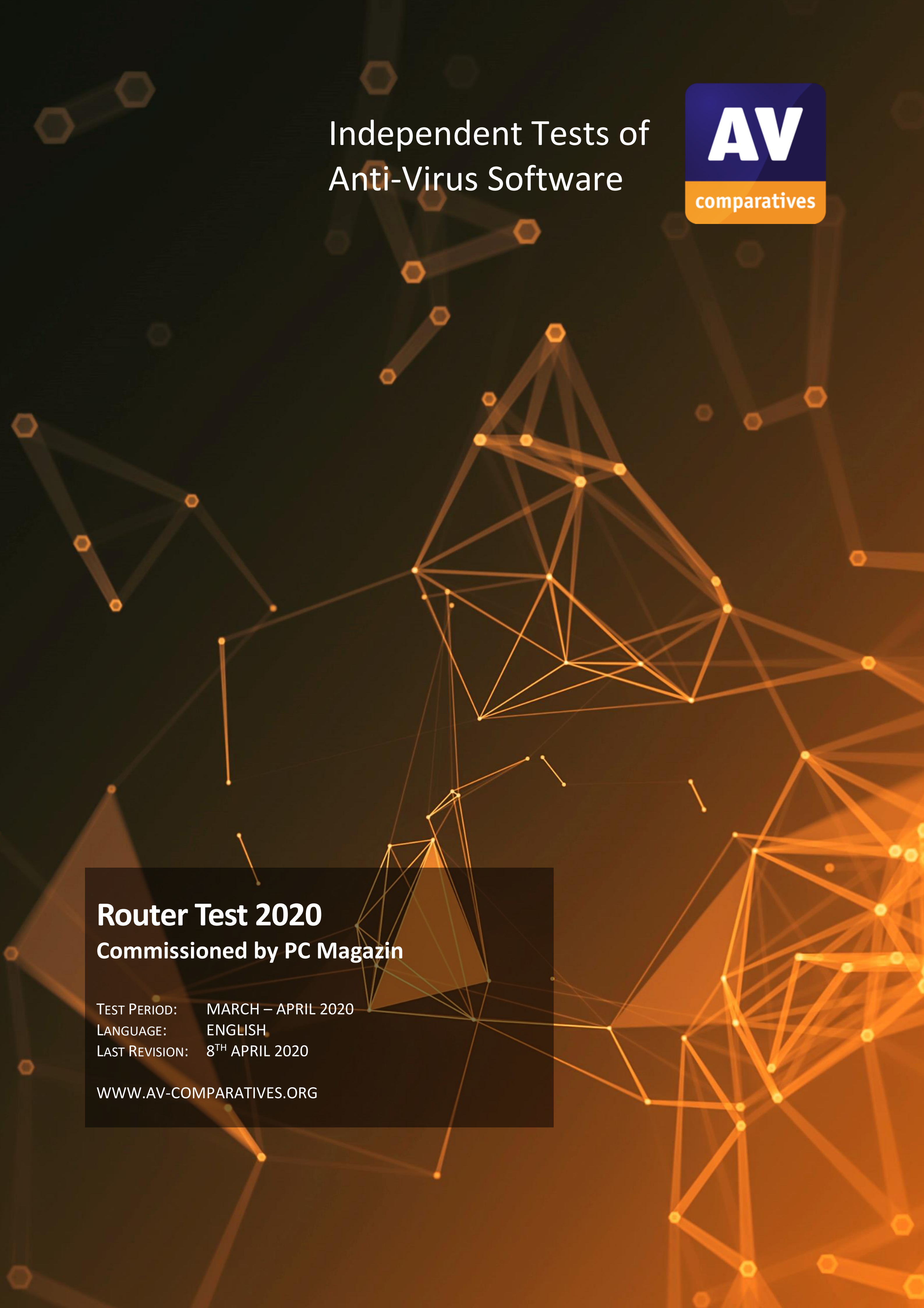

Independent Tests of
Anti-Virus Software

Router Test 2020

Commissioned by PC Magazin

Test Period:	MARCH – APRIL 2020
Language:	ENGLISH
Last Revision:	8TH APRIL 2020

WWW.AV-COMPARATIVES.ORG

Content

Introduction

On behalf of PC Magazin, five selected routers were tested for various security aspects and their available security functions (e.g. protection against phishing websites). Other useful functions that are additionally offered by the router (e.g. event logging and file / media release) were also checked. PC Magazin specified the test devices, the test methods and the test criteria on the basis of which the routers were to be evaluated. However, we decided to add some additional security-related items to the test criteria.

