Commies und Handys

Mobiltelefone in der Überwachungspraxis

Viele Ortsgruppen der Roten Hilfe haben schon mal Veranstaltungen mit der Datenschutzgruppe gemacht (vielen Dank dafür!). Bei diesen Gelegenheiten gehen die Wogen meist am höchsten, wenn die Rede von Mobiltelefonen ist. Dieser Artikel -- den ihr auch in Veranstaltungsform buchen könnt -- soll auf ein paar der Themen eingehen, die auf dem Gebiet repressionsrelevant sind. Um es vorweg zu nehmen: Dies wäre keine schlechte Zeit, in Panik zu verfallen.

Akkus raus

Es gehört mittlerweile zum guten Ton, bei mehr oder minder vertraulichen Treffen die Akkus aus Mobiltelefonen zu entfernen, da, so geht der Glaube, auch abgeschaltete Geräte als Wanzen gebraucht werden können.

Das ist zwar nicht falsch, blanke Panik ist aber gerade hier nicht angesagt. Am Anfang des grundlegenden Tricks steht die Funktion fast aller Telefone, zum einen Anrufe automatisch anzunehmen und dann auch nicht zu klingeln. Nehmt euch die Zeit und sucht die entsprechenden Einträge in den Tiefen der Menüs. Meist lässt sich sowas auch nur für einzelne eingehende Nummern einstellen. Wenn nun wer ein Telefon in die Hand bekommt und so eine Einstellung vornimmt, muss er/sie nur noch zur passenden Zeit anrufen und hört, was in der Umgebung des Telefons los ist.

Damit das geht, muss das Telefon natürlich im Standby-modus sein, einfaches Ausschalten würde also helfen. Dennoch ist die Sache mit den Akkus nicht schlichte Paranoia, denn bei Geräten, die eine Weckfunktion bieten (also mittlerweile eigentlich allen), kann man darum rumkommen. Dazu setzt man für die spannende Zeit (die dann aber vorher bestimmt werden muss) ein stilles Wecken, mit dem Nebeneffekt, dass das Telefon aufwacht und angerufen werden kann. Auch das könnt ihr eventuell selbst nachvollziehen, viele Telefone machen das aber mit ihrer üblichen Software jedenfalls ziemlich schwer.

Richtig tolle Überwachung ist das allerdings nicht, weil sie nicht besonders heimlich ist. Einerseits sendet das Mobiltelefon während des Überwachungsvorgangs wie närrisch, was sich etwa durch Störungen im Radio oder in der Audio-Hardware nahestehender Rechner bemerkbar machen kann (ihr kennt das wahrscheinlich vom normalen Telefonieren), und außerdem leert sich der Akku des Telefons viel schneller als gewohnt. Schließlich sind bei älteren Telefonen die nötigen Einstellungen auch schwer zu verstecken.

Wie auch immer: Gegen Angriffe dieser Art reicht eine handelsübliche Keksdose aus Blech. Probiert es: Legt euer Telefon in so eine Dose, stellt die Dose in die Nähe von einem Funkmast, der euer Netz ausstrahlt und ruft es an. Klingelt es, ist die Dose zu dünn, ist die Dose dick genug (es braucht nicht viel), wird es auch nicht klingeln, und mithin ist die ganze Überwachung beim Teufel. Im Ernstfall solltet ihr euer Telefon aber ausschalten, bevor ihr es in die Dose legt, da es sonst mit höchster Leistung nach (unerreichbaren, aber das weiß das Gerät ja nicht) Funkmasten sucht, was zwar der Überwachung nicht hilft, aber den Akku rapide leert.

Aufgeschmissen ist, wer ein modernes Telefon hat; die Grenze ist etwa dort, wo die Gurken Fotos speichern und Musikdateien abspielen können. Dann nämlich können die Schlapphüte das Ding aufwachen lassen, müssen es aber nicht anrufen, sondern können ein Programm starten, das einfach die Umgebungsgeräusche aufzeichnet und im internen Speicher ablegt. Sobald Daten unverfänglich übertragen werden können -- etwa, weil der/die BesitzerIn ohnehin telefoniert -- überträgt das Programm die gespeicherten Daten nach und nach auf einen irgendwo im Internet hängenden Rechner des „Bedarfsträgers“.

