2.5 Anonym telefonieren

Können Handys die Identität des Informanten enthüllen?

Reporter Feder und Informant Ehrlich meiden persönliche Treffen. Um sich abzustimmen, speichern sie Mails in einem toten Briefkasten. Dort landen auch die Beweise, die Ehrlich für den Korruptionsskandal in den Stadtwerken beibringt. Doch die Kommunikation per Mail oder Chat kann persönliche Treffen nicht immer ersetzen. Chefcontroller Ehrlich will Feder einen Blick in eine Akte gestatten, in der Decknamen und Zahlungen vermerkt sind. Das Kopieren der Seiten lehnt Ehrlich ab. Nur ein Dutzend Mitarbeiter kennt die Akte. Jede Version ist mit dem Namenskürzel des Empfängers versehen. Sollte eine Kopie der Akte jemals in die Öffentlichkeit gelangen, wäre Ehrlichs Identität sofort enthüllt. Deshalb will er dem Reporter nur einen Blick in die Papiere gestatten. Ehrlich und Feder vereinbaren ein Treffen außerhalb der Stadt. Auf der Fahrt plagt den Reporter ein ungutes Gefühl. Er erinnert sich an einen Radiobeitrag, der das Orten von Mobiltelefonen behandelt hat. Feder benutzt ein Firmenhandy. Und Ehrlich? Feder weiß es nicht. Ist es möglich, die Standorte der beiden Männer zu ermitteln? Kann durch die Handys nachvollzogen werden, dass sich Reporter Feder und Controller Ehrlich außerhalb der Stadt getroffen haben?

Der Peilsender in der Tasche

Die Herren Feder und Ehrlich riskieren Kopf und Kragen. Handys eignen sich perfekt zur Spionage. Kein elektronisches Alltagsgerät ist gefährlicher. Nicht einmal ein PC. Ein Handy kann abgehört werden. Nicht nur von Ermittlern, sondern auch von Privatpersonen. Es verrät den Aufenthaltsort seines Benutzers. Einem Ermittler ebenso wie dem Chef oder dem Ehepartner. Denn es funktioniert wie ein Peilsender. Damit nicht genug. Ein Handy kann als Wanze gegen seinen Besitzer missbraucht werden. Es zeichnet über das eingebaute Mikrofon heimlich dessen Gespräche auf. Ein Handybenutzer kann den Spieß auch umdrehen und sein Gerät als Wanze einsetzen, zum Beispiel, um Geschäftspartner abzuhören. (Fast) alles ist möglich. Selbst für technische Laien. Erschreckend, nicht wahr? Wir gehen alle Varianten durch und besprechen, wie man sich schützen kann. Dazu muss man aber wissen, wie ein Handy funktioniert.

Wie funktioniert ein Handy? Es besteht (im Prinzip) aus zwei Teilen: einem Computer mit Mikrofon und Lautsprecher sowie einer Funkanlage. Viele Benutzer glauben, ein Handy sei ein mobiles Telefon mit ein paar Spielereien. Das ist ein Irrtum. Der Handy-Computer ähnelt einem abgespeckten Laptop. Er ist nur kom-

plizierter zu bedienen. Als Computernutzer sind wir gewohnt, mit einer großen Tastatur und einer Maus zu arbeiten. Das Handy hat dagegen nur winzige Tasten. Zudem sind die Menüs beim Mobiltelefon verwirrender als beim Rechner – zumindest am Anfang. Hinzu kommen ungewöhnliche Befehle, mit denen das Telefon gesteuert werden kann, zum Beispiel *#06# (der Befehl enthüllt die Seriennummer des Geräts). Doch das darf nicht darüber hinwegtäuschen: Ein Handy ist ein vollwertiger Computer.

Es benötigt ein Betriebssystem, auf dem Programme laufen können. Die Firma Microsoft hat für Handys das Betriebssystem »Windows Mobile« entwickelt. An einer Alternative arbeitet Google. Sie trägt den Namen »Android« und integriert Dienste wie Google Maps oder Gmail. Marktführer ist jedoch eine Software, deren Name kaum bekannt ist. Sie heißt »Symbian«. Dahinter stehen die großen Handyhersteller wie Nokia und Ericsson. Eines ist allen Betriebssystemen gemein: Sie verwandeln Handys in mobile Büros oder Freizeitoasen. Texte und E-Mails schreiben, Präsentationen vorbereiten, Musik und Videos genießen – fast alles ist machbar.

Hier lauert zugleich die erste Falle für einen Handynutzer. Hunderte von Modellen überschwemmen den Markt. Jeder Mobilfunkkonzern wie T-Mobile, Vodafone oder E-Plus ordert bei den Handyherstellern spezielle Varianten. Die Vielfalt ist unüberschaubar. Nur die Hersteller kennen alle Funktionen ihrer Handys. Deshalb gilt: Wer mit seinem Handy diskret telefonieren will, sollte das einfachste Modell wählen, das er finden kann. Je weniger Software und Technik vorhanden ist, desto besser. Finger weg von schicken Geräten. Jedes zusätzliche Programm stellt ein weiteres Risiko dar.