Test setup

The router to be tested is placed in the lab network as shown in Figure 1, whereby it replaces the router supplied by the Internet service provider. Test computers 1 and 2 are connected directly to the test router via Ethernet or WLAN, and receive an internal IP address. This enables access to the router and further administration via the LAN. In addition, the guest-network function can be tested and port scans can be carried out over the LAN.

The test router receives a public IP address from the ISP, via which it communicates with two further test computers, numbered 3 and 4, via the Internet. The Greenbone OS runs on Test Computer 3 with the OpenVAS Vulnerability Scanner[1]. Test computer 4 provides malware files via HTTP, and additionally carries out port scans via WAN.

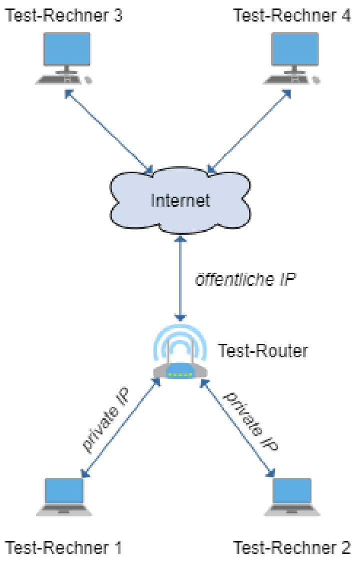

Figure 1 Test setup

Test procedure

For a better overview, the test criteria already defined by PC Magazin and supplemented by us were listed in three different test categories. This, along with the further procedure for testing, is explained in more detail in the next section. We conducted tests in the following categories:

- Security Features: these are features that play an important role in the security of the router, the various networks (main LAN, guest LAN, WAN,) and communication within and between the individual networks. These include passwords, firmware, administration, access rights, Wi-Fi, firewall and port forwarding.
- Quality Features: functions that are only indirectly related to security. They expand existing router functions with useful network services as well as “quality-of-life” (QoL) services. These includethe recording of events ("logging"), and sending notifications or file and media release via a storage medium connected to the router.

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

- Protection Functions: these are additional components that protect users from harmful websites or attacks from the Internet, as well as threats in the home network (e.g. infected network devices). Some routers offer optional third-party protection software. We differentiate between the following protective components:
  - Protection against phishing websites (phishing filter)
  - Protection against malicious websites
  - Protection against malicious files during the download
  - Protection against adult content and control of Internet access for children / adolescents (child protection and security)

The focus of the test process is primarily on the aspect of security. Therefore, the security features and protective functions are examined more closely, and quality features are only mentioned in passing. Most of the information about existing features was taken from the router's web interface and the product documentation.

To determine which ports are open by default on the respective LAN and WAN sides, the port scanner nmap[2] was installed on test computers 1 and 4 (see Figure 1). We checked the test products for further security flaws and other vulnerabilities with the help of the *OpenVAS Vulnerability Scanner*, which was set up on test computer 3. The router under test goes through a series of network vulnerability tests, which are made available via the *Greenbone Security Feed*[3], and updated daily to include the latest vulnerabilities. Finally, we tested the router for known vulnerabilities in WPS (Wi-Fi Protected Setup) by launching several brute-force attacks, with the help of Kali Linux and open source tools such as *Reaver*[4].

To test the phishing filter, 25 phishing websites were visited. Similarly, when testing protection against malicious websites, we tried to access 50 malware URLs, and download the malicious software behind them. When testing the protection against malicious files, 100 malware files were downloaded from the file server (test computer 4) via HTTP. When testing child protection, we visited 30 URLs that lead to adult and pornographic content. All of these web-based tests were performed using the *Google Chrome*[5] browser.

