»Der kleine Abhörratgeber« führt in angeblich hochkomplizierte Übertragungs-Techniken ein. Wie funktionieren die verschiedenen Varianten von Mikrofonen? Wo sitzt die Wanze? Was ist mit dem traditionellen Telefonverkehr und den drahtlosen Telefonsystemen, mit Radio, Bildschirm, Kabel, Kamera und nicht zu vergessen den Computernetzen, dem Internet und elektronischer Post. Der Band ist so aufgebaut, daß er als Handbuch nutzbar ist. Jedes Themenkapitel ist unabhängig von den anderen lesbar und verständlich.

Statt Verschwörungstheorie und Technikfeindlichkeit enthält der Band außerdem eine Diskette mit dem Verschlüsselungsprogramm Pretty Good Privacy (PGP, dt. Ziemlich Gute Privatsphäre).

ISBN: 3-89408-056-6

Der kleine Abhörratgeber

Edition ID-Archiv

Der kleine Abhörratgeber

Computernetze Telefone
Kameras Richtmikrofone

inkl. Diskette mit Verschlüsselungsprogramm

mit einem Nachwort von Otto Diederichs

Edition ID-Archiv

Der kleine Abhörratgeber

Computernetze, Telefone, Kameras, Richtmikrofone

Edition ID-Archiv
Berlin – Amsterdam

Titel der niederländischen Originalausgabe:
De muren hebben oren ...
Backslash, Hack-tic, Jansen & Janssen (Hg.)
Amsterdam 1994

Backslash, Hack-Tic, Jansen & Janssen,
AutorInnenkollektiv Keine Panik (Hg.)
Der kleine Abhörratgeber
Computernetze, Telefone, Kameras, Richtmikrofone
Mit einem Nachwort von Otto Diederichs
+ Diskette

Edition ID-Archiv
Postfach 360205
10972 Berlin
ISBN: 3-89408-056-6

1. Auflage April 1996

Titel
Eva Meier unter Verwendung eines
Fotos von Mike Schröder (argus)

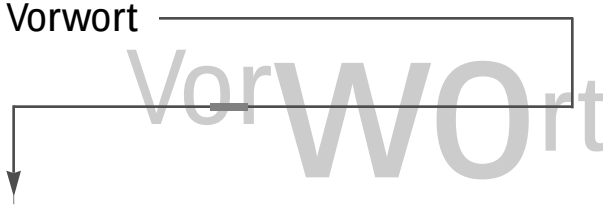
Layout
seb, Hamburg

Druck
Winddruck Siegen

Buchhandelsauslieferungen
BRD: Rotation Vertrieb
Schweiz: Pinkus Genossenschaft
Österreich: Herder Auslieferung
Niederlande: Papieren Tijger

Inhalt

Vorwort



Der kleine Abhörratgeber ist erstmals im Herbst 1994 in den Niederlanden unter dem Titel *De muren hebben oren* erschienen. Wir haben mit freundlicher Genehmigung der Herausgeberinnen dieses Buch übersetzt, aktualisiert und den technischen sowie juristischen Gegebenheiten in der BRD angepaßt.

Bespitzelung und Überwachung ist in der Regel eine Angelegenheit staatlicher Behörden, darauf geht Otto Diederichs in seinem Nachwort ausdrücklich ein. Sie gelten der Kontrolle innenpolitischer Opposition, von Wirtschaftsunternehmen oder Diensten konkurrenter Nationalstaaten. Mit der zunehmenden Technisierung der Gesellschaft wird es aber auch für Privatpersonen immer einfacher, sich die erforderlichen technischen Geräte und das notwendige »Know-How« zuzulegen, um beim Nachbarn mal eben über den Gartenzaun zu gucken.

Gegen einige »Überwachungstechniken« kann sich sehr leicht geschützt werden, gegen andere allerdings so gut wie gar nicht. Der kleine Abhörratgeber vermittelt das darum nötige Wissen, vor allem um mit der vermeintlich technischen Allmacht staatlicher Stellen und derlei Märchen aufzuräumen. Die einzelnen Kapitel des Buches sind auch unabhängig voneinander zu lesen und zu verstehen. Soweit es möglich war, sind sie in einfacher und verständlicher Sprache geschrieben, Fachausdrücke werden erklärt. Allerdings mußte bei einigen Passagen (wie etwa bei den computergestützten Verschlüsselungstechniken) etwas mehr ins technische Detail gegangen werden. Solche Stellen sind im Buch extra kenntlich gemacht und können je nach Interesse auch getrost überblättert werden.

Via Mailbox und Datenautobahn können heute binnen kürzester Zeit enorme Mengen an Information von einem zum anderen Ende der Welt transportiert werden. Dies birgt neue, bis vor kurzem undenkbare Möglichkeiten und Gefahren. Deshalb nimmt die Darstellung computergestützter Verschlüsselungsmethoden einen breiten Raum ein. Wir haben uns auch dazu entschieden, diesem Buch das Verschlüsselungsprogramm PGP (Pretty Good Privacy) auf Diskette beizulegen. PGP ist unserer Einschätzung nach das derzeit geeigneteste Verschlüsselungsprogramm. Der Austausch unserer Kommunikation muß frei und unkontrollierbar sein.

All jenen, die sich das Recht herausnehmen wollen, unzensiert und unbeobachtet vom »Großen Bruder« zu kommunizieren, wollen wir dieses Buch ans Herz legen. Außerdem ist es wirklich nicht teuer und auf seinem Umschlag steht in freundlichen Buchstaben KEINE PANIK.

Für alle in diesem Buch beschriebenen Schutzmaßnahmen gilt: die technische Entwicklung geht weiter und nichts, aber auch rein gar nichts, kann als absolut sicher gelten. Wir bedanken uns an dieser Stelle bei allen unseren Freundinnen und Freunden, die uns bei der Herausgabe der deutschsprachigen Ausgabe dieses Buches beraten und unterstützt haben, insbesondere bei *Cilip*.

AutorInnenkollektiv Keine Panik

Big Brother is Watching YOU

Es gibt in der BRD ein Grundgesetz. Im Artikel 1 steht, daß die Würde des Menschen unantastbar ist. Im Artikel 10 steht, daß es eine Unverletzlichkeit des Brief-, Post und Fernmeldegeheimnisses gibt. Das heißt, daß ohne spezielle Erlaubnis niemand die persönliche Kommunikation eines anderen überwachen darf. Die Ausnahmen von Artikel 10 werden durch besondere Gesetze geregelt, die Otto Diederichs am Ende dieses Buches erläutert.

Die staatlichen Behörden, die diese »Ausnahmen« durchführen, werden Geheimdienste genannt. Das sind in der BRD die Verfassungsschutzämter des Bundes und der Länder, die Staatsschutzabteilungen der Polizei, das Zollkriminalamt, der Militärische Abschirmdienst und der Bundesnachrichtendienst. Die Ausnahmen vom Artikel 1 werden in anderen Gesetzen geregelt.

Der Bundesnachrichtendienst mit Hauptsitz in Pullach bei München ist der größte und professionellste Abhör- und Entschlüsselungsspezialist der BRD. »Der Bundesnachrichtendienst sammelt zur Gewinnung von Erkenntnissen über das Ausland, die von außen- oder sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, die erforderlichen Informationen und wertet sie aus«, so steht es im Gesetz zum BND. Seit der Einführung des Verbrechensbekämpfungsgesetzes vom Dezember 1994 sind dem Treiben des Dienstes im Inland kaum mehr Grenzen gesetzt. Das Gesetz war vordergründig gegen die Bekämpfung des organisierten Verbrechens erlassen worden. Mußte der BND »innerdeutsche Zufallsfunde« bislang vernichten, so ist er nun dazu angehalten, diese Erkenntnisse an die jeweiligen Behörden von Staatsanwaltschaft, Zoll oder Polizei weiterzuleiten.

»Anders als alle Telefonüberwachungen ist die BND-Fernmeldeaufklärung nicht verdachtsbezogen. Es werden nicht zielgerichtet Straftäter, Verdächtige oder Kontaktpersonen überwacht. Vielmehr wird bewußt jedermann einbezogen, wenn mit Fernsprechteilnehmern im Ausland kommuniziert wird«, weiß der Bundesdatenschutzbeauftragte in seinem Tätigkeitsbericht 1994 zu berichten.

Die 7500 Mitarbeiter des dem Bundeskanzleramt unterstellten Dienstes scannen elektronische Post (E-Mail, Fax und Telefon) durch und benutzen dabei die beste Software, u.a. Wortbanken, die erfaßte Gespräche auf bestimmte Schlüsselbegriffe durchsuchen. Mehr als 50 Abhörstationen und ein Jahresetat von knapp 900 Millionen DM erlauben dem BND nicht nur Satellitenfunk, sondern auch jedweden Mobilfunk abzuhören.[1] Der Bundesdatenschutzbeauftragte ging für 1994 von täglich 100.000 überwachten Auslandskorrespondenzen und täglich etwa 4000 aufgezeichneten Gesprächen aus.[2] Und mit der neuen Fernmeldeanlage-Überwachungs-Verordnung (FÜV) wird dies noch einfacher.

Schöne Neue Welt

Aldous Huxley würde seine Zukunftsvision von der Schönen Neuen Welt etwas anders schreiben, wenn er die FÜV noch kennengelernt hätte, vielleicht auch das Bundeskabinett wegen geistigen Diebstahls verklagen. Seit dem 18. Mai 1995 ist die FÜV in Kraft.

Mit dieser Verordnung wird mehreres geregelt. Einerseits müssen die Betreibergesellschaften von Fernmeldeanlagen, z.B. für die Mobilfunknetze der Funktelefone, Abhörmöglichkeiten für die Sicherheitsbehörden schaffen. Festgelegt ist auch, welche Daten und Zusatzinformationen eines überwachten Anschlusses zu übermitteln sind. Gemeint sind damit die Nummern aller eingehenden und abgehenden Verbindungen, einschließlich aller mißglückten Versuche, die genutzten Dienste (z.B. Rufumleitungen), die benutzten Relaisstationen sowie sogenannte Verbindungsdaten wie Datum, Uhrzeit und Dauer der Kommunikation.

Da die Sicherheitsbehörden über leistungsfähige Software verfügen, sind sie damit ohne weiteres in der Lage Bewegungsbilder zu erstellen.

Was in den 70er und 80er Jahren noch als Rasterfahndung beeindruckte und teilweise sehr mühsam war, ist heute durch die größtenteils digitalisierte Datenübermittlung erheblich einfacher geworden. So läßt sich ohne große Mühe feststellen, wer nach 23.00 Uhr von Berlin aus in Paris anruft, oder von wo aus Handybesitzer Johann zwischen 16.00 und 18.00 angerufen hat.

Die Betreibergesellschaften für Mobiltelefone müssen genau definierte Schnittstellen zu Verfügung stellen, von denen aus die abgehörten Daten direkt, d.h. zeitgleich und unverschlüsselt, an die abhörende Einrichtung übermittelt werden können.[3]

In der Fernmeldeanlage-Überwachungs-Verordnung ist festgeschrieben, daß »die Überwachung von den ... Beteiligten nicht feststellbar« sein darf, und daß »die Überwachung und Aufzeichnung nicht in den Betriebsräumen des Betreibers« erfolgen darf. Nur »in Ausnahmefällen kann die Nutzung sonstiger Räume des Betreibers zu diesem Zweck erfolgen«.[4]

Die Diskussionen um die Einführung der FÜV verursachten in der ersten Jahreshälfte 1995 noch einigen Wirbel in der Presse. Das Bonner Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung bezeichnete die FÜV als Verschärfung und völlig neue Qualität beim Abhören.[5] Den meisten Ärger löste allerdings weniger die Tatsache aus, daß diese Verordnung nachhaltig in die Persönlichkeitsrechte und das Postgeheimnis eingreift, sondern daß die Betreiber der Fernmeldeanlagen die Kosten für die Überwachungsmaßnahmen selber zu tragen haben.[6]

Mailboxen

Die Fernmeldeanlage-Überwachungs-Verordnung (FÜV) trifft jeden Betreiber einer Fernmeldeanlage, »die für den öffentlichen Verkehr bestimmt ist« und damit auch Mailboxbetreiber, die schließlich ihre Mailbox bei der Telekom als solche anmelden müssen. Interessant ist hier der Punkt,

daß der Netzbetreiber, also der SysOp einer Mailbox, die Nachrichten dann unverschlüsselt weiterzuleiten hat. Das heißt noch lange nicht, daß du deine Daten nicht verschlüsseln darfst, das heißt nur, daß dein SysOp deine Daten nicht weiterverschlüsseln darf, bevor sie an einen der uns umsorgenden Sicherheitsdienste weitergeleitet werden.

Dieser Punkt wird heftig diskutiert. Wir sind der Meinung, daß Verschlüsselung nichts anderes als ein Briefumschlag für elektronische Post ist. Auch bei normaler Briefpost darfst du einen Briefumschlag benutzen, und es gibt bestimmte Gesetze, die es »Big Brother« erlauben, diesen aufzumachen und reinzugucken. Dagegen ist wenig zu machen. Wenn nun aber eine unerwünschte Person schlicht nicht in der Lage ist, einen Briefumschlag aufzumachen, dann ist das doch nicht dein Problem, oder?

Gesetzeslage zu Kryptographie und Europäische Perspektiven

Als Kryptoverfahren werden alle Verfahren bezeichnet, die zum Verschlüsseln oder Verschleiern geeignet sind. Häufig wird niemand aus der Kommunikation abgehörter Personen schlau, da diese in zunehmendem Maße Krypto-, also Verschlüsselungsgeräte, bzw. entsprechende Verschlüsselungssoftware verwenden. Der Krypto-Markt boomt.

Die rasante Entwicklung der Telekommunikationstechnik bildet eine Bedrohung für die »Sicherheitsbehörden«. Daß der Gesetzgeber der veränderten Praxis hinterherläuft, beweist die Tatsache, daß immer wieder neue Gesetzesvorschläge diskutiert werden. Trotz des Bestrebens, alle möglichen Kommunikationsformen in Gesetze einzubinden, ist es bisher nicht gelungen, mit den fortschreitenden Entwicklungen Schritt zu halten.

In der BRD gibt es zu Kryptographie noch keine bindende Gesetzgebung. Sowohl der Handel als auch die Benutzung von Verschlüsselungssystemen unterliegt unseres Wissens keiner weitreichenderen Regelung. 1992 gab es eine interne Diskussionsrunde, veranstaltet vom Bundesamt für Sicherheit und Informationstechnik, einer Einrichtung, die ursprünglich aus einer Dechiffrierabteilung des BND hervorgegangen ist,[7] bei der über die Einführung eines Krypto-Gesetzes diskutiert wurde. Vertreter von Bundeskriminalamt und Verfassungsschutz waren dafür, die Industrie dagegen.

Nach Informationen der Computerzeitschrift CHIP gibt es bereits Berechnungen des Bundesinnenministeriums zur Kosten-Nutzen Abwägung einer zentralen Krypto-Behörde, zur Zeit noch ohne Ergebnis. Von Seiten der CDU/CSU Fraktion werden Vorstellungen diskutiert, jegliche Verschlüsselungstechnik ganz zu verbieten oder zumindest nur staatlich lizensierte Kryptographie Versionen freizugeben.

Während es in manchen Ländern keine Kryptographiegesetze (BRD, Niederlande) gibt, ist in anderen Ländern die Benutzung sogar unter Strafe gestellt. In den Niederlanden liegt seit 1992 im Rahmen des Gesetzes zur Bekämpfung der Computerkriminalität eine Gesetzesinitiative fertig in der Schublade, die die Verschlüsselung von Informationen und Kommunikation regeln soll. Seit Dezember 1990 ist in Frankreich die Codierung nur mit einer Genehmigung zulässig und die wird an Privatpersonen nicht erteilt, ebenso in der Russischen Föderation, wo seit April 1995 die Anwendung und Herstellung von Verschlüsselungstechnik genehmigungspflichtig ist.

Anfang 1994 wurde auch bekannt, daß verschiedene niederländische Ministerien inoffiziell mit der National Security Agency, dem technischen Geheimdienst der USA, über ein Standard-Kryptosystem berieten. Die US-Regierung möchte ein weltweites Standard-Kryptosystem einführen, dessen Kernstück der Clipper-Chip ist. Ein winziger Chip, der in Telefone, Faxgeräte usw. eingebaut werden kann. 1993 erließ US-Präsident Clinton eine Direktive, in der er davon sprach, daß der Clipper-Chip die Datensicherheit erhöhen und Spionageaktivitäten ausländischer Nachrichtendienste durchkreuzen würde. Außerdem seien Ausfuhrbeschränkungen für andere Kryptosysteme unumgänglich. Diese Direktive löste eine heftige öffentliche Kontroverse aus, denn die NSA behält beim Clipper-Chip Zugang zu den Schlüsseln des chiffrierten Verkehrs und somit auch die Möglichkeit, den verschlüsselten Verkehr abzuhören. In den

USA bildeten sich Bürgerinitiativen, die gegen das Verschlüsselungsmonopol der NSA zu Felde zogen, denn sie sahen ihre Privatsphäre im digitalen Zeitalter bedroht. Gegenwärtig werden US-Behörden mit Kommunikationsgeräten der Firma AT&T, die den Clipper-Chip enthalten, umgerüstet.

Während die Gespräche zwischen den niederländischen Behörden mit der NSA vorerst im Sande verliefen, dürfte trotzdem zu erwarten sein, daß mit der europaweit forcierten Privatisierung von Post- und Telekommunikation auch hierzulande künftig Clipper-Chip-Geräte eingesetzt und angeboten werden.[8]

Zwar scheinen auch auf europäischer Ebene die grauen Männer den technischen Entwicklungen hinterherzulaufen, doch die Überlegungen, die dort angestellt werden, lassen wenig Gutes erahnen. Ende 1992 gab es einen Beschluß der EG-Innenminister, der besagte, daß Autotelefone kurzfristig anzapfbar sein müßten. Langfristig sollen Telekommunikationseinrichtungen standardmäßig mit Abhörmöglichkeiten ausgerüstet werden. Beides setzt sich heute in der Fernmeldeanlagen-Überwachungs-Verordnung der BRD um.

Im besten Orwellschen New-Speak wurde im Sommer 1995 von der Europäischen Union eine »Richtlinie zum Schutz personenbezogener Daten und der Privatsphäre« entworfen. Danach sollen

- personenbezogene Daten der Telekommunikation auch für andere Zwecke (z.B. Adressenhändler) zugänglich gemacht werden,
- die Gebühren der einzelnen Telefonbenutzer über mehrere Jahre in zentralen Datensammlungen erfaßt werden,
- die Vertraulichkeit der Datenverarbeitung sowie das Fernmeldegeheimnis vollständig entfallen.

Da die europäischen Gesetzgeber der Wirklichkeit hinterherzulaufen pflegen, können sich die LeserInnen dieses Buches leicht selber ausmalen, wo ihre Daten schon überall gespeichert sein werden.[9]

Anmerkungen

1 Chip 8/95, »Jeder ist verdächtig«
2 taz 14.7.95, »Grenzenloses Lauschen gestoppt«
3 telegraph 7/8-1995, »Ungeahnte technische Möglichkeiten«
4 taz 23.6.95, »Wie eine Spinne im Netz«
5 Funkschau 14/95, »Verbrechensbekämpfung contra Datenschutz«; Fiff-Büro, Reuterstr. 44, 53113 Bonn T. 0228-16-81547
6 Funkschau 13/95, »Mobilfunk: Streit um Abhörkosten«
7 taz 7.10.95, »Der BND hört alles«
8 William J.Clinton, The White House: Public Encryption Management Directive 15. April 1993, zitiert nach: Die Datenmafia, Egmont Koch/Jochen Sperber, Reinbek 1995
9 Der Spiegel 39/1995, »Hü oder Hott«

Das Abhören von Räumen

Die direkteste Kommunikationsform ist das Gespräch. Demzufolge ist Zuhören auch die direkteste Form, um über den Hörsinn etwas von jemandem aufzufangen. Beim Abhören handelt es sich dabei um Informationen, die nicht für einen bestimmt sind. Letzteres erfolgt äußerst häufig, und im Laufe der Zeit sind immer mehr Techniken entwickelt worden, die es dem Menschen ermöglichen, Ton und Gespräche aufzufangen.

Exkurs: Schwingung, Ton, Schall

Aber was ist nun eigentlich Ton? Ton ist Schall, und der hat mit Materiewellen zu tun: Teilchen beginnen zu schwingen, stoßen auf andere Teilchen, die daraufhin auch in Schwingung versetzt werden usw. Eine Schwingung (Welle), die an einer bestimmten Stelle beginnt, wird sich im Prinzip in alle Richtungen mit derselben Geschwindigkeit ausbreiten: Es entsteht eine Art kugelförmige »Außenhülle« aus Schall, die sich nach allen Seiten hin ausdehnt (ähnlich wie ein Luftballon, der immer weiter aufgeblasen wird). Diese »Außenhülle« wird Wellenfront genannt. Von einer gewissen Entfernung von der Schallquelle aus ist die Wellenfront bereits so breit, daß es für jemanden, der die Geräusche auffängt, so erscheint, als ob die Front »flach« wäre. Auch optisch kennen wir diese Erscheinung: Durch unsere beschränkte Sehkraft sehen wir den Horizont auch »flach«, während die Erde in Wirklichkeit rund ist.

Da »Schall« mit Materiewellen und Teilchen, die in Schwingungen versetzt werden, zu tun hat, könnten in einem luftleeren Raum keine Schallwellen entstehen, denn dort befinden sich keine Teilchen, die in Bewegung gesetzt werden können. Schallwellen gibt es nur dort, wo feste Materie, Flüssigkeiten oder Gase vorhanden sind.

Zwei Größen bestimmen die Schwingung der Teilchen und infolgedessen auch, wie die Schwingung auf Teilchen in der Nachbarschaft übertragen werden: die Frequenz, die sich auf die Geschwindigkeit bezieht, mit der das Teilchen schwingt, und die Amplitude, die den größten Ausschlag der Schwingung eines Teilchens von seiner Mittellage aus angibt.

Die Frequenz wird in Hertz (Hz) gemessen. Ein Teilchen mit einer Frequenz von 100 Hz schwingt 100 Mal pro Sekunde. Auf unserem Trommelfell werden die Frequenzen in unterschiedliche Tonhöhen »übersetzt«. Die Frequenz einer durchschnittlichen Stimme beträgt etwa 2.500 Hz, ein Ton von 50 Hz klingt beispielsweise äußerst tief. Unsere Ohren können Geräusche zwischen ungefähr 30 und 18.000 Hz wahrnehmen.

Die Amplitude wird von der Energiemenge bestimmt, die sich in einer Schwingung befindet. Jedes Teilchen, das anfängt zu schwingen, versetzt andere Teilchen in Schwingungen. Je weiter sich die Schwingung von der Schallquelle entfernt hat, desto mehr Teilchen werden von der Energie in einem dementsprechend großen Bereich betroffen sein. Die Schwingung wird also schwächer. An einem bestimmten Punkt wird der Schall so schwach, daß er von Menschen nicht mehr wahrgenommen werden kann. Die Amplitude wird in unterschiedlichen Maßeinheiten gemessen. Zum Messen der Lautstärke, also der Intensität des Schalls, werden meistens Dezibel (dB) verwendet.

Da Teilchen gleichzeitig Bestandteil von verschiedenen Schwingungen sein können, bestehen die meisten Geräusche, die wir erzeugen und wahrnehmen, nicht aus einer einzigen Tonhöhe. Es entsteht eine Schwingung, die sich aus einer speziellen Art Addition aller unterschiedlichen Frequenzen und Amplituden ergibt. Es würde in diesem Rahmen zu weit führen, diese mathematische Formel darzulegen.

Es ist jedoch wichtig, daß durch die Kombination von Tönen verschiedener Frequenz und Amplitude erkennbare Geräusche entstehen. Musik, Sprache und persönliche Sprachmerkmale (Stimme, Stimmfall, Betonung usw.) bestehen deswegen, weil wir sich daraus ergebende Geräusche wahrnehmen.

In bezug auf das Abhören, ist es wichtig zu wissen, daß auch das Umgekehrte möglich ist: und zwar die Zurückführung eines Geräuschs auf die unterschiedlichen Frequenzen und Amplituden, aus denen es besteht. Bestimmte Frequenzen können unterdrückt werden, wenn sie nicht relevant oder sogar störend sind. Dieses sogenannte »Filtern« wird in allen modernen Audiogeräten angewandt, um bestimmte Arten von Rauschen zu entfernen. Die übrigen Geräusche kommen dadurch besser zur Geltung.

Menschen hören mit ihren Ohren. Luftteilchen schwingen gegen das Trommelfell, das je nach Frequenzhöhe und Amplitudenpegel des Geräuschs in Schwingungen versetzt wird. Die Trommelfellbewe-

gungen werden durch Nerven registriert, welche die dazugehörigen Impulse an das Gehirn senden. In einem Mikrofon geschieht eigentlich genau dasselbe. Die Membran übernimmt die Funktion des Trommelfells. Dessen Bewegungen werden in ein elektrisches Signal umgesetzt, das wiederum aus einer Addition aller Frequenzen und Amplituden besteht, die gemeinsam das Geräusch bestimmen. Das elektrische Signal eines Mikrofons ermöglicht es, das Signal weiter zu bearbeiten: Es kann auf Kassette, CD oder ähnliches gespeichert werden. In gespeichertem Zustand können danach diverse Filtermethoden angewendet werden, um die Qualität der Bestandteile, die für den Nutzer interessant sind, zu verbessern.

