Süddeutsche.de Digital

20. Februar 2015, 17:13 Mobilfunk-Überwachung

Was Sie über den Sim-Karten-Hack wissen müssen

Britische und amerikanische Geheimdienste haben den größten Sim-Karten-Hersteller der Welt infiltriert. Sie können so unbemerkt Millionen Mobiltelefone überwachen. Wer ist betroffen, wie kann man sich schützen?

Von Simon Hurtz

Britische und amerikanische Geheimdienste haben sich Zugang zum Computernetzwerk des weltweit größten Herstellers von Sim-Karten verschafft. Das Investigativportal *The Intercept* hat Dokumente des Whistleblowers Edward Snowden ausgewertet. Demnach haben NSA und GCHQ bereits 2010 das niederländische Unternehmen Gemalto infiltriert. Die Geheimdienste haben offenbar Verschlüsselungscodes abgefangen, mit deren Hilfe sie sämtliche mobile Kommunikation überwachen können. Gemalto produziert jährlich rund zwei Milliarden Sim-Karten und beliefert alle großen Telekommunikations-Provider, darunter auch die Deutsche Telekom, Vodafone und Telefónica.

Welche Folgen hat der Hack?

"Wir haben erfolgreich mehrere Maschinen verwanzt und glauben, dass wir ihr gesamtes Netzwerk haben". Diese Erfolgsmeldung findet sich in einem geheimen GCHQ-Dokument. Dem "Mobile Handset Exploitation Team", einer gemeinsamen Einheit von GCHQ und NSA, ist es anscheinend gelungen, in großem Umfang Authentifizierungsschlüssel von Gemalto abzugreifen. Diese werden auf der Sim-Karte gespeichert und verschlüsseln die Übertragung zwischen Handy und Provider. Wer die Codes kennt, kann verschlüsselte Kommunikation im Klartext mitschneiden, selbst wenn die bisher als relativ sicher geltenden Mobilfunkstandards LTE oder UMTS verwendet werden. Die Späh-Attacken hinterlassen keine Spuren und können weder von Providern noch von Kunden nachvollzogen werden. Das sei "der Todesstoß für mobile Verschlüsselung", sagte ein Kryptographie-Spezialist *The Intercept*.

Wie reagiert Gemalto?

Paul Beverly, der stellvertretende Vorsitzende von Gemalto, sagte *The Intercept*, er

sei beunruhigt und sehr besorgt. Das Unternehmen selbst stand für Rückfragen nicht zu Verfügung, da derzeit alle Ressourcen in die Aufklärung fließen würden. Man habe keinerlei Informationen über einen möglichen Angriff gehabt und könne den Bericht bislang nicht bestätigen.

Wer ist davon betroffen?

Womöglich wurden noch andere Sim-Karten-Hersteller ausspioniert. In den Unterlagen des GCHQ heißt es, dass auch Giesecke & Devrient, ein deutscher Konkurrent von Gemalto ins Visier genommen worden sei. Dort gebe es bislang allerdings keine Anzeichen für eine Infiltrierung durch ausländische Geheimdienste, sagte ein Sprecher der *Süddeutschen Zeitung*. Man habe alle möglichen Sicherheitsmaßnahmen getroffen. Die Verschlüsselungscodes würden von Rechnern erzeugt, die nicht ans Internet angeschlossen seien.

Was bedeutet das für deutsche Kunden?

Fast alle Mobilfunk-Anbieter beziehen ihre Sim-Karten von mehreren Herstellern. Sämtliche großen deutschen und amerikanischen Provider kaufen auch bei Gemalto. Sprecher von Vodafone und Telefónica bezeichneten den Hack als "branchenweites Problem", zu dem allerdings noch keine weiteren Informationen oder Details vorliegen würden. Die Deutsche Telekom forderte schnelle Aufklärung von Gemalto und gab an, den von Niederländern genutzten Verschlüsselungsalgorithmus bei ihren eigenen Karten abgeändert zu haben. Bisher würden keine Erkenntnisse vorliegen, dass dieser zusätzliche Schutzmechanismus ebenfalls kompromittiert wurde. Ausschließen ließe sich das aber nicht. Potenziell ist also jeder betroffen, der ein Mobiltelefon mit einer Sim-Karte nutzt.

Was ist noch unklar?

Die Dimension der Späh-Attacke. Aus den Dokumenten geht nur hervor, dass Anfang des Jahres 2010 innerhalb von drei Monaten mehrere Millionen Schlüssel für Sim-Karten in Mobiltelefonen erbeutet wurden. Die von Gemalto produzierten Smartcard-Chips werden aber auch in elektronischen Personalausweisen, Bank- und Kreditkarten oder Tan-Generatoren für Online-Banking eingebaut. Laut *The Intercept* ist es bislang unklar, ob GCHQ und NSA auch Zugriff auf Schlüssel für diese Produkte erhalten habe. Das Bundesamt für Sicherheit in der Informationstechnik sieht die Sicherheit von elektronischen Personalausweisen und Reisepässen aber nicht in Gefahr.

Wie können sich Kunden schützen?

Die gute Nachricht: Mobilfunk-Nutzer sind nicht wehrlos. Selbst wenn die Sim-Verschlüsselung der Hersteller geknackt wurde, bleibt die Verschlüsselung

durch Kommunikations-Software bestehen. Die meisten großen E-Mail-Provider verwenden SSL/TLS-Verschlüsselung, die zwar auch geknackt werden kann, aber immerhin einen zusätzlichen Schutz bietet; noch sicherer ist die E-Mail-Verschlüsselung durch die Software PGP. Die besseren Alternativen zur Kommunikation per SMS sind Apps wie Textsecure, Telegram, Redphone oder Threema.