[2] https://nmap.org/
[3] https://www.greenbone.net/security-feed/
[4] https://github.com/t6x/reaver-wps-fork-t6x
[5] The *Safe Browsing* feature was deactivated before testing

Tested products

The following routers with the firmware version available at the time of testing were tested:

Vendor	Product	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

Test results

This section presents the results for each test category. For a better overview and understanding, this is done in the form of both tables and textual descriptions at the end of each table, the latter only discussing the most important results. To start with, it should be mentioned that all five routers with the respective firmware versions tested are not known to be affected by any serious vulnerabilities (e.g. kr00k). Neither of the tests with the OpenVAS scanner and the brute force attack via WPS produced any noteworthy results.

The Telekom Speedport Smart 3 could not be tested on the Internet due to local and manufacturer-specific restrictions. This router seems to explicitly require a DSL connection and contract with Deutsche Telekom, since attempts to use one of the LAN ports on the Telekom router as a WAN port were unsuccessful. Therefore, the tests of the safety features and protective functions could only be carried out to a limited extent in this case.

Symbols

The symbols used to evaluate the test criteria are shown in the table below, whereby a symbol can have more than one meaning depending on the context.

Symbol	Meaning
●	Function available and activated by default (e.g. automatically during/after setup); value can be changed
◐	Function available, but deactivated by default; value can be changed with restrictions
O	Function not available; value cannot be changed
n/a	No information; test could not be carried out

Security Features

	AVM Fritzbox 7590	Telekom Speedport Smart 3	TP-Link AX6000	ASUS RT-AX88U	Netgear RS400
Password					
Default password configured before Setup	●	●	O	●	O
Prompt to change (standard)password for Wi-Fi	O	O	●	●	●
Prompt to change (standard)password for router login	O	O	●	●	●
Check for password strength	●	O	O	O	O
Password restrictions (e.g. length, type of characters)	●	●	●	●	●
Firmware					
1-Click or manual update	1-click manual update	1-click manual update	1-click manual update	1-click manual update	1-click manual update
Secure, validated download for manual update	●	●	●	●	●
Update during setup	O	O	O	●	●
Automatic updates	●	◐[6]	O	O	●
Notification of update/prompt to update	●	●	●	●	●
Backup of router settings before update	●	O	O	O	O
Export router settings to file	●[7]	●	●	●	●
Administration					
Addition of additional users/user groups	●	O	O	O	O
Local access					
Access via hostname and/or IP address	Hostname, IP address	Hostname, IP address	Hostname, IP address	Hostname, IP address	Hostname, IP address
HTTPS supported	◐	O	◐	◐	●
Change user ID/username	●	O	O	●	O
Password can be changed	●	●	●	●	●
Change TCP/IP port	O	O	O	◐[8]	O

[6] Only if using Deutsche Telekom Internet service
[7] Additionally protected by password
[8] Only HTTPS-Port

Restrictions on local access					
IP address(es)	O	O	O	O	O
MAC address(n)	O	O	●	O	O
Only via HTTPS	O	O	O	O	O
Only via Ethernet	O	O	O	O	O
SSID and/or VLAN	O	O	O	O	O
No access for users of guest network	●	●	●	●	●
Remote access					
Available	●	O	●	●	●[9]
Deactivated by default	●	O	●	●	●
Access via IP address and/or hostname	IP address	O	IP address	IP address	Hostname
Change user ID/username	●	O	O	●	O
Change password	●	O	●	●	●
Change TCP/IP port	●	O	●	●	O
Restrictions on remote access					
IP address (n)	O	O	●	●	O
HTTPS only	●	O	O	●	●
Web interface					
Show registered/connected devices	●	●	●	●	●
Session timeout (auto-logout)	●	●	●	●	●
Change time limit for auto-logout	O	O	O	●	O
Only one session per user ID	O	O	●	●	●
Login with CAPTCHA	O	O	O	O	O
Logout from web interface possible	●	●	●	●	●
Lockout after too many failed login attempts	●	●	●	●	O[10]

[9] Only via VPN and Hostname (DDNS)