Ein Mobiltelefon, das, wie die Werbung verspricht, „Platz für 1800 Songs“ (also, sagen wir mal 2 GiB Massenspeicher) hat, kann im Prinzip einen Monat lang ununterbrochen Sprache in der Umgebung so aufzeichnen, dass sie noch verständlich ist. Etliche dieser modernen Telefone bieten „offizielle“ Schnittstellen, die den Betreibern die Installation von Software erlauben, so dass auch ein physikalischer Zugang enfallen kann, bei anderen können Fehler in der Betriebssoftware ausgenutzt oder wie bei „großen“ Rechnern Trojaner eingesetzt werden, um die nötigen Einstellungen und Programme auf die Maschine bringen.

Mit so einem modernen Telefon hilft also in erster Näherung nur Akku raus -- was wirklich auf den Dingern läuft, ist angesichts der ziemlich geschlossenen Architekturen der Betriebssysteme jedenfalls nochmal eine Größenordnung schwieriger rauszukriegen als bei Windows-Maschinen (ok, es gibt Ausnahmen, aber die sind eigentlich nur für Geeks interessant, die diesen Artikel nicht mehr brauchen). Also: Linke verwenden alte, gebrauchte Telefone nicht nur, weil die ArbeiterInnen, die den Kram herstellen, sich meist nicht gewerkschaftlich organisieren dürfen, sondern auch, weil es einfach sicherer ist.

Die Bundesregierung (Drucksache 16/6529) sagt übrigens, dass BKA, Zoll und Bundespolizei keine Mobiltelefone zur Überwachung einsetzen, will sich aber weder für ihre Geheimdienste noch für die Länderpolizeien festlegen. Die Zurückhaltung mag daran liegen, dass ein Angriff auf ein modernes Mobiltelefon letztlich dem Aufbringen des Bundestrojaners entspricht. Angesichts des Typenwirrwarrs im Mobilfunkbereich ist ein Angriff auf ein Telefon in aller Regel mit Softwareentwicklung verbunden; da diese für die Behörden recht aufwändig ist, dürfte das Ausmaß der akustischen Überwachung über Mobiltelefon verglichen mit konventioneller Verwanzung, Spitzeln usf. also derzeit eher überschaubar sein.

Bewegungsprofile

„Handys“ heißen auf Englisch Cell(ular)phones. Diesen Namen haben sie, weil ihre Funk-Infrastruktur in Zellen eingeteilt ist -- im Groben gehört zu jedem Sendemast eine Zelle. Solche Zellen gibt es in groß (im norddeutschen Tiefland sind durchaus 10 km Radius drin), in dichter besiedelten und bebauten Gebieten hat man aber mehr mit 300 Metern zu rechnen, in der U-Bahn oder wo immer viele Leute auf engem Raum telefonieren gerne noch weniger.

Solange ein Telefon läuft (also anrufbar ist), ist es immer in eine Zelle „eingebucht“ und mithin mindestens auf deren Abdeckungsbereich lokalisierbar. Häufig geht es durch genauere Analyse der eingehenden Signale auch noch genauer. Spätestens seit der letzten StPO-Reform (vgl. unseren Artikel zur Vorratsdatenspeicherung, RHZ 2/2007) darf die Polizei solche Daten in Echtzeit von den Telekoms abrufen.

Mit der Vorratsdatenspeicherung (VDS) kommt es noch bunter: Jedes Mal, wenn das Telefon etwa Gespräche oder Kurzmitteilungen empfängt oder versendet, entsteht ein Datensatz, der für ein halbes Jahr gespeichert wird und auch eine Positionsinformation trägt. Mit anderen Worten: solange euer Telefon anrufbar ist, kann sich der Staat mit guten Aussichten noch nach einem halben Jahr ansehen, wo ihr so wart. Abgesehen von der Abschaffung der VDS hilft da nur Ausschalten.

Bekannte Telefone

Eure Identität gegenüber Anbieter und Staat steht auf einer kleinen Chipkarte, der so genannten SIM-Karte, die ihr beim Abschluss eines Vertrages bekommt. Die Anbieter sind übrigens nach wie vor nicht verpflichtet, eine Ausweiskontrolle vorzunehmen -- aber das nur nebenbei. Auf dieser Karte seht die IMSI, die International Mobile Subscriber Identification, eine Zahl, die der Identität zugeordnet ist, die das Ding gekauft hat[1] .

