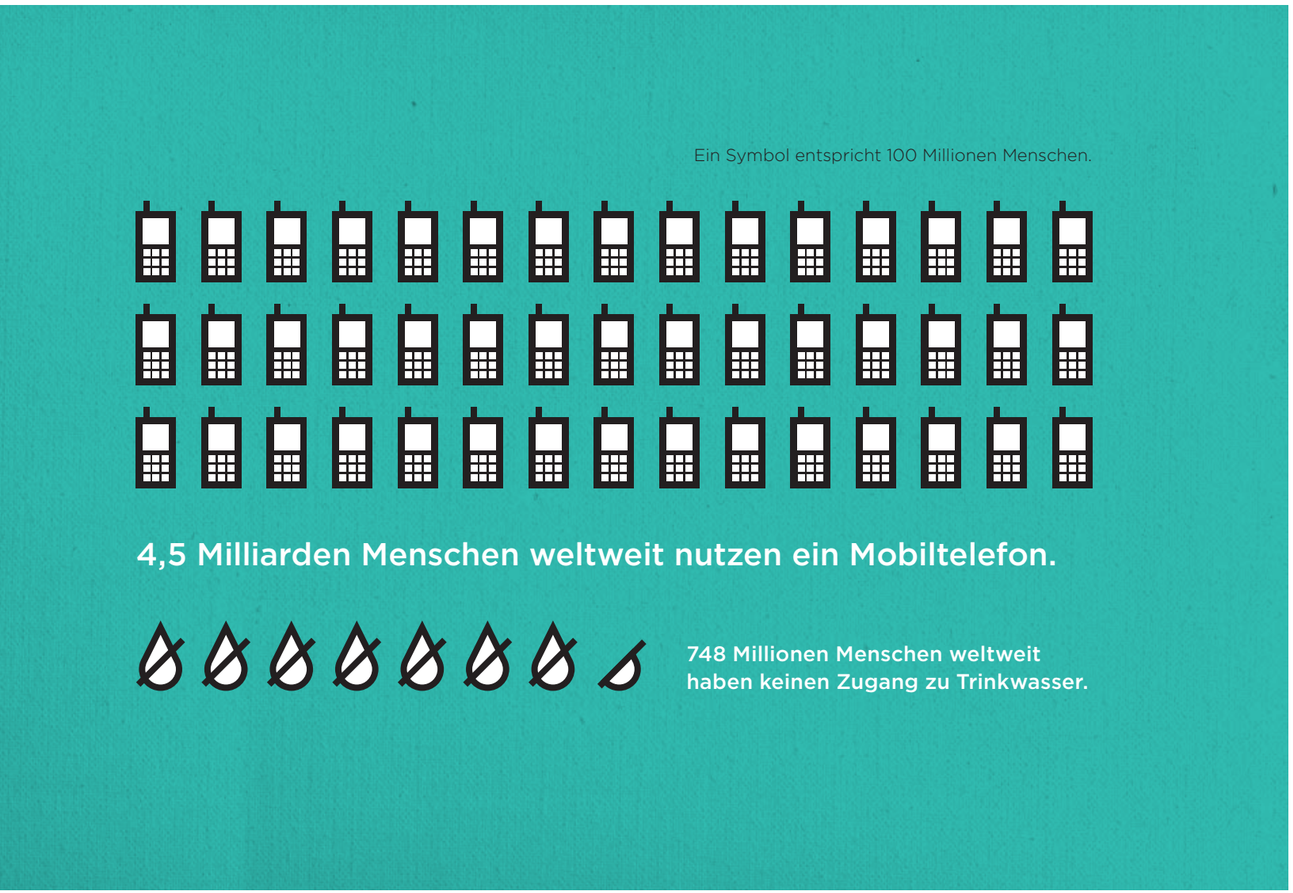
Schützt die Handys vor den Lauschern!

Mobiltelefonieren ist zum Grundbedürfnis geworden. Höchste Zeit, dass abhörsichere Handys zum Standard werden. Warum ist das eigentlich so schwer?

Text **Niels Boeing** Illustration **Michael Paukner**



Grundbedürfnis Kommunikation Die halbe Welt telefoniert heute mobil. Gut möglich, dass bald mehr Menschen ein Handy haben als Zugang zu Trinkwasser oder ausreichend Nahrung.