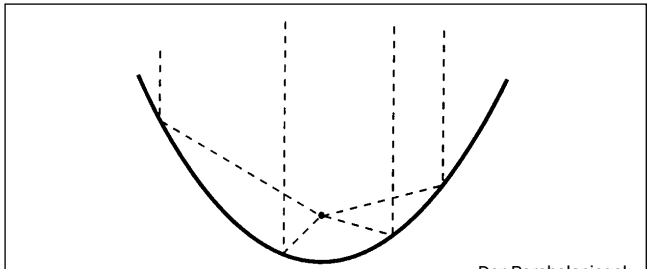
Zur Schallerzeugung benutzen wir unsere Stimmbänder, die über Schwingungen die sich daneben befindlichen Teilchen in Bewegung versetzen. Der Lautsprecher bildet die mechanische Variante der Stimmbänder. In einem Lautsprecher befindet sich eine Membran, die infolge eines elektrischen Signals in Schwingungen versetzt wird. Die Vehemenz und Geschwindigkeit, mit der die Membran schwingt, bestimmt dann wieder die Amplitude und Frequenz des erzeugten Schalls. In modernen Lautsprechern werden häufig zwei oder drei Membranen eingesetzt, weil es technisch nicht möglich ist, mit lediglich einer Membran schöne, naturgetreue hohe und tiefe Töne zu erzeugen.

Richtmikrofone

Es gibt eine ganze Reihe von Abhörtechniken. Die meisten werden zum Beispiel das Richtmikrofon kennen. In seinem Inneren befindet sich ein Teil, das Druck- bzw. Schallwellen in Elektrizität umwandelt. Das wichtigste Merkmal eines Richtmikrofons ist, daß ein »Spezialspiegel« verwendet wird, um Geräusche aus einer ganz bestimmten Richtung aufzufangen, so daß Hintergrundgeräusche aus anderen Richtungen herausgefiltert werden. Das Prinzip des sogenannten Parabolspiegels wird heutzutage vielfach angewendet. Dies ist beispielsweise bei Autoscheinwerfern der Fall. In diesen befindet sich eine relativ schwache Lampe, deren Licht über einen speziell geformten Reflektor so zurückgeworfen wird, daß es in eine einzige Richtung gesendet wird. Das Ergebnis ist ein kräftiger, konzentrierter Lichtstrahl.

Mathematisch läßt sich leicht errechnen, welche Form ein »Spiegel« haben sollte, um Schallwellen in einem Punkt zu bündeln (der sogenannte Brennpunkt oder Fokus). Die

praktische Anwendung dieser Theorie bildet der Parabolspiegel. Siehe nachstehende Skizze:



Der Parabolspiegel:
Alle Linien laufen im Brennpunkt zusammen.

Der Parabolspiegel wird zum Beispiel beim »Lauschen in den Weltraum« (Funkwellen-Sternwarten) und auch bei TV-Parabolantennen zum Empfangen von Satellitensignalen benutzt. Unter optimalen Verhältnissen und mit Hilfe moderner Filtertechniken ist es mit Richtmikrofonen möglich, auf Entfernungen mehrerer hundert Meter bishin zu ein paar Kilometern Gespräche aufzufangen. Die Wellenfront muß dann allerdings vollkommen gerade in das Mikrofon eingehen und völlig »flach« sein. Ein Problem dabei ist, daß extrem empfindliche Parabolrichtmikrofone auch äußerst empfindlich auf Abweichungen von den optimalen Verhältnissen reagieren.

Es gibt diverse Gründe, warum sich eine »ideale« Situation in der Praxis kaum ergibt. So kann die Wellenfront lediglich völlig gerade in das Mikrofon eingehen, wenn die abgehörten Personen stillsitzen. Außerdem dürfen sich zwischen Objekt und Mikrofon keine Hindernisse befinden. Gebäude, Bäume und Hügel bilden in diesem Zusammenhang störende Hindernisse.

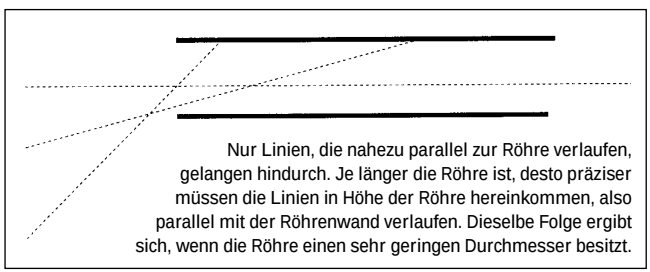
Es entsteht eine »flache« Wellenfront, wenn sich der Schall in alle Richtungen mit derselben Geschwindigkeit fortpflanzt. Das ist jedoch infolge unter anderem des Luftdrucks, der Luftfeuchtigkeit, der Windgeschwindigkeit, atmosphärischer Schichten und anderer Faktoren nicht immer der Fall. Jeder kennt das Phänomen, daß bei einem kräftigen

Sturm, das Geräusch schnell »verweht«. Aber auch Turbulenzen und Wärme, die durch eine vielbefahrene Straße verursacht werden, können die Arbeit mit einem Richtmikrofon über lange Entfernungen erschweren, beziehungsweise unmöglich machen.

Abgesehen davon besitzt das modernere Richtmikrofon einige andere Nachteile, es ist relativ teuer und seine Bedienung erfordert qualifiziertes Personal. Angesichts der Tatsache, daß für ein hochwertiges Richtmikrofon mehrere Zehntausend Mark hingeblättert werden müssen, werden sie nahezu ausschließlich von großen professionellen Lauschern benutzt. Und auch diese werden das Richtmikrofon nicht ohne weiteres routinemäßig benutzen, sondern nur innerhalb von Operationen, denen sie hohen Stellenwert beimessen.

Das kleinere Richtmikrofon ist ein Sammelname für eine Reihe von Techniken zum Auffangen von Geräuschen aus einer bestimmten Richtung, ohne daß dabei ein Parabolspiegel Anwendung findet. Das Grundprinzip ist sehr simpel: Alle Wellen, die aus einer anderen als der gewünschten Richtung kommen, werden unterdrückt. Falls das Signal, das übrig bleibt, sehr schwach ist, kann es mit Hilfe moderner Methoden verstärkt werden.

Das Grundprinzip ist leicht nachzuahmen, indem man eine Pappröhre an sein Ohr hält. Geräusche, die aus der Richtung kommen, in welche die Röhre gerichtet ist, sind dann gut zu hören, während andere Geräusche gedämpft werden (siehe Skizze).



Nur Linien, die nahezu parallel zur Röhre verlaufen, gelangen hindurch. Je länger die Röhre ist, desto präziser müssen die Linien in Höhe der Röhre hereinkommen, also parallel mit der Röhrenwand verlaufen. Dieselbe Folge ergibt sich, wenn die Röhre einen sehr geringen Durchmesser besitzt.

Es ist längst möglich, äußerst kleine Mikrofone zu bauen, in diesen Fällen wird eine dünne, kurze »Röhre« verwendet. Es gehört auch zu den Möglichkeiten, die Röhre mit einem speziellen akustischen Material auszutauschen, daß aus tausenden winzigen »Röhrchen« besteht. Ferner kann ein spezielles »Trommelfell« im Mikrofon benutzt werden. Indem man eine große Anzahl von Sensoren befestigt, ist zu ermitteln, welches Teil als erstes schwingt. Bei Geräuschen aus anderen Richtungen wird sich eine, zwar äußerst geringe, aber meßbare Verzögerung ergeben. Diese Signale können danach elektronisch herausgefiltert werden.

Alle diese Techniken werden bei den handelsüblichen Richtmikrofonen verwendet, die mittlerweile sehr verbreitet sind. Bei Musikkonzerten werden sie benutzt, um jedes Instrument einzeln unterscheidbar hören zu können, an modernen Videokameras befindet sich in der Regel ein gutes Richtmikrofon und sogar in einem Walkman besserer Qualität mit Aufnahmefunktion steckt gegenwärtig solch ein Mikrofon.

Für Abhörer haben kleine Richtmikrofone eine Reihe deutlicher Vorteile: Sie sind handlich, leicht zu verbergen und problemlos mobil einsetzbar. Sie sind auch äußerst einfach zu bedienen. Ohne daß weitere langwierige Einstellungen erforderlich wären, kann man einfach auf das abzuhörende Objekt zielen und mithören. Und sie sind billig genug (um die 1000 DM), um routinemäßig eingesetzt zu werden.

Die Empfindlichkeit genügt nicht, um über längere Entfernungen als 200 Meter noch ein erkennbares Signal aufzufangen. Sie sind jedoch dazu geeignet, einem Gespräch in einer vollen Kneipe, einem Theatersaal und ähnlichen Räumlichkeiten zu folgen. Voraussetzung ist allerdings, daß das Richtmikrofon immer auf die abgehörten Personen gerichtet ist. Wenn diese sich so schnell bewegen, daß das Richtmikrofon nicht hinterherkommt, wird das Abhörergebnis natürlich schlechter.

Reflexion

Reflexionsmethoden beruhen auf dem Prinzip, daß in einem Raum, in dem geredet wird, bestimmte Teile, wie Fenster mitschwingen. Mit Hilfe eines Laserstrahls, der auf das Fenster gerichtet ist, können diese Schwingungen aufgefangen

werden. Technisch ausgedrückt, wird das zurückkehrende Signal durch das Schallsignal aus dem Zimmer moduliert.

Möglicherweise mutet dies wie Science-fiction an, das ist es aber absolut nicht. Lasergeräte werden seit Jahren von Geheimdiensten effektiv eingesetzt. Im spezialisierten Fachhandel ist bereits für etwa 4000 DM ein komplettes Set mit Infrarotlaser, Auffanggerät und Filtern erhältlich, mit dem bis auf ca. 200 Meter Entfernung ziemlich gute Ergebnisse erzielt werden können. Nachteil ist auch hier, daß sich zwischen dem abzuhörenden Gebäude und dem Gerät eine »Sichtlinie« befinden muß.

Nicht nur Fenster, sondern auch Spiegel und Lautsprecher können als »Spiegel« benutzt werden. Hier ein Beispiel aus der Welt von James Bond. Vor etwa dreißig Jahren schenkten die Sowjets dem amerikanischen Botschafter in Moskau eine mit prächtigen Stichen geschmückte Wandtafel. Der CIA untersuchte sie, konnte nichts finden, und sie wurde also aufgehängt. Nach einer gewissen Zeit merkte der CIA, daß starke Mikrowellen, wie vom Mikrowellenherd bekannt, auf das Gebäude gerichtet waren. Nach langen Nachforschungen bekam der britische Geheimdienst heraus, daß die Wandtafel einen Hohlraum enthielt, der sich als »Spiegel« für Mikrowellen eignete.

Kontaktmikrofone

Auch der Einsatz von Kontaktmikrofonen erfolgt »passiv«: Lauscher brauchen sich keinen Zugang zu den Räumlichkeiten, die sie abhören möchten, zu verschaffen. Es gibt verschiedene Kontaktmikrofonarten, die auf unterschiedlichen technischen Prinzipien basieren. Das Grundprinzip ist allerdings bei allen dasselbe: Schall, der in einem Zimmer erzeugt wird, versetzt auch die Wände des betreffenden Raums in Schwingungen. Indem man diese winzigen Schwingungen auf der anderen Seite der Wand auffängt und verstärkt, ist es möglich, die Schwingungen wieder in verständliche Geräusche zu »übersetzen«.

Soweit die Theorie. In der Praxis erweist sich dies jedoch als schwieriges Unterfangen. Es ist schwer vorherzusagen, welche Art Wand die Schwingungen an welcher Stelle gut

leitet, und oftmals entstehen infolge von Schritten, Verkehr usw. »Hintergrundgeräusche«.

Für Abhörer ergeben sich hier folgende Vorteile: Das Mikrofon braucht nicht im Zimmer selbst installiert zu werden, und Kontaktmikrofone sind mit den üblichen Gegenabhörtechniken kaum aufzuspüren. Die ganze Anlage (Kontaktmikrofon, kräftiger Verstärker und ein Speichermedium wie ein Kassettenrecorder) kostet etwa 2000 DM, am Geld dürfte es also nicht liegen. Der große Nachteil ist, daß es beileibe nicht immer gelingt, eine gute Tonqualität zu erhalten. Wenn die Lage vor Ort zufälligerweise günstig und eine gut leitende Wand (oder Wasserleitung, Heizungsrohr usw.) vorhanden ist, so ist das Kontaktmikrofon ein effektives Mittel. Kontaktmikrofone gehören zur Standardausrüstung professioneller Lauscher.

Mikrofone in Räumlichkeiten

Ein im Raum installiertes Mikrofon bringt die beste Tonaufnahmequalität. In den USA und seit kurzem auch in den Niederlanden werden solche Aufnahmen in Gerichtsverfahren als beweiskräftiges Material zugelassen, in der BRD soll dies durch eine Gesetzesinitiative, dem sogenannten Großen Lauschangriff legitimiert werden. Daß dieses aber auch durch die Hintertür erfolgen kann, bekamen mehrere mutmaßliche Redakteure der Zeitschrift »radikal«, die von Juni bis Dezember 1995 im Knast inhaftiert waren, zu spüren. Ihr angeblicher Redaktionstreffpunkt in einem Haus in der Eifel war mit Wanzen gespickt. Die dort geführten Gespräche über Erscheinungsweise und Inhalt der Zeitschrift werden nun als Beweismittel gegen sie verwandt.

Dennoch haften auch an dieser Methode eine ganze Reihe Nachteile und praktische Probleme. So ist es erforderlich, den abzuhörenden Raum mindestens einmal zu betreten, was nicht immer einfach ist. Ferner besteht die Gefahr, daß die abzuhörenden Personen das Mikrofon finden und Gegenmaßnahmen ergreifen.

Das Verstecken von Mikrofonen bildet kein unüberwindbares Hindernis, da ein modernes Miniaturmikrofon mit Batterien kleiner ist als ein Fingerhut. Auch besteht die

Möglichkeit, piezoelektrisches Papier zu verwenden. Dieses »Papier« setzt Druckunterschiede in elektrische Impulse um, wodurch es sich hervorragend als Mikrofon verwenden läßt. Sicherlich lassen sich in einem Raum, in dem mit Papieren gearbeitet wird, immer eine Vielzahl von Versteckmöglichkeiten finden ...

Das komplizierteste Problem des Ganzen ist in der Regel der Transport nach draußen. Man kann sich dafür entscheiden, den Minikassettenrecorder im Abhörraum zu verstecken. Der Nachteil ist, daß ein solcher Recorder relativ groß ist und der Abhörer regelmäßig den Ort betreten muß, um die Bänder zu wechseln.

Es können auch Minisender mit drahtloser Verbindung benutzt werden. Dies verleiht dem Abhörer die Möglichkeit, die Signale in ein paar hundert Meter Entfernung aufzufangen. Obwohl die gegenwärtigen Sender so klein wie eine Streichholzschachtel und also relativ einfach zu verstecken sind, haben sie dennoch eine Reihe von Nachteilen. Die Batterien reichen höchstens für ein paar Wochen. Darüber hinaus gibt es verschiedene Techniken, mit denen die Sender geortet werden können.

In dem obengenannten Fall der Verwanzung einer angenommen Redaktionskonferenz der Zeitschrift »radikal« in der Eifel im September 1993, waren offensichtlich Wanzen u.a. in den Steckdosen (wegen der Stromversorgung) und in Tischbeinen versteckt worden. Die Aufzeichnung der Gespräche soll einige hundert Meter entfernt stattgefunden haben.[1]

Eine weitere Methode, das Schallsignal nach draußen zu transportieren, ist der Einsatz einer Kabelverbindung zu einem angrenzenden Raum. Dafür ist eine kleine Öffnung in der Wand erforderlich. In den meisten Räumlichkeiten ist das kein Problem (Steckdosen, Leitungen usw.). Die »Kabel« können auch aus hauchdünnen Glasfasern bestehen, die zum Beispiel von einem Metalldetektor nicht geortet werden können.

Eine interessante Glasfaservariante ist, nur eine einzige Faser im abzuhörenden Raum enden zu lassen. Von der »Empfangsseite« wird durch diese eine genauestens bestimmte Lichtart hindurchgeschickt, beispielsweise aus einem äußerst schwachen Laser oder einer gut justierten LED-Lampe. Eine LED ist eine kleine »Lampe«, die Licht in einer bestimmten Wellenlänge sendet. Jeder hat sie schon mal gesehen, Beispiele wären die kleinen roten, grünen oder gelben Lampen an modernen Stereoanlagen, Kameras u.ä. Die teureren Varianten sind präzise justiert. An der »Mikrofonseite« wird die Glasfaser von einer besonderen Membran bedeckt, welche die Lichtwellen zurückwirft. Diese Membran schwingt infolge produzierter Schallwellen auch mit und moduliert dadurch die Lichtwellen. Resultat ist ein extrem kleines »Mikrofon«, das praktisch nicht zu orten ist! Das Glasfasermikrofon ist, soweit wir wissen, noch nicht im Handel erhältlich, das Prinzip ist jedoch simpel. Ein paar Hobbybastlern in den USA ist es gelungen, solch ein Ding für ein paar tausend Mark an Materialkosten herzustellen.

Das Signal des Mikrofons kann auch über bereits vorhandene leitende »Verkabelung« transportiert werden. In diesem Zusammenhang sind Telefon, TV-Kabel, Stromnetz, Wasserleitungen und Heizungsrohre zu nennen. Der Vorteil ist offensichtlich: Es ist nicht erforderlich spezielle und auffallende Kabel zu verlegen. Außerdem kann das Signal auf diese Art und Weise mit niedriger Frequenz gesendet werden, wodurch es schwerer aufzuspüren ist. Auch für diese Techniken gilt, daß ein versierterer Elektroniktüftler für ein paar hundert Mark ein funktionierendes System basteln kann. Interessant ist die Tatsache, daß in den USA Experimente mit einem System durchgeführt werden, wonach es möglich sein soll, Nachrichten über das bestehende TV-Kabelnetz versenden zu können, um sich so an Spielen oder Diskussionsprogrammen zu beteiligen.

Auf diesem Prinzip soll das »interaktive TV« beruhen, daß auch bald in der BRD eingeführt wird. Mit einem Druck auf die Fernbedienung können dann Waschmaschinen und Bücher bestellt werden.

Gegenmaßnahmen

Bleibt uns noch, etwas über die andere Seite der Medaille zu melden: Wie können Lauschangriffe verhindert werden?

Das erste und wichtigste ist, dafür zu sorgen, daß die Schallwellen nicht unnötig weit reichen. Also leise sprechen, wenn es niemand hören soll. Ferner gibt es unterschiedliche Methoden, Geräusche zu dämpfen. Es ist zum Beispiel bekannt, daß große Betriebe wie Philips besondere Sitzungsräume besitzen, die vollkommen schalldicht sind. Für Privatpersonen ist dieses drastische Verfahren allerdings nicht realistisch.

Dennoch gibt es eine Reihe von Methoden, die eventuellen Abhörern die Arbeit ganz schön erschweren. Bestimmte Dämmaßnahmen am Gebäude, wie Doppelfenster anzubringen, wirken sich auf die Richtmikrofone und Laser-Reflexionsgeräte störend aus. Weiter kann es sinnvoll sein, erkennbare Öffnungen in der Wand (wie zu große Löcher für Heizungs- und Wasserleitungen) abzudichten.

Tarnung, beziehungsweise das Vermischen von Gesprächen mit allerlei Hintergrundgeräuschen (Radio, heulendes Baby) funktioniert meistens, wenn es sich nur um neugierige Nachbarn handelt, gegen professionelle Abhörspezialisten hilft es wenig. Es ist heutzutage technisch leicht möglich, bestimmte Geräusche herauszufiltern. Man denke zum Beispiel an die vielen sogenannten Soundmix- und Samplergeräte. In diesem Zusammenhang gilt die Regel, daß die Filterung von Geräuschen sich in dem Maße vereinfacht, wie die »Störungsquelle« bekannt ist. Eine Kassette der Lieblingsgruppe, die jeden Tag gespielt wird, eignet sich also absolut nicht. Auch der in alten Filmen häufig benutzte Trick, Wasserhähne zu öffnen, ist gegenwärtig nicht mehr so sinnvoll. Eine interessante Variante könnte der sogenannte »Sonic Jammer« (Akustischer Klemmer) sein. Diese Methode basiert auf dem Prinzip, daß ein Schallsignal erzeugt wird, daß für das menschliche Ohr nicht hörbar ist, aber ein Mikrofon hingegen ganz schön durcheinanderbringt. Über deren praktische Anwendungsmöglichkeiten und Beschränkungen ist allerdings noch wenig bekannt. Möglicherweise eine Herausforderung für begeisterte Heimwerker?

Die älteste und immer noch wirkungsvolle Methode ist, bestimmte Informationen einfach für sich zu behalten. Darüberhinaus gibt es auch noch eine Reihe anderer Methoden,

um miteinander geräuschlos zu kommunizieren, wie etwa die Zeichensprache für Gehörlose ... Die Wohnung für ein vertrauliches Gespräch zu verlassen, kann auch schon eine wirksame Möglichkeit sein. Die Frage, wohin der Ausflug in diesem Zusammenhang gehen soll, ist hier allerdings nicht ganz unerheblich. Im allgemeinen gilt, daß es viel schwieriger ist, technische Abhörhilfsmittel einzusetzen, wenn das Objekt mobil ist. Geht man in einem Wald spazieren, in dem Totenstille herrscht, ist es für die Lauscher einfacher, ein Richtmikrofon zu benutzen, als in einer Stadt mit Autos, Fußgängern und Straßenbahnen. Andererseits ist es dort jedoch nicht undenkbar, daß ein Abhörer direkt und ohne jegliche technische Hilfsmittel ein Gespräch mithören kann. So ist es an einem verkaufsoffenen Samstagnachmittag in einer vollen Fußgängerzone ziemlich schwer zu überprüfen, ob man verfolgt wird oder nicht.

Ferner ist es wichtig, einen Treffpunkt zu wählen, bei dem Mithörer nicht bereits im Vorfeld Maßnahmen treffen können. Regelmäßige »geheime« Besprechungen an einem Tisch im Café Klatsch und Tratsch bleiben nicht immer privaten Charakters ... Dabei bleibt es immer wichtig, sich bewußt zu sein, daß Abhörer auch die Fähigkeit des Lippenlesens beherrschen können. Diese Möglichkeit darf sicherlich nicht außer acht gelassen werden. Manche Leute können das sehr gut und mit Hilfe von Kameras sogar auf große Entfernungen. Dieses Risiko ist auf ein Mindestmaß zu begrenzen, indem man sich mehr dem Gesprächspartner zuwendet und gegebenenfalls etwas schneller und unartikulierter spricht.

Schließlich noch eine Reihe technischer Hinweise zum Orten von Abhörgeräten: Minisender sind am besten mit Hilfe von Spezialgeräten zu orten, die ein großes Spektrum an Funkfrequenzen aufspüren können und so angeben, ob sich in der Nähe ein Sender befindet. Mit Hilfe eines sogenannten Feldstärkemessers läßt sich ein Sender am billigsten orten. Dieses Gerät kann angeben, ob in der nahen Umgebung ein Signal gesendet wird (bei den meisten innerhalb eines Frequenzspektrums von etwa 30 kHz bis 2 MHz), aber nicht, was gesendet wird. Das heißt, daß das Gerät nicht an-

zeigen kann, ob die Strahlen vom eigenen Computermonitor, dem drahtlosen Telefon der Nachbarin, dem lokalen Sendemast fünf Häuserblöcke weiter oder einem Abhörsender stammen. Mit einer gewissen Erfahrung kann man, indem man planvoll an die Sache herangeht, dennoch ziemlich schnell die Unterschiede zwischen den verschiedenen Sendequellen erkennen. Die Geräte besitzen den Vorteil, daß sie in eine Jackentasche passen und also überall anwendbar sind. Dies ermöglicht zum Beispiel die Ortung eines Peilsenders an einem Auto. Die Preise liegen je nach Empfindlichkeit und Benutzerfreundlichkeit zwischen 300 und 1200 DM.

Peilsender mal anders: bequem von Zuhause aus ...

Am modernsten ist es natürlich, die Spur der Peilsender per Satellit zu verfolgen. Von den niederländischen Justizbehörden ist bekannt, daß die dafür bereits verschiedentlich ARGOS in Anspruch genommen haben. ARGOS ist ein für wissenschaftliche Zwecke gedachtes Computer- und Satellitensystem, das beispielsweise dafür benutzt wird, Tiere, die mit einem Sender ausgerüstet sind, zu orten. Justiz und Polizei nutzen dieses System unter anderem, um Drogentransporten mittels versteckten Peilsendern zu folgen. Das Signal der Sender, niedrig auf dem 400 MHz-Band, wird von mehreren Satelliten empfangen, wodurch eine exakte Ortsbestimmung möglich ist. Die Ortsbestimmung ist über ein Computersystem abzurufen. Dieses »Tracking-System« wird auch in der BRD bereits verschiedentlich angewendet. Beispielsweise von großen Fuhrunternehmen, die ihre Transport-LKWs mit solchen Sendern ausrüsten, die ein unveränderliches Signal aussenden. Damit weiß die Zentrale, wo sich ihre jeweiligen LKWs in Europa gerade befinden und ob die Ware, ihren vorgesehenen Bestimmungsort auch tatsächlich erreicht. Auch Luxuslimousinen, gerne geklaut und in andere Länder verschoben, wurden schon mit Sendern versehen. Damit sind die Fahrzeuge immer lokalisierbar und die Transportrouten von Schieberringen zu ermitteln. Verschiedene Autoversicherer geben Preisnachlässe auf Fahrzeuge, die mit solchen Systemen ausgestattet sind. Aber

der Halter eines solchen Fahrzeuges muß damit rechnen, daß Aufenthalt und Fahrtrouten permanent aufgezeichnet werden, auch wenn sein Auto gar nicht als gestohlen gemeldet wurde.

Die satellitengestützten Systeme senden ihre Signale allerdings nur in sehr großen Zeitabständen, manchmal nur alle 10 Minuten ein Signal, so daß sie für die Observation in einer Großstadt wahrscheinlich keine große Rolle spielen. Hierfür müssen Peilsender benutzt werden, die direkt vor Ort aufgefangen werden.

