Generalschlüssel zum Kabelnetz

AVM entweicht geheimer Krypto-Schlüssel

Im Speicher von Kabel-Fritzboxen wurde ein geheimer Krypto-Schlüssel entdeckt, den eigentlich nur AVM besitzen dürfte. Wer Zugriff darauf hat, kann fremde Anschlüsse übernehmen. Ausbaden müssen das vor allem die Kabel-Provider: Sie arbeiten seit Monaten daran, ihre Netze wieder abzusichern.

Von Ronald Eikenberg

Eine unerwartete Überraschung steckt in vielen Kabel-Fritzboxen: In einem schwer zugänglichen Speicherbereich liegt ein geheimer Krypto-Schlüssel, den eigentlich nur AVM besitzen sollte. Er gehört zum Hersteller-Zertifikat des Berliner Router-Bauers, das für die Absicherung der Kabelnetz-Verbindungen genutzt wird.

Vor einigen Monaten meldete sich der Sicherheitsexperte Joel Stein bei uns, der eine heikle Entdeckung gemacht hatte: Durch einen Trick war es ihm gelungen, einen Telnet-Server auf einer bei eBay erworbenen Kabel-Fritzbox zu starten. Das allein ist schon bemerkenswert: Zwar waren die DSL-Boxen von AVM bis 2015 mit einem Telnet-Server ausgestattet, den man nur noch aktivieren musste; auf den Kabel-Boxen ist Telnet hingegen seit jeher gesperrt. Nachdem ihm dieses Kunststück gelungen war, packte ihn die Neugier. Er sah sich im Dateisystem der Fritzbox um, auf das Nutzer normalerweise keinen Zugriff haben. Dabei stieß er auf die Zertifikate, mit denen die Fritzbox eine verschlüsselte Verbindung zur Gegenstelle des Providers aufbaut. Im Kabelnetz kommt die sogenannte Data Over Cable Service Interface Specification zum Einsatz, kurz DOCSIS. Über das integrierte Kabelmodem spricht die Fritzbox mit dem Cable Modem Termination System (CMTS) in der Kabelkopfstelle des Providers.

Bei diesem Verbindungsaufbau spielen Zertifikate eine entscheidende Rolle: Ein Kabelnetz ist ein Shared Medium, sodass Nachbarn ihren IP-Verkehr gegenseitig lesen könnten. Deshalb kommt zumeist Baseline Privacy Plus (BPI+) zum Einsatz, eine Krypto-Funktion, welche die Verbindung zwischen Fritzbox und CMTS absichert. Jedes Kabelmodem ist hierzu mit einem individuellen Zertifikat ausgestattet, das auf die MAC-Adresse des Modems ausgestellt ist. Damit weist sich das Modem gegenüber dem CMTS als legitim aus. Damit ein böswilliger Nutzer nicht mit einem selbst generierten Zertifikat fremde Anschlüsse übernehmen kann, nutzen die Cable-Modem-Zertifikate die digitale Unterschrift (Signatur) des Geräteherstellers als Sicherheitsmerkmal. Wie bei den SSL-Zertifikaten, die zur verschlüsselten Übertragung von Webseiten genutzt werden, gibt es auch hier eine Zertifikatskette. Die oberste Instanz, welche die Herstellerzertifikate signiert, ist die „EuroDOCSIS Cable Modem Root CA".

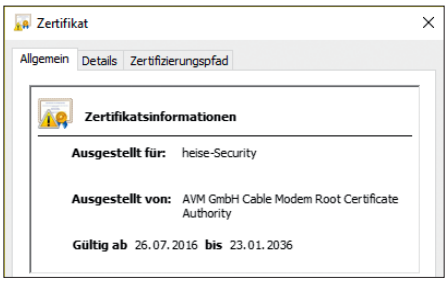
heise Tippgeber

Sie möchten uns anonym einen Hinweis geben? Kontaktieren Sie uns über: **https://heise.de/tippgeber/**