[10] Only restore password, no lockout

Smartphone App					
Available	●	O	●	●	●
User account with hardware vendor needed	O	O	O	O	●
Communication via Bluetooth and/or Wi-Fi	Wi-Fi	O	Bluetooth, Wi-Fi	Wi-Fi	Wi-Fi
Permissions required on smartphone	O	O	Location	Location	Location, camera
Logout from app	●	O	●	O	●
Wi-Fi					
Wi-Fi network activated by default	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
Network name (SSID) can be changed	●	●	●	●	●
Password can be changed	●	●	●	●	●
Can be deactivated via web interface	●	●	●	●	●
Can be switched of using on/off button	●	●	●	●	●
Time period for switching off can be defined	●	●	●	O	●
Access can be limited	●	●	●	●	●
Supported encryption methods	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					
Available	●	●	●	●	●
Activated by default	●	●	●	●	●
Can be deactivated	●	●	●	●	●
Vulnerable to brute-force attacks (e.g. Reaver, Pixie Dust)	O	n/a	O	O	O
Guest mode/network					
Available	●	●	●	●	●
Change name (SSID)	●	●	●	●	●
Change password	●	●	●	●	●
Prompt to change (default) password	O	O	O	O	O
Guest password must differ from private-LAN password	O	O	O	O	O

Traffic encrypted	●	●	◐[11]	●	◐[11]
Access to devices in private LAN (Wi-Fi)	O	◐	◐	◐	◐
Access to other devices in same guest network	◐	◐	◐	◐	◐
Access to devices in other guest networks	O	O	◐	O	◐
Guest network has time limits/restricted usage times	●	●	O	●	O
Time limits per user	O	O	O	O	O
Maximum number of users	unlimited	unlimited	unlimited	unlimited	unlimited
Bandwidth limit	O	O	O	●	O
Uses its own subnet, independent of private LAN	●	O	O	O	O
Login via dialog in operating system	●	●	●	●	●
Login via secure login page in browser	◐[12]	O	O	O	O
UPnP					
Available	●	O	●	●	●
Activated by default in LAN	●	O	●	●	●
Activated by default in WAN	●	O	●	●	●
Can be deactivated	●	O	●	●	●
Firewall					
LAN ports open/available	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
WAN ports open/available	O	n/a	O	O	O
Rules for incoming/outgoing requests	●	●	●	●	●
Port forwarding					
Available	●	●	●	●	●
Can be limited to source IP address and/or subnet	●	●	●	●	O
Usage times/time limits can be set	O	O	O	O	O

[11] unencrypted by default, but encryption available

[12] Login via HTTP

VPN					
Available	●	O	●	●	●
Supported protocols	IPSec, IPSec Xauth PSK	O	OpenVPN, PPTP	IPSec, OpenVPN, PPTP	OpenVPN
Additional features					
IPv6 supported	●	◐[13]	●	●	●
Dynamic DNS (DDNS) available	●	●	●	●	●
HNAP available	O	O	O	O	O
VLAN available	O	O	O	O	●
User account with hardware manufacturer needed	O	O	O	O	●
Can be reset to factory settings	●	●	●	●	●

[13] limited on LAN

Detailed results

All routers require the entry of a router password with a specified minimum length. However, the Fritzbox is the only test device to correctly check the strength of the entered password, and only allows passwords that are at rated as at least "medium" strength. All others simply inform the user via a dialog that the password entered is too short or insufficiently secure, and that another should be entered.

With Telekom, Asus and Netgear, classic and simple passwords such as "000000" or "password" are accepted. In the case of TP-Link, even passwords with only one character are accepted, which represents an increased security risk.

In the case of a manual firmware update, all routers force a secure download of their latest firmware via HTTPS from the manufacturer's website. The Telekom router only supports automatic updates for existing Deutsche Telekom connections.