In Berlin versteckte die Polizei 1988 bei einem Mann, gegen den zwei Ermittlungsverfahren wegen Einbruch anhängig waren, einen Peilsender im Auto. Diesem fielen zuerst die ihn verfolgenden Beamten auf, dann ein kleiner Kasten mit Antenne, der unter seinem Wagen mit zwei Magneten befestigt war. Als er den Kasten seinem Anwalt übergab, wurde der flugs von der Polizei beschlagnahmt. Kein Wunder, eine richterliche Anordnung zur Durchführung dieser Maßnahme hatte nicht vorgelegen.[2] Bei einem solchen Sender handelt es sich um einen Markierungssender, der ein bestimmtes Signal aussendet, daß den Verfolgern erlaubt, den eigenen Abstand zu dem Verfolgten zu bestimmen und so den Standort des Verfolgten einigermaßen genau herauszukriegen.

Es ist äußerst praktisch, zusammen mit einem Feldstärkemesser einen sogenannten Interzeptor zu benutzen. Dieses tolle Gerät, das oft kaum größer als ein Walkman ist, sendet ein Signal aus und scannt dann alle möglichen Frequenzbereiche durch, auf der Suche nach dem ausgesendeten Signal. Auf diese Weise können in der Nähe des Interzeptors angebrachte Sender/Wanzen geortet werden. Sind über das Gerät plötzlich die Stimmen anderer Leute in deinem Wohnzimmer zu hören, so wird es wirklich Zeit, gründlichere Nachforschungen anzustellen ...

Ein weiterer Vorteil ist, daß mit diesem Gerät auch der Funkverkehr von Personen, die einen observieren, abgefangen werden kann – sogar wenn man nicht genau weiß, auf welcher Frequenz dies erfolgt. Ein Nachteil des Apparats

besteht darin, daß er zur Ortung etwa eine Sekunde benötigt. Infolge dessen kann er äußerst kurze Impulse, wie sie oftmals von Peilsendern ausgehen, übersehen. Der Feldstärkemesser besitzt diesen Nachteil nicht, da er das elektromagnetische Feld auf einmal mißt, ohne dabei alle Frequenzen einzeln abzusuchen. Deshalb ist es am besten, eine Kombination aus Interzeptor und Feldstärkemesser zu verwenden. Der Preis eines Interzeptors liegt bei ungefähr 1500 DM.

Wenn man wirklich gründlich suchen möchte, wird man einen Frequenzzähler benutzen müssen, mit dem zu ermitteln ist, welches die Frequenz eines gesendeten Signals ist. Da der Sendeverkehr im Äther ziemlich strengen Bestimmungen unterliegt, ist es leicht, eine Anweisung der Herkunft des Signals zu erhalten, wodurch unschuldige und verdächtige Signale einfach zu identifizieren sind.

Frequenzzähler und verwandte Geräte eignen sich jedoch nicht für Laien oder gelegentliche Benutzer. Sie sind teuer (ein paar Tausend bis mehrere Zehntausend Mark) und um sie angemessen verwenden zu können, ist ein gutes technisches Fachwissen unabdingbar.

Scanner sind Geräte, die Frequenzen auf der Suche nach Sendern durchlaufen. Bis vor ein paar Jahren war der Betrieb dieser Geräte in der BRD verboten. Mittlerweile gibt es eine Gemeinde von Hobbyscannern, die sich ein Vergnügen daraus bereiten alle nur erdenklichen Funksprüche aufzufangen. Die einfachsten Handscanner sind bereits ab 300 DM zu kriegen. Solche die auf bestimmte engere Frequenzbereiche einstellbar sind, ab etwa 700 DM. Füher war es generell verboten, bestimmte Frequenzen, wie die des Polizeifunks abzuhören, darauf wurde auch bei den meisten Geräten hingewiesen. Um einen Funkscanner ordentlich bedienen zu können, braucht es allerdings etwas Erfahrung, denn aus dem Kauderwelsch der Hobbyfunker wird beim ersten Hören niemand schlau.

Übrigens gilt für alle diese Geräte, daß sie nicht unfehlbar sind: Die modernsten »spread-spectrum«-Sender (siehe das entsprechende Kapitel in diesem Buch) können sie beispielsweise nicht orten. Und selbstverständlich geben sie nur

über Abhöraktionen Auskunft, bei denen mit solchen Sendern gearbeitet wird.

Lauschangriffen mit Richt-, Kontakt- und Glasfasermikrofonen ist mit technischen Mitteln kaum etwas entgegenzusetzen. Manchmal ist es einfacher, die Personen zu erkennen, die jemanden abhören wollen, als die Geräte, mit denen sie das machen.

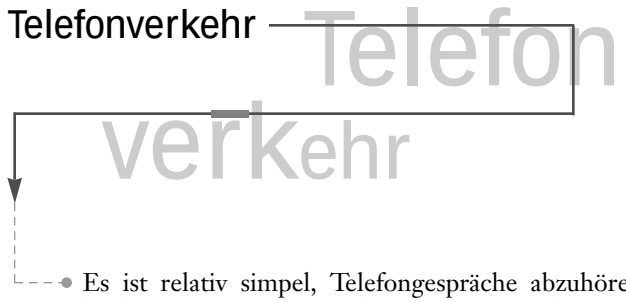
Manchmal gelingt dies allerdings auch mit den vorhin beschriebenen technischen Gegenmaßnahmen. So zeigte sich, daß in einem Fotokopierautomat in einem »sauberen« Raum in Stormont, dem Stadtparlament von Belfast, in dem sich Sinn-Fein-Vertreter zurückzogen, um sich während der Gespräche mit britischen Politikern in bezug auf den Friedensprozeß in Nordirland ungestört zu beraten, ein Abhörsender versteckt worden war. Dieser moderne Sender arbeitete auf einer Frequenz über 1000 MHz und benutzte »spread-spectrum«-Modulation. Der Sender wurde von Gerry Kelly während einer »Antiwanzenaktion« unter Verwendung eines Breitbandempfängers (»scanlock wideband receiver«) entdeckt. Die Entdeckung wurde den britischen Politikern mitgeteilt. Das Nothern Ireland Office verneinte, etwas mit dem Sender zu tun zu haben, republikanische Quellen wußten allerdings zu erzählen, daß es sich um eine typischen Wanze des britischen Geheimdienstes MI 5 handelte.

Anmerkungen

1 Der Spiegel 42/1995, »Big Bang in Wanderrath«

2 taz 21.7.1988, »Polizeilicher Piratensender«

Telefonverkehr



Es ist relativ simpel, Telefongespräche abzuhören. Privatdetektive, eifersüchtige Ehemänner, Betriebsspione, jeder, der etwas Geld für ein paar elektronische Geräte ausgeben möchte, kann mithören. Wie das in etwa funktioniert, und wie man etwas dagegen tun kann, ist in diesem Kapitel zu lesen.

Wir beginnen damit, ein paar Märchen zu widerlegen. Später beschreiben wir dann, wie Telefonleitungen angezapft werden und wie man sich davor schützen kann.

Die Märchen

• Ein Fax kann nicht abgehört werden.

Denkste! Früher war das lediglich mit Hilfe sehr teurer Geräte möglich, gegenwärtig sind jedoch Geräte erhältlich, die dieselbe Arbeit für ein paar Tausend Mark erledigen. Sogar ein Faxmodem kann dafür benutzt werden, den Faxverkehr einer angezapften Leitung lesbar zu machen.

• Computerverkehr ist nicht anzuzapfen.

Früher war dies tatsächlich ziemlich kompliziert. Nun ist alles, was über Telefonleitungen übertragen wird, aufzunehmen. Auf Band aufgenommener Modemverkehr ist im Handumdrehen in lesbare Sprache umzuwandeln und auszudrucken. Voraussetzung ist natürlich, daß die Nachrichten nicht verschlüsselt sind. Ein Computernetz erleichtert einem Abhörer die Arbeit ungemein. Er braucht lediglich alle Datenpakete, die ein Computer sendet und empfängt, zu kopieren und zu speichern. Bei den meisten Netzen ist dies ziemlich einfach: Im Prinzip kann jeder Computer alle Pakete, die gesendet werden, aufzeichnen. Es gibt gegenwärtig

Programme, die automatisch die gewünschten Pakete raussuchen.

• Ich habe doch einen Wanzendetektor!

Den hast du nicht. Die Mehrzahl der Geräte, die unter dem Namen »Wanzendetektor« oder ähnlichen Bezeichnungen im Handel erhältlich sind, spüren lediglich die einfachsten Abhörmittel auf. Mit dieser Art Detektoren ist zu ermitteln, ob jemand über einen anderen Apparat mithört. Auch eine parallele Anzapfstelle[1] kann damit entdeckt werden. Alle anderen Abhörmethoden sind mit diesen Geräten jedoch nicht aufzuspüren. Die Chance, mit solchen Detektoren eine Anzapfmethode, die über das Eigenbauniveau hinausgeht, zu entdecken, ist kleiner als die Chance, daß der Abhörer sich durch einen Fehler selbst verrät. Letzteres erlebte zum Beispiel die Redaktion der niederländischen Zeitschrift Hack-tic. Durch einen Anschlußfehler im Fernmeldeamt kamen sie dahinter, daß ihre Telefongespräche zerhackt (elektronisch verformt) an die Polizei oder den Verfassungsschutz weitergegeben wurden. Die Verformung sollte es den Postlern erschweren, selbst die angezapften Leitungen abzuhören.

• Ich rufe X an und bitte ihn schnell meine »sichere« Nummer zu wählen.

Bedauerlicherweise können professionelle Abhörspezialisten in sekundenschnelle eine andere Leitung anzapfen. Die Polizei hat in den meisten Fällen für diese Aktion nicht einmal eine zusätzliche Genehmigung nötig.

• Autotelefone und Handys können nicht abgehört werden.

Erzähle das mal einem beliebigen Besitzer eines Funkscanners oder beispielsweise der Utrechter Polizei. Letztere hörte zwei Jahre lang hunderte Autotelefone ab, um ein paar Gespräche herauszufiltern. Mit Scannern können nur mobile Telefongespräche, die analog funktionieren in der unmittelbaren Umgebung empfangen werden (mehr dazu im Kapitel Mobiltelefone). Es ist übrigens auch möglich, die Position eine Autos zu ermitteln, indem man die Bereitschaftssignale des Autotelefons oder des Handys anpeilt. Wir wer-

den uns im Kapitel »Drahtlose Telefonsysteme« hiermit eingehender befassen. Falls bekannt ist, welche Nummern die Autotelefonbenutzer anwählen, können die Gespräche im Fernmeldeamt abgehört werden. Ebenso wenn die Nummer des abzuhörenden Handys oder Autotelefons bekannt ist. Mit der seit 18. Mai 1995 in der BRD gültigen Fernmelde-Überwachungs-Verordnung müssen alle Betreiber digitaler Kommunikationstechniken, also auch die von Handys und Autotelefonen, bis zum Mai 1996 Abhörmöglichkeiten einrichten, die es den Sicherheitsbehörden erlauben, Inhalt und Kommunikationsprofil des jeweils abzuhörenden Anschlusses einzusehen.

• Von Telefonzellen aus kann man sicher telefonieren.

Telefonzellen sind genauso sicher wie Geschlechtsverkehr ohne Kondom: Es kann sehr lange gut gehen, aber früher oder später geht's schief. Die Post speichert die gewählten Nummern und staatliche Behörden – oder Privatdetektive mit Verbindungen – können sie anfordern. Die Polizei tut sich beim Abhören von Telefonzellen nicht schwer. Es wird einfach eine Wanze an der Telefonzelle angebracht, wenn dies »im Interesse der Ermittlungen« sein sollte. Dadurch, daß die Zellen öffentlich zugänglich sind, ist es darüber hinaus auch für Dritte außerordentlich einfach, dort einen Sender anzubringen.

Im Herbst 1989 kam die Polizei einem Berliner Trio auf die Spur, die mit Bombenanschlägen den Hertiekonzern erpreßt hatten. Ihr Fehler: Einer der Erpresser telefonierte von einer Telefonzelle in Belgien mit seinen Komplizen in Berlin-Neukölln und danach mit dem Hertie Konzern in Frankfurt/M. Was die Erpresser nicht wußten: Die belgische Telefongesellschaft speichert, angeblich nur aus Abrechnungsgründen, alle angerufenen Telefonnummern – auch die der Gespräche, die von Telefonzellen aus geführt wurden.[2]

• Es gibt besondere Telefonnummern, die einem verraten, ob man abgehört wird.

Blödsinn. Diese »Wanzen-Detektor«-Nummern, die für einen Haufen Geld verkauft werden, kontrollieren lediglich die Qualität der Telefonleitung. Jemand, der solch eine

Nummer wählt, hört einen Ton, der immer höher wird. Mit diesem Ton können die Telefonmonteure überprüfen, ob sich in der Leitung Filter befinden, die bestimmte Frequenzen herausfiltern. In dem Fall ist kein Ton zu hören. Es ist jedoch damit nicht zu hören, ob ein Abhörgerät an die Leitung angeschlossen ist.

Wo sitzt die Wanze, und wie funktioniert's?

• An der Leitung oder im Telefonapparat selbst

Für ziemlich wenig Geld sind Geräte erhältlich, die unmittelbar an die Telefonleitung von jemandem anzubringen sind. Die Apparate nehmen dann alle Gespräche auf, die über jene Leitung übertragen werden, oder senden sie über einen eingebauten Sender. Diese Art Wanzen sind weitgehend bekannt und mit Spezialgeräten, z.B. einem Interzeptor, leicht zu orten. In der eigenen Umgebung können solche Wanzen aufgespürt werden, indem man die Telefonleitung physisch überprüft.

Zum Einbau in den Telefonapparat selbst sind im Handel beispielsweise Abhörgeräte erhältlich, die den in alten Apparaten standardmäßig vorhandenen Kohlemikrofonen ähneln. Damit kann das Gespräch auch auf einer Funkfrequenz gesendet werden. Achte deshalb darauf, wer mit seinen Fingern an deinem Telefonapparat sitzt. Telefonmonteure sollten sich ausweisen, und man sollte immer in der Nähe bleiben, um zu gucken, was sie ausführen.

Allerdings solltest du wissen, daß du verbeamtete Abhörer hiermit kaum verunsichern wirst, auch ein Telekommitarbeiterausweis ist für die Staatsschutzbehörden kein Problem. Die Zusammenarbeit von Post, Telekom und Staatsschutzbehörden ist in der BRD sehr ausgereift. Allenfalls mittelmäßige Privatdetektive lassen sich vielleicht verschrecken.

• Im Schaltschrank

Jede Leitung führt früher oder später in einen Schaltschrank. Bei einem Wohnungskomplex steht dieser häufig im Keller. Es ist ziemlich einfach, dort eine Wanze anzubringen. Kurz mal eine Induktionsrolle[3] anbringen und fer-

tig ist die Laube. Professionelle Abhörspezialisten lassen sich kaum von ein paar Schlössern aufhalten, die den Keller und die Türen schützen sollten.

• In Telefonkästen

In den Telefonkästen auf der Straße laufen alle Kabel eines bestimmten Bezirks, z.B. eines Wohnblocks zusammen. Die Kabel können dort auch angezapft werden, wobei es möglich ist, die Daten über eine andere Fernsprechleitung sofort weiter zu schicken. Und wer wundert sich schon, wenn irgendein Monteur an den Kabeln eines Telefonkastens herumbastelt?

• In Fernmeldeämtern

Es ist ein Kinderspiel, innerhalb der Fernmeldeämter ein Abhörgerät anzuschließen. Das tatsächliche Abhören erfolgt in den meisten Fällen nicht im Fernmeldeamt selbst, sondern andernorts. Professionelle Abhörgeräte bestehen aus einer Haupt- und einer Arbeitseinheit (»master-« und »slave-unit«). Die Haupteinheit, die in der Regel beispielsweise im Abhörraum der Polizei steht, speichert die abgehörten Gespräche auf Band, Festplatte oder CD-ROM, während die Arbeitseinheit im Fernmeldeamt mit dem abzuhörenden Anschluß verbunden ist und die Gespräche an die Haupteinheit weiterleitet. Um zu verhindern, daß das Fernmeldepersonal mithören kann, werden die angezapften Daten oft auf einfache Art und Weise zerhackt. Bei Abhöranschlüssen innerhalb des Fernmeldeamts ist es äußerst fraglich, ob dies immer gemäß der Regeln der Strafprozeßordnung erfolgt.

Vor dem Mauerfall war in Berlin bekannt, daß in allen größeren Postämtern Stuben von den Allierten eingerichtet waren, in denen die Postüberwachung (Beamtenjargon »Prüfpost«) und oft auch die Telefonüberwachung stattfand. Allein im Postamt Wedding, das den französischen Allierten unterstand, befanden sich etwa 15 Tonbandgeräte zur Aufzeichnung überwachter Anschlüsse.[4]

• In Telefonzellen

Das Anzapfen von Telefonzellen kann auf diverse Arten und Weisen erfolgen. Über das Fernmeldeamt oder einfach in der Zelle. Im letzteren Falle wird ein Sender in der Zelle selbst versteckt, der meistens über die Spannung der Telefonleitung betrieben wird.

Als im November 1987 wieder einmal die Räumung der besetzten Häuser in der Hamburger Hafenstraße anstand, wurden mehrere Telefonanschlüsse rund um die besetzten Häuser, darunter mindestens drei Telefonzellen vom Hamburger Fernmeldeamt direkt zur zentralen Abhöranlage im Hamburger Polizeipräsidium umgeschaltet. Eine richterliche Anordnung wurde, wie so oft, erst später eingeholt. Hunderte von Telefongesprächen wurden auf Band aufgenommen und später abgetippt.[5]

• Drahtlose Telefone

Drahtlose Funktelefone sind eigentlich kleine Sender, die ein Signal zur Basisfunkstelle senden. Diese Basisfunkstelle gibt die Signale über die (übliche) Telefonleitung weiter. Drahtlose Telefone sind absolut nicht sicher. Jeder, der einen Funkscanner besitzt, kann mithören. Auch kann es passieren, daß Leute mit einem anderen Funktelefon deinem Gespräch folgen können.

Der »Schutz«, mit dem viele Funktelefonhersteller werben (»1000 Sicherheitscodes!«) sind Identifizierungscodes, die Handy und Basisfunkstelle miteinander austauschen, um zu verhindern, daß jemand mit einem anderen Telefon auf deine Kosten telefonieren kann. Diese »Sicherheit« hat also nichts mit Verschlüsselung oder Zerhacktechniken zu tun.

In der letzten Zeit kommen Telefone auf den Markt, die den Nachrichtenverkehr zwischen Basisfunkstelle und Handy zerhacken. Diese Telefone bieten zwar eine gewisse Sicherheit, ein professioneller Lauscher kann solch ein Gespräch jedoch entschlüsseln. Die Scramble-Telefone sind genauso verwundbar wie andere Funktelefone: Nach der Basisfunkstelle, also in der Telefonleitung, ist das Gespräch schließlich wieder entschlüsselt.

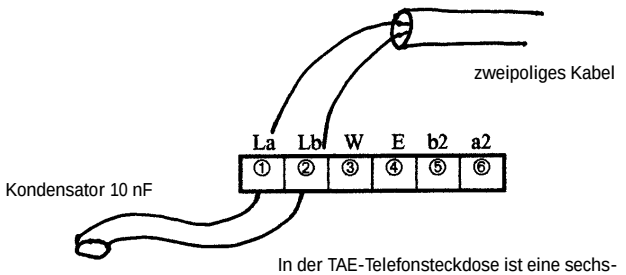
• »Frequency flooding« (Frequenzfluten), das Abhören einer Räumlichkeit mit Hilfe des Telefons

»Frequency flooding« ermöglicht es, über den Telefonhörer einen Raum abzuhören, während das Telefon nicht

benutzt wird. Das System kann bei jedem Telefontyp angewendet werden, aber vor allem die alten grauen Apparate mit Wählscheibe und Kohlenstoffmikrofon sind verwundbar. Frequency flooding funktioniert folgendermaßen: Über die Telefonleitung wird ein Hochfrequenzsignal, das von dem Signal, das normalerweise zu einem nicht benutzten Telefonapparat gesendet wird, zum Telefon geschickt. Durch das Signal wird das Mikrofon im Apparat aktiviert. Wenn in dem Raum, in dem sich das Telefon befindet, Geräusche zu hören sind, wird die Schwingung des Mikrofons beeinflußt (Modulation). Dadurch ändert sich auch das Signal in der Leitung. Dieses veränderte Signal wird vom Abhörer aufgefangen. Die Geräusche aus dem Zimmer werden aus dem Signal herausgefiltert und verstärkt. Daraufhin können sie zur Abhörzentrale geleitet und dort gegebenenfalls aufgenommen werden.

Wer vertrauliche Gespräche führt und befürchtet, daß das Telefon unter Frequency-flooding-Überwachung steht, kann dagegen eine Reihe von Gegenmaßnahmen treffen. Man kann natürlich einfach den Stecker aus dem Telefon ziehen, aber dann kannst du auch nicht mehr angerufen werden. Eine weniger rigorose Lösung ist, sich einen speziellen Tonfilter anzuschaffen, der vor den Telefonapparat zwischengeschaltet wird. Eine weitere Möglichkeit ist, im Stecker oder der Steckdose des Apparats einen Kondensator (10nF) anzubringen. Dadurch wird bewirkt, daß das zum Abhören erforderliche Signal in der Leitung kurzgeschlossen wird. Solch ein Kondensator kostet knapp eine Mark.

Anschließen eines 10 nF Kondensators an eine herkömmliche TAE-Telefonsteckdose. Der Kondensator wird parallel zu den beiden von der Post kommenden Anschlußkabeln angeschlossen.



In der TAE-Telefonsteckdose ist eine sechspolige Anklemmleiste. An die ersten beiden Kontakte (L_a und L_b) ist das von der Post kommende zweiadrige Anschlußkabel angeschlossen. Hier wird der 10 nF Kondensator angeschlossen.

Maßnahmen gegen das Abhören von Telefongesprächen

Mit den nachstehend angeführten Methoden sind nur bestimmte Wanzen zu finden. Ein Abhörgerät im Fernmeldeamt ist dadurch nicht aufzuspüren. Um zu erfahren, ob eine Leitung über das Fernmeldeamt angezapft wird, muß man schon eine(n) FreundIn bei der Post haben. Ein Abhöranschluß im Fernmeldeamt ist für interne MitarbeiterInnen fast immer zu erkennen.

• Die simpelste und billigste Methode ist, physische Nachforschungen anzustellen. Telefonabhörgeräte im Haus selbst sollten auf diese Art und Weise eigentlich aufzuspüren sein. Es ist schwer, alles zu kontrollieren, mit etwas Geduld und Erfindungsreichtum kommst du jedoch ein ganzes Stück weiter. Erst den Telefonapparat gut überprüfen. Nehme ihn auseinander und stelle einen Apparat desselben Typs daneben. Vergleiche die Telefone. Gibt es Einzelteile, die sich nicht im anderen Telefon befinden? Sind manche Einzelteile dicker als andere? Manchmal sind Wanzen nämlich als Transistor getarnt. Wie viele Kabel verlassen das Telefon? Bei manchen Bürotelefonen ist es ziemlich einfach, ein extra Kabelpaar an das Mikrofon anzuschließen und so die Gespräche andernorts abzuhören.

Verfolge auch die Kabel bis zu dem Punkt, an dem sie in der Wand verschwinden. Wenn sich draußen oder im Keller ein Schaltschrank befindet, solltest du diesen dann untersuchen, möglichst auch von innen.

• Abhörgeräte, die sich im Fernmeldeamt befinden, können mit Hilfe »weißer Rauschsignale« (statisches Rauschen) gestört werden. Das Rauschen wird durch die Filter des Fernmeldeamts mehr oder weniger entfernt, so daß dennoch ein ziemlich gut zu verstehendes Gespräch geführt werden kann. Die Abhörgeräte, die sich vor dem Fernmeldeamt befinden, nehmen dann Bänder mit Rauschen auf.

Lediglich mit modernsten Geräten kann noch ein erkennbares Gesprächs herausgefiltert werden.

• Es sind Geräte im Handel erhältlich, welche die Leitungsspannung während eines Gesprächs künstlich niedrig halten. Vorteil ist, daß ein eventuell angeschlossenes »drop-out«-Relais, ein Schalter, der benutzt wird, um einen Recorder zu steuern, nicht angeschaltet werden kann.

• Zum Kontrollieren der Leitung gibt es Meßgeräte, TDRs (»time-domain-reflectometry«-Messer = zeitbezogene Reflektionsmesser). Diese Meßgeräte funktionieren wie eine Art Radarsystem für Telefonkabel. Sie senden ein Signal und anhand des Echos ist zu ermitteln, wie lang die Leitung ist und ob störende Faktoren zwischengeschaltet sind. Im Prinzip sind diese Apparate ziemlich gut. Die Benutzung solcher Geräte erfordert jedoch spezifische Fachkenntnisse, wodurch nicht jeder mit ihnen umgehen kann. Die meisten Geräte sind darüber hinaus teuer (über 5000 DM). Gegebenenfalls ist es möglich, mit einem Volt/Ohmmeßgerät zu kontrollieren, ob die Spannung der Telefonleitungen gleichmäßig ist. Wenn Du mit dieser Methode gute Ergebnisse erzielen möchtest, so ist es jedoch erforderlich, die Leitung regelmäßig zu überprüfen und die Resultate aufzuschreiben. Es ist praktischer, ein professionelles Wanzensuch-Team anzuheuern, das ist allerdings auch teurer.

