	●	●

[13] eingeschränkt auf LAN

Detailergebnisse

Alle Router verlangen die Eingabe eines Router-Passworts mit einer vorgegebenen Mindestlänge. Allerdings prüft die Fritzbox als einziges Testgerät die Stärke des eingegebenen Passworts korrekt und erlaubt nur Passwörter, die mindestens als „mittel" gekennzeichnet werden. Alle anderen weisen lediglich den Benutzer über einen Dialog darauf hin, dass das eingegebene Passwort zu kurz/unsicher sei und ein anderes eingegeben werden sollte.

So kann es wie bei Telekom, Asus und Netgear vorkommen, dass klassische und einfache Passwörter wie „000000" oder „passwort" möglich sind oder wie im Falle von TP-Link sogar Passwörter mit nur einem Zeichen akzeptiert werden, was ein erhöhtes Sicherheitsrisiko darstellt.

Im Falle eines manuellen Firmware-Updates erzwingen alle Router einen sicheren Download ihrer neuesten Firmware über HTTPS von der Hersteller-Seite. Der Telekom-Router unterstützt automatische Updates nur bei bereits vorhandenen Anschlüssen von Deutsche Telekom.

Telekom unterstützt keinen HTTPS-Zugriff aus dem LAN, obwohl die zugehörigen Ports 443 und 8443 geöffnet sind. Hingegen hat Netgear als einziger Router diese Funktion standardmäßig aktiviert. Alle anderen bieten die Funktion zumindest im Webinterface an, haben sie jedoch standardmäßig deaktiviert. Mit Ausnahme des Telekom-Routers erlauben alle den Zugriff auf den Router aus dem WAN. Bei TP-Link ist hierbei kein HTTPS zwingend erforderlich. Netgear ermöglicht einen Remote-Zugriff nur über eine gesicherte VPN-Verbindung und den Hostnamen, welcher zuvor über DDNS eingerichtet werden muss. Zusätzlich haben wir uns angeschaut, ob die Router für die Anmeldung im Webinterface CAPTCHA[14] verwenden. Wir konnten diese Funktion bei keinem der getesteten Router feststellen, wodurch das Anmeldeformular theoretisch von einem Computer („Bot") automatisch ausgefüllt werden kann.

Weiters verhindern vier der fünf Router Brute-Force-Angriffe auf das Router-Passwort mit einem Lockout, welches den Zugang zum Router ab einer bestimmten Anzahl von falschen Anmeldeversuchen für mehrere Minuten bis Stunden sperrt. Netgear bietet als einziger Router kein richtiges Lockout an. Nach drei fehlgeschlagenen Anmeldeversuchen wird der Nutzer auf eine lokale Seite weitergeleitet, wo das Router-Passwort über die Seriennummer des Routers und über die vom Nutzer vordefinierten Sicherheitsfragen wiedergestellt werden kann. Über einen Klick auf „Zurück" im Browser stehen dem Nutzer ganz einfach drei neue Versuche zur Verfügung, um die Anmeldedaten des Routers zu erraten.

Alle Router verwenden standardmäßig die WPA2-Verschlüsselung für ihr Wi-Fi-Netzwerk und bieten auch weitere Kombinationen mit unter anderem WPA und wie im Falle von Asus WPA3 an. Bei TP-Link kann sogar noch die unsichere WEP-Verschlüsselung ausgewählt werden. Über den Test-Rechner 4 (siehe Abbildung 1) starteten wir eine Brute-Force-Attacke auf das WPS, welches bei allen Routern standardmäßig aktiviert ist. Alle Router bis auf Telekom konnten erfolgreich getestet werden und sind gegen derartige Angriffe geschützt.

[14] https://de.wikipedia.org/wiki/Captcha

Fritzbox, Telekom und Asus setzen standardmäßig die WPA2-Verschlüsselung für ihr Gast-Netzwerk ein. TP-Link und Netgear erlauben nach dem Aktivieren der Funktion zunächst ein offenes Gast-Netzwerk ohne Passwort zu nutzen. Jedoch kann der Nutzer eine der unterstützten Verschlüsselungsvarianten ähnlich zum privaten Wi-Fi-Netzwerk auswählen. Kein Router weist den Nutzer auf die Änderung des Standardpassworts für das Gast-Netzwerk hin, sofern eines ab Werk vergeben wurde. Darüber hinaus kann dasselbe Passwort für das private Wi-Fi und Gast-Netzwerk gesetzt werden, was ein weiteres Sicherheitsmanko darstellt. Einerseits können sich Gäste über ein einziges Passwort mit dem privaten LAN verbinden und andererseits erlaubt es Angreifern, sich Zugang zu beiden Wi-Fis zu verschaffen, indem sie Listen von bekannten Standardpasswörtern abarbeiten („Rainbow Tables“). Die Fritzbox erlaubt die Anmeldung im Gast-Netzwerk auch über eine vordefinierte Login-Seite im Browser, die allerdings die Anmeldedaten im Klartext über HTTP an den Router überträgt.