Einer ganzen Generation setzte der britische Autor Douglas Adams mit seiner BBC-Radioserie *Per Anhalter durch die Galaxis* einen Floh ins Ohr: Da gab es diesen kleinen, tragbaren Computer, der einem alle Fragen über die Welt beantworten konnte. Ende der siebziger Jahre noch eine Utopie, wurde dieses Gerät knapp drei Jahrzehnte später Realität, und sogar noch besser als bei Adams: Mit dem Smartphone kann man nicht nur das Internet anzapfen, sondern auch telefonieren. 1,8 Milliarden Menschen besitzen inzwischen dieses mobile kleine Wundergerät, im kommenden Jahr werden voraussichtlich eine Milliarde neue Geräte hinzukommen. Gut möglich, dass es in einigen Jahren mehr Smartphones gibt als Menschen mit Zugang zu sauberem Trinkwasser oder genug zu essen.

Die Faszination der totalen Kommunikation, die vom Smartphone ausgeht, hat indes eine dunkle Seite: Jedes Wort kann im Prinzip abgefangen werden und helfen, ein genaues Profil des Nutzers zu erstellen. Dass Telefone abgehört werden, ist an sich nichts Neues. Aber seit den Enthüllungen des Whistleblowers Edward Snowden wissen wir: Das Smartphone macht jeden, der es benutzt, potenziell nackt. Dabei sind es nicht nur Geheimdienste wie die National Security Agency NSA, die Gespräche mithören und Internetdaten aufzeichnen, auch Industriespione und Cyberkriminelle erfreuen sich am Zugriff auf die Geräte. Die IT-Branche reagiert darauf und entdeckt ein neues Produkt: das sichere Smartphone.

Vor einem Jahr bekam die Bundeskanzlerin mit dem SiMKo 3 der Telekom ein abgesichertes Mobiltelefon, das stolze 1700 Euro kostete, das »Merkelphone«. Vor fünf Monaten brachte dann SGP Technologies das »Blackphone« heraus, das erste abhörsichere Smartphone für Normalverbraucher. Es kostet nur ein Drittel so viel wie das Gerät von Angela Merkel und unterscheidet sich äußerlich nicht von üblichen Smartphones. Experten betrachten es als einen ersten Schritt: »Das Blackphone geht in die richtige Richtung, basiert aber immer noch auf dem herkömmlichen System, das eine große Angriffsfläche bietet«, sagt Michael Hohmuth, der mit seiner Firma »Kernkonzept« an der Entwicklung des Merkelphones mitgearbeitet hat.

Das Blackphone ist mit Apps der Firma Silent Circle ausgestattet, die Telefonate und SMS verschlüsseln. Die Apps funktionieren nach demselben Prinzip wie Pretty Good Privacy (PGP), weltweit unter den Mailverschlüsselungssystemen die Nummer eins. Der US-Informatiker Phil Zimmerman, der PGP erstmals 1991 veröffentlichte, ist einer der Gründer von Silent Circle. Eine weitere App namens Disconnect Wireless Security ermöglicht Blackphone-Nutzern, Webseiten und Onlinedienste aufzurufen und dabei möglichst wenig Spuren zu hinterlassen.

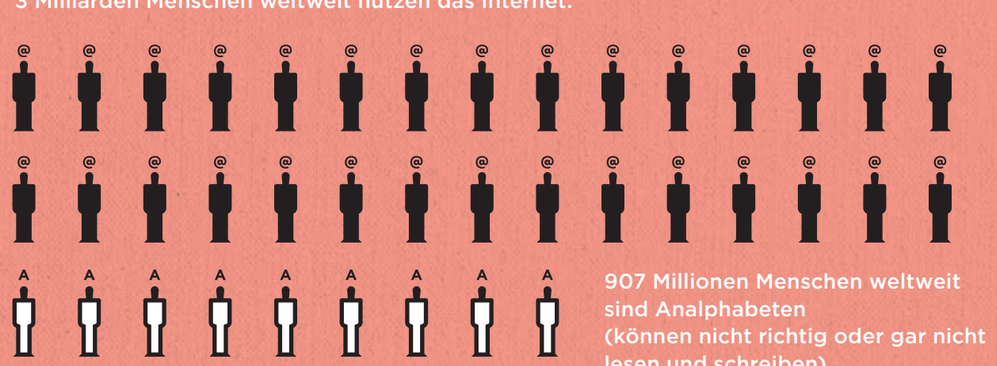
Während die Medien schon von einem »James-Bond-Smartphone« schwärmten, dämpfen Sicherheitsexperten die Euphorie. »Man kann Software nicht mit Software schützen«, sagt Peter Moebius vom Netzbetreiber Orange Communications. Das geringste Problem ist dabei noch, dass die Silent-Circle-App nur dann Lauscher aussperrt, wenn am anderen Ende der Verbindung ebenfalls ein Blackphone-Nutzer sitzt.