• Möchtest du ganz sicher wissen, daß nirgendwo, auch nicht im Fernmeldeamt, mitgehört wird, ist das Telefongespräch oder der Datenverkehr zu verschlüsseln. Verschlüsselung von Gesprächen ist kostspielig. Es sind Geräte erhältlich, die zwischen Telefon und Anschluß geschaltet werden und die Sprache in einen unentzifferbaren Tonsalat umwandeln. Du solltest möglichst ein Gerät wählen, das Sprache in digitale Signale umsetzt und danach die digitalen Signale verschlüsselt.[6]

• Eine einfache Methode, um unerwünschte Mithörer hinters Licht zu führen, ist, Gespräche in Codeform zu führen. Ein Code nützt im übrigen wenig, wenn er als solcher zu erkennen ist. Bei: »Das Päckchen ist in Sicherheit«, spitzt der Lauscher seine Ohren, während er bei: »Übrigens, Werner läßt dich schön grüßen«, einfach weiterdöst. Wirkungsvolle Codesätze sind oft in lange, langweilige Gespräche über beispielsweise das Wetter, neue Automarken, Computer oder sonstige alltägliche Themen eingebettet. Sinnvollerweise werden von verschiedenen Leuten nicht dieselben Codesätze verwendet und auch nirgendwo schriftlich hinterlegt. Leute, die sich lange Codesätze nicht merken können, wissen sich oftmals mit verschlüsselten Computerdateien zu helfen.

• Mit dem Erzählen von Falschinformationen kann man Abhörleute völlig aus dem Häuschen bringen und möglicherweise auch herausfinden, ob man abgehört wird.

Analyse des Telefonverkehrs

Auch ohne abgehört zu werden, können die Sicherheitsbehörden eine Menge erfahren. Die Telefongesellschaft speichert, wer mit wem und wie lange telefoniert hat. ALLE Nummern, die du anrufst, auch wenn keine Verbindung zustandekommt, werden registriert und in einem sogenannten »caller log« festgehalten. Die Tatsache, daß auf deiner Rechnungsübersicht keine für dich gebührenfreien Nummern aufgeführt werden, heißt noch lange nicht, daß diese Nummern nicht registriert werden. Sie werden halt bloß nicht auf die Rechnung geschrieben. Auch die Nummern, die von Telefonzellen aus angewählt werden, sind beim Fernmeldeamt registriert. Wenn jemand also sieht, daß du telefonierst, braucht derjenige sich lediglich das Datum und den Zeitpunkt zu notieren und kann so herausfinden, wen du angerufen hast.

Zum Anfordern eines »caller log« benötigt die Polizei keine spezielle Genehmigung. Nach Paragraph 12 des Fernmeldeanlagengesetzes dürfen Gerichte und Staatsanwaltschaft in Bagatellfällen Einsicht in Daten der Telekom nehmen (also wer telefoniert mit wem, wann und wie lange). Es ist demnach also möglich, daß die Behörden »für den Fall der Fälle« die Daten ganz Deutschlands speichern.

Indem »caller logs« einer Datennetzanalyse unterworfen werden, sind sehr interessante Informationen zu erzielen. Ein kleines Beispiel: Mona ruft oft Peter an. Nach einem mißlungenen Banküberfall (verübt von Peter) ruft sie gar

nicht mehr an. Das geht auch gar nicht, denn der hat sich abgesetzt. Mona telefoniert nun aber auf einmal irrsinnnig häufig mit Harry. Aus dieser Datennetzanalyse könnte nun die Schlußfolgerung gezogen werden, daß Harry weiß, wo Peter sich befindet. Natürlich braucht das nicht zu stimmen, womöglich hat Mona was mit Harry. Die Datennetzanalyse ist für die behördlichen Stellen jedoch interessant genug, um Harrys Leitung anzuzapfen.

ISDN

ISDN ist die Abkürzung von Integrated Services Digital Network (Integrierter digitaler Netzwerkservice). Alle Daten, auch Bild und Ton, können mit großer Geschwindigkeit (z.B. über Glasfaserkabel) digital gesendet werden. Die Gefahr, daß die Daten verformt werden, ist dabei viel geringer als bei herkömmlichen Telefonkabeln. Ein anderer »Vorteil« von ISDN ist die Leichtigkeit, mit der Daten abgeschöpft werden können: Das Anzapfen eines Gesprächs ist nun nicht aufwendiger als das Kopieren von ein paar Bitreihen.

Mit ISDN kann jeder Anschluß die Dienstleistung, genannt CID (Caller Identity = Anruferidentität), benutzen. CID zeigt die Nummer desjenigen, der anruft. In der BRD ist diese Möglichkeit infolge der Computerisierung der Fernmeldeämter nun für den normalen Telefonverkehr möglich. In einigen Berliner Senatsdienststellen ist dieses System bereits installiert. Damit wird es entsprechenden Unternehmen ermöglicht, beispielsweise im Finanzamt anzurufen und sich gleich in die eigene Lohnsteuererklärung einzuwählen. Die Identifizierung geschieht dabei über die Telefonnummer des Apparates, von dem aus angerufen wird.

Darüberhinaus bewahrt die Telekom alle Verbindungsdaten, also wer hat wen, wann, wie lange angerufen, aus Abrechnungsgründen 80 Tage auf. Danach werden die Daten angeblich gelöscht.

Anmerkungen

1 Paralleles Anzapfen erfordert meistens eine eigene Stromquelle (Batterie o.ä.). Solche Abhörgeräte sind leicht zu orten, da in der Leitung ein größerer Widerstand entsteht. Eine Reihen-Anzapfung wird meistens über den Strom der Telefonleitung gespeist. Sie sind schwerer zu orten als die meisten parallelen Abhörgeräte, verraten sich allerdings häufig dadurch, daß sie sich Strom aus der Telefonleitung »borgen«.

2 taz 29.05.1990, »Hertie-Trio vor Gericht«

3 Induktionsrolle: Wenn Strom durch eine Schaltung fließt, entstehen magnetische Schwingungen. Eine Induktionsrolle wandelt die Schwingungen wieder in Strom um. Der Strom kann dann zur Speisung eines Recorders oder eines Senders benutzt werden.

4 Antimilitaristische Stadtrundfahrt in West-Berlin, Berlin 1987

5 Der Spiegel 3/1988, »Knackpunkt umgeschaltet«

6 Siehe Kapitel »Sprachverschleierung«

Drahtlose Telefonsysteme

Nach dem Lesen des Kapitels über Telefonverkehr müßten bereits eine Menge Illusionen ins Wanken geraten sein. Ort und Identität eines Fernsprechteilnehmers können bereits in dem Moment festgestellt werden, in dem im Fernmeldeamt die erste Schaltung gelegt wird. Das gleiche gilt natürlich auch für Mobiltelefone, Handys, Autotelefone, egal in welchem Netz sie sind, und für alle anderen Funkverbindungen.

Die interessantesten Alternativen, die sich zum klassischen Telefon anbieten, sind die nicht ortsgebundenen Kommunikationsmittel. Das Autotelefon zum Beispiel. Mit 120 Stundenkilometern oder mehr durch die Landschaft rasend rufst du deinen Dealer an, um deine Designer-Droge zu bestellen. Eine Minute telefonieren und du bist schon wieder beinahe zwei Kilometer weiter. Gerüchte besagen, daß, weil vom PKW keine Kabel zum Fernmeldeamt laufen, die Gespräche nicht so einfach abzuhören oder zu orten sind. Auch könnte man mit einem Handy am Hauptbahnhof telefonieren und schnell in den nächsten Zug springen und spurlos verschwinden.

Wer der Post nicht ganz vertraut, kann also immer noch andere mobile Kommunikationsnetze nutzen. Der Äther ist grenzenlos und für jeden frei. Das ist leider kompletter Unsinn.

Mobiltelefone

Mobiltelefone sind Telefone, die du mit dir herumtragen oder in dein Auto einbauen kannst. In der BRD gibt es vier Mobiltelefonnetze: C-Netz, D1, D2 und E-Netz.

Die älteren Netze sind eingestellt worden. Das A-Netz gab es seit 1958 und hieß Öffentlicher Mobiler Landfunk, bis es 1977 aufhörte zu existieren. Das B-Netz wurde Mitte der 80er Jahre vom C-Netz abgelöst, es hatte wegen der veralteten Technik nur eine Kapazität von 27000 TeilnehmerInnen.

Funkfrequenzen gehören zu den weltweit begrenzten Resourcen. Sehr viele Frequenzen sind für Polizei, Militär und andere Behörden reserviert, so daß für Mobiltelefone nur bestimmte Frequenzabschnitte zugelassen sind. Im C-Netz ist das der Frequenzbereich 451,3 – 455,74 MHz und 461,3 – 465,74 MHz. Die Kapazität geht bis 850000 TeilnehmerInnen.

• Das C-Netz ist ein analoges Übertragungsverfahren, das heißt, daß es die Sprache, die in ein C-Netz Gerät hineingesprochen wird, nicht in Einsen und Nullen übersetzt. Trotzdem ist das, was im C-Netz gesprochen wird, wenn es mit einem normalen Scanner abgehört wird, nur ein Sprachsalat mit vielen »Krrks«. Du kannst zwar erkennen, daß es sich um eine menschliche Stimme handelt, aber was gesagt wird, versteht man nicht. Außer du hast einen Invertierungsdecoder. Das sind Geräte, die ab 350 DM zu kaufen sind. Modernere Scanner haben diese bereits eingebaut. Sie kosten etwa 1000 DM. Mit so einem Invertierungsdecoder ist jedem sprachinvertierten Gespräch mühelos zu folgen.[1]

Beim Telefonieren im mobilen zellular aufgebauten Sprechfunksystem muß die Zentrale wissen, wo sich das Gerät aufhält, um einen möglichen Wechsel in eine andere Funkzelle zu koordinieren. Dazu wird im C-Netz alle paar Millisekunden ein Datenpaket geschickt, daß diese Information enthält. Du nimmst das allenfalls als Fiepen oder Knacksen wahr. Außerdem wird die Sprache im Handy in kleine Stücke zerhackt, gespiegelt und manchmal auch noch komprimiert. Dieser Vorgang heißt Sprachinvertierung und wird auch von manchen Polizei- und Feuerwehrfunksystemen benutzt.[2] Um ihn wieder rückgängig zu machen, braucht man einen Sprachinverter oder Invertierungsdecoder, der die Datenpakete rauslöscht und die nur ein paar Millisekunden langen Sprachstücke wieder entspiegelt. Das C-Netz ist also nicht sehr privat. Jeder, der sich ein bißchen anstrengt, kann die Gespräche mithören.[3]

• Das D1, D2 und das E-Netz funktionieren nach einem digitalen Übertragungsverfahren. Das heißt, die Sprache wird vom Handy aus erst in lauter Einsen und Nullen übersetzt und dann durch den Äther geschickt. Zwar können diese elektromagnetischen Wellen auch mit jedem Scanner aufgefangen werden, aber die digitalen Zeichen müssen erst wieder in Sprache zurückübersetzt werden. Das besorgt ein Chip, der in jedem Handy eingebaut ist. Es gibt mittlerweile auch digitale Funkscanner, die aber noch recht teuer sind. Das Prinzip der digitalen Übertragungsverfahren ist schneller als die analogen Verfahren und weniger störanfällig. Außerdem hat das digitale Signal eine begrenzte Bandbreite, wodurch über eine Frequenz mehrere digitale Signale verschickt werden können. Voraussichtlich werden in den nächsten Jahren noch viel mehr Funkübertragungsverfahren digitalisiert.

• Das D1-Netz wurde 1991 von der Telekom in Betrieb genommen. Im Zuge der Postprivatisierung wurde auch ein privater Betreiber zugelassen, das ist die Mannesmann Mobilfunk GmbH, die Betreiberin des D2-Netzes. Technisch gibt es zwischen den beiden Betreibern keine Unterschiede, beide funktionieren nach dem GSM-Standard. Ebenso das E-Netz, das 1993 in Betrieb genommen wurde, Betreiberin ist die E-Plus Mobilfunk GmbH, eine Tochter der VEBA.[3]

Welche Wege nimmt ein Mobilfunkgespräch?

Autotelefone sind kleine Sender und Empfänger. Sie stehen mit einem Netz von Funkstellen in Verbindung, das seinerseits wiederum mit dem Telefonnetz der Bundespost verbunden ist. Das Prinzip ist eigentlich ganz einfach. Alle Mobilfunkverfahren sind nach einem zellularen Prinzip aufgebaut. Es gibt überall in den Städten, zunehmend auch auf dem Land und immer entlang der Autobahnen Sende- und Empfangsmasten, auch Funkfeststationen genannt, die für den Mobilfunk zuständig sind. Wenn du mit einem Handy die Telefonnummer deiner Mutter wählst, strahlt das Handy, das nichts anderes als ein kleiner Sender ist, Signale aus. Wenn diese auf eine geeignete Funkfeststation treffen, erkennt diese die Signale und gibt sie an die Funkvermittlungsstelle weiter. Dort wird entschieden, ob ein Gespräch über die normale Telefonleitung gehen soll, oder ob die Signale zu einer anderen Funkfeststation geleitet werden, weil deine Mutter bespielsweise auch so ein hübsches buntes Handy hat. Das ganze passiert in Bruchteilen von Sekunden.

Wenn du nun im Auto fährst, kann es sein, daß du die Funkzelle recht schnell wieder verläßt. Damit das Gespräch weitergehen kann, muß es nun von der nächsten Funkfeststation übernommen werden, die eine etwas andere Funkfrequenz hat. Diese übernimmt das Gespräch, nachdem es dem Handy mitgeteilt hat, daß es nun auf einer etwas anderen Frequenz senden muß, als jener auf der du eben noch gesprochen hast. Das geschieht, damit sich die benachbarten Funkfeststationen nicht gegenseitig stören. Hiervon merkst du selber überhaupt nichts. Aber es ist klar, daß die ganze Zeit Daten erhoben werden, um überhaupt lokalisieren zu können, wo du gerade bist.

Du kannst mit dem Handy jede Telefonnummer der Telekom anwählen (und umgekehrt) und vom E-Netz ins D-Netz oder sonstwohin telefonieren. Dafür haben die Betreiber Schnittstellen eingerichtet, die das ermöglichen. Die Technik ist dabei so aufgebaut, daß sich ein Gespräch, wenn es begonnen wird, seinen Weg selber sucht. Das heißt, es kann sein, daß ein Gespräch über die normale Telefonkabelleitung geht, oder es sucht sich einen Weg über irgendeine günstige Richtfunkstation. Die Betreiber haben dazu Verträge mit den anderen Anbietern geschlossen, in denen sie sich gegenseitig ihre Leitungen, bzw. Funkfrequenzen vermieten. Deshalb sind auch die Gespräche innerhalb eines Netzes billiger, als wenn du in ein anderes Netz hineintelefonierst.

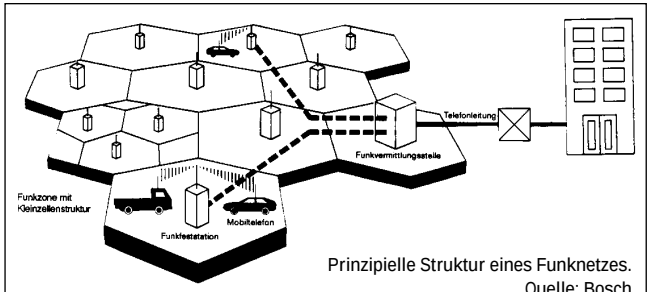
Was ist GSM?

Um die digitalen Übertragungsverfahren einheitlich zu gestalten, gab es 1982 eine Konferenz der EG-Postminister, auf der der GSM-Standard beschlossen wurde. GSM (Global System for Mobile Communication, Globales System für Mobile Kommunikation) regelt, in welcher Art und Weise die Sprache in digitale Signale umgewandelt, komprimiert und die Zeittakte in welchen sie gesendet werden, außer-

dem, welche Frequenzen für Hinweg, Rückweg und für die Verbindung der Feststationen benutzt werden.

Es ist immer wieder zu hören, daß der GSM-Standard ein hohes Maß an Sicherheit mit sich bringt, da die Daten verschlüsselt durch den Äther geschickt werden.

Das digitale Signal wird nämlich vor der Versendung einmal kodiert. Zu diesem Zweck wird der A5-Verschlüsselungsalgorithmus verwendet, der bis vor kurzem noch militärischen Zwecken vorbehalten war. Die Verwendung dieser Verschlüsselungstechnik galt lange als ein Hindernis für ein weltweites GSM-Netz. Es wurde behauptet, daß die Verschlüsselung so kompliziert sei, daß westliche Nachrichtendienste (wie die National Security Agency), die über ein solches Netz geführten Gespräche nicht mehr so ohne weiteres abhören könnten und es daher ideal für Kriminelle und Terroristen wäre. Das System darf deshalb nur an Betreiber verkauft werden, die bereit sind, ihr System offiziellen Überwachungskontrollen zugänglich zu machen. Das bedeutet, daß vorläufig lediglich NATO-Länder und der NATO freundlich gesinnte Staaten GSM benutzen dürfen. Mittlerweile ist auch dies bereits überholt, da die Kodierungen, mit denen GSM arbeitet, auch schon wieder entschlüs-



Prinzipielle Struktur eines Funknetzes.
Quelle: Bosch

selt wurden. Der Ehrlichkeit halber ist jedoch zu erwähnen, daß es zur Zeit erhebliche Anstrengungen und Investitionen bedarf, um GSM-Nachrichten entschlüsseln zu können.

Für jedes Handy brauchst du eine Telefonkarte, die eigentlich SIM-Karte heißt. SIM steht für Subscriber Identification Module, also die Benutzer-Identifizierungs Einheit. Auf dieser Karte ist deine Telefonnummer eingespeichert, sowie einige persönliche Daten. Der Zugang zu der Karte ist mit einem vierstelligen PIN-Code gesichert, wird dieser drei Mal falsch eingegeben, wird die Karte automatisch gesperrt.

Manche Leute wechseln öfters ihre Telefonkarten, das heißt, sie benutzen Karten, die anderen gestohlen oder abgekauft wurden. Damit hat das Gerät, von dem aus telefoniert wird, eine andere Telefonnummer (weil die nämlich mit der jeweiligen Karte festgelegt wird, die in das Gerät wandert). Da der GSM-Standard für die meisten europäischen Länder gilt, kann man diese Karten auch im Ausland kaufen, wo es teilweise auch billigere Tarife gibt. Diese Methode erschwert den staatlichen Abhörern ihre Arbeit erheblich, insofern diese nur deine bekannte Telefonnummer abhören. Wird eine Person aber gleichzeitig auch observiert, dann ist den Observierenden bekannt, wann und von wo aus sie telefoniert hat, und es kann herausgefunden werden, welche Telefonnummer sie tatsächlich benutzt. Kartenwechsel verschafft also einen kleinen Vorsprung, ist aber recht aufwendig und teuer, weil immer wieder neue Telefonkarten nötig sind.

Im GSM-Standard ist außerdem noch festgelegt, daß jedes Handy eine eigene Gerätenummer hat, die bei Bedarf und unabhängig von der Benutzertelefonkarte gesperrt werden kann, etwa wenn das Gerät geklaut wurde. Das heißt, es ist vorgesehen, daß bei jeder aufgenommenen Verbindung, auch die fest im Gerät gespeicherte Nummer übermittelt wird. Im D2-Netz wird dies seit August 1994 als zusätzlicher Service angeboten. Inwieweit das aber tatsächlich funktioniert, wissen wir nicht.

Wie sicher sind die Mobiltelefone?

Hinsichtlich des Schutzes der Privatsphäre sind die Schwachpunkte ganz offensichtlich. Wer sich wie die staatlichen Behörden der Mitarbeit der Post erfreuen darf, wird wenig Schwierigkeiten haben, Autotelefone abzuhören. Das Abhören von Autotelefonen im größeren Stil durch das Fernmeldeamt war bis vor kurzem noch mit technischen

Problemen verbunden, so sich der Teilnehmer während des Gesprächs bewegte und damit die Funkzelle wechselte. Aber genau deswegen wurde ja die neue Fernmeldeanlagen-Überwachungs-Verordnung (FÜV) verabschiedet.

Autotelefongespräche werden, wie gesagt, durch den Äther geschickt und sind so leicht aufzufangen. Sogar ein Scanner von ein paar hundert Mark genügt, um jedes im C-Netz geführte Autotelefongespräch mithören zu können. Wenn jemand zum Beispiel weiß, innerhalb welches Frequenzbereichs sich das Autotelefon befindet, ist es ein Kinderspiel, dies einzuprogrammieren und mitzuhören. Beim analogen C-Netz kann man den Gesprächen dann, vorausgesetzt man hat einen Invertierungsdecoder, folgen. Bei den digitalen Netzen wird ein digitaler Funkscanner benötigt (der über 30000 DM kostet),[5] außerdem muß ein Abhörer über die Möglichkeit verfügen, den A5 Verschlüsselungsalgorithmus knacken zu können. Das ist aber lediglich für Amateure ein mathematisch-technisches Problem. Nach Informationen der Computerzeitschrift CHIP macht das dem Bundesnachrichtendienst überhaupt keinen Kummer. Er ist in der Lage, jedes beliebige Mobilfunkgespräch über Richtfunkstationen abzuhören,[6] und die im GSM Standard verschickten Gespräche routinemäßig zu entschlüsseln.

So hat die Polizei von Utrecht beispielsweise im Rahmen einer Ermittlung gegen »schwere Kriminelle« zwei Jahre lang alle Autotelefongespräche in ihrem Bezirk aufgenommen, um am Ende ein paar Gespräche herauszufiltern. Keine gerade sehr selektive Ermittlungsmethode und eine Verletzung der Privatsphäre vieler hundert Menschen. Solche Fahndungsmethoden machen es »schweren Kriminellen«, die gerne Miettelefone benutzen (registriert auf einen anderen Fernsprechteilnehmer oder technisch angepaßte Autotelefone) nahezu unmöglich, sich einer Überwachung zu entziehen.

Aus zehntausenden Gesprächen, die auf Tonband festgehalten sind, können durch eine Stimmenanalyse, die Gespräche einer bestimmten Person ermittelt werden. Es ist dabei gleichgültig, über welche Nummern die Gespräche geführt wurden. Durch das »Stimmenprofil«, einer Spektralanalyse der Stimme, kann der Computer mühelos die gesuchte Stimme erkennen.

Es gibt auch Tricks, etwas selektiver mitzuhören. Für den professionelleren Abhörer ist es mit ein paar Zusatzgeräten (einem sogenannten Frequenzzähler und einem Computer) kein Problem, herauszufinden, auf welcher Frequenz das Gespräch eines Autos vor oder hinter ihm durchgegeben wird. Das berühmteste Opfer dieser Methode war der englische Kronprinz Charles, dessen intime Äußerungen an die Adresse seiner geheimen Mätresse der Boulevardpresse wochenlang hohe Auflagen besorgten.

Nur wenige Fernsprechteilnehmer sind sich bewußt, daß, wenn sie von einem Autotelefon aus angerufen werden, sie sich in einen gläsernen Bürger verwandeln und ihre Intimsphäre mit der eines Nachrichtensprechers in einer Livesendung vergleichbar ist.

Autotelefongespräche mitzuhören ist weder in den Niederlanden noch in der BRD gesetzlich verboten. Es ist lediglich nicht erlaubt, die dabei gewonnene Information zu verarbeiten, aufzunehmen, weiterzugeben, aber wen kümmert das schon?[7]

Wo ist das Handy?

Ein weiterer Nachteil der Mobiltelefone ist, daß auch das nicht benutzte Gerät immer leicht zu orten ist. Dank des Prinzips, daß das Mobiltelefon automatisch der Funkstelle seine Betriebsbereitschaft meldet, kann aufgrund des Identifikationscodes, den das Telefon der Funkstelle meldet, ermittelt werden, in welcher Funkzelle sich das Handy befindet. Anders gesagt: Wenn das Gerät eingeschaltet ist, weiß das Netz, wo du bist, auch wenn du nicht telefonierst. So kann das Mobiltelefon bis auf 500 Meter Genauigkeit geortet werden. Im E-Netz ist diese Ortung auf Grund der kleineren Funkzellen sogar noch genauer. Die Bestimmung des Aufenthaltsortes des Benutzers ist so genau, daß es sich für die Polizei lohnen würde, schweren Kriminellen ein kostenloses GSM-Gerät anzubieten.

Es gibt auch Anzeichen, daß die Daten ziemlich lange gespeichert werden. Dies wurde im Juni 1995 zwei Schwer-

bewaffneten zum Verhängnis, die mehrere Supermärkte überfallen hatten. Sie waren durch häufiges Telefonieren mit ihrem Handy aufgefallen. Die Polizei konnte dadurch ihren Standort ziemlich exakt bestimmen und die beiden festnehmen.[8]

Im Untersuchungsausschuß zum Tode Uwe Barschels (dem CDU-Politiker mit Kontakten zu Waffenhändlern, der trotz Ehrenwortes 1986 mit einer Flasche Rotwein tot in einer Genfer Badewanne aufgefunden wurde), konnte Monate später mit Hilfe der Post festgestellt werden, mit wem Barschel, wann von seinem Autotelefon aus gesprochen hatte.[9]

Trotz all dieser Nachteile gibt es auch in kriminellen Kreisen ziemlich viel begeisterte Mobiltelefonbenutzer. Besonders besser organisierte Banden verwenden ein fortwährend wechselndes Sortiment gestohlener Autotelefone, deren Identifikationscodes verändert werden. Man benutzt einen Apparat niemals lange hintereinander und hofft, so der Polizei immer eine Nasenlänge voraus zu sein. Es ist überflüssig zu erklären, daß dafür viele Investitionen getätigt werden müssen und eine Menge Fachkenntnisse erforderlich sind. Außerdem besteht, wie gesagt, die Gefahr, daß man durch Stimmenanalyse dennoch erwischt wird.

Abschließend kann gefolgert werden, daß analoge Mobiltelefone vorläufig ein äußerst indiskretes Medium sind. Mit der Einführung von GSM ist es zwar zu vermeiden, daß jeder einfach so mithören kann, staatliche Stellen genießen dieses Privileg jedoch weiterhin. Wer vermeiden möchte, daß seine Gespräche abgehört werden, wird auf Sprachverschlüsselungssysteme oder verschlüsselten Modemverkehr zurückgreifen müssen.