Der zweite Teil eines Handys ist die Funkanlage. Ihr Herzstück: eine SIM-Karte. SIM steht für Subscriber Identity Module. Mit der Karte identifiziert sich der Handybenutzer im Funknetz. Sie ist quasi der Türöffner. Die Karte besteht aus einem kleinen Prozessor mit einem Speicher. Eine PIN, die nur der Besitzer kennen sollte, verhindert, dass Fremde das Handy mit der Karte benutzen können. Die PIN muss eingetippt werden, damit die Karte die Verbindung zum Funknetz herstellt. Auf der SIM-Karte sind geheime Nummern und der Code für die Verschlüsselung der Gespräche gespeichert – zwei Punkte, denen wir uns noch ausführlich widmen werden. Die Karte dient auch als Telefon- und Notizbuch und speichert SMS-Mitteilungen.

Was geschieht, wenn Reporter Feder sein Mobiltelefon einschaltet? Ganz Deutschland ist übersät mit Funkzellen. Werfen Sie beim nächsten Spaziergang einen Blick auf Hausdächer. Sie entdecken Antennen und Sattelitenschüsseln für den Fernsehempfang. Und eventuell elektrische Geräte mit einer merkwürdigen Form. Sie erinnern an italienisches Brot, an Ciabatta. Die Geräte sind senkrecht an den Masten befestigt. In Großstädten sehen Sie sie alle paar Hundert Meter, auf

dem Land seltener. Es handelt sich um die Mobilfunkantennen der Basisstationen. Das Handy von Reporter Feder sucht den Kontakt zu einer solchen Basisstation. Es wählt die Zelle mit dem stärksten Signal aus und loggt sich ein. Spätestens jetzt ist es vorbei mit der Anonymität. Das Handy sendet zwei Nummern an die Basisstation: die IMEI und die IMSI. Sie sind so genial wie gefährlich. Denn beide Nummern werden weltweit einmalig vergeben. Was bedeutet das? Schauen wir uns die Details an.

IMEI steht für International Mobile Equipment Identity. Es handelt sich um eine 15stellige Seriennummer. Mit ihr kann jedes Gerät eindeutig identifiziert werden. Wohlgemerkt: das Gerät, die Hardware, die man in der Hand hält. Die IMEI verrät das Land, in dem das Handy zugelassen wurde, den Hersteller und eine Gerätenummer. Wozu dient die IMEI? Nehmen wir an, Ihr Handy wird gestohlen. Sie melden den Diebstahl ihrem Provider. Er setzt die IMEI auf eine schwarze Liste. Wenn der Dieb mit dem Handy telefonieren will, sperrt das Funknetz den Zugang. Das Gerät ist für den Dieb wertlos – zumindest in der Theorie. Die Praxis sieht anders aus. Für Funknetz-Betreiber macht die Liste nur Arbeit; sie wird angeblich stiefmütterlich behandelt. Zudem kann mit einer Software die IMEI verändert werden.

Sie können die IMEI ihres Handys leicht herausfinden. Die Nummer steht meist auf einem Typenschild unter dem Akku. Alternativ können Sie die IMEI mit einer Tastenkombination abfragen. Einfach Eintippen wie eine Telefonnummer, und die IMEI erscheint. Die Tastenkombination lautet: *#06#. Sind Sie an weiteren Kombinationen interessiert? Der schnellste Weg führt über eine Suchmaschine. Geben Sie den Namen des Handyherstellers und den Begriff »Tastencode« ein.

Die IMEI wird sehr wichtig werden für uns. Warum? Wir lernen später, wie man anonym per Handy telefonieren kann. Das geht recht einfach und ist auch legal. Man benutzt eine anonyme SIM-Karte. Die Anonymität verpufft aber sofort, wenn Sie für einen Anruf ein ausgemustertes Handy benutzen. Es sendet seine IMEI ins Funknetz, also jene Geräte-Nummer, mit der Sie früher unterwegs waren. Der Provider muss nur nachschauen, wer einst mit dieser IMEI telefoniert hat. Schon ist die Identität enthüllt.

Eine zweite Nummer, die ins Funknetz gesendet wird, nennt sich International Mobile Subscriber Identity, abgekürzt IMSI. Die IMSI wird ebenfalls weltweit einmalig von den Mobilfunknetzbetreibern vergeben. Sie befindet sich auf der SIM-Karte. Erinnern Sie sich noch an den kleinen Chip, den Sie nach dem Kauf des Handys im Akku-Fach befestigt haben? Das ist die SIM-Karte. Die IMSI besteht aus 15 Zeichen und identifiziert den Handybesitzer. Sie beginnt mit einem Ländercode. 262 steht zum Beispiel für Deutschland. Dann folgt der Netzbetreiber, zum Beispiel 03 für E-Plus. Das Ende bildet die Identifikationsnummer des Teilnehmers.

Fassen wir zusammen: Mit IMEI und IMSI kann jedes Gerät und jeder Benutzer weltweit eindeutig identifiziert werden. Wenn Reporter Feder anonym telefonieren möchte, benötigt er zwei Dinge: ein Handy und eine SIM-Karte, die nicht auf seinen Namen zugelassen sind. Dazu später mehr.