Auf der WAN-Seite sind keine kritischen Ports ab Werk geöffnet. Auf der LAN-Seite hingegen müssen Ports, wie z.B. 53 (DNS), 80 (HTTP) und optional HTTPS (443, 8443), standardmäßig geöffnet sein, damit der Router korrekt funktioniert und Nutzer Zugriff auf das Internet haben. Bis auf den Telekom-Router unterstützen alle UPnP und haben die Funktion standardmäßig aktiviert sowie Ports hierfür im LAN freigegeben.

Der Telekom-Router bietet nur eine Nutzung von IPv6 im LAN an. Alle übrigen Geräte können auch im Internet mit IPv6-Adressen kommunizieren. Das unsichere HNAP (Home Network Administration Protocol), das in der Vergangenheit mehrere Sicherheitslücken aufgrund von fehlerhaften Implementierungen aufwies[15], wird von allen Routern nicht unterstützt. Über den Netgear-Router kann ein VLAN im Heimnetzwerk eingerichtet werden. Für die Verwendung des Netgear-Routers, speziell für Netgear Armor, ist ein kostenloses Netgear-Konto zwingend notwendig.

[15] https://routersecurity.org/hnap.php

Qualitätsmerkmale

	AVM Fritzbox 7590	Telekom Speedport Smart 3	TP-Link AX6000	ASUS RT-AX88U	Netgear RS400
Protokollierung					
Verfügbar	●	●	●	●	●
Automatisch gelöscht bei	Ausschalten, Neustart	Ausschalten, Neustart	Ausschalten, Neustart	Werkeinstellungen zurücksetzen	Ausschalten, Neustart
Arten von Log-Dateien					
System, Fehler, Warnungen	●	●	●	●	●
Registrierung eines neuen Geräts	●	●	0	●	●
Normaler Internet-Datenverkehr	0	k.A.	0	0	0
Von Firewall geblockter Traffic (z.B. gesperrte Seiten)	●	k.A.	0	◐	●
Korrekte/Falsche Anmeldeversuche	●	●	0	●	●
Änderungen an Router-Konfiguration	●	●	●	●	0
E-Mail & Benachrichtigungen					
Verfügbar	●	●	●	●	●
Bei Fehlern, Warnungen, Statusänderungen	●	●	0	0	0
Bei Änderungen an Router-Konfiguration	●	0	0	0	0
Bei Firmware-Updates/-Installation	●	●	0	0	◐[16]
Bei An-/Abmeldungen im WLAN (z.B. Gast-WLAN)	●	0	0	0	0
Wenn Bedrohungen oder gesperrte Webinhalte erkannt/blockiert	0	0	0	●	●
Regelmäßige Systemprotokolle oder Statusberichte	●	●	●	0	●
Anzahl von Empfängern	1	1	1	1	2
Dateifreigabe					
Verfügbar	●	●	●	●	●
Integrierter Speicher (NAS)	●	0	0	0	0
Externer Speicher (USB)	●	●	●	●	●
Standardmäßig aktiviert	●	●	●	●	●
Kann deaktiviert werden	●	0	●	●	●
Zugriff von WAN-Seite, aber standardmäßig deaktiviert	●	0	●	●	●
Media-Server					
Verfügbar	●	●	●	●	0
Standardmäßig aktiviert	●	0	●	●	0
Kann deaktiviert werden	●	●	●	●	0
Weitere Merkmale					
Smart-Home oder Mesh-WLAN verfügbar	●	●	◐[17]	●	●
Sonstige	Tastensperre, 2FA	Schlafmodus, WLAN TO GO	TP-Link-Cloud	Setup Wizard, SSH, Telnet, AiCloud	Setup Wizard, Smartphone Setup, App Benachrichtigungen, ReadyCloud

[16] optional bei Registrierung eines Netgear-Kontos
[17] Smart Home nur in „Englisch“ verfügbar

Detailergebnisse

Alle Router erfassen verschiedene Ereignisse, wie z.B. Systemfehler, Anmeldung im WLAN und am Router oder blockierte Anfragen, unterschiedlich detailliert in ihren Systemprotokollen („Logs“). Jedoch werden keine herkömmlichen Anfragen, welche das Surfverhalten von Nutzern im Internet widerspiegeln und für Tracking missbraucht werden könnten, in den Logs protokolliert. Bei Asus bleiben die Logs auch nach dem Ausschalten oder Neustart des Routers erhalten.

Bei TP-Link ist die Funktion „Smart Home“ im Webinterface nur sichtbar, wenn die Sprache auf „Englisch“ eingestellt ist. In allen anderen Sprachen ist diese ausgeblendet.