Funkfrequenzen der Mobiltelefone:

C-Netz: 451,3 – 455,74 MHz und 461,3 – 465,74 MHz.
D1-Netz: 890,0 – 915,0 MHz (Sendefrequenzen der Mobilstationen/Handys); 935,0 – 960,0 MHz (Sendefrequenzen der Basisstationen)
D2-Netz: wie D1-Netz
E-Netz: 1710 – 1880 MHz

Andere drahtlose Telefonsysteme – schnurlose Telefone

In der letzten Zeit werden immer häufiger schnurlose Telefone verwendet, die mit einer Funkstelle in Verbindung stehen, die an das Fernmeldenetz angeschlossen ist. Die meisten Geräte funktionieren auf eine Entfernung von 50-500 Metern, oftmals auch weniger. Die Kommunikation verläuft durch den Äther und kann im Prinzip abgefangen werden. Mit etwas technischem Fachwissen ist es sogar nicht schwer, in die Funkstelle des Nachbarn einzubrechen und kostenlos zu telefonieren.

Die am weitesten verbreitete Technik ist die nach dem CT 1-Standard, bei dem die Sprache unverschlüsselt und unverschleiert übertragen wird, bzw. nach dem CT 2-Standard, bei dem die Sprache verschleiert wird. Bei beiden Gerätetypen können mit im Fachhandel erhältlichen Funkscannern die Gespräche abgehört werden, wobei beim CT 2 Standard ein mittlerweile ebenfalls im Fachhandel erhältlicher Invertierungsdecoder erforderlich ist. Es ist also ohne weiteres möglich, mit so einem Funkscanner die Gespräche in der Nachbarschaft mitzuhören.[10]

Neuere schnurlose Telefone, die dann auch um einiges teurer sind, verwenden den DECT-Standard, bei dem die Daten digitalisiert werden, so daß zum Mithören das Übertragungsprotokoll bekannt sein muß. Hierbei gibt es einige Geräte, die auch verschlüsseln können, davon wird aber bislang kaum Gebrauch gemacht. Der DECT-Standard soll ab 1997 zum europäischen Standard für schnurlose Telefone werden, bis dahin jedenfalls ist noch mit vielen Geräten zu rechnen, die kaum Privatsphäre garantieren.[11]

Anrufbeantworter

Heike hat sich einen neuen Telefonanrufbeantworter zugelegt und Marina möchte sie dazu beglückwünschen. Im Hintergrund hat Marina das Radio laufen, das unablässig Hits von sich gibt. Sie ruft Heike an, der Anrufbeantworter meldet sich und Marina hält den Telefonhörer vor das Radio. Aber anstatt nun Heike die lieben Grüße zu übermitteln, spult der Anrufbeantworter nun scheinbar ganz von alleine alle eingegangenen Nachrichten ab, und alle wundern sich.

Fast alle modernen Anrufbeantworter haben die Möglichkeit zur Fernabfrage. Dazu wählst du die Nummer deines Apparates und gibst mit dem Mehrtonwahlpiepser, der bei fast allen Anrufbeantwortern mitgeliefert wird, deinen »Geheimcode« ein. Meistens ist das eine dreistellige Zahlenkombination, die dem Anrufbeantworter als Piepsen dreier verschiedener Töne übermittelt wird. Gäbe es nun eine Maschine, die in der Lage wäre, sehr viele dieser Piepstonkombinationen zu senden, könnte damit in die meisten Anrufbeantworter eingedrungen und dann entweder die eingegangenen Nachrichten abgehört oder auch ein neuer Ansagetext draufgesprochen werden. Eine solche Maschine zu bauen, ist für den Interessierten nicht weiter schwer.[12] Vom Prinzip her gibt es dazu zwei Möglichkeiten. Entweder der Codeknacker produziert ein Geräusch, das alle 10 Zahlenpiepstöne auf einmal von sich gibt. Das wird für die billigeren Anrufbeantworter ausreichen, da diese nicht überprüfen, ob falsche Töne gesendet werden, sondern nur auf die richtigen Töne reagieren. Oder ein solcher Codeknacker geht in kurzer Zeit viele Dreitonkombinationen durch.

Die meisten billigen Anrufbeantworter machen allen nur erdenklichen Unfug, wenn ihnen wie im obigen Beispiel eine Musiksendung vorgespielt wird, weil sie dabei wie auf die drei Piepstöne reagieren.

Raumüberwachung per Anrufbeantworter

Da auch der Anrufbeantworter ein Mikrofon bzw. einen Lautsprecher besitzt, was bei den meisten Geräten das gleiche ist, sind Anrufbeantworter anfällig für Raumüberwachungen, die »frequency flooding« (Frequenzfluten) benutzen. Dazu haben wir bereits im Kapitel »Wo sitzt die Wanze und wie funktioniert's« bereits etwas geschrieben. Beim Frequenzfluten muß das angeflutete Telefon nicht klingeln!

Manche Anrufbeantworter haben auch eine eingebaute Möglichkeit zur Raumüberwachung. Dazu muß von einem anderen Apparat angerufen werden, wieder eine meist dreistellige Piepstonfolge übersendet werden, und sofort ist hören, was in dem Raum, wo das Gerät steht, gesprochen wird. Beispielsweise kannst du damit überprüfen, ob dein Babysitter vielleicht gerade eine wilde Party feiert. Auch gibt es Anrufbeantworter, die dabei nicht einmal klingeln. Sollte jemand deinen Fernabfragecode kennen oder wird dieser per Schnelldurchlauf mit einem Codeknacker geknackt, oder hast du mal einen Stromausfall und dein Fernabfragecode wurde gelöscht, können unerwünschte Dritte bei dir mithören.[13]

Als Gegenmaßnahme ist es sicherlich am einfachsten, den Anrufbeantworter auszuschalten, aber dann kannst du keine Nachrichten mehr empfangen. Den Anrufbeantworter in den Kühlschrank zu stellen oder ein lautes Radio daneben, wird den unterbezahlten Privatdetektiv in die Verzweiflung treiben, professionelle Abhörer sind damit aber kaum zu beeindrucken.

Anmerkungen

1 Scanner aktuell Nov./Dez. 1995, (zum Thema Scanner sehr lesenswerte Zeitschrift, Bürgerweg 5, 31303 Burgdorf) »Invertierungsdecoder«: C1-Digital von der Firma VHT Implex, V. Hoppenheit, Bredenstr. 65, 32124 Enger, kostet 548,– DM. Der Handscanner Albrecht AF 400-INV, lieferbar ab Dezember 1995, Preis unter 1000,– DM über Andys Funkladen, Admiralstraße 119, 28215 Bremen.

2 Scanner Frequenztabelle, 27 MHz bis 10 GHz, A. Janson/J. Bergfeld, München 1995, 39,80 DM

3 BOS-Funk, Funkbetrieb bei Polizei, Feuerwehr und Rettungsdiensten. M. Marten, Siebelverlag 1994, 2 Bände à 29.80 DM

4 Alles über Mobilfunk, Dienste, Anwendungen, Kosten, Nutzen, Duelli, Harald/Pernsteiner, Funkschau, München 1992

5 Funkschau 14/95, »Lauscher in der Leitung«

6 CHIP August 1995, »Jeder ist verdächtig«

7 Die rechtliche Lage ist in der Tat etwas verzwickt. Mit einem Scanner dürfen nur für die Allgemeinheit bestimmte Aussendungen empfangen werden. Nach 201 StGB macht sich strafbar, wer das nicht öffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört. Andererseits macht sich der Betreiber eines Scanners nach 18, 11 FAG dann strafbar, wenn er Nachrichten empfängt, die von einer öffentlichen Zwecken dienenden Fernmeldeanlage übermittelt werden und für ihn nicht bestimmt sind und er den Inhalt

oder die Tatsache des Empfanges anderen mitteilt. Das heißt, es ist nicht strafbar, wenn du versehentlich in das Mobilnetz hineinhörst, sondern erst wenn du dies anderen mitteilst. Eine gute Zusammenfassung der rechtlichen Lage findet sich in »Scanner im Dschungel der Gesetze« von M. Riedel in Scanner aktuell Nov./Dez. 1995

8 Der Spiegel 14.8.95, »Im eigenen Netz«

9 Deutsche Polizei 8/89, »Aus dem Auto in die Datenbank«

10 Mobilfunk und Datenschutz, Materialien zum Datenschutz, Hg. Berliner Datenschutzbeauftragter, Pallasstr. 25–26, 10781 Berlin

11 Alles über schnurlose Telefone, Bräuer/Arens/Zimmers, München 1994, 69,– DM

12 Datenschutz-Nachrichten 3/1994, S. 2

13 Datenschutz-Nachrichten 6/1994, S. 17

Funkrufempfänger (Pager)

Funkruf
empfänger
(Pager)

Ein unentbehrlicher Apparat für Feuerwehrleute, angehende Eltern und (noch) nicht erfolgreiche Geschäftsleute ist der Funkrufempfänger. Es ist eine Lösung für weniger wohlhabende Leute, mit der sie permanent erreichbar sind.

Die Geburt steht vor der Tür und deine Partnerin legt sehr viel Wert auf deine Anwesenheit. Du bist aber unterwegs und suchst die Flohmärkte nach einem Kinderwagen für Drillinge ab. Aber du hast einen Funkrufempfänger mitgenommen. Das einzige, was deine Partnerin machen muß, ist die Zugangsnummer des Funkrufempfängers anzurufen. Der Empfänger in deiner Tasche fängt an zu piepsen und/oder zu vibrieren. Bei manchen Funkrufempfängern (Cityruf und Scall) ist es möglich, einen Zahlencode mitzusenden (höchstens 14 Zahlen) und bei den modernsten Typen kannt man sogar achtzig Buchstaben und Zahlen mitsenden. Dann ist auf einem Minibildschirm zu lesen, in welchen Abständen die Wehen kommen, wo du anrufen sollst oder welche Namen sie sich im letzten Moment ausgedacht hat.

Sobald im Fernmeldeamt eine telefonische Meldung für einen bestimmten Funkrufempfänger eingeht, wird zunächst über das Sendernetz ein Identifizierungscode gesendet. Der Funkrufempfänger erkennt daraufhin seinen Erkennungscode und reagiert darauf. Im Gegensatz zum Funktelefon werden beim Funkruf Informationen nur von einem Absender zu einem Empfänger transportiert. Gearbeitet wird auf einer festen Frequenz.

In der BRD gibt es das Eurosignal, das schon 1974 eingeführt wurde und auch in der Schweiz und Frankreich funktioniert. Es arbeitet im Bereich von 87,340 und 87,365 MHz. Es können bis zu vier Tonsignale übersendet werden.

Das Gerät, welches man mit sich herumträgt, heißt Europiepser. Allerdings gibt es das System nur in den alten Bundesländern, in den neuen wurde es erst gar nicht eingeführt.

Dann gibt es seit 1989 den Cityruf, der in allen Großstädten der BRD funktioniert. Cityruf arbeitet im Bereich 469 MHz, Ende 1991 gab es bereits über 130000 Kunden in der BRD. Es gibt den Cityruf Text, bei dem bis zu 80 Ziffern oder Buchstaben gesendet, Cityruf Numerik, bei dem bis zu 15 Ziffern übersendet und Cityruf Ton, bei dem vier Tonsignale übersendet werden können.

Nur beim Cityruf Ton kann der Empfänger über das normale Telefon (Vorwahl 0154) angerufen werden, bei den anderen beiden Systemen ist ein Modem, ein spezieller von der Telekom vertriebener Tonsender, oder ein Datex-J Anschluß und ein Modem notwendig.

Seit Januar 1994 gibt es auch das Omniport System, das dem Cityruf ähnlich ist, bloß, daß die zu übermittelnde Nachricht über alle UKW-Radiosender, genau wie die Verkehrsfunkinformation (Radio-Paging), ausgestrahlt wird.

Dann gibt es noch Scall, das über die Telefonnummer 01681 zu erreichen ist. Es können bis zu 15 Ziffern und Tonsignale übersendet werden, die das Gerät dann speichert. Bei Scall fallen keine monatlichen Grundgebühren an, der Nutzer muß sich auch nicht mit seinem Namen irgendwo anmelden, das Gerät wird einfach gekauft, der Empfänger kostet je nach Anbieter ab 100 DM aufwärts.[1] Die Anbieter werben mit dem Bild des modernen Yuppies, der seiner Freundin einen Scall schenkt, damit sie immer für ihn erreichbar ist. Ein Pager bietet also durchaus die Möglichkeit, eine einseitige Verbindung herzustellen, bei der, ohne daß der Anrufer sich zu identifizieren braucht, eine (Code)nachricht gesendet werden kann. Da der Pager nicht zu orten ist, ist er in den USA ein beliebtes Instrument für Drogenkuriere. Der Kurier hat einen Pager, der piept, wenn ein neuer Auftrag kommt. Der Pager zeigt den vorher vereinbarten Code an, aus dem beispielsweise hervorgeht, welche Menge, wann und wohin geliefert wird.

Die Frequenzen der Funkrufempfängernetze sind mit einem normalen Empfänger/Scanner leicht zu ermitteln. Mit

Hilfe eines Computers und eines Umwandlers von etwa 250 DM, der das Funkrufempfängerprotokoll (Pocsag) in lesbare Zeichen umsetzt, können Funkrufempfängernachrichten empfangen werden. Auch der Funkrufempfänger ist also nicht gerade ein sehr intimes Kommunikationsmittel.

Die Nachteile von Pagern

Der Nachteil von Pagern, wie Scall ist, daß es Funklöcher gibt. So funktioniert Scall nur in einem Radius von 50km um die Großstädte herum, und manchmal funktioniert es gar nicht, so etwa wenn du gerade in der Tiefgarage bist. Da die Funkrufempfänger (Pager) keinen Sender haben, gibt es auch keine Bestätigung, ob der Anruf angekommen ist. Der Anrufer kann also nie zu 100% sicher sein, ob die gewünschte Nachricht den Empfänger erreicht hat.

Außerdem braucht man dazu eigentlich noch ein Telefon, das im Tonwahlverfahren, auch Mehrfrequenzwahlverfahren (MFV) genannt, arbeitet. Das sind diese Telefone, die für jede Zahl einen unterschiedlichen Piepston ausschicken. Da in der BRD erst in kommender Zeit das gesamte Telefonsystem auf Tonwahl umgestellt wird, haben bislang nur neuere Telefone diese Möglichkeit. In Telefonzellen, die mit Telefonkarten betrieben werden und bei neueren Telefonen mußt du die folgenden drei Tasten drücken, um die MFV-Töne zu erzeugen, nämlich »->>«, »*« und »->>«. Zur Bestätigung endest du mit »#«. Hast du noch ein altes Telefon, das im Pulswahlverfahren arbeitet oder möchtest du einen Pager wie Scall über eine altmodische Telefonzelle anrufen, so mußt du dann über einen Sprachcomputer gehen, dem du die Zahlen laut und deutlich vorsprechen mußt. Ist die Verbindung schlecht, oder du sprichst etwas undeutlich, schaltet sich der Sprachcomputer einfach ab, und du mußt es wieder von vorne versuchen. Das kann ausgesprochen lästig sein.

Dieses Problem kannst du dadurch lösen, daß du dir einen Tonwahlsender zulegst. Das sind die kleinen Dinger, die du auch bei neueren Telefonanrufbeantwortern mitgeliefert kriegst, um eine Fernabfrage des Anrufbeantworters auszuführen. Das Gerät ist so groß wie eine Zigarettenschachtel

und hat Tasten. Du hältst es einfach an den Telefonhörer und gibst dann deine Zahlenfolge ein. Diese Geräte sind im Fachhandel ab 5 DM erhältlich.

Exkurs: Funkrufempfänger-joy-riding in den Niederlanden

Der Funkrufempfänger ist im Prinzip ein geeignetes Medium, mit dem nicht zu ortende, einseitige Kommunikationsverbindungen hergestellt werden können.

Anke und Carla können einander nicht anrufen, da das Telefon möglicherweise abgehört wird. Da sie nicht in der gleichen Stadt wohnen, überlegen sie, wie sie dennoch fernmündlich miteinander kommunizieren können.

Anke könnte von einer Telefonzelle aus zu einer Funkrufempfängernummer, die nicht von ihr selbst ist, eine Codenachricht senden. Carla, für die die Nachricht bestimmt ist, muß wohl permanent oder zu einem vereinbarten Zeitpunkt den Funkrufverkehr abhören. Wenn sie Nachrichten sieht, die der vorher vereinbarten Verschlüsselungsmethode ähneln, kann sie eine von Anke gesendete Codenachricht empfangen, erkennen und entziffern. Für den tatsächlichen Besitzer der Funkrufempfängernummer ist es eine unverständliche Nachricht und er wird denken, daß es sich um einen kleinen Irrtum handelte. Die Nachricht von Anke trampt gewissermaßen mit dem Funkrufverkehr eines anderen mit. Dies ist selbstverständlich nicht ganz gemäß der geltenden juristischen Bestimmungen.

Zu dieser Form des »joy-riding« eignen sich am besten die numerischen Funkrufempfänger. Sie sind von einer Telefonzelle aus relativ einfach zu bedienen. Die Codemöglichkeiten beschränken sich auf eine 14stellige Zahl. Die alphanumerischen Funkrufempfänger, mit denen eine Textnachricht gesendet werden kann, sind nur über einen Operator zu erreichen. In diesem Fall würde die Stimme von Anke auf Band aufgenommen werden, und das möchte sie nicht. Anke kann auch mit Hilfe eines PC eine Textnachricht senden. (Hast du übrigens schon mal versucht, von einer Telefonzelle aus zu modemen?)

Was ist für das »joy-riding« nötig? Zum Empfangen: Ein einfacher Empfänger/Scanner, der in der Lage ist, die Funkrufempfängerfrequenzen einzufangen, einen simplen Personal Computer, einen Funkrufempfänger-Umwandler (der das Funkrufempfängerprotokoll in lesbare Zeichen umwandelt) und die zum Umwandler gehörende Software (ein simples Kommunikationsprogramm). Umwandler und Software sind in den Niederlanden über Hacktic erhältlich (Tel. 0031-20-6222885).

Zum Senden: Eine Telefonzelle mit Tastwählern (Drucktasten mit Piepstönen). Ferner müssen Aufrufnummern von Funkrufempfängernummern bekannt sein. Um diese zu ermitteln, müssen erst ein paar Nachforschungen angestellt werden. In den Niederlanden zum Beispiel muß eine Funkrufempfängernummer mit der Zahlenreihe »06-5« anfangen. Danach sind noch sieben weitere Zahlen einzugeben.

Die Funkrufempfängernummer muß sich in einer der nachstehenden Nummernreihen befinden:

		Entsprechende Frequenz
Benelux:	06-57500000/06-5799999	164.3500 MHz
Niederlande:	06-58000000/06-58749999	154.9875 MHz
Niederlande:	06-58750000/06-59549999	159.9900 MHz

Numerische Funkrufempfänger enden immer mit einer 1 oder einer 5, es gibt allerdings »tone-onlys« (Funkrufempfänger, die nur ein paar Töne erzeugen), die mit diesen Zahlen enden.

Du versuchst nun eine Nummer, die sich in einer dieser Reihen befindet. Erhältst du daraufhin die Meldung »Funkrufempfängeranmeldung akzeptiert«, hattest du mit einem »tone-only«-Empfänger zu tun, und damit kommst du nicht weiter. Erhältst du die Nachricht: »Geben Sie Ihre Information ein«, so handelt es sich um einen numerischen Empfänger, den du benutzen könntest. Du gibst dann einen 14stelligen Zahlencode ein (mit ›#‹ schließen) und hängst wieder auf.

Zu Hause setzt du dich an den Computer und schaust dir die eingegangenen Funkrufempfängernachrichten der letzten Periode an, unter denen befindet sich ganz gewiß die gesendete Nachricht. Der Funkrufempfängerverkehr steht jetzt offen. Es könnten die Vereinbarungen hinsichtlich Kodierung und Sendezeiten etc. getroffen werden.

In der Praxis könnte es so aussehen, daß man vereinbart, einmal am Tag eine Stunde lang den Funkrufempfängerverkehr abzuhören. Sollte es etwas zu vermelden geben, kann man innerhalb jener Stunde zu einer Telefonzelle gehen, ruft die Nummer an und gibt dann den Zahlencode ein. Die Empfängerseite braucht nur noch die vom Computer erstellte Liste der Funkrufempfängernachrichten durchzugehen und den vereinbarten Code zu entschlüsseln.

Die einzige Art und Weise, wie du geortet werden kannst, ist, wenn du regelmäßig von derselben Telefonzelle aus mit derselben Funkrufempfängernummer Nachrichten verschickst. Dabei besteht die Gefahr, daß der tatsächliche Besitzer der Nummer über die für ihn unverständlichen Nachrichten mit der Zeit mißtrauisch wird und Nachforschungen anstellen läßt.

Anmerkung

1 Funkschau 15/95, »Immer auf Abruf: Paging«

Der freie Äther

Wenn du mit dem Service der Post nicht zufrieden bist, so besteht im Prinzip die Möglichkeit, eine eigene Verbindung herzustellen. Ein Funkempfänger an der einen und ein weiterer Funkempfänger an der anderen Seite und du bist einen ganzen Schritt weiter. Mit Leitungen, Fernmeldeämtern oder Telefongebühren hast du dann nichts mehr zu schaffen. Du funkst deine Nachrichten durch den Äther und erhältst von der anderen Seite die Antwort. Selbstverständlich ist das alles nicht so einfach, wie es zunächst klingen mag.

Da gibt es zum Beispiel die Gesetzgebung. Um zu vermeiden, daß jeder einfach macht, was ihm in den Sinn kommt, ist die Benutzung des Äthers an gewisse Bestimmungen gebunden. Für allerlei unterschiedliche Zwecke sind die Frequenzbereiche vereinbart worden, innerhalb derer – oder in den meisten Fällen innerhalb derer nicht – gefunkt werden darf. Deine Nachbarn werden es wahrscheinlich nicht gerade angenehm finden, wenn du Gespräche führst, die ihr Lieblingsprogramm auf der Deutschen Welle übertönen. Das ist denn auch verboten, und wenn du es trotzdem machst, darfst du damit rechnen, daß früher oder später der Funkkontrolldienst deine Geräte beschlagnahmt.

Es sind Frequenzbereiche festgelegt, innerhalb derer du senden darfst, für die du jedoch eine Genehmigung brauchst. Du mußt dich registrieren lassen und ebenso mußt du berücksichtigen, daß du gefunden wirst, wenn du dich nicht an die Regeln hältst.

In den Niederlanden sind zum Beispiel eine Reihe von Frequenzbereichen völlig offen gelassen. Da darfst du machen, was du willst. Voraussetzung ist, daß du dabei zugelassene Geräte benutzt und die Gesetze des Landes nicht verletzt.

Der Einfachheit halber kannst du davon ausgehen, daß alles, was durch den Äther geschickt wird, von irgendeiner Behörde registriert wird. Dadurch bist du an Beschränkungen gebunden. Leute, die sich dem Gesetz entziehen wollen, achten darauf, daß sie nicht so einfach mit ihren Geräten zu orten sind. Sie wissen natürlich, daß ein großer Antennenpark auf dem Dach oder eine ungewöhnlich große Leistung des Senders schnell auffallen. Kleinere und mobile Sender beschränken allerdings die Reichweite des Senders.

Wer dennoch über längere Entfernungen Nachrichten versenden will, kann auf das Packet-Radio (auch Paket-Funk) zurückgreifen. Hierbei reisen die Daten über verschiedene Weitergabestationen durch den Äther. Es besteht auch die Möglichkeit, (un)kodierte Computernachrichten zu versenden und zu empfangen. In der BRD gibt es zwei Packet-Radio Systeme. Das eine ist im CB-Funk-Bereich, wo die Post zwei Kanäle für die Übersendung digitaler Daten freigegeben hat. Das andere System heißt Modacom und ist ein kommerzieller Datenfunkdienst.

Packet-Radio

Packet-Radio (auch Paket-Funk) ist ein digitales drahtloses Kommunikationsnetz, das das »packet-switching«-Protokoll benutzt. Das klingt komplizierter als es ist. Es funktioniert mit einem Computer und einer Art Modem. Die Übermittlung von Nachrichten erfolgt nicht über das Telefonnetz, sondern durch den Äther. Dafür ist eine kleine Investition von Geld und Energie erforderlich. Das Prinzip von Packet-Radio ist, daß digitalisierte Daten in Pakete aufgeteilt und dann verschickt werden, daher auch der Name.

»Packet-switching« funktioniert wie ein gut geregeltes, höfliches Gespräch zwischen zwei Funkempfängern: Anke wartet bis Ben fertig ist und bestätigt danach den Erhalt und antwortet. Es wird dabei überprüft, ob die Daten gut angekommen sind. Sollte dies nicht der Fall sein, wird das »Paket« erneut gesendet und zwar solange, bis das »Paket« des Senders und des Empfängers identisch sind. Diese Technik

gewährleistet einen fehlerlosen, störungsfreien Empfang digitaler Daten.

Der Netz-Aspekt von Packet-Radio beruht auf einer Reihe von Vereinbarungen und Konventionen. So können zwischen zwei Funkempfängern, die einander wegen der großen Entfernung zwischen den Stationen nicht direkt erreichen können, Verbindungen hergestellt werden. Es werden dann eine oder mehrere Zwischenstation gesucht, die bereit sind, als Kommunikationsvermittler zu fungieren.

Kalle, unsere fiktive Zwischenstation, erhält eine Nachricht von Anke, auf der die Adresse von Ben steht, und funkt sie dann an ihn oder, für den Fall, daß Ben zu weit weg ist, an Paul. Im Sprachgebrauch der erfahrenen Paket-Funker (und davon gibt es weltweit eine ganze Menge) werden die Stationen von Kalle und Paul als »digipeaters« (digital repeaters) bezeichnet.

