

13.10.2011. Der Standard

Sicherheitsrisiko: Telefonieren am Handy

Österreichs Mobilfunknetze sind nur mangelhaft gegen Abhören und Datenklau geschützt

Die Sicherheit der österreichischen Mobilfunknetze liegt europaweit im unteren Mittelfeld. Zu diesem Fazit kommt Karsten Nohl angesichts ihm vorliegender Ergebnisse von Test-Hacks in drei österreichischen Mobilfunknetzen aus den vergangenen Tagen. Nohl, von Security Research Labs, der sich seit einigen Jahren als GSM-Hacker und technischer Experte intensiv mit den GSM-Sicherheitsstandards beschäftigt, stellt fest, dass die analysierten Netze von A1/Mobilkom, T-Mobile Österreich und Orange auf die gleiche überholte Technologiebasis wie viele andere Mobilfunkbetreiber weltweit setzten: „Zusätzliche Schutzmaßnahmen, wie sie an vielen Stellen in Europa zurzeit ausgerollt werden, sind in Österreich nicht zu finden.“ Nohl stellt allen drei Betreibern ein schlechtes Zeugnis aus; es gebe keinen Marktführer in punkto Sicherheit. „Die österreichischen Netze zeigen noch keine Anzeichen der technischen Härtung, nicht einmal bei schnell umgesetzten Sicherheitsfixes, die der Dachverband der Netzbetreiber seit mehreren Jahren propagiert“, sagt Nohl.

Die Sicherheitslücke ist seit Jahren bekannt

Seit längerem ist bekannt, dass die Übermittlung und Verschlüsselung von Handytelefonaten zu knacken ist. Im Dezember 2009 veröffentlichte Karsten Nohl auf der Tagung des Chaos Computers Clubs (CCC) erste Resultate eines Hacks, mit dem er die Sicherheit des GSM-Netzes testete. Das Ergebnis: Mit wenig technischem Aufwand ist es möglich, eine bestehende Mobilfunktelefonverbindung mitzuhören und die Gesprächsdaten zu entschlüsseln. Die GSM Association (GSMA), die weltweite Vereinigung der Mobilfunkanbieter, bestritt damals in einer ersten Reaktion, dass so ein Angriff möglich sei. Nach mehreren veröffentlichten Test in den vergangenen Jahren, gesteht die GSMA die technische Machbarkeit zu. GSM-Sniffing stelle aber keine Gefährdung dar: „Das Abhören von GSM ist immer noch ziemlich schwierig und benötigt weitreichendes, technisches Know-how (und kriminelle Absicht). Wir haben keinen Hinweis darauf, dass es in wirklichen Netzen gegen wirkliche Nutzer angewendet wird“, sagt James Moran, Sicherheitschef der GSMA. Trotzdem weist er GSM-Kunden auf mögliche Gefährdungsrisiken hin, wenn sie sensible Daten über Mobilfunknetze austauschen.

Veraltete Standards

Das grundlegende Problem ist der verwendete Verschlüsselungsstandard A5/1 des GSM-Mobilfunknetzes, der aus den 90er Jahren stammt. Dieser Standard hielt den Angriffen der Hacker nicht lange stand. Inzwischen bedarf es zwar einigen Fachwissens, aber relativ wenig an technischer Ausstattung, um Handytelefonate abzuhören. Trotzdem wird der bessere A5/3-Standard, der die Sicherheit des Mobilfunks verbessern könnte, nur langsam eingeführt. Die GSMA begründet das mit langen Endwicklungszeiten, Planungszeiten der Roadmaps für Produkteinführungen und Testphasen. Endgültige Abhilfe wird wohl erst der vollständige Umstieg auf den 3G-Standard/UMTS

beziehungsweise den 4G-Standard/LTE schaffen. Ob und wann diese Standards allerdings flächendeckend auch außerhalb von Großstädten verfügbar sein werden, ist fraglich.

Möglichkeiten des Missbrauches

Das besondere an GSM-Sniffing sei, dass es nicht nachweisbar ist, weil es keine Spuren hinterlässt, sagt Nohl. Ihn treibt nicht die wirtschaftliche Verwertung von gehackten Daten an, sondern das Offenlegen von Schwachstellen der Übertragungsstandards. Die Möglichkeiten für kriminelle Aktivitäten mit dem relativ kostengünstigen GSM-Sniffing sind weitreichend und fangen beim Ausspähen von Geschäfts- oder Börseninformationen erst an: „Neben dieser klassischen Industriespionage schafft das GSM-Belauschen sicher auch Anreize für Stalker, Einbrecher, Privatdetektive, und andere graue Gestalten“, sagt Nohl.

Unerklärliche Kosten auf der Telefonrechnung

Ein weiteres Risiko, das vielen nicht bewusst, besteht für Nohl in der Möglichkeit der missbräuchlichen Verwendung von Nummern für Gespräche und Kostenabrechnungen. In fast allen getesteten Mobilfunknetzen finde eine Senderauthentifizierung nur unregelmäßig und nicht vor jedem Gespräch statt. Einzige Ausnahme in Österreich war laut Angaben von Nohl das Netz von T-Mobile, in dem vor dem Versand jeder SMS die Identität des Senders abgefragt wird. Ohne Authentifizierung kann ein Angreifer mit den Authentifizierungsdaten - die er mittels GSM-Sniffing herausfinden kann - die Telefonnummer des abgehörten Teilnehmers verwenden und auf dessen Kosten telefonieren. Unerklärliche Anrufe zu Mehrwertnummern auf der Telefonrechnung könnten eine Folge dieses Missbrauches sein. Möglich sind aber auch beispielsweise Belästigungsanrufe oder Bombendrohungen unter der Verwendung fremder Mobilfunknummern.

Mit relativ einfachen Mitteln wie einer Authentifizierung vor jedem Telefongespräch wäre es den Mobilfunkbetreibern möglich, solche Sicherheitslücke zu schließen. Weitere Möglichkeiten, um GSM-Sniffing einzuschränken, wären die Übernahme der neuen technischen Änderungen des GSM-Standards, die 2008 eingeführt wurden. „Diese Maßnahmen können schnell und kurzfristig umgesetzt werden, ohne die Versorgung des Kunden zu unterbrechen, um die Risiken eines Angriffes auszuschließen“, sagt James Moran von der GSMA.

Der nächste Schritt: mobile Datenübertragung

Für die mobile Datenübertragung wird der Umstieg auf Long Term Evolution (LTE), die vierte Generation des Mobilfunks, einen wichtigen Schritt hin zu mehr Sicherheit bedeuten. James Moran setzt auf diesen Standard: „So wie UMTS das GSM-Netz verbessert hat, steht LTE für eine weitere Verbesserung von UMTS.“ Der Druck auf die Mobilfunkbetreiber ist groß: Im August dieses Jahres gelang es Karsten Nohl, den GPRS-Standard zu entschlüsseln und mobile Datenübertragungen mitzuschneiden.

<http://derstandard.at/1318461131886/Analyse-Sicherheitsrisiko-Telefonieren-am-Handy>