Vor dem Beginn der VDS war die IMSI im Wesentlichen das einzige Datum, das die Staatsgewalt hatte, um Telefonierende zu identifizieren. Inzwischen sind die Telekoms verpflichtet, beim Einbuchen eines Telefons auch noch dessen (des Telefons!) Nummer, die International Mobile Equipment Identification IMEI, abzufragen. Der früher lediglich unsinnige Tausch von Geräten zu Demos und Aktionen wird damit praktisch gefährlich, weil die Staatsgewalt ganz einfach fragen kann, mit welchen SIM-Karten denn ein bestimmtes Telefon schon betrieben wurde und so unter Umständen weitere Daten zu „Netzwerken“ erhält.

Zuhause lassen

Eine der am meisten ignorierten Empfehlungen von Demoratgebern ist erfahrungsgemäß die, das Telefon

daheim zu lassen, vor allem, um die darin enthaltenen Adressbücher vor staatlichem Zugriff zu schützen. Durch die VDS ist diese Empfehlung glücklicherweise weitgehend gegenstandslos geworden, denn die Polizei bekommt entsprechendes in besserer Qualität (weil mit der Intensität des Kontakts gewichtet) von den Telekoms. Einzig gespeicherte Kurzmitteilungen und ggf. weitere gespeicherte Daten (etwa Fotos oder Termine) wären da noch reizvoll. Trotzdem mag es sich ja lohnen, Telefonnummern bekannter Stadt- oder Landräte unter fantasievollen Bezeichnungen wie „Dr. Feelgood“ oder „Maulwurf“ zu speichern -- aliquid semper haeret.

Telefone, die während der Demo Verbindungen aufnehmen, ermöglichen den Behörden allerdings eine spätere Lokalisierung und mithin die Erstellung von ungefähren Teilnahmelisten, etwa über die Differenz zwischen den Telefonen, die während einer Demo in den betreffenden Funkzellen unterwegs waren zu denen, die ansonsten da sind. In dem Sinn: Das bloße Mitführen ist bedeutend schlimmer geworden als die Beschlagnahme.

IMSI-Catcher

Ein IMSI-Catcher ist eine Art gefälschter mobiler Mini-Funkmast, zumeist in einem Kleinbus montiert -- die Idee ist, allen Telefonen in einer Umgebung von vielleicht 20 Metern zu sagen, sie sollten sich doch gerade mal auf einer schönen, kräftigen neuen Funkzelle einbuchen. Die Telefone tun das und geben dabei ihre IMEIs und IMSIs preis. Dass dabei mal eben Gespräche unterbrochen werden (weil die Funkzelle nämlich nur eine Fälschung ist), ist laut höchstrichterlichem Beschluss im Interesse der öffentlichen Sicherheit hinzunehmen.

Zweck der Übung ist zweierlei: Einerseits kann so recht einfach festgestellt werden, wer alles in der näheren Umgebung herumspringt (die Telefone müssen dazu keine Verbindungen aufnehmen), andererseits kann, etwa bei Observierungen, festgestellt werden, welches Telefon das Überwachungsopfer bei sich hat -- das ist insbesondere dann interessant, wenn sich dieses eine „graue“, nicht auf es registrierte SIM-Karte beschafft hat. Also: Wenn pötzlich alle Gespräche in der Umgebung abreißen, mag der Funkmast spinnen. Oder die Staatsgewalt hinter euch her sein.

Fazit

Das Mobiltelefon ist, vor allem im Zusammenhang mit der Vorratsdatenspeicherung, zur ersten Anlaufadresse der Staatsgewalt geworden, wenn sie Dinge über euch rauskriegen möchte. Darum lohnt sich das Abschalten oder Nichthaben massiv. Alte, abgegrabbelte Geräte, deren Funktionen ihr auch halbwegs nutzt, sind ökologisch, sozial und politisch die richtige Wahl. Insbesondere wird ein Telefon sicherer, je weniger Speicher drin ist und je weniger Programme darauf abgelegt werden können. Back to the nineties. Mit dem Handy von Vorgestern hilft eine Keksdose, die als Nebennutzen gleich noch eure RFID-Kärtchen sicher beherbergen kann.

Datenschutzgruppe der Roten Hilfe Heidelberg

datenschutzgruppe@rotehilfe.de

PGP Fingerprint: a3d8 4454 2e04 6860 0a38 a35e d1ea ecce f2bd 132a

http://www.datenschmutz.de

[1] Vielleicht ist für mancheN der vom AK Vorratsdatenspeicherung angeregte SIM-Tauschdienst unter http://www.daten-speicherung.de/kartentausch nicht uninteressant.