

## Nach dem Telekom-Angriff: So schützt man seinen Router

07.12.2016, 13:36 | IT, New Media & Software

Pressemitteilung von: *reichelt elektronik*

Presseagentur: *reichelt elektronik*

---



Internet-Router können mit ein paar Klicks wirkungsvoll geschützt werden

Der Hacker-Angriff auf rund 900.000 Telekom-Router zeigt, dass Internetnutzer sich Gedanken über die Sicherheit ihrer Router machen müssen. Ein wirkungsvoller Schutz ist mit wenigen Klicks möglich.

-----  
Sande, 07.12.2016 - Der Router ist das Tor zum Internet - über ihn kommen die Daten aus dem World Wide Web auf unsere Computer und Smartphones. Dieses Tor gilt es gut zu schützen, damit keine unerwünschten Besucher durchkommen können. Wie das mit wenigen Klicks geht, zeigt reichelt elektronik in seinem Online-Magazin (<https://www.reichelt.de/magazin/> (<https://www.reichelt.de/magazin/>)).

### Voreingestellte Passwörter ändern

Grundvoraussetzung für die Absicherung von Routern: sichere Passwörter verwenden und möglichst alle unbeaufsichtigten Türen nach außen schließen. Der erste Schritt ist daher, das Admin-Passwort für den Router selbst sowie das Passwort für das WLAN-Netz zu ändern. Die voreingestellten Passwörter - und sind sie noch so kryptisch - stammen in der Regel aus einem simplen Algorithmus und können vor allem bei älteren Modellen allein aus den Gerätedaten entschlüsselt werden.

### WLAN-Zugänge verschlüsseln

So wie man seine Wohnungstür nicht mit einem einfachen Zimmerschloss verschließt, sollte der Router mit der sichersten Verschlüsselungsmethode abgesichert werden. Das ist aktuell der WPA2-Standard. Beherrscht der Router selbst nach einem Software-Update nur WEP und WPA, sollte er ausgetauscht werden. Viele Router bieten zum vereinfachten Verbindungsaufbau die sogenannte WPS-Funktion, mit der WLAN-Geräte ohne lästige Passwortheingabe verbunden werden können. Das spart zwar Zeit, ist aber unsicher.

Gästen sollte man nicht sein WLAN-Passwort geben, mit Misstrauen hat das nichts zu tun. Vielmehr lässt sich so verhindern, dass von den Gästen versehentlich Schadsoftware in das heimische Netzwerk übertragen wird. Die meisten modernen Router bieten ein sogenanntes Gastnetzwerk zum Surfen, das keinen Zugang zum heimischen Netz erlaubt.

Auch die Hintertüren nicht vergessen

Ist das Netzwerk an der Vordertür gesichert, gilt es auch die Hintertüren zu schließen. Dazu gehört das Netzwerkprotokoll UPnP, das die Kommunikation zwischen Multimediageräten wie Fernseher und Foto-Server erleichtert. Über UPnP können aber auch Unbefugte sämtliche Router-Einstellungen verändern und dann Schadsoftware ins Netzwerk laden. Deshalb sollte UPnP unbedingt deaktiviert werden. Gleiches gilt für den Fernzugriff, wenn man nicht unbedingt von unterwegs die Router-Konfigurationen ändern muss. Kontrolliert werden sollte auch, ob die sogenannten Ports geschlossen sind. Über sie können bestimmte Computer und Programme im heimischen Netzwerk aus dem Internet angesprochen werden. Wer das nicht benötigt, sollte alle Ports schließen. Ganz wichtig: Um gegen Angriffe aus dem Internet gewappnet zu sein, sollte auf dem Router immer die aktuelle Gerätesoftware (Firmware) arbeiten. Viele Geräte bieten dafür eine automatische Update-Funktion an, die unbedingt aktiviert werden sollte. Wie das funktioniert, erklärt reichelt elektronik ebenfalls in seinem Online-Magazin (<https://www.reichelt.de/magazin/> (<https://www.reichelt.de/magazin/>)).

-----  
Pressekontakt:

reichelt elektronik  
Herr Sebastian Bley  
Elektronikring 1  
26452 Sande

fon ..: +49 (0)4422 955 485  
web ..: <http://www.reichelt.de>  
email : [bley@reichelt.de](mailto:bley@reichelt.de)

## **Portrait**

Über reichelt elektronik:

reichelt elektronik (<http://www.reichelt.de>) bietet als einer der größten europäischen Online-Distributoren für Elektronik und IT-Technik mehr als 70.000 Produkte mit einem sehr guten Preis-Leistungs-Verhältnis bei höchster Verfügbarkeit und kürzester Lieferzeit an. Mit dem breiten Sortiment an elektronischen Bauelementen ist reichelt seit mehr als 45 Jahren der ideale Partner in Sachen Bauelemente-Beschaffung. Der Elektroniker findet im Onlineshop ICs und Mikrocontroller, LEDs und Transistoren sowie Widerstände, Kondensatoren, Steckverbinder und Relais. Auch Werkzeuge und Messgeräte in hoher Qualität, wie Lötstationen, Multimeter oder Oszilloskope, sind im Produktprogramm enthalten. Das preisgünstige Sortiment aus der PC- und Netzwerktechnik mit internen und externen Festplatten, AMD- oder Intel-CPU's, Arbeitsspeicher sowie WLAN-Routern, Powerlines und Patchkabeln ist sowohl für den Privat- wie auch für den Businesskunden interessant. Daneben findet sich im Produktprogramm eine große Auswahl

an Unterhaltungselektronik rund um Beamer, TV-Geräte, Sat-Spiegel, LNBs und Receiver - aber auch Zubehör wie Verbrauchsmaterial, HDMI-Kabel, Batterien und Akkus.

---

News-ID: 930499 • Views: 123 (Stand: 12.05.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/930499/Nach-dem-Telekom-Angriff-So-schuetzt-man-seinen-Router.html>