

Mindestsicherheit für Internet-Router

Die BSI-Richtlinie TR-03148 ist ein wichtiger Schritt zu mehr Router-sicherheit. Leider greift sie stellenweise zu kurz.

Mit der im Oktober 2018 veröffentlichten technischen Richtlinie „Secure Broadband Router“, kurz TR Router, will das Bundesamt für Sicherheit in der Informationstechnik Verbraucher besser schützen. Die BSI TR-03148 (ct.de/y4wf) definiert verpflichtende sowie optionale **IT-Sicherheitsmaßnahmen, die die Routerhersteller umsetzen sollen**. Das können sie durch eine Kennzeichnung am Gerät zeigen.

Routerkäufer sollen so unter anderem erfahren, wie lange ein Gerät Updates erhält. Die TR verpflichtet die Hersteller insbesondere, schwere Sicherheitslücken zeitnah zu schließen. Dadurch sollen die Systeme widerstandsfähiger gegen Standardangriffe werden.

Die TR Router schreibt beispielsweise vor, dass nur solche Dienste auf dem Gerät laufen, die für die vom Nutzer aktivierten Funktionen erforderlich sind. Der Hersteller muss veröffentlichen, welche weiteren Dienste für den Betrieb des Routers unverzichtbar und deshalb immer aktiv sind. Ferner muss eine Firewall mit Filter und zustandsorientierter Paketprü-

fung (Stateful Packet Inspection, SPI) implementiert sein.

Die Richtlinie definiert zusätzlich Mindestforderungen an die Zugangs-sicherheit: Werkspasswörter dürfen keine Herstellerinfos enthalten, müssen mindestens acht Zeichen lang sein und aus Buchstaben und Ziffern bestehen. Das WLAN inklusive Gastnetz muss mindestens mit WPA2 verschlüsselt sein.

Die Richtlinie ist indes keineswegs verpflichtend. So antwortete AVM, Hersteller der besonders hierzulande verbreiteten Fritzboxen auf unsere Anfrage: „Wir pflegen unsere Produkte regelmäßig und über viele Jahre. Und mit jedem Update bringen wir unsere Produkte auf einen aktuellen und sicheren Stand. Ein Abgleich mit der jetzt veröffentlichten TR Breitband-

router zeigt, dass unsere eigenen Sicherheitsrichtlinien tiefgreifender und umfassender sind.“

Die Telekom will die Richtlinie erfüllen, aber nicht nachträglich für ältere Geräte: „Daher stehen wir klar zu den Zielen der neuen Technischen Richtlinie des BSI und haben bereits damit begonnen, diese für die kommenden Speedport-Router umzusetzen.“

Lancom Systems antwortete: „Wir begrüßen und unterstützen die Router-TR. Alle Geräte von uns, die das aktuelle LCOS 10.20 [...] installiert haben, erfüllen die Vorgaben.“

(Ulrich Hottelet/amo@ct.de)

BSI TR-03148: Secure Broadband Router: [ct.de/y4wf](https://www.ct.de/y4wf)

Anno 2018 darf IPv6 in einer Sicherheitsrichtlinie nicht mehr optional sein. Für ein Drittel aller heise-online-Besucher ist es schon Alltag.

4.7 Option: Internet Protocol version 6 (IPv6)

The router SHOULD implement Internet Protocol version 6 (IPv6) and offer its services accordingly. Due to the importance of the Internet Control Message Protocol (ICMP) when using IPv6 it is **RECOMMENDED** that the router only supports the types of messages marked with an "X" in [Table 7: ICMPv6 message types](#). The router MUST NOT forward inbound IPv6 traffic, if it does not belong to a known connection.

ICMPv6 message type	In the private network	From the public network	To the public network
Destination unreachable (1)	X	X	X
Packet too big (2)	X	X	X
Time exceeded (3)	X	X	X
Parameter Problem (4)	X	X	X
Echo-Request (128)	X (1)		X (1)
Echo-Response (129)	X (2)	X (2)	
Multicast (130-132, 143, 151-153)	X (3)	X (3)	X (3)
Router (133, 134)	X (3)		
Neighbor (135, 136)	X (3)	X (3)	X (3)

Wifi 6 für Firmen

HPE hat seine ersten **11ax-Access-Points für Firmen** ins Programm genommen: Die Modelle Aruba AP 514 und AP 515 sollen Energie übers LAN-Kabel beziehen, wobei für volle WLAN-Performance PoE+ (IEEE 802.3at) bereitstehen muss. Dann funken sie im 5-GHz-Band mit 4 MIMO-Streams (4,8 GBit/s brutto im 160-MHz-Kanal).

An Standard-PoE (802.3af) beschränken sich die APs auf 2 MIMO-Streams. Das Dualband-WLAN ist bereits für die neue Verschlüsselung WPA3 inklusive der Hotspot-Erweiterung Enhanced Open zertifiziert. Daneben sind auch Bluetooth 5.0 und ZigBee für IoT-Anwendungen an Bord, beispielsweise zum Anbinden intelligenter Türschlösser oder elektronischer Regaletiketten. HPE Aruba listet die jetzt erhältlichen APs mit stolzen 1100 US-Dollar. (ea@ct.de)



Der Access Point HPE Aruba AP 515 funkt nach dem kommenden WLAN-Standard IEEE 802.11ax (Wifi 6) mit bis zu 4800 MBit/s.

Multi-Gigabit-LAN für PCs

Buffalos PCI-Express-Karte LGG-PCIE-MG rüstet bei PCs und Servern einen bis zu **10 GBit/s schnellen LAN-Anschluss** gemäß NBase-T nach, der an älteren oder längeren Kabeln notfalls auf 5 oder 2,5 GBit/s herunterschaltet. Damit soll die Transferleistung gegenüber dem etablierten Gigabit-Ethernet mindestens verdoppelt werden (c't 15/2018, S. 102).

Treiber gibt es für Windows ab 7 und Windows Server ab 2012. Da das Board laut Hersteller einen Tehuti-MAC-Chip und einen Marvell-PHY-Baustein nutzt, sollte es mit den Tehuti-Treibern (ct.de/y4wf) auch mit Linux und macOS funktionieren. Buffalo beziffert die maximale Leistungsaufnahme mit 6 Watt. Die Karte kostet 149 Euro. (ea@ct.de)