Das Problem, Smartphones zu schützen, ist weitaus komplexer. Als in den achtziger Jahren die ersten digitalen Mobilfunknetze nach dem GSM-Standard errichtet wurden, bauten deren Architekten schon Sicherheitsvorkehrungen ein – allerdings mit zwei Schwachstellen. Zwar ist die Datenübertragung zwischen Mobiltelefon und Funkmast verschlüsselt, doch beide müssen sich nicht voreinander authentifizieren. Ein Lauscher kann ein Gerät dazwischenschalten, das dem Telefon vorgaukelt, ein Funkmast zu sein, die Gesprächsdaten mitschneiden und dann an den eigentlichen Funkmast weiterleiten. Das Prinzip nutzt wohl auch das US-Justizministerium seit 2007 mit Cessna-Flugzeugen, die es über amerikanische Großstädte fliegen lässt, um Telefondaten abzugreifen.

Zweiter Knackpunkt: Die Verschlüsselung ist für heutige Computer viel zu schwach. »Mit Angriffen über sogenannte Rainbow Tables können Sie die in wenigen Sekunden knacken«, sagt Antonius Klingler vom Bundesamt für Sicherheit in der Informationstechnik. »Rainbow Tables« wird eine mathematische Struktur genannt, mit der sich einfache Kennwörter oder Schlüssel ermitteln lassen. Moderne Mobilfunknetze verwenden sehr lange Digitalschlüssel. Dadurch ist zwar die Übertragung in der Mobilfunkzelle sicher. Aber hinter dem Funkmast werden die Daten über Internetleitungen weitertransportiert – und »an den Hauptleitungen, den Backbones, sind die Sprachdaten wieder unverschlüsselt«, so Klingler. Die NSA greift bekanntermaßen bei den Betreibern der Backbones Daten ab.

Soll ein Gespräch diskret durchs Netz gehen, muss es zusätzlich zur Transportverschlüsselung in der Mobilfunkzelle eine eigene Verschlüsselung bekommen. So, als ob man Wertsachen nicht einfach in einen Tresor legt, sondern sie erst in einen kleineren Safe steckt, der dann ins Tresorfach kommt. Diese zusätzliche Verschlüsselung besorgen Apps wie Red Phone.

Was aber, wenn der Angreifer das Betriebssystem des Smartphones selbst mit einem eingeschmuggelten Programm kontrolliert? Ein solcher Trojaner könnte das Gespräch direkt am Mikrofon mitschneiden, bevor die Verschlüsselung überhaupt einsetzt, oder er könnte auf den Schlüssel selbst zugreifen. Will man dies verhindern, muss man das System umbauen. Zum Beispiel mithilfe eines sogenannten Mikro-



kerns. »Der klemmt sich zwischen die Hardware und das Betriebssystem«, sagt Michael Hohmuth. Der Mikrokern, den er mitentwickelt hat, steckt auch im Merkelphone. Er wirkt wie eine Brandmauer, mit der in einem militärischen Gebäude die Leitstelle geschützt wäre, wenn ein Feuer die anderen Teile des Gebäudes zerstören würde. Er sorgt auch dafür, dass das Betriebssystem – und ein etwaiger Angreifer – den Schlüssel nie zu Gesicht bekommt.

