

29.12.2010

Handy-Telefonate mit einfachen Mitteln abhören

Forscher demonstrieren günstige Abhörmethode mit alten Mobiltelefonen

Die Forscher Karsten Nohl und Sylvain Munaut haben auf dem Hackerkongress des Chaos Computer Clubs [27C3](#) erfolgreich [demonstriert](#), wie man mit günstigen Mitteln Gespräche über GSM-Mobilfunknetze abhören und mitschneiden kann. Den Forschern nach benötigt es dafür lediglich die Telefonnummer der ins Visier genommenen Zielperson, eines gewöhnlichen Handys sowie kostenlos im Internet verfügbarer Open-Source-Software. Vergleichbare Profigeräte für Behörden und die Polizei würden mit 40.000 bis 50.000 Euro zu Buche schlagen.

Heimliche Lokalisierung

Bevor der Lauschangriff stattfinden kann, müsse den Experten nach zunächst die Zielperson bzw. dessen Handy lokalisiert werden. Dies sei mangels entsprechender Schutzvorrichtungen der Mobilfunknetzbetreiber möglich. Ein Angreifer könne über so genannte stille SMS an das abzuhörende Telefon, von denen die Zielperson nichts mitbekommt, oder alternativ defekte Kurzmitteilungen sukzessive auf die Mobilfunkzelle genau den Standort ausmachen. So erfahre der Späher nicht nur die genaue Position sondern mit der IMSI (International Mobile Subscriber Identity) und der TMSI (Temporary Mobile Subscriber Identity) des Nutzers auch zwei weitere wesentliche Informationen zur Filterung der Daten aus dem Mobilfunknetz.

Verschlüsselung aufgehoben

Wie berichtet, stellt die Verschlüsselung des GSM-Netzes dann keine große Hürde mehr dar. Das Handy, welches zum Belauschen eingesetzt wird, muss mit einer speziellen aber frei verfügbaren Firmware bespielt, vom Uplink-Filter befreit und zur effektiven Auswertung der Daten und Aufzeichnung der Telekommunikation mit einem Notebook verbunden werden.

Ogleich dies natürlich alles spezielles Know-How benötige, ermögliche Nohls und Munauts Methode eine äußerst effektive Alternative zu Profigeräten. Um dies zu beweisen, demonstrieren die Forscher einen Abhörvorgang in einem bestehenden GSM-Netz eines bekannten Mobilfunkanbieters.

Schutz

Den Experten nach seien die Mobilfunkbetreiber angehalten, Vorkehrungen zu treffen. Unter anderem könnte man das Risiko schon durch die häufigere Erneuerung der Netz-Schlüssel eindämmen. Handynutzer könnten ihr Mobiltelefon zum Schutz auf reine 3G-Telefonie umstellen. Dies ist allerdings nur in seltenen Fällen möglich bzw. ob der teils lückenhaften 3G-Netzabdeckung nur bedingt praktikabel. (zw)

<http://derstandard.at/1293369650500/27C3-Handy-Telefonate-mit-einfachen-Mitteln-abhoeren>

Zugriff am 15.04.2011