Telekom does not support HTTPS access from the LAN, even though the associated ports 443 and 8443 are open. By contrast, Netgear is the only router to activate this function by default. All others offer the function at least in the web interface, but have it deactivated by default. With the exception of the Telekom router, all allow access to the router from the WAN. With TP-Link, HTTPS is not an absolute requirement. Netgear only allows remote access via a secure VPN connection and the host name, which must be set up beforehand via DDNS. We also looked at whether the routers use CAPTCHA to log on to the web interface. We could not find this function in any of the routers tested, which means that the registration form can theoretically be filled in automatically by a computer ("bot").

Four of the five routers prevent brute-force attacks on the router password with a lockout, which blocks access to the router, for something between several minutes and some hours, after a certain number of incorrect login attempts. Netgear is the only router that does not offer a real lockout. After three unsuccessful login attempts, the user is redirected to a local page, where the router password can be restored using the router's serial number and the security questions predefined by the user. By clicking on "Back" in the browser, the user can then easily make three new attempts to guess the router's login data.

By default, all routers use WPA2 encryption for their Wi-Fi network, and also offer other combinations with WPA or, in the case of Asus, WPA3. TP-Link allows the insecure WEP encryption to be used. Using test computer 4 (see Figure 1) we started a brute force attack on the WPS, which is activated by default on all routers. All routers except for Telekom passed this test successfully and were protected against such attacks.

Fritzbox, Telekom and Asus use WPA2 encryption for their guest network as standard. After activating the function, TP-Link and Netgear initially allow an open guest network to be used without a password. However, the user can select one of the supported encryption variants similar to the private Wi-Fi network. No router notifies the user of the change in the default password for the guest network, if one was assigned ex-works. In addition, the same password can be set for the private Wi-Fi and guest network, which is another security flaw. On the one hand, guests can connect to the private LAN using the same password, and on the other hand, attackers can gain access to both Wi-Fi networks by working through lists of known standard passwords (“rainbow tables”).

The Fritzbox also allows you to log into the guest network via a predefined login page in the browser that transmits the login data to the router in plain text via HTTP.

No critical ports are open at the factory on the WAN side. On the LAN side, ports such as 53 (DNS), 80 (HTTP) and possibly HTTPS (443, 8443), must be open by default so that the router works correctly, and users have access to the Internet. Except for the Telekom router, all support UPnP and have activated the function by default and released ports for this in the LAN.

The Telekom router only offers use of IPv6 in the LAN. All other devices can also communicate on the Internet with IPv6 addresses. The unsafe HNAP (Home Network Administration Protocol), which in the past had several security gaps due to incorrect implementations, is not supported by any of the routers. The Netgear router lets you set up a VLAN in the home network. A free Netgear account is mandatory for using Netgear Armor.

Quality features

	AVM Fritzbox 7590	Telekom Speedport Smart 3	TP-Link AX6000	ASUS RT-AX88U	Netgear RS400
Logging					
Available	●	●	●	●	●
Automatically deleted by	Switching off and restarting	Switching off and restarting	Switching off and restarting	Resetting to factory settings	Switching off and restarting
Type of log files					
System, errors, warnings	●	●	●	●	●
Registration of new device	●	●	O	●	●
Normal Internet traffic	O	n/a	O	O	O
Traffic blocked by firewall (e.g. blocked websites)	●	n/a	O	◐	●
Successful/unsuccessful login attempts	●	●	O	●	●
Changes to router configuration	●	●	●	●	O
E-Mail & notifications					
Available	●	●	●	●	●
For errors, warnings and status changes	●	●	O	O	O
For changes to router configuration	●	O	O	O	O
For firmware updates/installation	●	●	O	O	◐[14]
For WLAND login/logout (e.g. guest WLAN)	●	O	O	O	O
When threats/blocked web content are detected	O	O	O	●	●
Regular status reports	●	●	●	O	●
Number of recipients	1	1	1	1	2
File sharing					
Available	●	●	●	●	●
Integrated storage (NAS)	●	O	O	O	O
External storage (USB)	●	●	●	●	●
Activated by default	●	●	●	●	●
Can be deactivated	●	O	●	●	●
Accessible from WAN, but deactivated by default	●	O	●	●	●
Media Server					
Available	●	●	●	●	O
Activated by default	●	O	●	●	O
Can be deactivated	●	●	●	●	O
Additional features					
Smart Home or Mesh-WLAN available	●	●	◐[15]	●	●
Other	Physical button lock, 2FA	Standby mode, WLAN TO GO	TP-Link-Cloud	Setup Wizard, SSH, Telnet, AiCloud	Setup Wizard, Smartphone Setup, App Notifications, ReadyCloud