Folgen wir den Spuren, die Herr Feder im Funknetz hinterlässt. Er hat sein Handy eingeschaltet und die beiden Nummern übermittelt. Feder ist jetzt eindeutig identifiziert. Oder genauer: das Gerät und der Name seines Besitzers. Damit nicht genug. Der Handy-Provider weiß auch, wo sich Gerät und Benutzer befinden. Warum? Es ist ein weit verbreiteter Irrglaube, dass ein Handy-Anruf von Funkstationen über ganz Deutschland verbreitet wird. Das Gegenteil ist der Fall. Das Handy von Herrn Feder steckt in einer kleinen Funkzelle. Ein Anruf wird punktgenau in diese Zelle vermittelt. Das bedeutet: Anrufe per Handy legen nur eine kurze Strecke per Funk zurück – und zwar den Weg von der nächsten Basisstation zum Mobiltelefon.

Nehmen wir an, Informant Ehrlich urlaubt im Bayerischen Wald. Reporter Feder tourt durch Hamburg. Ehrlich ruft Feder an – von Handy zu Handy. Was geschieht? Ehrlichs Mobiltelefon klinkt sich bei der nächsten Basisstation im Bayerischen Wald ein. Sie ist vielleicht einen Kilometer entfernt. Dann wandert der Anruf über Kabelleitungen durch ganz Deutschland Richtung Norden – bis zur Basisstation, in deren Nähe sich Feder aufhält. Sie schickt den Anruf per Funk zu Herrn Feder. Das bedeutet: Es existiert nur ein kleiner Unterschied zwischen Telefonaten im Fest- und im Funknetz: Bei Mobiltelefonen legen die Gespräche ein kurzes Stück in der Luft zurück.

Eine faszinierende Technologie – aber mit einem Nachteil: Das Handy wird zum Peilsender. Eine Funkzelle bedient rund 50 Telefonierer. In Großstädten lässt sich der Standort des Handybenutzers recht genau bestimmen. Bewegt sich der Telefonierer, kann ihm gefolgt werden. Er wird von Funkzelle zu Funkzelle weitergereicht. Der Vorgang heißt Handover. Es entsteht ein Bewegungsmuster. In Großstädten kann ein Handybesitzer bis auf 300 Meter genau geortet werden (und in bestimmten Bereichen wie der Innenstadt noch präziser). Auf dem Land sind die Abstände zwischen den Basisstationen größer: bis zu 1,5 Kilometer.

Was bedeutet das für das Geheimtreffen von Reporter Feder und Informant Ehrlich? Sollte ein Staatsanwalt im Bestechungsskandal ermitteln, könnte der Journalist ein Überwachungsziel sein. Das Handy funkt munter die Position von Feder durch. Am Treffpunkt erscheint auch das Handy von Informant Ehrlich in der Funkzelle. Dem Ermittler ist jetzt ein leichtes, die Quelle von Feder zu enthüllen. Der Name taucht in den Ermittlungsakten auf, die später im öffentlichen Prozess verwendet werden. Informant Ehrlich dürfte seine Stelle verlieren – ein Risiko, das vermieden werden kann.

Nicht nur staatliche Ermittler können Standorte eines Handys (und somit des Benutzers) bestimmen. Zahlreiche Websites bieten diesen Service an. Sie haben sich entweder seriöse Namen gegeben wie handy-ortung.org oder kommen flapsiger daher wie trackyourkid.de. Die Idee ist immer dieselbe: Ein User registriert seinen Namen und das Handy bei dem Ortungsdienst. Er wählt eine Zahlungsart. Dann nimmt er das Handy, das überwacht werden soll, und verschickt eine oder mehrere SMS (abhängig vom Netzbetreiber). Der Service bestätigt die Anmeldung, ebenfalls per SMS. Der ganze Vorgang dauert ein paar Minuten. Ab jetzt kann der Benutzer des Handys stets geortet werden. Der Späher loggt sich auf der Seite des Services ein, drückt den Button »Orten« – und es erscheint ein Bild wie 81.

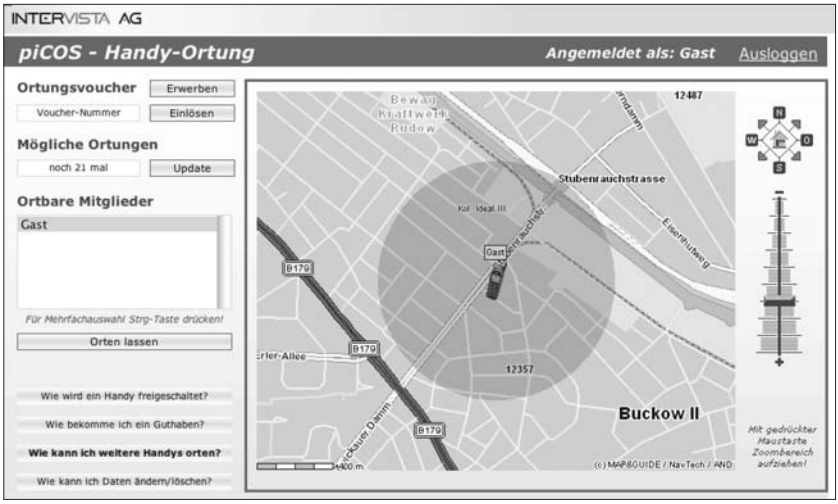

Bild 81: Handy-Ortung im Internet (hier: www.picosweb.de)