Schutzfunktionen

	AVM Fritzbox 7590	Telekom Speedport Smart 3	TP-Link AX6000	ASUS RT-AX88U	Netgear RS400
Schutz vor Phishing-Webseiten					
Verfügbar	O	k.A.	◐	◐	●
Schutz (25 URLs)	O	k.A.	84%	84%	96%
Schutz vor bösartigen Webseiten					
Verfügbar	O	k.A.	◐	◐	●
Schutz (50 URLs)	O	k.A.	100%	100%	100%
Schutz vor bösartigen Dateien					
Verfügbar	O	k.A.	O	O	O
Schutz (100 Malware-Dateien)	0%	k.A.	0%	0%	0%
Kinderschutz und -sicherung					
Verfügbar	◐	◐	◐	◐	◐
Schutz (30 URLs)	70%	k.A.	67%	97%	100%
Einschränkungen für Zeitraum, Nutzungsdauer, Webseiten	●	●	●	●	●[18]

Detailergebnisse

Zu den Ergebnissen ist ausdrücklich zu sagen, dass all diese Tests nur eine Momentaufnahme darstellen. Auch wenn im Test 100% der verwendeten Stichproben geblockt wurden, bedeutet dies nicht, dass sich der Nutzer auf einen 100%-igen Schutz von Seiten des Produktes verlassen kann.

Die Schutzfunktionen *Antivirus* bei TP-Link und *AiProtection* bei Asus werden von Trend Micro zur Verfügung gestellt, *Armor* bei Netgear stammt von Bitdefender. Bei diesen Schutzlösungen konnten sämtliche Malware-Dateien von unserem Datei-Server heruntergeladen werden. Wir vermuten, dass Router-Hersteller freiwillig auf diese Zusatzfunktion verzichten, da ansonsten jeder einzelne Download vom Router geprüft werden muss. Dieser Prüfvorgang könnte je nach Größe von Malware- bzw. Clean-Dateien und Schutztechnologie durch die schwache Rechenleistung der Router mehrere Minuten dauern und folglich eine längere Download-Zeit sowie eine negative Nutzererfahrung mit sich bringen. Solche Funktionen sind normalerweise nur in professionellen Security-Lösungen zu finden. Anhand dieser Ergebnisse ist anzunehmen, dass die integrierten Schutzfunktionen bösartige Webseiten lediglich anhand ihrer URL blockieren.

Da mit dem Telekom-Router keine Internetverbindung während der Tests hergestellt werden konnte, war es uns nicht möglich, die Schutzfunktionen im vollen Umfang zu überprüfen. Laut Webinterface ist eine Kindersicherungsfunktion verfügbar, die allerdings nur das Setzen von Zeitpunkten und Port-Sperren erlaubt, aber sonst keine Einstellungen für einen Schutz vor nicht-jugendfreien Inhalten bietet.

[18] Über eigene Smartphone-App

Fazit

Bei allen Testprodukten sind keine bekannten Sicherheitslücken oder Schwachstellen in ihrer getesteten Firmware-Version festgestellt worden und keine kritischen Ports auf der WAN-Seite standardmäßig geöffnet. Ebenso ist der Zugriff auf freigegebene Speichermedien aus dem Internet bei jenen Produkten, die diese Funktion unterstützen, ab Werk deaktiviert.

Vier von fünf Produkten lassen den Zugriff auf die web-basierte Administration-Oberfläche des Routers über HTTP aus dem internen Netzwerk zu, wobei HTTPS aktiviert werden kann. Der Netgear hat HTTPS aus dem LAN standardmäßig aktiviert. Allerdings verfügt Netgear als einziger Test-Router über kein richtiges Lockout, wenn versucht wird, die Anmeldeinformationen für den Router durch einfaches Brute-Forcing zu erraten.

Erfreulicherweise ist bis auf den TP-Link-Router bei allen die Weboberfläche aus dem Internet nur per HTTPS erreichbar. Der Telekom Speedport bietet keinen Zugriff aus dem Internet an.

Alle Produkte zwingen den Nutzer, ein Router-Passwort mit einer vorgegebenen Mindestlänge zu vergeben, jedoch prüft nur die Fritzbox die Stärke des eingegebenen Passworts korrekt. Drei Produkte erlauben es, schwache und leicht zu erratende Passwörter (z.B. „000000“ oder „passwort“) zu definieren. Bei TP-Link werden sogar Passwörter mit nur einem Zeichen akzeptiert. Die unsichere WEP-Verschlüsselung, die für das WLAN von TP-Link weiterhin ausgewählt werden kann, stellt ein mögliches Sicherheitsrisiko dar. Hinzukommt, dass bei allen getesteten Routern die Passwörter für das private WLAN und Gast-WLAN nicht zwingend unterschiedlich sein müssen.

Trotz Erkennungsraten von 100% in den Schutzfunktionstests von TP-Link, Asus und Netgear kann im Allgemeinen nicht von einem 100%-igen Schutz vor sämtlichen Bedrohungen aus dem Heimnetzwerk und Internet ausgegangen werden. Die durchgeführten Tests und Ergebnisse stellen lediglich eine Momentaufnahme auf einer Stichprobe dar und können zu einem späteren Testzeitpunkt ganz anders ausfallen. Um sich als Nutzer besser vor Angriffen aus dem Internet zu schützen, raten wir zur Installation eines zusätzlichen Antiviren-Programmes eines anerkannten Herstellers am Endgerät des Nutzers.

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives
(April 2020)