Exkurs: Packet-Radio

Ein Datenpaket ist in der folgenden Weise aufgebaut:

Start-Flag	1 Byte	Anfang
Adresse		7 Byte Adresse
Steuer-Flag	1 Byte	Regelung des Verbindungsauf- und -abbaus
Datenblock	max. 256 Byte	hier sind die Informationen
Prüfsumme	2 Bytes	Überprüfung, ob die Nachricht vollständig angekommen ist
Ende-Flag	1 Byte	

Anfang und Ende-Flag markieren Beginn und Ende eines Datenpaketes, das Softwareprogramm setzt in das Adreßfeld automatisch, das Rufzeichen der angefunkten CB-Station. Mit dem Steuerflag wird geregelt, wie das Datenpaket weiterzuverarbeiten ist und der Verbindungsauf- und abbau vonstatten geht. Wird zum Beispiel ein Datenpaket verstümmelt, dann teilt der Datenempfänger dem Datensender mittels des Steuer-Flag mit, daß die gefunkten Daten unbrauchbar sind. In diesem Fall wird das Datenpaket so oft gesendet, bis es der Empfänger verarbeiten kann. Die Daten selber sind im Datenpaket, bis zu 256 Byte sind hier möglich. Erfahrungsgemäß sollte bei schlechter Verbindung aber auf 32 oder 64 Byte runtergegangen werden. Ist die in den beiden Prüfbytes enthaltene Prüfsumme des gesamten Datenpaketes in Ordnung, können die Daten im Rechner weiterverarbeitet werden.

Packet-Radio im CB-Funk

Mitte 1994 wurden vom Bundespostministerium die Kanäle 24 und 25 des CB-Funkbereiches für die digitale Datenfunkübertragung freigegeben. Die Technik ist erstaunlich einfach und darüber hinaus auch nicht teuer. Es braucht nur ein paar Handgriffe, um die Daten aus dem PC auf die Reise zu schicken. Alles was du dafür brauchst ist ein PC, ein Funkmodem und ein CB-Funkgerät. An einem Ende wird das CB-Funkgerät über das Funkmodem an die serielle Schnittstelle des PC angeschlossen, am anderen Ende ist die Funkantenne. Weiter ist noch ein Kommunikationsprogramm nötig und schon kann es losgehen. Im Fachhandel ist das ganze für etwa 200 DM inklusive Software erhältlich.

Zum Übertragen wird Packet-Radio verwendet. Das Übertragungsprotokoll nennt sich AX.25 und gewährleistet, daß die übertragenen Datenpakete fehlerfrei ankommen, ebenso die notwendigen Informationen wie Absender, Adresse und die Angaben zur Weiterverarbeitung des Datenpakets.

Da CB-Funkgeräte nur eine maximale Sendeleistung von 4 Watt haben dürfen, ist der Senderadius jedoch sehr gering, in der Regel um die 5 bis 10km, im flachen Land und mit einer guten Antenne bis zu 50km. Es ist allerdings anzumerken, daß viele CB-Funker unerlaubt stärkere Sender an ihr Gerät anschließen und so die CB-Funkkanäle zumeist hoffnungslos überlastet sind. Packet-Radio ist geeignet, Verbindungen über mehrere hundert Kilometer aufzubauen. Allerdings sind dafür mehrere Relaisfunkstationen (»digipeaters«) notwendig. Davon kann es maximal sieben geben. Die Datenübertragungsrate ist mit 1200 baud sehr langsam und bei schlechtem Wetter muß eventuell das Übertragungsprotokoll angepaßt werden. Je mehr Relaisfunkstationen benutzt werden, desto langsamer wird die Übertragungsrate. CB-Funk und Packet-Radio eignen sich nicht dazu, umfangreichere Datenmengen über eine große Entfernung zu übertragen. Die Übermittlung kurzer Nachrichten ist allerdings gut möglich.

Da der CB-Funk öffentlich ist, ist diese Methode alles

andere als privat. Da auch das Datenübertragungsprotokoll einsehbar ist, kann jeder die Nachrichten mitlesen. Die Anwendung von Kryptographieverfahren drängt sich hier förmlich auf.[1]

Auf Sendung

Die Möglichkeiten von Packet-Radio hängen selbstverständlich von den zur Verfügung stehenden Geräten ab. Und dennoch kannst du, ohne allzu hohe Ansprüche, mit einem gewöhnlichen Funkgerät bereits eine Menge erreichen. Alles, was du für Packet-Radio im CB-Funk brauchst, haben wir im Prinzip schon beschrieben: PC, Funkgerät, Funkmodem, Antenne, Software und etwas Zeit und Energie.

Wenn sich ein störender Sender in der Nähe befindet, sorgt das Kommunikationsprotokoll dafür, daß die Daten aus deinem Funkgerät so oft wiederholt werden, bis sie einwandfrei und ohne Fehler übertragen wurden. Damit sind aber auch Nachteile verbunden. Wenn Anke über eine kurze Entfernung eine Datei von beispielsweise 1 Kilobyte senden möchte und sie das Pech hat, daß ihr Nachbar ein schlecht eingestelltes Funkgerät hat, so hätte sie die Nachricht schneller mit dem Fahrrad überbracht.

Theoretisch können mit Hilfe eines CB-Funkgerätes ein paar Hundert Kilometer überbrückt werden. Allerdings werden hierzu nicht genehmigte, »frisierte« Funkgeräte benutzt. Mit den legal erhältlichen Geräten können aber durchaus einige Dutzend Kilometer überbrückt werden. Dieses sogenannte Punkt-zu-Punkt-Kommunikationssystem ist eine attraktive Alternative zur Bundespost. Mit anderen kannst du dir ein eigenes Netz aufbauen. Das geht zum Teil über bestehende Stationen, bei denen du dir gleichsam einen Schlüssel borgst, um Post abzuholen oder einzuwerfen. Alles hängt davon ab, wie gut du mit der Software umgehen kannst. Wer ein solches Netz errichtet, fängt in der Regel erstmal klein an.

Anke wohnt in Stadt A, während ihre Freunde und Freundinnen sich in den Städten B, C und D befinden. Jede schafft sich ein Funkgerät mit der höchstzulässigen Funkleistung an. Dadurch, daß Ankes Stadt zentral liegt, ist sie diejenige, die direkt mit allen anderen kommunizieren kann. Anfangs machen sie es sich nicht allzu schwer und vereinbaren ein Funkschema. Zu einem bestimmten Zeitpunkt ist die Station von Anke empfangsbereit, Nachrichten können gesendet werden. Da sie keine Lust hat, alle Nachrichten, die da so ankommen, durchzusehen, wird ein Adreßprotokoll vereinbart. Der erste Buchstabe bezeichnet den Sender, der zweite die Adressatin. Der DOS-Standard mit acht Buchstaben wird beibehalten, es bleiben also noch eine Reihe Buchstaben übrig. Mit denen kann zum Beispiel das Datum angegeben werden. Anke sieht sofort, für wen die Nachricht bestimmt ist und funkt diese an B, C oder D weiter. Dies ist die elementarste Form des »routen«, des Weiterleitens einer Nachricht. Ist man mit dem System vertraut, kann das »routen« automatisiert werden. So kann die Station eine »digipeater«-Funktion erhalten. Gewisse Kenntnisse über die Adressen im Packet-Funk sind hierfür von Vorteil. Alle, die sich ein bißchen mit internationalen Computernetzen auskennen, können hier übrigens am Anfang helfen.

Mit Hilfe der Adresse wird dem »digipeater« mitgeteilt, wohin die Information weitergefunkt werden soll. Das wichtige ist nun, einen »gateway« – eine Zugangstür, bzw. eine Verbindung zwischen zwei verschiedenen Netzen – zu finden. Zum Beispiel vom CB-Funk zum Zwei-Meter-Band, von wo aus Zugang zu einem weltweiten Netz von Packet-Radio besteht.

Eine andere Möglichkeit wäre es, einen »gateway« direkt vom CB-Funk aus zu den internationalen digitalen Datennetzen zu suchen. Wenn die Daten mit der richtigen Adresse ausgestattet sind, wäre es ohne weiteres möglich, diese Nachricht an eine Nutzerin des Internets oder von APC (siehe Kapitel Computernetze) weiterzuleiten. Vorläufig ist dies aber noch Zukunftsmusik. Damit würde sich die Mobilität von Packet-Funk erheblich verbessern, ein tragbares Modem und Funkgerät würden genügen. Gerade Organisationen, die in Gegenden mit schlechter Infrastruktur arbeiten, könnten mit wenig Aufwand eine internationale Datenkommunikation betreiben. Darüberhinaus bietet sich Packet-Radio auch als geeignete Alternative an, sollte in

kommender Zeit ein neues Gesetz zur Einschränkung von Verschlüsselungstechniken im »normalen« Telekommunikationsnetz verabschiedet werden.

Modacom

Zur mobilen Datenkommunikation gibt es seit 1993 auch das von der Telekom Tochter DeTeMobil betriebene System Modacom. Dazu benötigst du ein angemeldetes Funkmodem und bist mit einem Laptop sogar beweglich. Modacom funktioniert wie die anderen Funknetze nach einem zellularen Prinzip und ist bundesweit zu empfangen.

Das Funkmodem sendet ein Signal aus (eine achtstellige Zahl, die in der Hardware festgelegt ist), das dem Funknetz mitteilt, wer sich da meldet. Hast du deine Rechnung bezahlt, sendet das Funknetz nun deine Nachricht aus. Modacom funktioniert nach dem Prinzip des »Datenfischens«. Das heißt, es steht die ganze Zeit auf Bereitschaft und sobald eine Nachricht auf das passende Funkmodem trifft, wird die Datei gefischt und dies wird dem Funknetz mitgeteilt. Die Übertragung der Daten erfolgt unverschlüsselt. Allerdings werden sie nach der sogenannten Trellis-Kodierung zerwürfelt, wodurch sie fehlerfreier ankommen. Das für die Datenübetragung verwendete Protokoll wird von den Herstellern geheimgehalten. Die Anwendung eigener Verschlüsselungssoftware wird bei Modacom empfohlen. Die Übertragungsrate beträgt 9600 baud, ist bei schlechtem Wetter aber wesentlich geringer.

Modacom ist für staatliche Stellen leicht abzuhören, da sie Zugang zu den Übertragungsprotokollen haben. Es ist lediglich eine Zeitfrage, bis Hacker die Protokolle geknackt haben. Auch die Identifizierung durch einen im Funkmodem selbst festgelegten Code ist problematisch. Findige Hacker sind durchaus in der Lage, Maskeraden zu entwerfen, die eine richtige Absenderadresse vorgaukeln, womit sie auf Kosten andere Leute funken können. Auch sind Bewegungsprofile durch Modacom erstellbar, derzeit sind die Funkzellen aber noch viel gröber als beim D1-Netz, so daß die Lokalisation eher ungenau ist.[2]

Spread spectrum

»Spread spectrum« (verteiltes Spektrum) ist eine Kommunikationstechnik, die bis Anfang der 90er Jahre ausschließlich militärischen Zwecken diente. Allmählich ist auch ein kommerzieller Markt entstanden. Einige werden schon mal von LANs (Local Area Networks) gehört haben. Das sind Netze, die Computer über Kabel miteinander verbinden. Dadurch kann beispielsweise Post über die Computer innerhalb eines Gebäudes geschickt werden. Nun sind auch »Funk-LANs« (RLANs – Radio Local Area Networks) erhältlich, die eine drahtlose Verbindung zwischen einer bestimmten Anzahl von Computern ermöglichen.

Willst du ein Radioprogramm empfangen, so mußt du das Radio auf eine bestimmte Sendefrequenz einstellen. Unterschiedliche Sender benutzen verschiedene Frequenzen. Jedem Sender ist ein bestimmter Bereich auf dem Band zugewiesen, innerhalb dessen er sich konzentriert. Dieser Bereich, die Wellenlänge, muß so groß sein, daß ein benachbarter Sender nicht gestört wird. Von der Länge des Bandes hängt ab, wieviele Sender auf einem Frequenzband senden können.

Ein Beispiel: Die UKW-Wellenlänge reicht von 88-108 MHz. Beträgt die Bandbreite eines Senders 1 MHz, so passen 20 Sender auf das UKW-Band. Beträgt die Bandbreite der Sender aber nur 0,2 MHz (200 kHz), dann passen 100 Sender auf das betreffende UKW-Band.

Sollen nun 200 Sender auf das UKW-Frequenzband passen, so muß die Wellenlänge der einzelnen Sender verringert werden. UKW-Sender benötigen aber eine minimale Wellenlänge von 200 kHz, ansonsten kannst du die Hifi-Qualität vergessen. Auch die anderen Schmalbandfrequenzen wie die MW-Frequenz, Funkamateur-Bänder oder Polizeibänder funktionieren nach dem gleichen Prinzip. Die Frequenz wird mit einer möglichst kleingehaltenen Wellenlänge gesendet, die jedoch groß genug sein muß, um die gewünschte Information zu übertragen.

»Spread spectrum« arbeitet dagegen mit einer möglichst großen Wellenlänge. Sie ist erheblich größer, als für die In-

formationsübermittlung tatsächlich erforderlich wäre. Die Information wird mit einem pseudozufälligen (»pseudo random«)[3] Signal kodiert und auf der Betriebsfrequenz des Senders ausgestrahlt (»direct sequence«). Eine andere Methode ist, die Beriebsfrequenz mit einem pseudozufälligen Signal zu kodieren, damit sie dauernd wechselt. Auf jeder Frequenz wird dann nur ein kleines Stück der Information gesendet (»frequency hopping«).

Die Streuung durch das »spread spectrum« kann so groß sein, daß bei einem Radio-Empfänger lediglich ein Rauschen zu hören ist. Ein Radio-Empfänger »hört« jeweils nur ein kleines Stück des Frequenzbandes. Um die verstreuten Signale auffangen zu können, sind spezielle Breitbandempfänger erforderlich. Der Breitbandempfänger muß über einen entsprechenden Decoder zur Umwandlung der Signale verfügen.

Es läßt sich leicht erklären, warum das Militär an dieser Technik so enorm interessiert ist – ohne den richtigen Decoder bleibt das Signal unverständlich und ist kaum aufzuspüren. Zudem ist es kaum möglich, einen solchen Sender zu stören. Stört man die gesamte Bandbreite, so wird gleich jeglicher Funkverkehr lahm gelegt.

Auch bestimmte Abhörsender arbeiten nach dem »spread-spectrum«-Prinzip. Bei »spread spectrum« sind die Funkwellen in einem großen Rauschen versteckt. Dadurch kann der Sender mit Hilfe der gängigen Ortungsapparatur nicht entdeckt werden (siehe auch Kapitel »Das Abhören von Räumen«).

Es ist absehbar, daß »spread spectrum« zur Datenübermittlung in Zukunft häufiger im kommerziellen Bereich genutzt wird. Da die Sendeleistung über ein breites Band verteilt wird, kann sie durch die bestehenden Frequenzbänder benutzt werden, ohne den Empfang von Schmalbandsendern zu stören. Dadurch ist es möglich, mehr Nutzer für ein Frequenzband zuzulassen. Ein anderer Vorteil ist die Sicherheit dieser Kommunikationsform, da die Daten immer verschlüsselt gesendet werden. Ein RLAN-System mit 100 Nutzern, das mit »spread spectrum« arbeitet, braucht nicht mehr als eine Funkfrequenz und 100 verschiedene Kodiersignale.

»Spread-spectrum« kann auf verschiedenen Frequenzbändern angewendet werden. Funkanlagen am Arbeitsplatz oder drahtlose Handys zu Hause wären denkbare zukünftige Möglichkeiten. Im kommerziellen Handel sind solche Geräte jedoch noch kaum erhältlich.

Dadurch, daß für einen Schmalbandempfänger lediglich ein Rauschen zu hören ist und normale Radiosender von dem »spread-spectrum« nicht gestört werden, könnten auch besondere Sendegenehmigungen entfallen. In den USA ist ein RLAN-System der Firma NCR[4] ohne spezielle Genehmigung zugelassen. Soweit wir wissen, sind »spread-spectrum«-Geräte in der BRD derzeit aber noch nicht erhältlich.

Anmerkungen

1 CHIP 8/95, »Luftpost zum Nulltarif, DFÜ per CB-Funk«. Komplett Set: 40 Kanal CB-Funkgerät CV 2000 und CV-CB-COM Funkmodem inklusive Software »Primus« für knapp 200,– DM erhältlich.

2 Mobilfunk und Datenschutz, Materialien zum Datenschutz, Berliner Datenschutzbeauftragter (Hg)

3 »Nahezu zufälliges« Signal. Das heißt, daß das Signal innerhalb einer bestimmten Zeitspanne zufällig Werte annehmen kann. Diese Zeitspanne kann beispielsweise 1 Sekunde oder aber auch 4,5 Tage betragen.

4 »Digitale-Analoge Technologie«, Oktober 1992, S. 24

PCs, Bildschirme und Kabel

Alle elektrischen Geräte, also auch dein PC strahlen elektromagnetische Wellen aus. Diese gehen vom Bildschirm und von den elektronischen Bauteilen im Geräteinnern aus. Je schlechter ein PC abgeschirmt ist, desto leichter fällt es, diese Strahlung aufzufangen. Mit relativ viel Aufwand kann die elektromagnetische Strahlung wieder in Signale zusammengesetzt werden, die denen entsprechen, die aus dem Gerät kommen.

Dein PC ist sicherlich noch mit anderen Geräten (Drukker, Modem, Netzwerk) verkabelt. Diese Verbindungskabel bieten weitere Angriffspunkte für unerwünschte Mithörer. Je schlechter ein Kabel isoliert ist, desto einfacher ist es, Signale von den Kabeln abzufangen. Auch nehmen andere Kabel, die in der Nähe des Computers verlaufen, Abstrahlungen auf. Mit relativ aufwendigen Methoden können diese aufgefangen und aufbereitet werden.

Bildschirme

Computer-Bildschirme »abzuhören«, ist ziemlich einfach. Es ist bekannt, daß dies bereits seit geraumer Zeit von militärischen und anderen Geheimdiensten gemacht wird. In den USA gelten seit den 60er Jahren sogenannte »Tempest«-Sicherheitsstandards für alle Geräte, die im militärischen und polizeilichen Bereich benutzt und die damit gegen Bildschirm-Abhörtechniken geschützt werden. Die Quelle von potentiellen Abhörern ist die sogenannte Reststrahlung der Computer, eine Strahlung, die in schwacher, jedoch ortbarer Form sogar durch die Wände einer Wohnung dringen und von außen aufgefangen werden kann.

Das Abhören

Rita sitzt in ihrem Büro an ihrem Computer und hat Lust, bei ihrer Arbeit ein wenig Musik zu hören. Sie nimmt das Transistorradio, zieht die Antenne heraus und stellt ihren Lieblingssender ein. Leider ist die Empfangsqualität miserabel. Auch wenn sie einen anderen Sender einstellt, bleibt der Empfang schlecht. Zufälligerweise stellt sie ihren Computer aus und was zeigt sich? Der Empfang ist wieder gut. Aus diesem Beispiel ist ersichtlich, daß der Computer nicht nur als Textverarbeitungsgerät, sondern auch als Störsender funktionieren kann. Physikalisch werden beide Signale zur elektromagnetischen Strahlung gerechnet.

Bildschirmstörsignale enthalten dieselben Informationen wie die Signale, die auf dem Computerbildschirm erscheinen. Einige Spezialisten bastelten einmal ein wenig an einem gewöhnlichen Fernsehgerät[1] herum, um damit Bildschirmstörsignale festlegen zu können. Nach ein paar Experimenten erhielten sie ein einwandfreies Bild, das sie auf Foto und Video festhalten konnten. Ein normaler Fernsehempfänger kann demnach so manipuliert werden, daß dadurch die Information rekonstruiert wird, die auf dem Bildschirm eines in der Nähe befindlichen Computers gerade sichtbar ist. Weitere Versuche erbrachten, daß Bildschirmstörsignale eines Computers bis auf eine Entfernung von über 1km feststellbar sind. Die Strahlung von älteren Computerbildschirmen ist in der Regel stärker und daher auch weiter entfernt meßbar als die der neueren Bildschirmtypen.

In den letzten Jahren konnten auch die Hersteller in Europa dazu bewogen werden, Bildschirme zu produzieren, die weniger Störsignale ausstrahlen. Weniger wegen der Abhörgefahr, sondern weil die Strahlung allgemein für gesundheitsschädlich erachtet wird. Die meisten neuen Monitore sind relativ strahlungsarm, senden entsprechend weniger Bildschirmstörsignale und dürften aus größeren Entfernungen kaum zu orten sein. Generell geht von Schwarzweiß-Bildschirmen weniger Strahlung aus als von Farbmonitoren. Es gibt auch Bildschirme, die ohne Bildröhre arbeiten wie die LCD-Bildschirme, die bei tragbaren Computern Ver-

wendung finden. Sie verbrauchen viel weniger Strom, sind fast strahlungsfrei und damit kaum abzuhören.

Gegenmaßnahmen

Der Bildschirm kann gegen elektromagnetische Strahlung abgeschirmt werden, eine relativ teure und technisch ziemlich komplizierte Angelegenheit. Der Computer müßte beispielsweise in einem hermetisch geschlossenen Metallschrank aufgestellt oder ein Störsender im Arbeitsraum angebracht werden. Letzteres müßte so erfolgen, daß der Computer störungsfrei arbeitet, die Bildschirmstörsignale jedoch im Rauschen untergehen. Der Sender müßte mit einer Breitbandantenne mit einer Leistung von um die 0 dbmW (1 Milliwatt) ausgerüstet sein. Juristisch ist es allerdings nicht gestattet, einen solche Sender zu verwenden. Die Wahrscheinlichkeit, daß der Funkkontrolldienst ihn zufällig ortet, ist jedoch gering, sofern jemand nicht unnötig auf sich aufmerksam macht und etwa den Radioempfang seiner Nachbarn stört.

Mehrere Computer in einem Raum aufzustellen, bietet keinen Schutz vor Lauschangriffen. Es ist aber möglich, Bildschirme mit Hilfe kryptographischer Techniken so umzurüsten, daß die Rekonstruktion von Bildinformationen durch Bildschirmstörsignale nahezu unmöglich wird. Es müßte hierzu nur die Linienschreibfrequenz nach einer (pseudo)zufälligen Methode verändert werden. Dazu taugliche Bildschirmtypen sind im regulären Handel jedoch noch nicht erhältlich. Bleibt also derzeit nur die Nutzung von LCD-Schirmen. Diese gibt es nicht nur für tragbare Computer, sondern auch für »normale«. Bedauerlicherweise sind sie aber ziemlich teuer.

Kabel

Eine andere Strahlungsquelle bilden die Kabel, mit denen der Computer an Peripheriegeräte wie Drucker und Modems gekoppelt wird. Über die damit verbundenen Abhörmöglichkeiten ist uns wenig bekannt. Die Strahlung ist so stark, daß in überbelegten Büros, in denen zu viele Kabel sind, Störungen entstehen können. Auch kann die Strahlung außerhalb der Räumlichkeiten aufgefangen werden.[2] Wir wissen nicht, wie schwierig es ist, auf diese Art gewonnene Information zu entschlüsseln. Glücklicherweise gibt es eine simple Lösung, um dem vorzubeugen. Abgeschirmte (geerdete) Spezialkabel kosten im Handel kaum mehr als ungeerdete. Allerdings sollte auch eine gute Erdung der Stromzufuhr von Computer und Peripheriegeräten vorgenommen werden.

Das Bundesamt für Sicherheit und Informationstechnik führte 1995 einen Versuch durch, bei dem zwei PCs desselben Netzwerkes mit einem Kabel verbunden wurden. In direkter Nähe dieses Kabels lief eine Telefonleitung lang. Die Telefonleitung wurde an einer beliebigen Stelle angezapft und es gelang die Informationen, die auf dem PC-Kabel entlangflossen, aufzufangen und wieder lesbar zu machen. Das elektrische Prinzip hierfür nennt sich Überkoppeln (kapazitives und induktives). Um jedes Kabel, in dem Ströme fließen, besteht ein mehr oder weniger großes elektromagnetisches Feld. Liegt in der Nähe eines solchen Kabels ein anderes, so springt gewissermaßen etwas von dem Strom über.[3]

Grundsätzlich ist auch eine andere Abhörmethode vorstellbar, wie etwa Hochfrequenzen in einen Raum einzustrahlen. Die zurückkommenden Hochfrequenzen könnten dann so verändert sein, daß sie die Informationen beinhalten, die gerade auf einem PC bearbeitet werden.[4] Genaueres ist uns nicht bekannt, nur, daß ein mit hochfrequenten Wellen bestrahlter PC, störanfällig wird, es etwa zum Ausfall der Maus kommen kann.[5]

Anmerkungen

1 Auf der Grundlage des gesendeten Strahlungsfeldes ist es möglich, das Bild, das auf dem Computerbildschirm sichtbar ist, mit Hilfe eines normalen Fernsehbildschirms zu rekonstruieren. Das vom Bildschirm gesendete Signal enthält jedoch nur alle Informationen des ursprünglichen Videosignals, aber nicht die erforderlichen Synchronisationssignale. Das heißt, daß sich das Fernsehbild in sowohl vertikaler als horizontaler Richtung bewegen wird, was zu keinem

sichtbaren Resultat führt. Wenn dem Videosignal allerdings Synchronisationssignale hinzugefügt werden, wird der Fernsehbildschirm das Bild problemlos wiedergeben.

2 Eck, W. van, »Electromagnetic radiation from video display units: An eavesdropping risk?«, PTT-research, April 1985; »Beyond van Eck phreaking«, John J. Williams & Family, Consumertronics, 2011 Cresent DR., P.O. 537 Alamogordo, NM 88310.

