2016/49 Inland

https://shop.jungle.world/artikel/2016/49/kein-fall-fuer-die-cyber-nato

Der Angriff auf Router der Telekom

Kein Fall für die Cyber-Nato

Von **Enno Park**

Am ersten Advent fielen 900 000 Router der Telekom aus. Das ist aber kein Grund für blinden Netzaktionismus.

Während am Adventssonntag die erste Kerze angezündet wurde, ging für fast eine Million Kunden der Telekom das Internet aus. Was wie ein großflächiger Cyberangriff auf das Telekom-Netz aussah, war wohl nur Kollateralschaden der tagtäglich im Netz herumwühlenden Scripte und Viren. Es gab einen Angriff – wer dahintersteckt, ist bislang nicht bekannt –, aber das Ziel war nicht das Telekom-Netz, sondern ein Standardprotokoll, das den kryptischen Namen »TR-069« trägt und der Fernwartung von DSL-Routern dient. Haben solche Router eine bestimmte Sicherheitslücke, kann ein Angreifer sie per Fernzugriff kapern und für Angriffe aller Art zweckentfremden. Deshalb scannen Angreifer ununterbrochen und automatisiert das Internet nach Geräten mit unter anderem dieser Sicherheitslücke. Das geht normalerweise geräuschlos vonstatten.

Die 900 000 ausgefallenen Telekom-Router hatten diese Sicherheitslücke nicht, aber dafür einen anderen Software-Fehler: Werden sie mit sehr vielen solcher TR-069-Anfragen konfrontiert, stürzen sie ab, funktionieren jedoch nach einem Neustart wieder. Der Ausfall war deshalb höchstwahrscheinlich nicht im Sinne der Angreifer.

Die Telekom hat schnell und vorbildlich reagiert, die Adresse der Schadsoftware im Netz gesperrt und für die Router ein Update bereitgestellt. Ob sie besser hätte vorbeugen können, ist fraglich. Entgegen anderslautender Gerüchte, wonach die Sicherheitslücke seit Jahren bekannt sei, waren die Telekom-Router durchaus geschützt und konnten nicht von den Angreifern übernommen werden. Wahrscheinlich ist schlicht noch niemand auf die Idee gekommen, diese konkrete Konstellation zu testen.

Es klingt abgedroschen, aber 100prozentige Sicherheit gibt es nicht. Die Hersteller können noch so sorgfältig prüfen, früher oder später findet sich doch eine Sicherheitslücke, an die niemand gedacht hat. Dagegen helfen nur regelmäßige Updates oder ein von Grund auf anders konzipiertes Internet. Sensible Infrastruktur sollte grundsätzlich nicht am öffentlichen Internet hängen und wem durch Ausfälle Schaden droht, sollte einen Ersatz-Router oder eine zweite Leitung parat halten.

Geradezu albern sind hingegen die Reaktionen aus der Politik, etwa wenn Rainer Wendt, der Vorsitzende der Deutschen Polizeigewerkschaft, über Cyberterroristen schwadroniert,

die schlimmer seien als der IS. Konstantin von Notz (Bündnis 90/Die Grünen) fordert, die Telekom solle ihren Kunden eine Entschädigung zahlen.
Der Telekom-Vorstandsvorsitzende Timotheus Höttges fordert sogar eine »Cyber-Nato«, die künftig auf solche Angriffe reagieren soll – obwohl niemand auch nur den geringsten Anhaltspunkt hat, wer die Angreifer eigentlich sind. Außerdem sollten, so Höttges, die Hersteller von Routern und anderen Geräten gesetzlich verpflichtet werden, kurzfristig Updates bereitzustellen. Das ist zwar sinnvoll, hat aber einen faden Beigeschmack, schließlich müsste die Telekom das mit ihrer Marktmacht bei ihren Lieferanten auch so schon durchsetzen können. Sorgen sollte man sich jedenfalls nicht um die ausgefallenen Router, sondern um die Geräte, die still und leise per TR-069 gekapert wurden und unauffällig ihren Dienst verrichten – bis sie Teil des nächsten großen Angriffs im Internet sind.