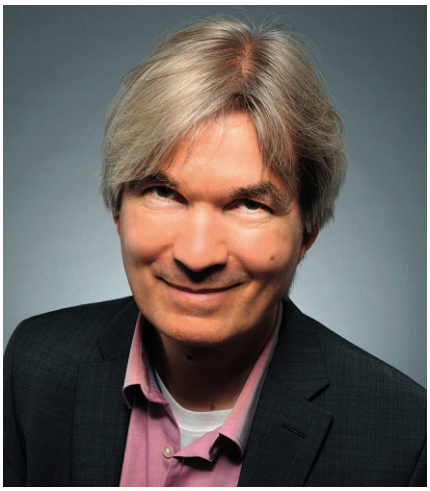
Das Böse ist immer und überall: Angriffsziel »Home Office«

Montagabend ist bei uns Krimizeit. Vor kurzem gab es dabei ein Wiedersehen mit dem Ex-James Bond P*ierce Brosnan*. Der hatte in seiner Firma einen jungen Mann, der vorgab früher bei der NSA gewesen zu sein, also jene US-Amerikaner, die keine IT-Barrieren kennen und die praktisch mit Ihnen Kaffee trinken, ohne dass Sie es mitbekommen. Jener junge Mann wollte unbedingt Herrn *Brosnans* Tochter näher kennenlernen, was *Pierce* aber nicht wollte und so »hackte« sich jener Ex-NSA-Mann einfach in das Heimnetz der Familie und beobachtete auf riesigen Monitoren jedes Geschehen im Hause von *Pierce*, gruselig.

Von der Fiktion zur Realität: Laut Angaben eines Online-Artikels bei **Heise.de** geraten jetzt immer mehr WLAN-Router in den Fokus von Kriminellen, natürlich mit dem Hintergrund, dass momentan immer (noch) viele zu Hause im Home-Office sitzen. Innerhalb von wenigen Monaten hat sich dabei die Zahl der Angriffe fast verzehnfacht. Allein im März, so der Text, hätte es 194 Millionen (!) unberechtigte Login-Versuche gegeben, um auf diesem Weg an sensible Firmendaten zu gelangen, die jetzt nicht mehr durch die Infrastruktur des Unternehmens geschützt sind. Der WLAN-Router steht dabei – als erstes Gerät des Heimnetzes – im Mittelpunkt der Attacken.

Kontraproduktiv ist dabei das Verhalten vieler Anbieter von Routern. Eine Untersuchung des Fraunhofer Instituts ergab, dass es um die Sicherheit der Geräte häufig nicht gut bestellt ist. Viele Hersteller entwickeln gar keine Sicherheitsupdates für ihre Geräte. Informationen über zahlreiche Router-Schwachstellen sind somit lange im Umlauf. Bei 22 der 127 getesteten Router gab es seit zwei Jahren keinerlei Updates der Firmware. Im schlimmsten Fall basierte diese wichtige interne Software auf einem Linux-Kernel, der knapp 18 Jahre alt war. Auch Exploit-Schutzmaßnahmen und Sicherheitsprobleme mit voreingestellten Passwörtern standen im Fokus der Untersuchung. Alles in allem schnitten die Produkte von AVM, Asus und Netgear noch am besten ab. Um das Home-Router-Angebot zukünftig sicherer zu machen, könnte eine Prüfspezifikation des BSI (Bundesamt für Sicherheit in der Informationstechnik) dienen, die Anfang Juli veröffentlicht wurde. Mit deren Hilfe sollen Hersteller und Prüfer die Sicherheit der Geräte untersuchen können.

Vielen Ihrer Kunden wird allerdings kaum bewusst sein, ob das Gerät im Anschlussraum (oder wo auch immer) noch den aktuellen Standards entspricht. Ein mit der Zeit gehender Betrieb, der u.a. im Netzwerk-Segment arbeitet, darf, ja muss seinem Kunden hier beratend zur Seite stehen und hat Lösungen für ein sicheres Heimnetz im Gepäck, die er installieren und konfigurieren kann. Lassen Sie sich dabei auch nicht von den nervenden »Was-soll-das-kosten-Gesprächen« vom Weg abbringen. Dieser für die Datensicherheit so wichtige Bereich benötigt Profis wie Sie es sind.



Marcel Diehl,
Redaktion »de«