Ortungsdienste sind eine zweischneidige Angelegenheit. Sicherlich ideal für Eltern, die den Schulweg ihres Kindes sichern möchten. Aber auch für Männer oder Frauen, die ihren Partner überwachen wollen. Oder für Chefs, die ihren Mitarbeitern nachspionieren. Ihnen muss es nur gelingen, das Mobiltelefon für ein paar Minuten zu entführen – schon ist es bei einem Ortungsdienst angemeldet. Dem Handynutzer bleibt verborgen, dass er geortet wird. Einige Dienste akzeptieren sogar Pseudonyme und können anonym bezahlt werden.

Wie können Reporter Feder und Informant Ehrlich verhindern, dass ihr Treffen geortet wird? Der einfachste Weg: Einer lässt das Handy am Arbeitsplatz zurück,

am besten eingeschaltet. Selbst wenn es altbacken klingt: Es geht auch ohne Mobiltelefon. Muss Controller Ehrlich immer erreichbar sein? Wohl kaum. Er (oder Feder) werden auch zwei Stunden ohne Mobiltelefone überleben.

Leider reicht das Ausschalten des Handys nicht immer aus, um der Ortung zu entgehen. Das Mobiltelefon funkt eventuell doch noch seinen Standort durch. Sie müssen deshalb den Akku entfernen. Checken Sie in der Betriebsanleitung, ob eine zusätzliche Batterie im Gerät eingebaut ist. Falls ja, muss auch sie entfernt werden. Noch sicherer ist es, zusätzlich die SIM-Karte auszubauen.

Eine ungewöhnliche Idee kommt vom Bundesamt für Sicherheit in der Informationstechnik. Ein Sprecher sagte in einem Interview: »Bei Manipulationsverdacht hilft nur ein faradayscher Käfig: Sie können das Handy in einen Metall-Käfig oder eine Metall-Folie einpacken, so dass die Funkverbindung dadurch unterbrochen ist.«

Noch wirkungsvoller als eine Folie funktioniert eine Handytasche mit dem Namen PhoneShield. Sie wird von der britischen Firma Disklabs verkauft. Die Tasche verhindert, dass sich ein Mobiltelefon mit dem Funknetz verbindet. Sie ist vor allem für Ermittler gedacht, die verhindern wollen, dass ein sichergestelltes Telefon per Funk nachträglich manipuliert wird. Durch ein Sichtfenster können die Beamten das Handy bedienen. Normalerweise nutzen Polizisten für diese Arbeit einen abgeschirmten Raum.

Ein Handy kann aber auch als Wanze, also als Abhörgerät, eingesetzt werden. Entweder vom Besitzer, um Dritte auszuspionieren. Oder von Dritten, um den Besitzer auszuforschen.

Das Handy als Wanze

Der US-Mafioso John Ardito trug sein Handy stets bei sich. Auch bei Treffen mit seinen Anwälten in den Restaurants der New Yorker Bronx. Was der Pate der Genovese-Familie nicht ahnte: Das FBI hatte sein Handy manipuliert. Obwohl das Gerät ausgeschaltet schien, zeichnete das Mikrophon jede Silbe auf und funkte sie den Ermittlern. Der Pate wurde verhaftet.

Das Handy von Ardito war verwanzt. Leider können nicht nur Mafia-Fahnder Lauschangriffe gegen Kriminelle starten. Für rund 150 Euro im Jahr kann auch ein technischer Laie ein Handy verwanzen. Das ist in Deutschland illegal und kann mit einer Haftstrafe geahndet werden. Da es aber möglich ist, sollten Sie die Gefahr kennen – und Wege, um sich zu schützen.

Die Spionage-Software heißt Flexispy und wird von der thailändischen Firma Vervata vertrieben. Auf der Webseite des Unternehmens steht in holprigem Deutsch: »FlexiSPY ist ein Programm, daß alle Aktivitäten des Handy auf dem

[e]s installiert ist, unbemerkt überwacht. Schützen Sie Ihre Kinder, finden Sie heraus ob Ihr Partner Sie betrügt. Die möglichkeiten sind endlos.«

Das Deutsch ist zwar nicht perfekt – dafür funktioniert die Software scheinbar umso besser. Eine Journalistin von Xonio.com, einer Technik-Website, testete das Programm und verwanzte ein Mobiltelefon. Ihr Fazit: »Bei einem Gespräch, bei dem das Handy auf einem Tisch in unmittelbarer Nähe lag, konnten wir alles verstehen.«

Wie funktioniert Flexispy? Der Spion meldet sich auf der Website der Firma an, wählt den Service aus und bezahlt per Kreditkarte. Er erhält eine E-Mail mit einem Produktschlüssel. Nun muss der Spion das Mobiltelefon, das verwanzt werden soll, in die Hände bekommen. Wenige Minuten reichen, um das Programm zu installieren – falls das Handy einen eingebauten Browser besitzt. Der Spion surft auf die Hersteller-Site, gibt den Produktschlüssel ein und lädt die Software aufs Handy. Er schaltet das Mobiltelefon aus, dann wieder ein. Mit einem Geheimcode wird ein Optionsmenü aufgerufen und die Software konfiguriert. Ab jetzt kann das Mobiltelefon per Textnachricht (SMS) oder Anruf ferngesteuert werden.

