

07.02.2011. Zeit Online

Jede SMS kann mitgelesen werden

Handys lassen sich abhören, der Standard GSM wurde geknackt. Doch Mobilfunkanbieter sehen keine Sicherheitsmängel. Wie Hacker unsere Mobilfunkgeräte sicher machen wollen.

Das weltweite Mobilfunksystem ist veraltet, und wer telefoniert, dem kann jeder zuhören, zumindest im Prinzip. Das sagt Karsten Nohl, Kryptograf, Hacker, der Sperrcodes knackt und Fehler findet. Um Nutzer zu warnen – und Anbieter.

Plötzlich wird es ganz still im Saal. Gebannt verfolgen etwa tausend Zuschauer, wie zwei junge Männer an einem Tisch sitzen, vor sich einen Laptop und ein paar Mobiltelefone. Eine halbe Stunde lang haben sie ihr Vorhaben erklärt. Mehr als vier alte Handys, Stückpreis zehn Euro, und ein gängiger Computer mit frei zugänglicher Software sei nicht nötig, haben sie gesagt. Schon könne man sich eine eigene Sende- und Empfangsstation bauen und damit jedes Mobilfunkgespräch und jede SMS-Nachricht abhören und entschlüsseln.

Berlin, Kongresszentrum am Alexanderplatz, Ende Dezember. Der Computerwissenschaftler Karsten Nohl und sein belgischer Kollege Sylvain Munaut wollen demonstrieren, wie leicht sich über Handy geführte Telefongespräche abhören lassen.

Sie haben die Arbeitsweise von "Base Stations", "Frequency Hopping" und all den anderen technischen Elementen, mit denen das Mobilfunksystem arbeitet, erklärt. Nun folgt der praktische Teil. Zunächst führen sie vom einen Ende der Bühne zum anderen ein kurzes Telefonat miteinander, dann schweigen sie. Nur auf der Leinwand hinter ihnen erscheinen Hunderte von Datenzeilen in rasender Folge, deren Bedeutung sich bei diesem Chaos Communication Congress, der jährlichen Versammlung der globalen Hackergemeinde, nur den Insidern erschließt. Die Spannung steigt. Dann kommt die Erlösung.

"Hello, Karsten here, how are you?", tönt es durch die Lautsprecher, und eine weitere Stimme antwortet, "Hi, I am fine", der Beginn des kurz zuvor geführten Gesprächs. Der Rest ist nicht mehr zu verstehen. Brausend erhebt sich der Applaus, minutenlang. Bescheiden senkt Nohl den Kopf und murmelt ein "Thank you" ins Mikrofon. Aber ein Lächeln kann er sich nicht verkneifen.

Denn er hat demonstriert, dass eines der wichtigsten technischen Systeme der Welt gravierende Schwächen hat und hoffnungslos veraltet ist: Das "Global System for Mobile Communications", kurz GSM. Mehr als vier Milliarden Menschen weltweit kommunizieren mit ihren Handys über das System. Und jeder kann ihnen im Prinzip dabei zuhören.

Ob bei Geschäftsleuten oder Politikern, Staatsanwälten oder Polizisten, die höchst vertrauliche Informationen über ihre Mobiltelefone austauschen. Sie alle mögen darauf vertrauen, dass ein Lauschangriff allenfalls von amtlichen Ermittlern mit staatlicher Erlaubnis über Anschlussstellen in den Netzwerkzentralen erfolgt. Doch das große Lauschen ist offenkundig auch ganz anderen Akteuren möglich: privaten Detekteien, Wettbewerbern und Kriminellen.

Zwar kritisieren Fachleute schon seit mehr als zehn Jahren, dass die GSM-Technik unsicher sei. Doch stets behaupteten Hersteller und Netzbetreiber, das sei übertrieben. So erklärte eine Sprecherin des Weltverbandes der Mobilfunkindustrie (GSMA) noch im Dezember 2009, das Entschlüsseln des Mobilfunkcodes sei nur "theoretisch möglich, aber praktisch unwahrscheinlich". So war die Demonstration des Gegenteils beim Hackerkongress eine weitere Etappe in einem seit langem geführten Streit. Und sie zeigt, wozu "Hacken" gut ist.

