Millionen SIM-Karten sind nicht sicher

21. Juli 2013

zeit.de

Viele SIM-Karten nutzen einen veralteten Verschlüsselungsstandard. Sie können per SMS aus der Ferne gehackt werden, ohne dass der Handy-Besitzer es merkt.

SIM-Karten sind so etwas wie der Tresor unserer Identität. Je mehr Dinge Mobiltelefone können und je verbreiteter sie sind, desto mehr übernehmen sie für uns die Funktion, unser Leben zu bewahren und zu verwalten. Geldbörse, Passwortspeicher, Nahverkehrpass, Zugangsberechtigung – vieles, wofür es bislang einzelne Plastikkarten oder Bargeld brauchte, geht inzwischen mit dem Mobiltelefon.

Dessen Sicherheitszentrale ist die SIM. Denn die kleine Karte sorgt dafür, dass sich der Besitzer des Telefons im Mobilfunknetz identifizieren kann. Sie speichert die Schlüssel, um die Identität zu belegen und um sämtliche Kommunikation zu chiffrieren. Leider ist dieser Tresor häufig nur mit einem ziemlich billigen Schloss verriegelt, sagt Karsten Nohl.

Nohl ist nicht irgendein Hacker, der über ein Problem gestolpert ist. Nohl ist Kryptograph, hat einen Doktortitel in Computer Engineering und beschäftigt sich seit vielen Jahren mit der Verschlüsselung bei Mobilfunkverbindungen.

Er war beteiligt an dem Projekt, das DECT gehackt hat – das sind die schnurlosen Telefone, die inzwischen in fast jedem Haushalt stehen; er hat die Verschlüsselung von GSM geknackt – das ist der Standard der zweiten Generation, mit dem Handys telefonierten, bevor neuere wie 3G (dritte Generation) und LTE (vierte Generation) entwickelt wurden. Und er hat 2009 GPRS aufgebrochen – die sogenannte Paketvermittlung, mit der Handys Daten übertragen.

Veralteter Schlüssel

Nun hat sich Nohl zusammen mit mehreren Mitarbeitern seiner Firma Security Research Labs die SIM-Karten vorgenommen. "Eigentlich hatten wir gedacht, dass SIM vergleichsweise sicher sind und gute Verschlüsselung nutzen. Zumindest waren bisher keine Sicherheitslücken bekannt", sagt er. Daher seien sie selbst überrascht gewesen über die Probleme, die sie entdeckten.

Es sind vor allem zwei: Erstens nutzen viele – und viele meint viele Millionen SIM-Karten weltweit – einen veralteten Verschlüsselungsstandard namens DES. DES stammt aus den siebziger Jahren und gilt schon lange nicht mehr als sicher. Dank seines kurzen Schlüssels von nur 56 Bit Länge kann er mit vertretbarem Aufwand geknackt werden. Und zweitens ist auf vielen Karten die Software so schlampig implementiert, dass sie gehackt werden kann.

Die Folge: Nohl ist in der Lage, in manchen Fällen mit nur einer SMS, die er an ein Telefon verschickt, dieses zu kapern und komplett zu übernehmen. Er braucht dazu lediglich die Mobilfunknummer des Nutzers und etwas Glück, dass dessen SIM die veraltete

Verschlüsselung verwendet. Ohne dass der Nutzer es merkt, kann der Angreifer dann von dem fremden Telefon aus SMS verschicken, Anrufe auf eine neue Nummer umleiten oder gar Gespräche mithören. Er kann aus der Ferne die Karte klonen und mit dem Klon auf Kosten des Nutzers telefonieren.

Das ist längst nicht der erste Hack von Mobiltelefonen. Vor allem für Androidgeräte existieren Viren, um die Telefone zu übernehmen. Doch braucht es, damit diese Angriffe funktionieren, die Mitarbeit des Telefonbesitzers. Er muss mindestens einmal eine Mail öffnen oder eine Eingabe bestätigen.

Der Angriff von Nohl hingegen hat eine neue Qualität. Bei dem SIM-Hack muss der Inhaber des Handys selbst nichts tun, ja er bemerkt ihn nicht einmal. "Die SIM bietet einen ähnlich tiefen Zugriff auf ein Telefon wie ein Virus, der Angriff mit einem Virus ist aber viel leichter zu entdecken", sagt Nohl.