Das Spionagetool leistet ganze Arbeit. Das Mikrofon kann heimlich eingeschaltet und ein Gespräch belauscht werden – wie im Fall von US-Mafioso Ardito. Jeder Anruf, den der Ausspionierte tätigt oder empfängt, wird registriert. Telefonnummer und Dauer können auf der Vervata-Website abgerufen werden. Das gilt auch für Textnachrichten. Sie werden nicht nur protokolliert, sondern Wort für Wort aufgezeichnet.

Wie kann man sich gegen diese Spionage schützen? Die gute Nachricht: Die Software funktioniert nur mit modernen Handys, die einen Browser besitzen. Wer – wie bereits empfohlen – zum diskreten Telefonieren ein möglichst einfaches Gerät benutzt, scheint (noch) sicher.

Die Telefonrechnung ist die Achillesferse von Flexispy. Die ausspionierten Daten müssen zum Server der Herstellerfirma in Bangkok übertragen werden. Das Handy geht nach einem Telefongespräch oder dem Versenden einer SMS heimlich ins Internet. Wer seine Handyrechnung auf verdächtige Online-Verbindungen kontrolliert, kann Flexispy entlarven.

Eine weitere Alternative: Laden Sie die kostenlose Testversion des Virenscanners »F-Secure Mobile Anti-Virus« auf das Telefon herunter. Er erkennt Flexispy. Die Software finden Sie unter http://mobile.f-secure.de. Ein Installations-Guide (auf Deutsch) beschreibt, wie das Programm benutzt wird.

Am einfachsten ist jedoch folgender Trick: Lassen Sie Ihr Handy in der Jacke oder der Handtasche stecken. Dicker Stoff bringt jedes herkömmliche Mikrofon zum Schweigen. Stellen Sie im Gegenzug den Klingelton etwas lauter. Dann entgeht Ihnen auch kein Anruf.

Noch zwei Sicherheitshinweise, die unbedingt beachtet werden sollten. Wie wir gesehen haben, kann ein Handy in wenigen Minuten verwanzt werden. Es muss nur kurz einem zwielichtigen Zeitgenossen in die Hände fallen. Schädliche Programme können aber auch per Funk auf ein Mobiltelefon gelangen. Zum Bespiel per Klingelton. Es gilt als schick, wenn das Handy einen Anruf mit einer ungewöhnlichen Melodie ankündigt. Die Töne können einfach und direkt von Websites installiert werden. Und mit Ihnen manchmal auch Spionagesoftware. Deshalb sollten Sie entweder auf diesen Gag verzichten oder nur Klingeltöne von seriösen Anbietern herunterladen. Das gilt auch für Handy-Spiele. Sie können ebenfalls mit Spionagesoftware verseucht sein.

Eine weitere Gefahrenquelle sind »Schnittstellen«. Ein komisches Wort für eine sehr praktische Funktion. Sie haben zum Beispiel ein Video per Handykamera gedreht. Wie kommt das Video auf den Computer? Ein Techniker würde sagen: per Schnittstelle. Sie können zum Beispiel das Handy mit einem Kabel an den Computer anschließen. Die Schnittstelle ist also der PC-Eingang. Sie können aber auch Funkwellen nutzen, um das Video auf den Computer zu senden. Dann entfällt der Kabelsalat. Beispiele für diese Art der Übertragung sind Bluetooth oder WLAN. Wir müssen uns an dieser Stelle nicht mit den technischen Details beschäftigen. Wichtig ist nur: Sollten Sie diese Funktionen jemals aktiviert haben, dann ist das Mobiltelefon gefährdet. Also bitte abschalten.

Im vorherigen Abschnitt wurde der Besitzer des Handys ausspioniert. Er kann den Spieß aber auch umdrehen und sein Telefon als Wanze einsetzen. Auch das ist illegal und wird bestraft. Dennoch soll es häufig vorkommen, besonders bei Geschäftsgesprächen. Sie kennen die Szene. Eine wichtige Verhandlung. Beide Seiten wollen das Beste herausholen. Sie versuchen, die Grenzen auszuloten. Nach zwei Stunden bittet ein Gesprächspartner um eine kurze Pause. Er möchte austreten. Er verlässt den Raum. Sein Handy bleibt – wie zufällig – auf dem Konferenztisch zurück. Die Verhandlungspartner nutzen die wenigen Minuten, um schnell ihre Taktik abzustimmen. Ein Fehler. Die Person, die den Raum verlassen hat, hört alles mit. Und zwar live.