Während Computertechnologien im Alltag vieler Menschen immer wichtiger werden, sparen Hersteller und Betreiber bei der Sicherheit und operieren mit veralteter oder ungeprüfter Software, die für die Nutzer erhebliche Risiken birgt. Diese Praxis gerät jedoch immer stärker unter Druck. Denn die weltweit vernetzte Gemeinschaft aus unabhängigen Programmierern und Sicherheitsforschern, die dagegen vorgehen, wächst beständig. Sie begeistern sich für die Technik, aber sie wollen sich den Geschäftsstrategien der Konzerne nicht unterwerfen und fordern die Offenlegung und Prüfung von deren Software. Darum knacken sie geheime Sperrcodes, weisen Sicherheitslücken nach, schreiben bessere Software, die offen zugänglich und überprüfbar ist (Open-Source). So formieren sie eine Art Gegenkultur des Computerzeitalters.

Zu der zählt auch Karsten Nohl, der so hartnäckig gegen die Nachlässigkeit der Mobilfunkbetreiber zu Felde zieht. Gerade 29 Jahre alt und ausgestattet mit einem Diplom in Elektrotechnik sowie einem amerikanischen Dokortitel der Computerwissenschaft, ist Nohl ein gefragter Experte für die Sicherheit von chipgesteuerten Zugangskarten. Seine Wohnung in Prenzlauer Berg steht voll mit der nötigen Ausrüstung – vom hochauflösenden Mikroskop für die Analyse der Mikrochips bis zum Hochleistungsrechner für komplexe Verschlüsselungsmathematik.

SMS-Software gefährlich manipulierbar

Beim Beratungskonzern McKinsey hielt es ihn nur ein Jahr, bevor er sich selbstständig machte. Seitdem ist er gleich mit mehreren Dax-Konzernen im Geschäft, die für die Sicherheit ihrer Zugangssysteme lieber auf Berater vertrauen, die nicht von den Herstellern bezahlt werden.

Es gelte, so beschreibt Nohl sein Motiv, die "Alltagstechnik" sicher zu machen. Über deren Gefahren seien die meist "unbedarften Nutzer" viel zu wenig informiert, "oft auch deshalb, weil die Produzenten oder Betreiber selbst nicht genau Bescheid" wüssten. Daher verstehe er sich als "Botschafter zwischen den Welten" der Wirtschaftslenker auf der einen und der Hackercommunity auf der anderen Seite.

Dieses Zusammenspiel ist bei der Entwicklung von Internet und den zugehörigen Rechnern schon seit vielen Jahren gang und gäbe. Auch dort sind es fast immer freie Programmierer, die Sicherheitslücken aufdecken und so dazu beitragen, das Netz sicherer zu machen. Über Smartphones und tragbare Rechner wird aber nun auch das Mobilfunksystem zusehends selbst zu einem Teil des World Wide Web. Darum ist es keineswegs Zufall, dass Hacker aller Länder jetzt auch diese Technologie mit aller Kraft genauer unter die Lupe nehmen.

Doch anders als bei den Programmen, mit denen das Internet läuft, hält die beteiligte Industrie von Apple bis Vodafone den Code für die im Mobilfunk angewandte Software bis

heute unter Verschluss und verhindert so deren Fortentwicklung. Das halten Kritiker wie Nohl für unverantwortlich. Denn damit zementieren die Netzbetreiber und ihre Lieferanten eine Struktur, die in den achtziger Jahren des vergangenen Jahrhunderts geschaffen wurde und die längst nicht mehr den heutigen Anforderungen entspricht.

Damals waren es noch die staatlichen Telefongesellschaften Europas, die miteinander den GSM-Standard vereinbarten, der später weltweite Verbreitung fand. Seinerzeit schien ausgeschlossen, dass irgendwer außerhalb dieser geschlossenen Gesellschaft mit eigenen Sendestationen in dieses Netz eindringen könnte. Zudem stand die Politik noch ganz im Bann des Kalten Krieges. Sichere Verschlüsselungsmethoden galten als militärisches Geheimnis und durften keinesfalls Anwendung im zivilen Leben finden. Doch was damals seine Logik hatte, macht das GSM-Netz heute höchst anfällig.

Nicht nur ist die Verschlüsselung leicht zu brechen. Als weitere Schwäche gilt der Umstand, dass die Sendestationen sich gegenüber den Handgeräten nicht "authentifizieren", sich also nicht mit einem vorgegebenen Code "ausweisen" müssen. Darum verbinden sich die Telefone auch mit "gefälschten" Basisstationen, die gar nicht zum offiziellen Netz zählen.

Auch die Software für das Versenden der Kurznachrichten ist primitiv und gefährlich manipulierbar. All das kritisieren Fachleute seit vielen Jahren. Und rein technisch wären alle diese Mängel auch leicht zu beheben. Doch die Mobilfunkindustrie scheut die Kosten und verschanzt sich hinter ihrem Softwaregeheimnis.

<http://www.zeit.de/digital/mobil/2011-02/Handy-Hacker-Mobilfunk>