Tages-Anzeiger

ETH-Forscher hacken Handynetz der Zukunft

Swisscom, Sunrise und Salt lancieren 5G bereits 2019. Dabei weist das Handynetz Sicherheitslücken auf, die vor der Einführung nicht behoben werden können.

Wie sicher sind sensible Daten auf dem Handy? Diese Frage wird die Nutzer auch noch in Zukunft beschäftigen. Foto: Guido Mieth (Getty Images)

Das Handynetzwerk der nächsten Generation muss höchsten Ansprüchen genügen. Es soll mit gigantischen Datenmengen umgehen können und gleichzeitig sicherstellen, dass Handys nicht gehackt werden. Und nicht nur Handys. Heute hängen alle möglichen Gerätschaften am mobilen Datentropf – bald auch solche, die über Leben und Tod entscheiden: selbstfahrende Autos zum Beispiel oder Beatmungsmaschinen für todkranke Patienten.

Die Supertechnologie, die das leisten soll, hat einen Namen: 5G. Alle Schweizer Telecomfirmen haben bereits 5G-Antennen getestet und schwärmen von deren Geschwindigkeit und Sicherheit. Swisscom verspricht, bis 2020 sämtliche Schweizerinnen und Schweizer mit 5G versorgen zu können – mit Ausnahme von ein paar Bewohnerinnen und Bewohnern in entlegenen Alpentälern.

Möglicherweise preschten Swisscom und ihre Konkurrenten zu schnell vor. In einer noch unveröffentlichen Studie, die dieser Zeitung vorliegt, haben Forscher der Zürcher Hochschule ETH aufgezeigt, wie die 5G-Technologie manipuliert werden kann, um sich zum Beispiel Zugriff auf den Standort angeschlossener Handys oder Autos zu verschaffen. Dabei war genau dies das Versprechen von 5G: mit den Spionagelücken aufzuräumen.

Gläserne Handynutzer

Damit sich heute ein Handy ins Mobilfunknetz einwählen kann, müssen sich Gerät und Netzwerk miteinander bekannt machen; das geschieht mittels digitalem Händeschütteln. Nur so können Daten sicher vom Handy des einen Nutzers via Mobilfunknetz auf das Gerät eines anderen Nutzers übermittelt werden.

Dieser komplexe Prozess konnte nie zur vollen Zufriedenheit von Sicherheitsexperten gelöst werden. Mit der richtigen Ausrüstung sind Cyberkriminelle in der Lage, jedes Mobilfunknetz auszutricksen, um die Identität von Mobiltelefonen zu stehlen. Cyberangreifer können so Telefongespräche abhören oder per Handy verschickte E-Mails abfangen. Ein ähnliches Verfahren setzten die kürzlich in der Schweiz aufgeflogenen russischen Spione beim Hacken von WLAN-

Barnaby Skinner
Datenjournalist
@BarJack

Artikel zum Thema

Andere Messmethode - schon wären stärkere Antennen erlaubt

Trotz Bedenken vor möglichen gesundheitlichen Folgen: Nationalräte wollen mit einem Trick die geltenden Strahlenschutzgrenzwerte umgehen. Mehr...
Jon Mettler. 19.04.2018

5G-Pläne von Swisscom & Co. ausgebremst

Strenger Strahlenschutz bei Handy-Antennen: Der Ständerat ist gegen eine Lockerung. Was das bedeutet. Mehr...
Jon Mettler. 06.03.2018

Stationen in einem Lausanner Hotel ein.

Die 5G-Technologie versprach, diese Spionage-Löcher zu stopfen. Doch genau das kann die Technologie offenbar nicht einlösen. Noch immer ist es möglich, gezielt Handynutzer ohne deren Wissen zu orten und auszuspionieren. Zu diesem Schluss kommen die Autoren der Studie. «Es hat sich gezeigt, dass der Standard nicht ausreicht, um alle kritischen Sicherheitsziele zu erreichen», sagt Ralf Sasse, ETH-Forscher und Mitautor der Studie. Es kämen sogar neue Sorgen hinzu: «Bei einer schlechten Implementation ist es möglich, dass Anwenderinnen und Anwendern die Mobilfunknutzung Dritter in Rechnung gestellt werden.» Für viele Privatkunden ist dies die wohl noch gravierendere Sicherheitslücke, als gezielt abgehört zu werden. Wenn es ums Portemonnaie geht, hört der Spass auf – selbst beim Handy.

Die ETH-Autoren machen in der Studie diverse Vorschläge, wie die Lücken gestopft werden könnten. «Das Problem der fingierten Rechnung kann leicht behoben werden», sagt Sasse. Schwerwiegender sei das Problem der unerlaubten Standortabhörung. Sie lasse sich wegen der Architektur von 5G technisch nicht mehr rückgängig machen. Dafür müsse die Netzwerkstruktur von Grund auf neu gebaut werden. Deshalb gilt: Wer sich künftig mit seinem Handy in ein 5G-Netzwerk wählt, muss wohl damit leben, dass Cyberkriminelle unerlaubt Standortdaten aufzeichnen können.

Gerade in Zeiten, in denen russische Spione gezielt Schweizer ausspionieren, keine sehr beruhigende Aussicht. Auch deshalb, weil 5G künftig noch breiter genutzt wird als der aktuelle **Mobilfunk**. Die Telecomfirma Sunrise glaubt, die Datenverbindung sei so zuverlässig, dass Privatkunden künftig auf die stationäre Internetanbindung verzichten könnten.

Die Swisscom sieht bei den Geschäftskunden am meisten Potenzial. Sie arbeitet in einem Pilotprojekt mit der Medizintechnikfirma Ypsomed in Burgdorf BE daran, ganze Produktionslinien per Mobilfunk zu steuern.

Kein Aufschub für 5G

Die Firma Salt sagt, sie werde 5G nicht einführen, sollte die Technologie unsicher sein. Sunrise setzt auf einen abweichenden Standard von 5G, der von den neu entdeckten ETH-Sicherheitslücken nicht betroffen sein soll. Und die Swisscom wies darauf hin, dass die ETH-Studienresultate auf Annahmen basierten, die im Feld nicht validiert seien. Ausserdem leiste ihr 5G-Lieferant, die Netzwerkfirma Ericsson, einen aktiven Beitrag zur global organisierten Arbeitsgruppe 3rd Generation Partnership Project (3PGG). Die 3PGG mit Sitz in Südfrankreich sorgt dafür, dass Mobilfunknetze weltweit die gleichen Sicherheitsstandards erfüllen.

Ebendiese Arbeitsgruppe haben die ETH-Studienautoren schon im August über die Sicherheitslücken informiert. Die 3PGG bestätigt, dass die ETH zu Recht darauf hingewiesen habe. Teilweise seien die Probleme bereits behoben. Allerdings nicht alle. Die Analyse dauere noch an, und es sei nicht abzusehen, wann sie abgeschlossen sei. Einen Grund, den kommerziellen Start von 5G hinauszuschieben, erkennt 3PGG trotzdem nicht.

(Redaktion Tamedia)

Erstellt: 09.10.2018, 19:28 Uhr