Die Gefahr, von einem manipulierten Mobiltelefon abgehört zu werden, ist nicht gering. Viele Handys verfügen über diese Funktion. Sie heißt »automatische Rufannahme«. Die Idee: Sie wollen erreichbar sein, haben aber – im wahrsten Sinne des Wortes – beide Hände voll zu tun. Zum Beispiel der Konditor, der gerade im Kuchenteig knetet. Oder der Automechaniker, der mit verölten Händen an einem Getriebe schraubt. In solchen Situationen können Sie einen Anruf nicht annehmen, ohne das Mobiltelefon zu verdrecken.

Die Lösung des Problems ist die automatische Rufannahme. Der Benutzer stöpselt ein Headset ins Handy, bestehend aus Kopfhörer und Mikrofon. Er aktiviert die automatische Rufannahme. Bei einem Anruf klingelt das Telefon mehrere Male

und schaltet sich automatisch ein – ohne dass die Tastatur berührt wird. Eine praktische Funktion – die aber sofort von zwielichtigen Zeitgenossen zweckentfremdet wurde. Der Trick: Der Spion aktiviert nicht nur die automatische Rufannahme, sondern gleichzeitig das Profil »Lautlos«. Das bedeutet: Bei einem Anruf schaltet sich das Handy automatisch ein – ohne Klingelton und ohne blinkendes Display. Der Geschäftspartner, der in unserem Beispiel den Raum verlassen hat, kann mit einem zweiten Telefon sein Handy auf dem Konferenztisch anrufen. Es schaltet sich lautlos ein und überträgt die Gespräche der Geschäftspartner.

Ob der Trick klappt, variiert von Handy zu Handy. Die Hersteller reagieren unterschiedlich auf die Gefahr. Bei einigen Modellen funktioniert die automatische Rufannahme nur, wenn ein Headset verwendet wird. Bei anderen Geräten kann in diesem Modus der Klingelton nicht abgeschaltet werden. Sicher ist nur: Dem Handy auf dem Konferenztisch ist nicht anzusehen, ob es manipuliert wurde. Für einen umsichtigen Menschen gilt deshalb: keine vertraulichen Gespräche in der Nähe herrenloser Handys.

Fassen wir zusammen: Selbst ein Laie kann ein Mobiltelefon in eine Wanze verwandeln. Er muss das Gerät nur in die Finger bekommen. Der Rest ist in Minuten erledigt. Deshalb können bei Handys Sperrcodes festgelegt werden. Vor jedem Anruf muss die Geheimnummer eingegeben werden. Das ist zwar nervig, verhindert aber, dass Ihr Gerät heimlich bei einem Ortungs- oder Abhördienst angemeldet werden kann.

Leider gibt es noch mehr Möglichkeiten, Sie auszuspionieren. Ihnen widmen wir uns im nächsten Abschnitt.

Ein Wolf im Schafspelz

Die Spionagemethoden, die bis jetzt besprochen wurden, haben eines gemein: Sie funktionieren nur, wenn das Handy in fremde Hände gerät. Es existieren aber auch Abhörmethoden, bei denen das nicht nötig ist.

Ein Blick zurück auf die Funktionsweise des Handynetzes. Es besteht aus vielen Funkzellen. Wird ein Handy eingeschaltet, sucht es nach dem Signal der nächst gelegenen Funkzelle. Es loggt sich mit zwei Nummern ein: der IMSI und der IMEI. Beide werden weltweit einmalig vergeben. Die IMSI ähnelt einer Telefonnummer, die IMEI einer Gerätenummer.

Wenn Teilnehmer A ins Mikrofon spricht, sendet das Handy die Worte zu der Funkzelle. Sie speist das Gespräch ins Festnetz ein. Dort wandert es zu Teilnehmer B. Benutzt B ebenfalls ein Handy, wird das Gespräch zu seiner nächstliegenden Funkzelle geleitet und von dort gesendet. Das bedeutet: Handy-Gespräche verlaufen nur eine kurze Strecke über den Äther. Dafür aber verschlüsselt. Handy und

Funkzelle handeln dazu einen Code aus. In der Funkzelle wird das Gespräch entschlüsselt und ins Festnetz weitergeleitet.

Wer kann Gespräche belauschen? Und wie? Am einfachsten haben es Ermittler, denen ein Richter das Abhören genehmigt hat. Sie loggen sich beim Netzbetreiber ein. Dort müssen die Gespräche bestimmte Stationen passieren. Sie wurden inzwischen entschlüsselt. Die Fahnder schalten sich an einer Station ein und können bequem mithören. Fachleute bezeichnen diesen Vorgang als »Ausleiten« eines Gesprächs.

Schwieriger ist es, ein Handy illegal abzuhören. Der Lauscher muss sich in derselben Funkzelle befinden wie sein Opfer. Nehmen wir als Beispiel Reporter Feder. Ihm aufzulauern, dürfte schwer werden. Er ist viel unterwegs, zieht von Funkzelle zu Funkzelle. Ein Lauscher müsste ihm dicht auf den Fersen sein, zumindest in einer Großstadt. Das setzt viele Verfolger voraus – ein unwahrscheinliches Szenario. Der Verlag und die Wohnung dürften hingegen realistischere Ziele für Lauscher sein.