[14] Optional, when registering a Netgear account

[15] Smart Home only available if interface language set to English

Detailed results

All the routers record events such as system errors, WLAN registration and blocked requests, in different ways in their system logs. However, no conventional requests (which reflect the surfing behaviour of Internet users on the and could be misused for tracking) are recorded in the logs. In the case of Asus, the logs are retained even after the router is switched off/restarted. With TP-Link, the "Smart Home" function is only visible in the web interface if the language is set to English. It is hidden in all other languages.

Protection features

	AVM Fritzbox 7590	Telekom Speedport Smart 3	TP-Link AX6000	ASUS RT-AX88U	Netgear RS400
Protection against phishing websites					
Available	O	n/a	◐	◐	●
Protection rate (25 URLs)	O	n/a	84%	84%	96%
Protection against malicious websites					
Available	O	n/a	◐	◐	●
Protection rate (50 URLs)	O	n/a	100%	100%	100%
Protection against malicious files					
Available	O	n/a	O	O	O
Protection rate (100 malicious files)	0%	n/a	0%	0%	0%
Parental controls					
Available	◐	◐	◐	◐	◐
Protection rate (30 URLs)	70%	n/a	67%	97%	100%
Can be restricted by specific time, time period, website type	●	●	●	●	●[16]

Detailed results

Regarding the results, it should be said that all these tests only represent a snapshot in time. Even if 100% of the samples used were blocked in the test, this does not mean that the user can rely on the product to protect against 100% of all possible threats in the future.

TP-Link's Antivirus and Asus' AiProtection protection functions are provided by Trend Micro, while Netgear's Armor is supplied by Bitdefender. In spite of these protection solutions, we were able to download all the malware files from our file server, without a single one being blocked. Based on these results, it can be assumed that the integrated protection functions only block malicious websites based on their URLs. We suspect that router manufacturers voluntarily forego analysis of the malware files themselves, because this would result in a huge drain on the router's limited processing power. Such checks could take several minutes and result in a much longer download time and hence a negative user experience. Such functions are normally only found in professional security solutions.

Since no Internet connection could be established with the Telekom router during the tests, it was not possible for us to fully check the protective functions. According to the web interface, a parental control function is available; this allows the setting of times and port locks, but otherwise offers no protection against adult content.

[16] Via own smartphone app

Conclusion

For all tested products, no known security gaps or weaknesses were found in their tested firmware version and no critical ports on the WAN side were opened by default. Access to shared storage media on the Internet was also deactivated by default in products that support this function.

Four of five products allow access to the router's web-based administration interface via HTTP from the internal network, whereby HTTPS can be activated. The Netgear router has HTTPS from the LAN activated by default. However, Netgear is the only test router that does not have a proper lockout mechanism to prevent simple brute force techniques being used to access the router.

Apart from the TP-Link router, the respective web interfaces can only be accessed via the Internet using HTTPS. The Telekom Speedport does not offer access from the Internet. All products force the user to assign a router password with a specified minimum length, but only the Fritzbox checks the strength of the entered password correctly. Three products allow you to define weak and easy-to-guess passwords (e.g. "000000" or "password"). In the case of TP-Link, even passwords with one character are accepted. The insecure WEP encryption, which TP-Link still offers for its WLAN, represents a possible security risk. In addition, not all the tested routers require the passwords for the private WLAN and guest WLAN to be different.

Despite detection rates of 100% in the malicious-website-protection functions of TP-Link, Asus and Netgear, 100% protection against all threats to the home network cannot generally be assumed. The results of the tests we performed only refer to the specific threats used, and are a snapshot in time. To better protect yourself against attacks from the Internet as a user, we advise you to install an additional antivirus program from a recognized manufacturer on the end device of the user.

Copyright and Disclaimer

AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

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

AV-Comparatives
(April 2020)