Bild: Deutsche Telekom

T-bakel

Weltweiter Angriff auf Router trennt Telekom-Kunden vom Netz

Die Deutsche Telekom wurde Opfer eines groß angelegten Angriffes auf DSL-Router. Dabei weisen ihre Geräte die attackierte Schwachstelle wohl gar nicht auf. Da der Konzern den angegriffenen Fernwartungs-Port nicht eingeschränkt hatte, mussten die Kunden trotzdem unter den Folgen leiden.

Von Fabian A. Scherschel

Am letzten November-Wochenende fand der wahrscheinlich größte Angriff auf die Kunden eines deutschen Internet-Providers statt: Etwa 900.000 Telekom-Kunden mussten für ein bis zwei Tage ohne Internet und Telefon auskommen. Die Telekom reagierte zwar schnell und vorbildlich, um das Problem in den Griff zu bekommen, allerdings war zu diesem Zeitpunkt das Kind schon in den Brunnen gefallen.

Der verflixte Port 7547

Am Unglücks-Wochenende hatten unbekannte Angreifer einen seit Wochen bekannten Exploit für mehrere DSL-Router mit dem quelloffenen Code des Internet-of-Things-Botnetzes Mirai kombiniert und aufs Netz losgelassen. Über eine Sicherheitslücke in Zyxel-Routern des irischen Providers Eir und bei weiteren Providern in anderen Ländern wurden haufenweise Router gekapert. Der Mirai-ähnliche Wurm bombardierte daraufhin das weltweite Netz mit Schadcode-Paketen, um weitere verwundbare Geräte zu infizieren.

Speedport-Router der Telekom wiesen zwar diese Lücke nicht auf, hatten aber wohl ein ganz anderes Problem: Die wiederholten Angriffe brachten die Geräte zum kompletten Stillstand. Tausende Telekom-Kunden standen deshalb ohne funktionierenden DSL-Zugang da.

Die Telekom bekam das Problem schlussendlich in den Griff, indem sie in ihrem gesamten Netz allen Traffic für Port 7547 blockierte. Später schob man Software-Updates nach, die vermutlich die DoS-Schwachstelle in den betroffenen Speedport-Modellen stopften.

TR-069, TR-064

Der TCP-Port 7547 ist Teil des Fernwartungsprotokolls TR-069, mit dem Internet-Dienstleister DSL-Equipment einrichten, konfigurieren und updaten. Über diesen Port können Wartungsserver der Telekom bei den Routern anklopfen, um diesen zum Beispiel mitzuteilen, dass ein Software-Update für sie bereitsteht.

Router kontaktieren im Rahmen der Fernwartung nur voreingestellte Server. Darüber hinaus ist die TR-069-Kommunikation laut Telekom verschlüsselt und authentifiziert. Es ist also sehr schwer, von außen in diese Verbindung einzudringen. Der Anklopf-Port kann aber von jedem be-

liebigen System aus angesprochen werden. Zwar muss sich das anklopfende System authentifizieren, um Funktionen im Sinne des Protokolls auszuführen, der offene Port erlaubt aber grundsätzlich erst einmal Verbindungen von überall her. Allein das stufen Sicherheitsexperten bereits als Nachlässigkeit ein. Schließlich ist das Vermeiden unnötiger Angriffsvektoren eine der wichtigsten Sicherheitsmaßnahmen.

Die Anfang November in den Eir-Routern entdeckte Lücke befindet sich zwar im verwandten Protokoll TR-064 (LAN-Side CPE Configuration), involviert aber auch Port 7547. Dieses Protokoll ist nicht dafür gebaut, von jedermann angesprochen zu werden, da man darüber DNS- und NTP-Einstellungen der DSL-Endgeräte mit einem einfachen POST-Request ändern kann, ohne sich anmelden zu müssen. Das Protokoll sollte eigentlich nur von der LAN-Seite des Routers, also aus dem Heimnetz des Kunden, erreichbar sein. Zyxel, der Hersteller des Eir-Routers, stellte diese Funktion aber auf der externen Schnittstelle des Routers über den TR-069-Anklopf-Port bereit, der aus dem öffentlichen Netz erreichbar ist.