Der Funkverkehr kann mit zwei Methoden abgehört werden. Geheimdienste verwenden sogenannte IMSI-Catcher. Sie haben die Größe eines Laptops. IMSI-Catcher simulieren Funkzellen. Sie senden starke Signale aus. Ein Handy, das sich in der Nähe befindet, nimmt sofort Kontakt auf. Denn Mobiltelefone suchen stets nach dem stärksten Signal. Es verspricht die beste Sprachqualität. Der Catcher nutzt dieses Verhalten – wie ein Wolf im Schafspelz. Er schaltet sich zwischen Handy und Funknetz. Das Mobiltelefon wird angewiesen, die Verschlüsselung abzuschalten. Nun kann der Besitzer des IMSI-Catchers alle Gespräche mithören.

Ein deutscher Hersteller solcher Geräte soll die Münchner Firma Rohde & Schwarz sein. Experten berichten, dass dort die Modelle GA 900 und GA 901 gefertigt werden. Auf der Firmenwebsite werden die Geräte aber nicht erwähnt.

International bietet rund ein Dutzend Firmen IMSI-Catcher an. Zum Beispiel unter http://pgis.4t.com. Meist werden die Geräte nur an staatliche Stellen verkauft. Es soll jedoch ein grauer Markt existieren. Über den Preis kursieren fast nur Gerüchte. Ein Hersteller veröffentlicht auf seiner Website den stolzen Kaufpreis von 420.000 $ pro Gerät.

Für die Verschlüsselung von Handys wird der Standard A 5/1 verwendet. Er ist schwach. Die Technik-Website ZDNet schreibt zu dem Thema: »Mittlerweile ist es möglich, mit Standard-Hardware ein mitgeschnittenes GSM-Telefonat … innerhalb von etwa zwei Stunden zu entschlüsseln … Noch für 2008 werden erste Geräte für das Abhören durch jedermann erwartet. Damit lassen sich im Umkreis von etwa zwei Kilometern alle Handy-Gespräche und SMS abhören. In Deutschland sind Entwicklung, Besitz und Betrieb eines solchen Gerätes strafbar.«

Eine zweite Variante, um Mobiltelefone zu belauschen, funktioniert über Richtfunkstrecken. Zum Hintergrund: Ein Gespräch wird zwischen Handy und Funkzelle verschlüsselt übertragen. Der Standard ist zwar alt, verhindert aber, dass problemlos mitgehört werden kann. Die Funkzelle empfängt das Gespräch und entschlüsselt es. Die Daten werden ins Festnetz weitergeleitet.

Nicht immer geschieht das auf direktem Wege. Oft werden Gespräche über Richtfunkstrecke zu einem Sammelpunkt gefunkt und von dort ins Festnetz geleitet. Der Haken: Die Gespräche verlassen die Funkzelle unverschlüsselt. Sie können auf der Richtfunkstrecke abgehört werden, allerdings mit höherem technischem Aufwand. Eine Privatdetektei wird den Aufwand kaum betreiben; ein Geheimdienst schon.

Wie kann sich Reporter Feder gegen das Abhören seines Handys schützen? Leider nur sehr schwer. Er und seine Gesprächspartner können Handys benutzen, die Gespräche verschlüsseln. Wie das TopSec GSM. Es wird von Rohde & Schwarz angeboten, also jener Firma, die auch den IMSI-Catcher im Programm haben soll. Damit Lauscher keine Chance haben, müssen beide Teilnehmer ein solches Handy benutzen. Auf dem Display wird die Verschlüsselung angezeigt – siehe Bild 82.

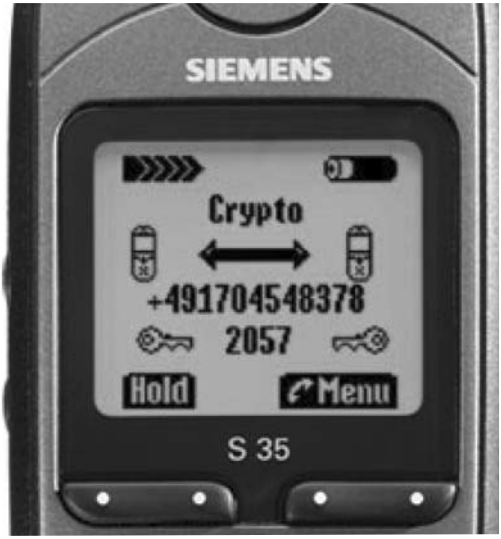

Bild 82: Das Display des TopSec GSM zeigt ein verschlüsseltes Gespräch an

Ein weiterer Anbieter von Geräten, die verschlüsseln können, ist die Berliner Firma GSMK. Sie bietet mehrere Varianten ihres Cryptophone an – unter anderem für Mobilfunk, Festnetz und Satellit. Das Unternehmen ist unter http://www.gsmk.de zu erreichen. Ähnliche Produkte bietet Beaucom an, zu erreichen unter http://www.beaucom.de. Die Firma Secusmart in Düsseldorf bietet einen Chip an, der ins Handy gesteckt wird und Gespräche verschlüsselt. Sie finden das Unternehmen im Internet unter http://www.secusmart.de

Einen anderen Weg geht die Münchener Firma SecurStar, zu erreichen unter http://www.securstar.com. Sie verkauft eine Software, die auf modernen Handys installiert wird. Ihre Name: Phone-Crypt. Jeder Teilnehmer benötigt das Programm, um verschlüsselt telefonieren zu können. Ein ähnliches Konzept verfolgt das nordhessische Unternehmen Safe-com mit seinem Produkt Babylon nG, zu erreichen unter http://www.safe-com.com.