Generalschlüssel gefunden

Im Speicher der Fritzbox liegt aber nicht nur das Schlüsselpaar des individuellen Modem-Zertifikats, sondern auch der geheime Generalschlüssel von AVM, mit dem das Modem-Zertifikat unterschrieben wurde. Das ist fatal, denn mit diesem Schlüssel kann man Zertifikate für beliebige MAC-Adressen im Namen von AVM signieren. Wer böse Absichten hegt, kann sich mit einem solchen Zertifikat im Namen eines anderen Kunden beim Provider anmelden und dessen Anschluss übernehmen, um auf fremde Rechnung und mit fremder Identität auf das Internet zuzugreifen. Uns wurde ein digitales Zertifikat zugespielt, das mit dem geheimen AVM-Schlüssel signiert wurde. Statt einer MAC-Adresse enthält es die Zeichenfolge „heise-Security". Es belegt, dass man den AVM-Schlüssel tatsächlich als kompromittiert betrachten muss.

In Foren stießen wir auf Hinweise darauf, dass AVM offenbar bereits damit



Uns wurde ein Zertifikat mit der digitalen Signatur von AVM zugespielt, das es nicht geben dürfte. Das ist der Beweis dafür, dass der geheime Krypto-Schlüssel des Herstellers kompromittiert ist.

begonnen hatte, das Zertifikat gegen ein neues auszutauschen. Allerdings wussten die Forenteilnehmer zu diesem Zeitpunkt offenbar noch nicht, warum: Sie beklagten sich lediglich darüber, dass einige Kabel-Fritzboxen den Dienst verweigerten und suchten nach Lösungen. Bei den betroffenen Geräten handelt es sich offenbar um Router, die noch nicht mit dem neuen Zertifikat ausgestattet waren; der Provider hatte aber seinerseits das alte bereits gesperrt. Damit das neue Zertifikat auf alte Boxen kommt, müssen die Provider die Installation anstoßen – und das tun sie in der Regel nur bei den Miet-Routern, die sie fernkonfigurieren dürfen. Sobald ein Provider das kompromittierte Zertifikat in seinem CMTS blockiert, kommen Fritzboxen mit dem alten Zertifikat nicht mehr ins Netz. Sie können weder das neue Zertifikat beziehen noch kann es der Nutzer nachrüsten, da es bei den Kabel-Boxen aus Provider-Beständen nicht vorgesehen ist, händisch Updates zu installieren. Offenbar bestückt AVM seit Herbst 2015 neu ausgelieferte Fritzboxen sowohl mit dem neuen als auch mit dem alten Zertifikat.

AVM reagiert

Nachdem wir den Sachverhalt geklärt hatten, baten wir AVM bereits Ende August um Stellungnahme. Das Unternehmen erklärte, dass der „Anlass für den Zertifikatswechsel die Vermutung war, dass ein Zertifikat nicht mehr vertrauenswürdig sein könnte". Es gebe kein reales Sicherheitsproblem, da ein Zertifikatsmissbrauch „netzseitig" erkannt und verhindert werden könne. Woran ein Provider einen Missbrauch mit einem Zertifikat erkennen soll, das eine gültige Herstellersignatur trägt, erklärte das Unternehmen nicht. Obwohl das Zertifikat offensichtlich kompromittiert ist, hatten laut AVM zum Redaktionsschluss noch nicht alle Provider den Wechsel vollzogen – und das über zwei Monate nach unserer ersten Kontaktaufnahme. Weitere Hintergründe möchte AVM erst liefern, wenn alle Provider reagiert haben. So bleibt uns das Unternehmen bisher unter anderem eine Antwort auf die Frage schuldig, wie und warum der geheime Hersteller-Schlüssel überhaupt auf die Fritzboxen kam.

Bei uns meldete sich zwischenzeitlich ein Insider aus dem Dunstkreis der Provider und beklagte, dass AVM die Tragweite des Problems nicht kommuniziert habe. Der Router-Hersteller soll lediglich einen Zertifikatstausch empfohlen haben. Dass der alte Schlüssel kompromittiert wurde, erfuhr unser Kontakt nur durch Zufall. Diese Darstellung könnte erklären, warum sich einige Provider so viel Zeit mit dem Wechsel lassen, etwa um das neue Zertifikat huckepack mit dem nächsten Firmware-Update auszuliefern. Jeder Eingriff bedeutet ein gewisses Ausfallrisiko.

(rei@ct.de) c't