3 Bundesamt für Sicherheit und Informationstechnik, »Überkoppeln auf Leitungen«, Faltblatt Nr. 4, April 1995

4 Bundesamt für Sicherheit und Informationstechnik, »Bloßstellende Abstrahlung, eine wenig erkannte Gefahr«, Faltblatt Nr. 12, August 1995

5 1995 wurde vom Bayerischen Landesdatenschutzbeauftragten ein 486 Compac-PC mit SNI Bildschirm und UNIX Mehrplatzsystem auf Strahlung untersucht, die Daten enthalten könnte. Während sich Bildschirm, PC und Verbindungskabel selber als strahlungsarm erwiesen, konnten über dem Netzkabel Störströme noch in 30m Entfernung gut nachgewiesen werden. Wie weit diese Abstrahlungsstörströme geeignet sind, Daten wieder lesbar zu machen, wurde aber nicht untersucht. (KES, Zeitschrift für Kommunikations- und EDV-sicherheit Nr. 4, August 1995, S. 42 f.)

Datenverschleierung

Der Rest des Buches beschäftigt sich nun größtenteils mit den verschiedenen Methoden der Informationsverschleierung. In aller Regel müssen für die Datenübermittlung ja Kanäle benutzt werden, die auch unerwünschten Schnüfflern offen stehen, bzw. die oft sehr einfach zu knakken sind. Können Nachrichten leicht aufgefangen werden, liegt es auf der Hand, den Informationsaustausch für ungebetene Gäste unverständlich zu machen. Im folgenden werden wir traditionelle wie moderne Möglichkeiten der Text- und Sprachverschleierung beschreiben und deren Zuverlässigkeit behandeln. Zunächst erklären wir die klassischen Methoden, weil auf deren Prinzipien auch die moderneren, digitalisierten Varianten basieren.

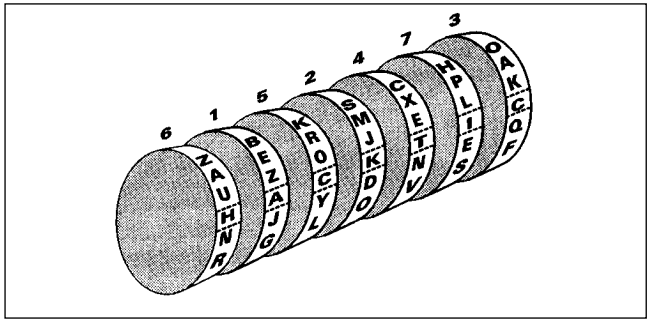
Ältere Geheimschriften

Geschriebene Nachrichten zu kodieren, ist ein jahrhundertealtes Verfahren. Schon Julius Cäsar vertraute seinen Boten nicht, über die er seine Anweisungen und Botschaften den verschiedenen Adressaten zukommen ließ. Deshalb veränderte er in der Nachricht jedes ›a‹ in ein ›d‹, jedes ›b‹ in ein ›e‹ usw. Gelangte er an das Ende des Alphabets, so begann er einfach wieder von vorn. Nur diejenigen, die diese Regel, »gehe im Alphabet drei Stellen weiter«, kannten, waren in der Lage seine Nachrichten zu verstehen. Cäsar benutzte vermutlich immer eine Austausch-Regel, wechselte jedoch die Anzahl der Stellen, die weitergeschoben werden mußten. Die von ihm angewandte Regel würde heute als »Algorithmus« bezeichnet werden, die Anzahl der zu versetzenden Stellen wäre der Schlüssel. Der Originaltext hieße heute »Klartext«, die bearbeitete Nachricht wäre ein »kodierter«

Text. Kodieren ist das Umsetzen der tatsächlichen Nachricht in eine verschlüsselte, die dann entsprechend wieder »dekodiert«, entschlüsselt werden muß. Verschleierungsmethoden heißen Kryptosysteme. Es gibt Kryptosysteme für Text und auch für Sprache, die sich Kryptographen ausdenken. Krypto-Analytiker sind ihrerseits wieder diejenigen, die sich darauf spezialisiert haben, den Code zu knacken.

Cäsars Methode ist ein Beispiel des Substituierungssystems: Nicht die Reihenfolge der Buchstaben in seiner Nachricht wurde verändert, sondern die Buchstaben selbst. Bei anderen Methoden werden sogenannte Permutationen angewendet, das heißt, daß nicht die Buchstaben selbst, sondern deren Reihenfolge geändert wurden.

Bereits am Ende des 19ten Jahrhunderts wurde die Tabellen- oder Scheibenmethode erfunden. Bei dieser Idee kamen schnell auch spezielle Chiffrier- oder Entschlüsselungsmaschinen zur Anwendung. Die Buchstaben des Alphabets wurden, willkürlich (zufällig) gemischt, auf den Rand einer runden Scheibe geschrieben. Danach wurde noch eine Reihe solcher Scheiben hergestellt, bei denen das Alphabet bei jeder Scheibe in einer anderen Form durcheinander gebracht worden war. So entstanden verschiedene Scheiben mit jeweils unterschiedlichen Tabellen.



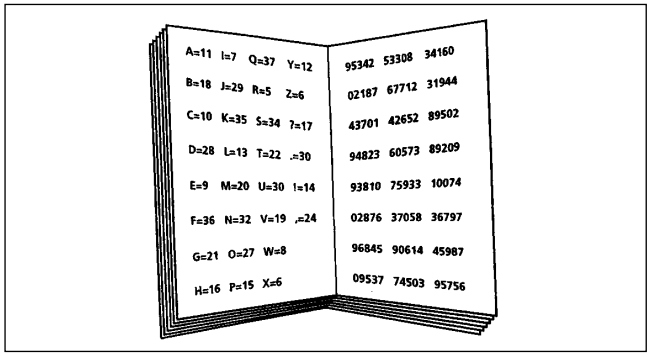
Diese Scheiben wurden in der vereinbarten Reihenfolge, dem Anfangsstand, nebeneinander auf eine Achse geschoben, um die sie sich drehen konnten. Die Nachricht wurde erstellt, indem die verschiedenen Scheiben gedreht wurden.

Der verschlüsselte Text kam zustande, indem jede Scheibe in einer bestimmten Häufigkeit in eine vereinbarte Richtung gedreht wurde (Schlüssel). An der Stelle, an der erst der Klartext stand, befand sich nun der chiffrierte Text. Bei längeren Nachrichten mußte dieses Verfahren selbstverständlich wiederholt werden. Zu diesem Zweck wurde der Klartext in Blöcke geteilt, die so groß waren wie die Anzahl Scheiben der Maschine. Je Buchstabenblock wurde dann dieselbe Drehung angewendet. Heutzutage würde dies »Blockverschlüsselung« heißen. Die Entschlüsselung erfolgte in der umgekehrten Reihenfolge, Sender und Empfänger mußten also über dieselbe Maschine verfügen.

Im Zweiten Weltkrieg benutzten die Deutschen einen auf diesem Grundprinzip basierenden Apparat mit fünf Scheiben, die Enigma. Sie änderten regelmäßig die Schlüssel. Für die Alliierten war es äußerst schwierig, die Nachrichten zu entschlüsseln, bis sie eines Tages in den Besitz eines Enigma-Apparats und des (möglichen) Anfangsstands kamen. Mit Hilfe eines Computers, der damals unter größter Geheimhaltung zum Knacken feindlicher Codes entwickelt worden war, konnten alle möglichen Schlüssel innerhalb relativ kurzer Zeit ausprobiert werden. Nach dem Krieg verkauften die Amerikaner »Dritte-Welt«-Ländern Enigma-Apparate und »vergaßen« dabei zu erwähnen, daß das System bereits geknackt worden war. Bei der Enigma war der Besitz des Geräts, und damit die Kenntnis des Algorithmus', zum Entschlüsseln des Codes von großer Bedeutung. Gegenwärtig ist die Geheimhaltung eines Algorithmus sehr viel weniger wichtig. Mathematiker haben bewiesen, daß Kryptosysteme so anzufertigen sind, daß das Kennen des Algorithmus oder der Besitz des Kryptoapparats nicht dazu führen muß, daß das System geknackt wird.

Eine weitere Verschlüsselungsmethode aus der Zeit von vor dem Computer ist wahrscheinlich osteuropäischer Herkunft. Bei dieser Methode werden Buchstaben des Klartexts mit Zahlen ausgetauscht. Danach werden die Zahlen einer mathematischen Bearbeitung unterworfen. Diese Methode könnte noch bei Spionen in Benutzung sein, die ihren Computer verloren haben.

Die Spionin und ihre Chefin besitzen ein identisches Heft in Streichholzschachtelgröße. Auf dem Umschlag des Heftes stehen die Buchstaben des Alphabets und noch ein paar Zeichen, hinter denen eine Zahl steht, mit der sie ausgetauscht werden müssen. Im Rest des Hefts, das einen langen Schlüssel darstellt, stehen lediglich fünfstellige Zahlenreihen.



Wenn die Spionin die Nachricht: »with love« chiffriert, wandelt sie erst mit Hilfe des Umschlags des Hefts »with love« in Zahlen um, zum Beispiel w=8, i=7, t=22, h=16 usw. Das Ergebnis gruppiert sie in Fünferreihen, die letzte Reihe ergänzt sie nötigenfalls mit Nullen.

w	i	t	h		l	o	v	e
8	7	22	16		13	27	19	9

Das ergibt also: 87221 61327 19900

Danach wählt die Spionin aus dem Buch eine Seite. Die erste Zeile beginnt zum Beispiel mit: 95342 53308 34160. Die Zahlen schreibt sie unter ihre »Zahlennachricht«:

VERSCHLÜSSELN	ENTSCHLÜSSELN
87221 61327 19900 »with love«	72563 14625 43060 Code
95342 53308 34160 Schlüssel	95342 53308 34160 Schlüssel
72563 14625 43060 Code	87221 61327 19900 »with love«

Die beiden Reihen addiert sie, ohne die Zehnerstellen zu übernehmen, also so, daß 8+9=7 ergibt und nicht 17, 5+7=2 und nicht 12 usw.[1] Wenn sie sich davon vergewissert hat, daß sie sich nicht verrechnet hat, schickt sie das Ergebnis ihrer Chefin, die, wie gesagt, genau dasselbe Heft besitzt. Die verwendete Schlüsselseite wird nach Verwendung vernichtet.

Die Entschlüsselung erfolgt nach dem umgekehrten Verfahren. Anstatt die Zahlen nun zu addieren, wird der Schlüssel vom Code substrahiert. Sollte das Ergebnis negativ sein, wie bei 7-9, so verfährt die Cheffin so, als ob dort 17-9 stehen würde. So erhält sie »with love« in Zahlen, die sie mit Hilfe des »Umschlags« wieder in die ursprüngliche Nachricht umsetzen kann.[2]

In Wirklichkeit war die ganze Operation noch komplizierter: Sicherheitshalber wurde die kodierte Nachricht mit unsichtbarer Tinte auf den Brief geschrieben und man kritzelte danach darüber irgendeinen nichtssagenden Text.

Beachtenswert ist, daß bei dieser Methode je Buchstabe und nicht wie bei der Enigma je Buchstabenblock eine bestimmte Bearbeitung erfolgte. Dieses Verfahren würde nun Stromverschlüsselung genannt werden. Auch ist der verschlüsselte Text länger als der Klartext, während er bei der Enigma genau dieselbe Größe besitzt.

Es wäre möglicherweise nicht einmal so schwer, dieses System zu knacken, wenn die Spionin eine bestimmte Seite, also den Schlüssel, nicht nur einmal verwenden würde. Methoden, bei denen der Schlüssel nach Benutzung aufgegessen, verbrannt oder auf eine andere Art und Weise vernichtet wird, gehören zur »one-time-code-pad«-Kategorie. Die Sicherheit des Systems beruht nicht nur auf der einmaligen Benutzung des Schlüssels. Von essentieller Wichtigkeit ist auch die Tatsache, daß der Schlüssel im voraus nicht einkalkuliert werden kann. Dies funktioniert lediglich auf der Grundlage, daß aus ein paar Zahlen des Schlüssels keine Schlüsse hinsichtlich des Rests der Zahlen des Schlüssels gezogen werden können. In solch einem Falle heißt so ein Schlüssel »random« (zufällig). In der Praxis ist das Zustandebringen eines zufälligen Schlüssels eine äußerst komplizierte Angelegenheit.

Digitale Verschleierung

Mit dem Auftauchen des Computers haben sich die Möglichkeiten von Code-Knackern vergrößert, aber auch die der verschlüsselnden Personen sind nahezu grenzenlos geworden. Nicht nur die Rechenkapazität des Computers, sondern auch die Tatsache, daß er einen Text in Einsen und Nullen speichert, Bits genannt, erweitert die Möglichkeiten (zum Beispiel A=1000001). Code-Knacker können bei ihren Bemühungen nun weniger sprachspezifische Methoden benutzen. Auch neue mathematische Erkenntnisse führten dazu, daß immer komplexere Algorithmen in Computerprogramme (Software) oder elektronische Schaltungen (Hardware/Chips) »eingebaut« werden konnten. Substituierungen, Permutationen, Tabellen und mathematische Bearbeitungen kommen in unterschiedlichen Kombinationen in den derzeit zu unterscheidenden Verschlüsselungsprogrammen vor.

Die modernen digitalisierten Kryptosysteme sind in diverse Verschlüsselungsmethoden einzuteilen. Es gibt Block- und Stromverschlüsselungen, mit denen gegenwärtig die Bearbeitung je »Block bits« oder »je Bit« gemeint ist. Methoden also, bei denen ein Originalbit in einen anderen Bit umgewandelt wird, und Methoden, bei denen der Klartext und der verschlüsselte Text nicht genauso lang sind. Bei manchen Kryptosystemen wird der Schlüssel mit Hilfe einer bestimmten Methode aus dem Klartext abgeleitet, bei anderen wird er unabhängig von diesem hergestellt. Es gibt Systeme, bei denen der Schlüssel nur einmal benutzt wird und Systeme, die einen identischen Schlüssel mehrmals verwenden.

Ferner kann ein Unterschied zwischen den erwähnten herkömmlichen Verschlüsselungsmethoden, mit nur geheimen Schlüsseln, und einem völlig anderen Konzept, das die Welt seit Mitte der siebziger erobert, und zwar »public key« (öffentlicher Schlüssel), gemacht werden. Wir werden uns diesem Thema später noch einmal widmen. Und um es alles noch komplizierter zu machen, kann gesagt werden, daß in der Praxis allerlei Kombinationen von Kryptoprinzipien verwendet werden.

Außer der Einteilung hinsichtlich der verwendeten Technik, auf der Kryptosysteme basieren, können sie in bezug auf Zuverlässigkeit, Benutzerfreundlichkeit, die Computerzeit, die sie in Anspruch nehmen, den Preis usw. beurteilt werden. Ohne den Anspruch erheben zu wollen, daß wir alles umfassend behandeln können, werden wir nun die Qualität einer Reihe einfach anzuschaffender Systeme unter die Lupe nehmen. Eine gewisse Relativierung ist jedoch angemessen: Was heute sicher als sicher gilt, braucht das morgen nicht mehr zu sein.

»One-way-code-pad«-Stromverschlüsselung

Als nicht zu knackende konventionelle Kryptosystemen gelten die Stromverschlüsselungssysteme, die über einen Schlüssel verfügen, der genügend zufällige Eigenschaften besitzt, mindestens genauso lang wie die Originalnachricht ist und darüber hinaus einmalig benutzt wird. Wir werden diese sogenannten »random«-Schlüssel nun unter die Lupe nehmen. Wir gehen dabei von der Tatsache aus, daß Krypto-Experten in der Regel über die Rezepte (in Hardware- oder Softwareform) verfügen, mit denen der Schlüssel hergestellt wird. Trotzdem soll es unmöglich sein, den gesamten Schlüssel zu bestimmen, auch nicht, wenn durch eine Panne Teile des Schlüssels bekannt wurden. Es geht also um die Frage, wie ein solcher »random«-Schlüssel angefertigt wird.

Das Rauschen eines UKW-Radios, die Strahlung der Sonne und ein Lottoergebnis beispielsweise sind zufälliger Art, weil sie keiner Formel unterliegen. Auch bestimmte elektronische Bestandteile, wie Dioden und Transistoren, können ein willkürliches Rauschen erzeugen. Solche Komponenten werden aus diesem Grunde denn auch bei manchen Hardware-Schlüsselerzeugern verwendet. Eine andere Methode zur Anfertigung hardwaremäßiger Schlüssel ist die Verwendung sogenannter Schubregister, die besonders in Sprachverschleierungsgeräten benutzt werden. Eine richtige »random«-Wirkung ist damit allerdings niemals zu erzielen.

In Softwarerezepten zum Erzeugen eines Schlüssels kann am besten die menschliche Unberechenbarkeit als willkürliche Quelle benutzt werden.

Denkbar wäre in diesem Zusammenhang zum Beispiel der Moment, an dem jemand am Computer ein bestimmte Handlung verrichtet (Computeruhr), an die Tasten auf der Tastatur, die jemand wählt, an den Zeitraum, der zwischen unterschiedlichen Tastenanschlägen liegt u.ä. Je mehr unvorhersehbare Momente, desto besser. Auch mit dieser Methode bleibt es jedoch schwer, eine völlige »random«-Wirkung zu erzielen.

Es wäre jedoch falsch, sich auf Programme zu verlassen, die zur Erzeugung eines Schlüssels nur Faktoren benutzten, die zwar sehr undurchschaubar oder kompliziert erscheinen, aber tatsächlich laut einer Reihe ziemlich einfacher Regeln funktionieren, wie die Zeit, die ein Computer benötigt, um eine bestimmte Berechnung auszuführen oder eine Datei auf der Festplatte zu speichern.

Die Unvorhersehbarkeit des Schlüssels ist auf jeden Fall für die Sicherheit einer Methode von großer Bedeutung. Um einen verschlüsselten Text zu erhalten, genügt die sogenannte »XOR«-Bitoperation[3], die bei vielen Verschlüsselungsmethoden Anwendung findet. Das XOR-Prinzip bedeutet, daß ein Bit aus der Nachricht mit dem entsprechenden Bit aus dem Schlüssel verglichen wird. Weichen die Bits voneinander ab, dann wird in den verschlüsselten Text an dieselbe Stelle eine »1« gesetzt. Sind sie gleich, so kommt in die kodierte Nachricht eine »0«. Mit derselben Bitoperation erhält man auch wieder die ursprüngliche Nachricht. Zum Beispiel:

VERSCHLÜSSELN (XOR)	ENTSCHLÜSSELN (XOR)
1101011 Klartext	1001010 Verschlüsselter Text
0100001 Schlüssel	0100001 Schlüssel
1001010 verschlüsselter Text	1101011 Klartext

Ist der Schlüssel zufällig genug, eignet sich diese simple Operation tatsächlich zur Verschlüsselung.[4] Das System ist sicher, weil Code-Knacker nicht viel mehr anstellen können, als alle möglichen Schlüssel auszuprobieren. Die Anzahl vorstellbarer möglicher Schlüssel ist natürlich fast unendlich groß, infolgedessen benötigt sogar ein leistungsstarker

Computer der gegenwärtigen Generation fast endlose Berechnungen. Ein sicheres System also, aber durchaus mit einer Menge lästiger Nachteile.

Das Verschlüsseln und Senden großer Dateien von der Festplatte wird relativ viel Zeit beanspruchen. Das ist natürlich äußerst unangenehm, wenn es häufiger gemacht werden muß. Darüber hinaus wird zur Kommunikation je Person immer ein anderer Schlüssel benutzt, während möglicherweise mit vielen Leuten kommuniziert wird. In diesem Falle muß ein ganzer Stapel Disketten vor unbefugtem Zugriff geschützt werden. Der Schlüssel muß dabei erst auf eine sichere Art und Weise ausgetauscht werden. Für Regierungen und finanzkräftige Organisationen ist dies wahrscheinlich kein großes Problem, aber für uns? Noch unangenehmer wird es, wenn irgendetwas mit der Kommunikation schief geht. Wenn nur ein einziges Bit abhanden kommt, so muß der »Klartext« erneut kodiert und geschickt werden.

Kurzum, solche Systeme sind nicht gerade sehr benutzerfreundlich. In manchen Situationen sind solche Unannehmlichkeiten vielleicht in Kauf zu nehmen. So benutzte in El Salvador die Widerstandsbewegung FMLN ein solches System, ebenso wie auch diverse andere lateinamerikanische Guerillagruppen.

»One-way-code-pad«-Stromverschlüsselung: »digital random«

»Digital random« besteht aus Software und einem Hardware-Schlüsselerzeuger (110–250V). Die Software eignet sich lediglich für DOS-Geräte. Der Schlüsselerzeuger ist ein Kasten mit elektronischen Schaltungen, der an den Computer gekoppelt werden kann. Das Prinzip des Schlüsselerzeugers basiert auf dem Rauschen, das mit Hilfe einer Zener-Diode zu erzeugen ist. Dieses Rauschen wird verstärkt und digitalisiert. So werden einzigartige Reihen willkürlicher Bits hergestellt. Der Erzeuger ist so entworfen worden, daß er gegen Lichtnetz- und andere Störungen unempfindlich ist. Der Bitstrom aus dem Erzeuger wird über ein Softwareprogramm gesteuert. Es ist möglich, das Ergebnis hinsichtlich Zufälligkeit und, in verschlüsselungstechnischer Hin-

sicht, schwacher »random«-Reihen, das heißt mit einer ungleichmäßigen Verteilung des Spektrums, zu kontrollieren (für ersteres Run-Test und Chi-Quadrattest und letzteres die Spektralanalyse). Die Herstellung von Schlüsseln beschäftigt einen Computer dann übrigens stundenlang. Das Verschlüsselungsprogramm gründet sich auf der XOR-Operation, die wir oben erläutert haben. Selbiges Programm entfernt nach dem Senden einer Nachricht automatisch den verwendeten Teil des Schlüssels. Nach unserem Wissensstand sind mit Hilfe dieses Systems kodierte Nachrichten noch nie in die falschen Hände geraten. Kosten: etwa 1000 DM für Software, Erzeuger, Kabel usw., Informationen sind über Backslash erhältlich.

Blockverschlüsselung: DES

Zur dubiosen Kategorie zählt unserer Ansicht nach die Standard-DES-Verschlüsselung. DES ist die Abkürzung für »Data Encryption Standard«, die als Chip geliefert wird und auch als Softwareprogramm erhältich ist (z.B. pc-DES). DES wurde in den siebziger Jahren von IBM entwickelt. Laut Gerüchten zwang die »National Security Agency« (NSA) den Betrieb, das System absichtlich mit Schwachstellen auszurüsten. Die NSA ist der US-amerikanische militärische Abschirmdienst und wurde 1952 eingerichtet und ist als einer der wichtigsten Abhör- und Verschlüsselungs- bzw. Entschlüsselungsdienste der Welt anzusehen. Allein schon für das Abfangen internationaler Kommunikation soll der Dienst jährlich etwa 30 Milliarden Dollar ausgeben.

1971 wurde DES in den USA zum Standard hochgejubelt. Genehmigt von einer Regierung, die ihre Geheimnisse übrigens nicht DES anvertraut! Augenblicklich ist dieser Algorithmus im kommerziellen Bereich zur Sicherung der Datenkommunikationen die (noch) am meisten benutzte Methode. Elektronische Briefe, gespeicherte Daten und Sprache können mit DES verschleiert werden.

DES ist ein zur Ver- und Entschleierung von Blöcken von 64 Bit entworfenes Blockverschlüsselungssystem. Der verwendete Schlüssel ist ebenfalls 64 Bit lang, es werden jedoch lediglich 56 Bit wirklich benutzt.[5] Tatsächlich besteht

der Algorithmus aus einer Aneinanderreihung unterschiedlicher Bearbeitungen: in den meisten Fällen auf Tabellen basierende Permutationen und Substituierungen. Für die zu unterscheidenden Bearbeitungen werden meistens wechselnde Schlüssel verwendet, die aus einem Hauptschlüssel abgeleitet sind.

Die Entwurfskriterien, auf der sich die diversen Schritte bei DES gründen, sind geheim. Die Funktion ist lediglich in Form wenig übersichtlicher Tabellen freigegeben worden. Dadurch ist es schwer, herauszufinden, von welchen analytischen oder mathematischen Funktionen die diversen Verarbeitungsphasen festgelegt werden. Wissenschaftler haben natürlich bereits allerlei Versuche unternommen, DES auseinanderzunehmen, hatten jedoch nur für einzelne Bestandteile des Algorithmus Erfolg. Viele schließen jedoch nicht aus, daß es doch noch eine »Hintertür« gibt, die es ermöglicht, aus dem verschlüsselten Text den Klartext abzuleiten.

Exkurs: Der DES Algorithmus und DES-»modes«

Das DES-System kann auf vier verschiedene Arten und Weisen (»modes«) funktionieren.

Die simpelste Methode (ECB = »electronic code book«) läuft darauf hinaus, daß der DES-Algorithmus für jeweils 64 Bit Klartext benutzt wird, dabei besteht keinerlei Zusammenhang mit den vorherigen Blöcken. Dies ist die schwächste Methode. Bei einer weiteren Möglichkeit (CBS = »cipher block chaining«) erfolgt, bevor die DES-Verschlüsselung beginnt, bei jedem folgenden Block erst mit dem vorherigen bereits verschlüsselten Block eine XOR-Operation (eine sogenannte modulo 2 Addition). Der erste Block wird um modulo 2 mit einem zufälligen Schlüssel, initialer Vektor genannt, addiert. Solch ein initialer Vektor ist auch für die dritte Methode (CFB = »cipher feedback«) erforderlich. Jetzt wird es jedoch noch ein wenig komplizierter: Die Eingabe für DES besteht nicht einfach aus einem Block mit 64 Bit Klartext oder »geXORdem« Text wie bei den oben beschriebenen Möglichkeiten. Es wird zwar ein Block aus 64 Bit eingegeben, dieser setzt sich nun jedoch völlig anders zusammen. Zur Erläuterung wählen wir als Beispiel für die Länge der Bitreihen, mit denen gearbeitet wird, 10, es hätte allerdings jede andere Zahl zwischen 1 und 64 sein können. Außerdem setzen wir voraus, daß der initiale Vektor auch 10 Bit lang ist, was nicht unbedingt so sein muß.

