Viele Router, viele Sicherheitsprobleme

Angriffswelle auf WLAN-Router

Die Firmware vieler WLAN-Router ist entweder veraltet oder wird nicht umgehend mit Sicherheitsupdates versorgt. Das ist riskant für Router-Besitzer, weil die Angriffe drastisch zunehmen, während viel mehr Nutzer auf sichere Router im Homeoffice angewiesen sind.

Von Fabian A. Scherschel

Aktuell greifen Kriminelle viel mehr Home-Router an als je zuvor, wie aus einer Studie des Antiviren-Herstellers Trend Micro hervorgeht. Zwischen September und Dezember 2019 hat sich die Zahl fast verzehnfacht, nämlich von 23 auf 249 Millionen unberechtigte Login-Versuche. Allein im März dieses Jahres registrierte das Unternehmen fast 194 Millionen solcher Angriffe. Die Sicherheitsforscher gehen davon aus, dass mit der Verlagerung von Firmendaten in Heimnetzwerke solche Attacken für Kriminelle weit lukrativer werden.

Die aktuelle Angriffswelle führen anscheinend Profis, die Brute-Force-Verfahren skriptgesteuert anwenden, um Zugangsdaten diverser Internet-of-Things-Geräte zu knacken. Home-Router stehen auf Grund ihrer zentralen Lage im Netzwerk der Opfer im Visier der Angreifer: Der Router ist das erste Gerät des Heimnetzes, das aus dem Internet ansprechbar ist. Er eignet sich zudem als Brückenkopf für weitere Angriffe auf IoT-Geräte dahinter. Ziel der Angreifer ist es, die Geräte in ein Botnetz einzuspannen, um damit etwa DDoS-Angriffe auf Firmen-Websites zu führen.

Firmware oft veraltet

Dass Home-Router immer mehr in den Fokus professioneller Angreifer rücken, könnte daran liegen, dass es um die Sicherheit solcher Geräte anhaltend schlecht bestellt ist. So hat zum Beispiel das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) die Firmware von 127 nicht näher genannten Home-Routern der Hersteller Asus, AVM, D-Link, Linksys, Netgear, TP-Link und Zyxel auf Sicherheitslücken abgeklopft. Huawei-Router haben die Forscher nicht untersucht, da der Hersteller keine Firmware-Dateien auf seiner Website bereitstellt. Aus gleichem Grund hat Fraunhofer auch die verbreiteten Provider-Router nicht berücksichtigt.

Das Ergebnis dieser Teiluntersuchung ist ernüchternd: Viele Hersteller entwickeln gar keine Sicherheitsupdates für ihre Geräte, sodass Informationen über viele alte Router-Schwachstellen lange im Umlauf sind. Die Fraunhofer-Forscher hatten die Firmware der Router mittels eigener Methoden automatischen Tests unterzogen und so ermittelt, von wann der darin enthaltene Linux-Kernel stammt. Zudem haben die Forscher untersucht, ob gängige Exploit-Schutzmaßnahmen umgesetzt sind und ob Sicherheitsprobleme wie voreingestellte Passwörter vorhanden waren.

Für 22 der 127 getesteten Geräte sind seit zwei Jahren gar keine frischen Firmware-Updates erhältlich. Mehr als ein Drittel der Gerätefirmware basiert auf Linux-Kernelversionen, die seit mindestens neun Jahren keine Sicherheitsupdates erhalten. Die Firmware eines Linksys-Geräts gründet gar auf einem knapp 18 Jahre alten Linux-Kernel. Das Bild setzt sich bei den Exploit-Abwehrmaßnahmen fort: Auch hier könnten die Hersteller viel mehr tun, um ihre Router sicherer zu machen. Immerhin schnitten die AVM-Router mit Abstand am besten ab, ASUS und Netgear konnten ebenfalls ein paar lobende Worte der Tester verbuchen.

BSI will mehr Sicherheit

Dass die vielfältigen Sicherheitslücken in Home-Routern gestopft werden müssen, hat auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) erkannt und Anfang Juli eine neue Prüfspezifikation für Router im Endkundenbereich veröffentlicht. Auf dieser Basis sollen Hersteller, Prüfer und „andere Interessierte“ die Sicherheit von Home-Routern untersuchen können. Laut BSI will man so Testergebnisse vergleichbar machen, damit das Home-Router-Angebot insgesamt sicherer wird. Anhand der neuen Prüfspezifikation lassen sich Router im Rahmen der vom BSI gegen Ende 2018 veröffentlichten technischen Richtlinie für Home-Router-Sicherheit auch zertifizieren.

Bleibt zu hoffen, dass die Prüfkriterien dazu führen, dass Kunden künftig die Sicherheit von Routern besser vergleichen können und die Sicherheit überhaupt ein wichtiges Kaufkriterium wird. *(rei@ct.de)* c't

Sicherheitsbericht & BSI-Spezifikationen: ***ct.de/yjmp***

Brute-Force-Angriffe auf Router

Laut Trend Micro nehmen Brute-Force-Angriffe auf Router seit Oktober 2019 erheblich zu. Allein im Mai 2020 hat der Antiviren-Hersteller fast 200 Millionen Attacken dieser Art gezählt.