Alle Lösungen haben drei Nachteile:

- Handys und Software sind für den Käufer eine »Black Box«. Er kann nicht wissen, ob die Geräte oder Programme versteckte Funktionen aufweisen. Der Käufer vertraut sich der Firma an. Selbst Prüfsiegel können nicht mehr als ein Hinweis sein.
- Jeder Gesprächspartner benötigt ein Gerät (bzw. die Software). Für die Mitarbeiter einer Firma kein Problem – für einen Reporter mit wechselnden Informanten schon. Für sensible Fälle könnten allerdings zwei, drei Geräte in einer Redaktion liegen und bei Bedarf verteilt werden.
- Der Preis. Schnell kommen mehrere Tausend Euro zusammen. Größere Firmen können die Summe verkraften; freie Journalisten wohl eher seltener.

Fassen wir zusammen: Staatliche Stellen können mit richterlicher Erlaubnis Telefonate schnell und bequem abhören. Wer Handy-Gespräche illegal belauschen will, muss (noch) einen größeren Aufwand betreiben. Er benötigt einen IMSI-Catcher. Für Geheimdienste dürfte es kein Problem sein, die Geräte zu erwerben. Für Privatpersonen schon. Sie müssen auf den grauen Markt ausweichen. Mit speziellen Handys (oder Software) kann man sich vorm Abhören schützen. Jedoch benötigen alle Teilnehmer diese Geräte (oder Programme).

Ein generelles Problem bleibt: Ein geschickter Datenspion, dem ein Handy für wenige Minuten in die Finger gerät, kann es manipulieren. Spionagesoftware für Mobiltelefone steckt zwar noch in den Kinderschuhen. Aber man kann davon ausgehen, dass sich diese Situation ändern wird. Je intelligenter die Telefone werden, desto mehr Schädlinge dürften entwickelt werden. Eine Entwicklung, die bereits bei Computern beobachtet wurde.

Ist diskretes Telefonieren also Utopie? Nein. Es existieren Mittel und Wege. Einfach, günstig und praktisch. Zwei Punkte sollten die Grundregeln für das Alltagsgeschäft bilden:

1. Verhindern Sie, dass Ihre Telefonnummer (oder die des Verlages) bei Anrufen übertragen wird. Ansonsten wird Ihre Nummer in der Telefonanlage des Gesprächspartners festgehalten – ein unnötiges Risiko für den Angerufenen. Achtung: Sicherheitsbehörden können die Nummer eines Anrufers trotzdem anzeigen lassen.
2. Meiden Sie bei sensiblen Gesprächen die Telefonanlage Ihres Verlags. Rufen Sie von Privathandy zu Privathandy an. Warum? Auch Verlage zeichnen die Anrufe ihrer Mitarbeiter auf. Soll der Geschäftsführer erfahren, wer sie mit Informationen versorgt?

Können Handys die Identität des Informanten enthüllen?

Reporter Feder und Informant Ehrlich wollen in nächster Zeit auf persönliche Treffen verzichten. Das Risiko ist zu hoch. Ihre Gesichter sind bekannt. Werden sie zusammen gesehen, fliegt die Anonymität von Ehrlich auf. Jedoch: Persönliche Gespräche müssen möglich sein. Oft überschlagen sich die Ereignisse. Der Geschäftsführer der Stadtwerke versucht, mit falschen Fakten dem Vorwurf der Bestechlichkeit zu entrinnen. Ehrlich muss den Reporter schnell erreichen können, um die Angaben des Geschäftsführers zu entlarven. Aber wie soll das gehen? Gespräche über die Telefonanlage der Stadtwerke scheiden aus. Jede Verbindung wird protokolliert, jeder ein- und ausgehende Anruf festgehalten – ein viel zu hohes Risiko, um die Anlage zu nutzen. Auch bei Handy-Telefonaten ist Ehrlich unwohl zumute. Die Staatsanwaltschaft ermittelt im Bestechungsskandal. Kontrollieren die Ermittler auch die Verbindungsdaten von privaten Handys, um dem Informanten von Reporter Feder auf die Spur zu kommen? Ehrlich hat keine Antwort. Er will auf Nummer sicher gehen. Aber wie?

Die Geheimtricks

Reporter Feder und Informant Ehrlich können zahlreiche Tricks anwenden, um Lauschern das Leben zu erschweren. Dieser Abschnitt behandelt überwiegend Mobiltelefone. Festnetzgeräte werden nur vereinzelt erwähnt; sie sind für diskrete Gespräche weniger geeignet. Der Internet-Telefonie ist ein eigener Abschnitt am Ende des Kapitels gewidmet. Noch ein Hinweis: Die hier beschriebenen Methoden wurden kurz vor Veröffentlichung des Buches getestet. Sie funktionierten zu diesem Zeitpunkt. Doch Mobilfunk und Internet verändern sich schnell – technisch