Ronald Eikenberg

Kabelbruch

Schwerwiegende Sicherheitslücken bei Kabel Deutschland

Durch Schwachstellen im Netz von Kabel Deutschland hätten Angreifer die Anschlüsse der fast drei Millionen Breitbandkunden übernehmen und sogar die vom Provider verordneten Zwangsmodems manipulieren können – vermutlich seit über zehn Jahren.

Das Kabel-Deutschland-Netz stand bis vor kurzem sperrangelweit offen: Durch Versäumnisse bei der Absicherung konnte man nicht nur die Telefonanschlüsse der Kunden kapern, sondern auch über ein Wartungsnetz in deren lokale Netze einsteigen – etwa, um den Internetverkehr zu belauschen oder Rechner anzugreifen.

Alles begann mit einer zufälligen Entdeckung des Linux-Entwicklers Alexander Graf. Er wollte eine eigene Fritzbox als VoIP-Telefonanlage am Kabel-Deutschland-Anschluss einsetzen, jedoch hat der Provider die dazu nötigen VoIP-Zugangsdaten unter Verschluss gehalten. Graf wollte sich nicht damit abfinden, seine Telefone an das vom Provider gestellte Zwangsmodem anschließen zu müssen. Also versuchte er, die Daten aus dem Provider-Modem zu extrahieren. Schließlich fand er einen Weg, auf das Embedded-Linux des Modems zuzugreifen und kam so auch an seine Zugangsdaten.

Wartungsnetz stand offen

Doch hier ist die Geschichte noch nicht zu Ende: Als er sich in dem Embedded-System umsah, stieß er auf eine Netzwerkverbindung namens wan0, die für den Nutzer im Normalbetrieb unsichtbar ist. Es handelt sich um das Wartungsnetz des Providers, über das er etwa im Support-Fall aus der Ferne auf das Modem zugreifen kann. Graf fand heraus, dass er dort nicht allein ist: Über das versteckte Netz konnte er ungehindert die Modems anderer Kunden unter anderem via Telnet ansprechen. Ein Login als Wartungstechniker scheiterte allerdings zunächst an einer Passwortabfrage.

Das sollte jedoch kein Hindernis sein: Graf entdeckte im Dateisystem seines Modems nämlich auch das dazugehörige Kennwort im Klartext. Es zeigte sich, dass man damit auf andere Kabel-Deutschland-Modems administrativ zugreifen konnte. Die Modems waren also nicht nur über andere Kundenanschlüsse erreichbar, sondern fatalerweise auch noch alle mit dem gleichen Passwort geschützt. Über diese Wartungs-Shell hätte man beliebige Linux-Binaries in die Modems einschleusen können. So wäre es möglich gewesen, den Datenverkehr mitzuschneiden, zu manipulieren oder Geräte im Heimnetz der Kunden anzugreifen.

Übernahme fremder Anschlüsse

Darüber stellte sich heraus, dass auch die sogenannte Provisionierung unzureichend geschützt war, über die der Provider die VoIP-Zugangsdaten an die Modems verteilt. Mit Modem-Zugriff konnte man die Konfigurationsprofile anderer Kunden abrufen und damit ihren Telefonanschluss übernehmen. Mit bösen Absichten hätte man so Anrufe in fremdem Namen sowie hochpreisige Telefonate zu Premium-Diensten führen können.

Das Unternehmen hatte offenbar nicht damit gerechnet, dass sich jemand Zugriff auf das Zwangsmodem verschaffen und so einen tiefreichenden Einblick ins System erhalten könnte. Dabei ist die Vorgehensweise von Alexander Graf wahrlich nicht außergewöhnlich und in Bastlerkreisen durchaus üblich. Nachdem sich Graf einen Überblick über das Ausmaß des Sicherheitsproblems verschafft hatte, wollte er den Provider darüber in Kenntnis setzen, dass dringender Handlungsbedarf besteht.

c't informiert Vodafone

Er setzte sich mit c't in Verbindung, mit der Bitte, die relevanten Details an Kabel Deutschland, das inzwischen zu Vodafone gehört, weiterzugeben. Nachdem wir das Problem verifiziert hatten, informierten wir den Provider Anfang November über den Ernst der Lage. Das Unternehmen versprach, der Sache auf den Grund zu gehen. Zwischenzeitlich hatte der Provider seine Wartungszugänge laut Graf von Telnet auf SSH umgestellt – das sorgte allerdings nur bedingt für Sicherheit, da das genutzte SSH-Passwort unzureichend geschützt im Modem gespeichert wurde.

Am 10. Dezember erklärte das Unternehmen schließlich, dass die Schwachstellen geschlossen wurden. „Durch neue Schutzfilter im Vodafone-Netzwerk sind die Modems – und damit die Daten der Kunden – vor potenziellem Missbrauch noch besser geschützt und erlauben ausschließlich die für unsere Kunden erforderliche Kommunikation mit dem Netzwerk." Tatsächlich blockiert Vodafone im Wartungsnetz nun den TCP-Verkehr zwischen Kundenanschlüssen. Auch die Provisionierung wurde abgesichert.

Vodafone bestätigte gegenüber c't, dass alle 2,8 Millionen Breitbandanschlüsse des Unternehmens betroffen waren. Angeblich wurden die Schwachstellen bislang nicht für Angriffe missbraucht. Unsere Frage, wie lange die Lücken in der Infrastruktur klafften, blieb unbeantwortet. Möglicherweise existieren die Probleme schon, seitdem es Internet über Kabel anbietet – also seit über zehn Jahren. Auch wenn Vodafone die Probleme bei Kabel Deutschland in den Griff bekommen hat, ist die Lage weiter problematisch: Es dürfte im Nachhinein schwer nachweisbar sein, dass ein Kunde tatsächlich einen bestimmten Anruf getätigt oder eine bestimmte Datenverbindung aufgebaut hat – schließlich hätten auch Dritte vermutlich über Jahre hinweg auf Anschluss und Modem zugreifen können. Ferner entdeckte c't im Herbst, das zwei verbreitete Zwangsrouter des Providers auch lokal über WLAN angreifbar sind. Das Unternehmen hat daraufhin Sicherheits-Patches an 1,3 Millionen Geräte verteilt.

Alexander Graf plante bei Redaktionsschluss, seine Forschungsergebnisse am 27. Dezember auf dem 32. Chaos Communication Congress (32C3) in Hamburg zu präsentieren. Sobald es von Grafs Vortrag einen Videomitschnitt gibt, werden wir ihn unter dem c't-Link am Ende des Artikels hinterlegen. (rei@ct.de)

c't Mitschnitt 32C3-Vortrag: ct.de/y8q4