Diese Schwachstelle in den Eir-Routern führte dazu, dass Angreifer mit einem Befehl zum Einfügen eines neuen Zeit-Servers Schadcode einschleusen konnten, der dann vom Router ausgeführt wird. Ein trivialer Weg, um verwundbare, aus dem öffentlichen Netz erreichbare Geräte mit einem Wurm zu bespielen, der sie in ein Botnetz einreiht und sich direkt auf die Suche nach weiteren Opfern macht.

Noch mal Glück gehabt

Der Botnetz-Traffic, der aus dem Internet in das Netz der Telekom prasselte, legte einige Speedport-Modelle (W 921V, W 723V Typ B und W 921 Fiber) lahm, da in deren TR-069-Anklopffunktion eine Schwachstelle steckte. Der Sicherheitsforscher Ralf-Philipp Weinmann konnte dies mit der ungepatchten Firmware nachstellen. Da bei den Telekom-Routern die TR-064-Umsetzung nicht verwundbar war, konnten die Angreifer die Router jedoch nicht in ihr Botnetz einreihen.

Insoweit hatten die Telekom-Kunden Glück: Ihre Router wurden nicht gekapert und es wurde verhindert, dass 900.000 Telekom-Router in eine neue Version des IoT-DDoS-Botnetzes Mirai eingereiht wurden. Das ist allerdings ein schwacher Trost für die Kunden, deren Router bei dem Angriff aus dem Netz geschossen wurden. *(fab@ct.de)* c't

Fabian A. Scherschel

Macht die Schotten dicht!

Telekom-Kunden wurden überhaupt nur deshalb Opfer der Angriffe, weil es die Telekom im Vorfeld versäumt hatte, den Zugriff auf Port 7547 auf die eigenen Server zu beschränken und stattdessen zuließ, dass beliebige Clients in Irland, Russland und Brasilien Endkunden-Geräten im Telekom-Netz auf diesem Port erreichen konnten. Damit hat man eine verbreitete Strategie unter Sicherheitsexperten außer Acht gelassen, die besagt, dass die Angriffsfläche für Systeme so klein wie möglich zu halten ist.

Auch wenn keine Lücke im Fernwartungsprotokoll der Router bekannt war, bedeutet ein offener, von außen erreichbarer Port immer ein Risiko, das man wenn möglich vermeiden sollte. Die Kunden des Bonner Providers haben nun den Preis dafür gezahlt, dass die Telekom dies nicht getan hat. Ein Provider muss davon ausgehen, dass seine Router Schwachstellen haben. Und er muss alles dafür tun, mögliche Angriffe auf diese zu minimieren.

Einträge im Support-Forum der Firma zeigen: Mitarbeiter der Telekom wurden schon Anfang 2014 von Kunden darüber informiert, dass der TR-069-Anklopf-Port aus dem öffentlichen Netz erreichbar ist. Die Telekom stellte sich schon damals auf den Standpunkt, dass dies kein Problem darstelle, da TR-069 ausreichend abgesichert sei und Anklopfen ohne gültige Anmeldedaten kein Sicherheitsrisiko darstelle. Wie sich jetzt gezeigt hat, war das gleich in mehrfacher Hinsicht ein Trugschluss: Bestimmte Zyxel-Router lassen sich auch ohne Authentifizierung kapern und viele Speedports der Telekom zumindest lahmlegen.

Telekom-Chef Höttges rief unlängst auf der Sicherheitskonferenz des Konzerns zum Cyberkrieg auf: Jeder einzelne müsse aufrüsten, die Politik müsse Angriffe ächten, eine Art Cyber-NATO sei gefragt. Vielleicht sollten wir erst einmal alle Ports dicht machen, die wir nicht unbedingt brauchen – dann müssen wir weniger verteidigen.