Einen ähnlichen Ansatz hat der Sicherheitstechnikkonzern Giesecke & Devrient in Zusammenarbeit mit dem Chiphersteller ARM entwickelt. Auf dem Smartphone-Prozessor gibt es eine »vertrauenswürdige Ausführungsumgebung«, TEE genannt. Es ist eine Art Sicherheitszone. »Wenn Sie auf einem TEE-fähigen Smartphone die PIN Ihres Bankkontos eingeben, läuft diese Abfrage nicht im ›normalen‹ Betriebssystem«, sagt Bernhard von Canstein von Giesecke & Devrient. Das verhindert, dass ein Trojaner im Gerät den Touchscreen kapert und das Eintippen der PIN-Zahlen ausspäht. Das TEE-System ist bereits in einigen Samsung-Geräten der Galaxy-Reihe eingebaut.

Aber auch der Schlüssel selbst muss in Sicherheit gebracht werden – am besten mittels Hardware. »Ein Chip ist eine Festung«, sagt von Canstein. Einen solchen Chip hat etwa die Nürnberger Firma Certgate entwickelt. Er sitzt auf einer MicroSD-Karte, die eigentlich ein Speichermedium für Musik und Bilder ist. Man steckt sie in den kleinen Kartenschlitz, den viele Mobiltelefone haben. Mithilfe der »cgCard« lassen sich auch Daten auf dem Smartphone selbst verschlüsseln: E-Mails, SMS oder Notizen, die man nicht in falschen Händen wissen möchte. »Die Karte funktioniert wie eine Wegfahrsperre beim Auto, ohne sie funktioniert fast nichts mehr im Smartphone«, sagt Stefan Schmidt-Egermann von Certgate.

Leider haben auch diese Lösungen zwei Haken. Sie sind noch sehr teuer und schützen nicht vor einer Auswertung der Verbindungsdaten. Denn jeder Mobilfunkbetreiber notiert, um wie viel Uhr wir einen Freund anrufen, von welcher Funkzelle aus wir dies tun und wie die Nummern der beiden Smartphones lauten, die da miteinander kommunizieren. Die NSA greift diese Verbindungsdaten bei den Netzbetreibern ab. Allein aus Uhrzeiten und Standorten lässt sich so der Weg eines Nutzers durch die Stadt nachzeichnen – Tag für Tag, Woche für Woche. Die Privatadresse, der Arbeitsplatz, die besuchten Restaurants und Geschäfte können schon Beruf und Einkommenshöhe verraten. Firmen wie Sense Networks nutzen dieses »Reality Mining«, um Werbung zu platzieren. Die NSA setzt es ein, um Komplizen eines Terrorverdächtigen zu finden: Ihm könnte jenes Gerät gehören, das in den Bewegungskarten immer wieder in dessen Nähe auftaucht.

Virtuelle Tunnel und Brandmauern sollen den Handynutzern ihre Privatsphäre zurückgeben

Eine letzte Verschleierungstaktik bleibt noch: Datentunnel. »Heute ist es üblich, Gespräche paketorientiert mittels Voice over IP zu übertragen«, sagt Jens Heider vom Fraunhofer-Institut für Sichere Informationstechnologie. Das Gespräch wird verschlüsselt über eine Art Labyrinth aus Datentunneln ins Internet geschickt. Dabei gelangt es in einem Zickzackkurs über diverse Server zum Gesprächspartner – der freilich an einem der »Tunnelausgänge« erreichbar sein muss. Die Geheimdienste können dann zwar sehen, unter welcher Internetadresse das Gespräch ins Netz gestartet ist, aber danach verliert sich die Spur.

Experten gehen jedoch davon aus, dass die NSA längst Gegenmaßnahmen entwickelt, um auch die Datentunnel zu infiltrieren. Ein Wettrüsten ist im Gange – ob Nutzer mit technischen Hilfsmitteln ihre Privatsphäre zurückgewinnen, weiß niemand. Ohne gesunden Menschenverstand wird es jedenfalls nicht gehen. »All diese neuen Geräte helfen wenig, wenn Sie damit im Café oder im Bus telefonieren«, sagt Jens Heider. Und ganz wichtig: »Sie müssen das Smartphone in bar bezahlen! Nur dann nämlich klebt an der Gerätenummer nicht vom ersten Tag an Ihr Name.« —

Niels Boeing *benutzt bis heute kein Smartphone. Allerdings weniger aus Furcht vor Überwachung, sondern weil ihm die Auswertung von Nutzerdaten und Ortsangaben durch Hersteller und Onlinedienste suspekt ist.*