Der erste DES-Eingabeblock besteht aus (64-10) Nullen und 10 Bit

initialem Vektor (IV). Von dem Ergebnis nach der DES-Bearbeitung werden die an der linken Seite stehenden 10 Bit genommen und um modulo 2 zu den ersten 10 Bit Klartext addiert (T1): Damit erhalten wir das erste Stück verschlüsselten Text von 10 Bit (C1). Der zweite DES-Eingabebefehl besteht aus (64-10-10) Nullen, 10 Bit IV und 10 Bit C1. Von dem Ergebnis nach der DES-Bearbeitung werden wiederum die ersten 10 Bit genommen und um modulo 2 zu den zweiten 10 Bit Klartext addiert (T2). Der dritte Eingabeblock besteht aus (64-10-10-10) Nullen, 10 Bit IV, 10 Bit C1 und 10 Bit C2. So geht das immer weiter. Im weiteren Verlauf der Bearbeitung werden immer die Bits an der linken Seite, also hintereinander die IV, C1 usw., aus dem Eingabeblock verschwinden, da mit immer mehr Blöcken mit 64 Bit gearbeitet wird. Wenn wir die »10« mit einer zufälligen Zahl »k« austauschen und kDES bedeutet, daß von der Eingabe der DES-Operation lediglich die ersten k-Bits genommen werden, so sieht das obenstehende als Formel folgendermaßen aus:

C1=T1 XOR kDES (0,IV)
C2=T2 XOR kDES (0,IV,C1)
C3=T3 XOR kDES (0,IV,C1,C2) usw.

Im OFB-»mode« (Output Feedback) werden auch k-Bit-Blöcke und der initiale Vektor zur Eingabe für DES benutzt. Der DES-Algorithmus wird in dem Falle jedoch nur dafür angewandt, um pseudozufällige Bitreihen zu erzeugen, die modulo 2 mit dem Klartext addiert werden und so den verschlüsselten Text ergeben. Daraus ergibt sich folgende Formel:

C1=T1 XOR kDES (0,IV) = T1 XOR Q1
C2=T2 XOR kDES (0,IV,C1) = T2 XOR Q2
C3=T3 XOR kDES (0,IV,C1,C2) = T3 XOR Q3 usw.

Trotz aller Möglichkeiten von DES kann angesichts der gegenwärtigen technischen Entwicklungen behauptet werden, daß die Schlüssellänge, nämlich 56 Bit, beim Standard-DES-Verfahren zu klein (geworden) ist. »Es ist möglich, mit einer Million Dollar ein Gerät zu bauen, das innerhalb von sieben Stunden jeden DES-Schlüssel finden kann. Das heißt, daß das Gerät durchschnittlich alle dreieinhalb Stunden eine DES-Verschlüsselung brechen kann ... Für zehn Millionen Dollar haben Sie eine Maschine, die dafür im Durchschnitt lediglich noch 21 Minuten benötigt und mit 100 Millionen sind das nur noch zwei Minuten ... Ich bin mir sicher, daß die NSA angesichts ihres Budgets es innerhalb von ein paar Sekunden kann!«[6] Während die bundesdeutschen Landeskriminalämter mehrere Wochen brauchen, um DES-Verschlüsselungen zu knacken, muß davon ausgegangen werden, daß versiertere Behörden, wie der Verfassungsschutz oder der BND, dazu kaum mehr als ein paar Minuten benötigen. Zur Erhöhung der Zuverlässigkeit wird deshalb DES-Hardware auf den Markt gebracht, bei der mehrmals verschlüsselt wird, manchmal mit Algorithmen, die nicht auf DES basieren, oder mit längeren Schlüsselreihen.
Mittlerweile sind in den USA Programe erhältlich, die es Menschen ermöglichen, die ihr DES Paßwort vergessen haben, dieses wiederzuentdecken. Verschlüsselungsprogramme, die DES benutzen sind PC-DES, PC-Secure und Norton Diskreet, um nur einige aufzuzählen. Wer auf DES vertraut ist selber schuld.

IDEA

Eine Alternative zu DES ist IDEA (International Data Encryption Algorythm). Auch mit IDEA können Texte, gespeicherte Daten und Sprache verschleiert werden. Es handelt sich um ein schweizerisches Produkt, das von Xuejia Lai und James Massey ausgetüftelt worden ist und als Hardware und Software erhältlich ist. Der Algorithmus, der im Gegensatz zu DES gut bekannt ist, basiert auf diversen mathematischen Bearbeitungen und besteht auch aus mehreren Schritten. Der verwendete Schlüssel ist hier 128 Bit lang. Im Durchschnitt ist IDEA doppelt so schnell wie DES.

IDEA ist zu neu, als daß man sich bereits definitiv über dessen Sicherheit äußern könnte. Die Erfinder haben jedoch ihr bestes gegeben, um das Rezept gegen alle bekannten möglichen Angriffstechniken der Code-Knacker zu immunisieren. In diversen akademischen und militärischen Kreisen wird nun daran gearbeitet, das System zu brechen. Unseres Wissens bisher erfolglos, dabei ist es jedoch noch die Frage, ob wir die ersten sein werden, die über einen eventuellen erfolgreichen Versuch in Kenntnis gesetzt werden.

Exkurs: Der IDEA Algorithmus

Der Algorithmus arbeitet mit Blöcken aus 64 Bit und verwendet einen Schlüssel von 128 Bit. In der IDEA-Software werden diese Schlüssel an Hand der Nachricht selbst erzeugt. Der IDEA-Algorithmus wird achtmal durchlaufen, der erste Eingabeblock aus 64 Bit ist

der Klartext in Form von Nullen und Einsen. Der zweite Eingabeblock wird durch das Ergebnis der ersten Runde bestimmt, der dritte Eingabeblock ergibt sich aus dem Resultat der zweiten Runde usw. Die mathematischen Bearbeitungen, die innerhalb des IDEA-Rezepts verwendet werden lauten:

(a) XOR (modulo 2 Addition)
(b) Addition modulo 2^16
(c) Multiplikation modulo 1 + 2^16

In jeder Runde wird der 64-Bit-Eingabeblock in vier Blöcke aus 16 Bit verteilt (X1, X2, X3, X4) und werden sechs Unterblöcke aus 16 Bit des Schlüssels verwendet (S1, S2, S3, S4, S5, S6). Insgesamt werden zum Schluß 52 Schlüssel-Unterblöcke benutzt worden sein, 6 je Runde und 4 zwecks einer letzten Bearbeitung des Ergebnisses der achten Runde. Die Schlüssel-Unterblöcke werden folgendermaßen hergestellt: Erst werden die 128-Bit-Schlüssel in 8 Blöcke von 16 Bit aufgeteilt. 6 für die erste Runde und nochmal 2 für die zweite Runde. Danach wird der Schlüssel 25 Bit nach links rotiert und wieder in 8 Blöcke von 16 Bit aufgeteilt. Von diesen werden vier für die zweite Runde und vier für die dritte Runde verwendet. Der Schlüssel wird dann erneut 25 Bit nach links rotiert und es werden abermals 8 Blöcke von 16 Bit erstellt. Dies wiederholt sich bis zum Ende des Algorithmus. In jeder Runde geschieht folgendes:

1) X1 und S1 werden multipliziert (c)
2) X2 und S2 werden addiert (b)
3) X3 und S3 werden addiert (b)
4) X4 und S4 werden multipliziert (c)
5) XOR-Operation (a) mit den Ergebnissen von Schritt 1 und 3
6) XOR-Operation (a) mit den Ergebnissen von Schritt 2 und 4
7) Multipliziere das Ergebnis von Schritt 5 und S5 (c)
8) Nun wird das Ergebnis von Schritt 6 und 7 addiert (b)
9) Multipliziere das Ergebnis von Schritt 8 und S6 (c)
10) Das Ergebnis von Schritt 7 und 9 wird addiert (b)
11) XOR-Operation (a) mit den Ergebnissen von Schritt 1 und 9
12) XOR-Operation (a) mit den Ergebnissen von Schritt 3 und 9
14) XOR-Operation (a) mit den Ergebnissen von Schritt 2 und 10
13) XOR-Operation (a) mit den Ergebnissen von Schritt 4 und 10

Die Ergebnisse von Schritt 11, 12, 13 und 14 sind die Ergebnisse einer Runde. Vor der Eingabe der folgenden Runde (außer bei der letzten Runde) werden die zwei inneren Bitblöcke ausgetauscht.
Nach der letzten Runde wird das Ergebnis wie folgt bearbeitet:

1) X1 und S1 werden multipliziert (c)
2) X2 und S2 werden addiert (b)
3) X3 und S3 werden addiert (b)
4) X4 und S4 werden multipliziert (c)

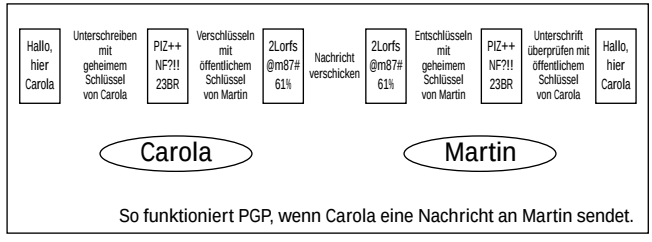
Die Ergebnisse dieser Berechnungen werden wieder zusammengefügt, damit ist der verschlüsselte Text fertig. IDEA besitzt dieselben vier Installations-Methoden (»modes«) wie DES.

»Public key«

In den 70er Jahren entstand ein neues Konzept innerhalb der Kryptologie, und zwar »public key«. Bei »public key« besitzt jede Person eine einzigartige Kombination zweier unterschiedlicher, jedoch zueinander gehörender Schlüssel, einen öffentlichen und einen privaten Schlüssel. Diese Schlüssel müssen so entworfen sein, daß das, was mit dem öffentlichen verschlüsselt ist, nur mittels des privaten entschlüsselt werden kann.

Zweck des Ganzen ist es, daß zum Beispiel Martin an Carola seinen öffentlichen Schlüssel über einen frei zugänglichen Kanal schicken kann. Carola kann ihre Nachricht an Martin mit diesen Schlüssel kodieren. Martin entschlüsselt die Nachricht mit seinem Privatschlüssel. Solange er den Schlüssel gut geheim hält, gibt es niemanden, der die Nachricht sonst noch lesen könnte.

Wenn es sich um ein gut aufgebautes System handelt und Carola auch Martin ihren öffentlichen Schlüssel übermittelt hat, kann Carola ihren Privatschlüssel wieder als Sicherheit dafür benutzen, daß sie es war, die Martin die Nachricht gesendet hat. Jeder Idiot, der Martins öffentlichen Schlüssel besitzt, kann ihm schließlich eine kodierte



So funktioniert PGP, wenn Carola eine Nachricht an Martin sendet.

Nachricht schicken. Carola unterzeichnet zu diesem Zweck die besagte Nachricht erst mit ihrem privaten Geheimschlüssel und versieht sie gleichsam mit ihrer »digitalen Unterschrift«. Sobald Martin die Nachricht erhält, entschlüsselt er sie erst mit seinem Privatschlüssel und überprüft danach Carolas Unterschrift mit ihrem öffentlichen Schlüssel. Voraussetzung ist, daß Carolas öffentlicher und privater Schlüssel ein Schlüsselpaar sind.

RSA

Code-Knacker können bei »public key« eine zusätzliche Angriffstechnik anwenden. Sie können nämlich versuchen den privaten Geheimschlüssel auf irgendeine Art und Weise aus dem öffentlichen Schlüssel abzuleiten. Die meisten im Laufe der Zeit erfundenen Rezepte zur Anfertigung von Schlüsselpaaren erwiesen sich in diesem Punkt nicht resistent gegenüber Knackern. Das einzige Rezept, das für sicher erachtet wird, ist das sogenannte RSA-System, das nach seinen Entwicklern Rivest, Shamir und Adleman benannt worden ist. Das System basiert auf der Tatsache, daß es zwar einfach ist, zwei Zahlen, die nur durch sich selbst geteilt werden können, also Primzahlen, zu multiplizieren, daß es allerdings erheblich schwerer ist, aus der Summe wieder die ursprünglichen Primzahlen zu ermitteln. Wenn die Primzahlen groß genug sind, wird das sogar unmöglich.

Wenn das Produkt der Primzahlen einen Zahl aus bis zu 200 (Dezimal)zahlen ist, so dauert es mit der derzeitigen Rechengeschwindigkeit von Computern einige Millionen Jahre, um die ursprünglichen Primzahlen zu finden. Um etwas von der Sicherheit des RSA-Systems verstehen zu können, kannst du dir folgendes vorstellen:

Es werden zwei unendlich große Telefonbücher einer imaginären Stadt zusammengestellt. Das eine Buch wird nach Nummern sortiert und das andere nach Nachnamen. Das Telefonbuch mit Nachnamen wird veröffentlicht und selbst behältst du das Nummernbuch. Menschen, die dir das Wort »DOOF« schicken wollen, suchen im Namentelefonbuch einen Nachnamen, der mit D anfängt, zum Beispiel »Dänicken«, dann einen mit einem O, beispielsweise

»Odenbach«, usw. Die Nachricht, die sie senden möchten, besteht danach nur aus den Telefonnummern von Dänicken, Odenbach und den anderen gewählten Leuten. Du besitzt das nach Nummern sortierte Buch und kannst die Nachricht entschlüsseln. Weil die Telefonbücher nahezu unendlich dick sind, ist das Sortieren des öffentlichen Buches nach Nummern ein unausführbares Unternehmen und es würde endlos dauern, zu versuchen, die richtige Telefonnummer zu finden.

Der große Vorteil von »public key« ist, daß der Austausch von Schlüsseln einfacher geworden ist und du nicht erst einen Kurier schicken mußt. Und es sind keine Stapel von Disketten vor Unbefugten zu schützen. Das große Problem beim RSA-Algorithmus liegt darin, daß der Verschlüsselungs- und Entschlüsselungsprozeß äußerst zeitraubend ist. In der Praxis benutzt denn auch niemand das RSA-System in seiner reinsten Form, allein schon aus dem Grunde nicht, daß konventionelle Schemen nicht schwächer zu sein brauchen als die »public-key«-Verschlüsselung. Das nachstehende Programm, PGP, benutzt denn auch eine Kombination aus »public key« und dem eher erwähnten IDEA.

Exkurs: Der RSA-Algorithmus

Der Algorithmus, der den Schlüssel anfertigen muß, selektiert erst zwei hohe Primzahlen a und b. Von diesen Primzahlen wird das Produkt n ermittelt. Also:

$$n = a \times b$$

Danach wird eine Zahl e festgelegt, und zwar so, daß:

$$3 < e < (a - 1)(b - 1)$$

und der größte gemeinsame Teiler von e und (a – 1)(b – 1) 1 ist, beziehungsweise e ist hinsichtlich (a – 1)(b – 1) die relative Primzahl. Mit Hilfe der Zahl e wird Zahl d berechnet, und zwar so, daß:

$$d \times e = 1 \bmod (a - 1)(b - 1)$$

ist, d ist also die Umkehrung von e. Der öffentliche Schlüssel besteht nun aus dem Zahlenpaar (e,n). Die Größen a, b, und d sind geheim. Das Erstellen des verschlüsselten Codes funktioniert folgendermaßen. Die Originalnachricht wird in Blöcke B geteilt, und verschlüsselt:

Code = B^e mod n

Die Funktionsweise des Systems beruht auf der Tatsache, daß e zwar einfach aus d errechnet werden kann, dies umgekehrt jedoch nicht der Fall ist. Es ist nahezu unmöglich, d auf der Grundlage nur des öffentlichen Schlüssels (e,n) zu ermitteln. Um d zu errechnen müssen a und b auch bekannt sein.

PGP

»Pretty Good Privacy« (PGP) ist ein von Phil Zimmermann entwickeltes Software-Paket. Es wird vor allem zur Verschlüsselung von E-Mail benutzt, es lassen sich damit jedoch selbstverständlich auch Dateien verschlüsseln. PGP kostet nichts und erfreut sich mittlerweile weltweiter Beliebtheit.

PGP hat in den USA die Diskussion über das Verbot von – nicht seitens der Regierung genehmigten – Verschlüsselungssystemen angefacht. Es ist bereits länger so, daß Gesetzesdiener und Geheimdienste die Verbreitung guter Verschlüsselungsprogramme und Veröffentlichungen darüber behindern. 1991 gab es im US-Senat die Gesetzesvorlage 266, die glücklicherweise nicht verabschiedet wurde. In dieser sollte geregelt werden, daß alle Anbieter von Verschlüsselungstechniken Hintertüren einbauen, die es der Regierung ermöglichen, verschlüsselte Nachrichten wieder zu entziffern. Dementsprechend verärgert war die NSA wohl, als Phil Zimmermann sein PGP herausbrachte, er wurde mit einem Verfahren wegen Verstoß gegen den Export von Kriegswaffen, zu denen Kryptosysteme offensichtlich gehören, belangt. (Ein Spendenkonto für Phil Zimmermann findet sich auf der beiliegenden Diskette unter PGP.TXT).

Regierungen, Geheimdienste und Militärs scheinen sich nun bewußt zu werden, daß sie sich in einer Lage befinden, die lästiger ist als vor dem Computerzeitalter. Früher konnten sie noch in Briefschlitzen angeln, Briefe unauffällig mit Dampf öffnen, Telefongespräche abhören und aufzeichnen, was infolge des arbeitsintensiven Charakters dieser Maßnahmen gezwungenermaßen selektiv erfolgen mußte.

1993 wurde nach jahrelanger Vorbereitung durch die NSA eine neue Verschlüsselungstechnologie namens Clipper

eingeführt. Kernstück ist ein Chip, der nach einem geheimgehaltenen Verfahren arbeitet. Die US-Regierung hat die Kommunikationsindustrie aufgefordert, diesen Chip in alle Geräte einzubauen, die eine »sichere« Kommunikation gewährleisten sollen, wie Telefone, Faxgeräte usw. Tatsächlich werden US Regierungsstellen bereits mit diesem von »AT&T« produzierten Geräten umgerüstet. Der Haken bei Clipper ist, daß jeder Chip seinen individuellen Schlüssel bekommt, und die Regierung erhält Kopien dieser Schlüssel.

Deshalb gibt es PGP. PGP ist kostenlos und kann an jede/n weitergegeben werden. Wenn sich PGP einbürgert, heißt dies, daß das Lesen (elektronischer) Post anderer Leute wieder eine zeitraubende Beschäftigung wird, die nicht im großen Stil eingesetzt werden kann, sollte es denn überhaupt gelingen, die Post zu lesen.

PGP verwendet die Algorithmen RSA, IDEA und wenn Nachrichten unterschrieben werden MD5.

Mit dem RSA Algorithmus erzeugt PGP ein Schlüsselpaar: einen öffentlichen Schlüssel, der verschickt werden kann und einen privaten Schlüssel, der gut geschützt zu Hause bleiben sollte. Der private Schlüssel ist zusätzlich mit einem Paßwort (Mantra) geschützt.

PGP erzeugt mit IDEA für jede Verschlüsselung einen zufällig ausgewählten Schlüssel, der nur ein einziges Mal verwendet wird, und verschlüsselt hiermit die Nachricht. Anschließend wird dieser Einmalschlüssel mit dem öffentlichen Schlüssel des Empfängers codiert und in die verschlüsselte Nachricht hineingeschrieben. Die Empfängerin kann nun mit Hilfe ihres privaten Schlüssels den Einmalschlüssel wieder herstellen und die gesamte Nachricht entziffern.

Außerdem können Nachrichten vom Verschickenden unterschrieben werden. Dazu benutzt PGP eine Methode, die MD5 (Message Digest 5) heißt. MD5 erzeugt aus einer Nachricht eine 128-bit Zahl, das ist sowas ähnliches wie eine Quersumme, die die Nachricht eindeutig bestimmt. Anschließend wird diese 128-bit Zahl mit dem privaten Schlüssel automatisch codiert und zusammen mit dem Datum, wann die Nachricht erstellt wurde, an die Nachricht angehängt. Beim Entschlüsseln wird diese 128-bit Zahl wieder ent-

schlüsselt und das Programm überprüft automatisch, ob sie zu der Nachricht paßt. Damit ist die Überprüfung gewährleistet, daß die Nachricht auch tatsächlich vom Unterzeichnenden stammt. Das Handbuch zu PGP findet sich auf der beiliegenden Diskette.

Exkurs: Kritik an PGP

PGP ist eines der Systeme, die (noch) nicht zu knacken sein sollen. Es ist wohl möglich, daß ein Dritter den öffentlichen Schlüssel auf dem Weg zum Adressaten abfängt, ihn etwas bearbeitet und danach weitersendet. Wenn du mißtrauisch bist, mußt du den ursprünglichen Schlüssel mit dem angekommenen vergleichen.[7] Ferner behaupten manche Leute, daß die Art und Weise, mit der bei PGP Primzahlen gewählt und überprüft werden, verbesserungsfähig sei.[8]

Aus dem Programmiercode soll abzuleiten sein, daß »unter den ungünstigsten Umständen« hinsichtlich einer gewählten Primzahl eine Wahrscheinlichkeit von 6,25% besteht, daß sie gar keine Primzahl ist. Weil je Schlüsselpaar zwei Primzahlen gewählt werden müssen, gibt es »im ungünstigsten Fall« also eine durchschnittliche Wahrscheinlichkeit von 12,5%, daß eine der beiden Zahlen keine Primzahl ist. Das Programm enthält zwar einen Test (Fermat's Little Theorem), um zu überprüfen, ob eine gewählte Zahl wirklich eine Primzahl ist, aber manche Zahlen (Carmichael-Nummern) entgehen dem Test. Obwohl nicht viele dieser Nummern existieren, ist es empfehlenswert, bessere Kontrolltests zu verwenden, als jene, über die PGP verfügt (und zwar Solovay-Strassen und Miller-Rabin). PGP ist völlig von den Primzahlen abhängig, deshalb ist vorgeschlagen worden, dem Nutzer selbst die Möglichkeit zu bieten, selbst die Primzahlen einzustellen. Die Antwort von Zimmerman auf diese Kritik läuft auf folgendes hinaus. Die Wahrscheinlichkeit, daß sich »die ungünstigsten Umstände« einstellen, ist an sich auch wieder sehr gering. Die wirkliche Wahrscheinlichkeit, daß eine Nichtprimzahl entsteht, ist sehr viel kleiner als die genannten Prozentsätze. Mit den besagten Prozentsätzen müßte auf dem eigenen PC innerhalb eines Abends eine Nichtprimzahl zu finden sein. Das entspricht nicht den Tests, die Zimmermann selbst und andere ausführten. Laut Zimmerman ist dabei die Wahrscheinlichkeit, daß eine Nichtprimzahl gewählt wird, die auch noch eine Carmichael-Nummer ist, und also von Fermats Test nicht erkannt wird, sehr gering.

Bist du jedoch nicht von Zimmermann überzeugt, so kannst du beim PGP-Programmcode (Quellcode), der völlig freigegeben ist, eine Änderung durchführen. Suche in der Datei »genprime.c« die Funktion »slowtest«. Die Prozentsatzeinstellung läßt sich dort leicht finden:

```
for (i=); i<4; i++) {..}
```

Ändere »4« in eine höhere Zahl. Die Wahrscheinlichkeit einer Nichtprimzahl beträgt unter den ungünstigsten Umständen mit »4« 1/16 (16=2^4). Nimmst du nun 10, was die Kritiker durchaus für sicher erachten, so verringert sich die Wahrscheinlichkeit einer Nichtprimzahl auf 1/1024 (1024=2^10) beziehungsweise 0,1%. Den Ursprungscode mußt du danach erneut kompilieren. Die Zeit zur Anfertigung von Schlüsseln wird nun allerdings, je nach der Leistung des Computers, auf mehrere Stunden verlängert.

Es ist auch nicht weiter verwunderlich, daß die Befürworter eines Chiffrierverbots auch dafür plädieren, einen neuen Verschlüsselungsstandard einzuführen. DES ist veraltet, und ein neues genehmigtes Chiffriersystem wäre die Voraussetzung, ein Verbot anderer Systeme zu ermöglichen. Das System, daß sich dafür eignen würde, heißt »Skipjack« und ist in Form eines Chips, der »Clipper« genannt wird, erhältlich. Der Algorithmus, über den weiter nicht viele Einzelheiten in Erfahrung zu bringen sind, ist von der NSA entwickelt worden und funktioniert mit einem speziellen »Hauptschlüssel«, mit dem der 80-bit lange Schlüssel, der zur Kommunikation verwendet wird, chiffriert wird. Außerdem besitzt jedes Gerät, ein paar einzigartige Nummern, die auch mit den Nachrichten mitgesendet werden. Der Lieferant händigt diese Nummern zusammen mit dem Namen des Kunden den Regierungsbehörden aus. Die können anhand der Gerätenummer den Hauptschlüssel suchen. Um unerwünschter Nutzung einigermaßen vorzubeugen, wird der Hauptschlüssel in zwei Teile getrennt und von verschiedenen staatlichen Behörden gespeichert. Es sind beide Schlüsselteile erforderlich, um die verschleierte Information dennoch mithören zu können. Nur Regierungsfunktionäre mit Sonderbefugnis erhalten offiziell zu den beiden Hauptschlüsselteilen Zugang.

Auch die Deutsche Telekom bietet über ihre Tochterfirma Telesec einen Verschlüsselungschip an, mit dem dann elektronische Kommunikation (Telefon, Fax, Modem) verschlüsselt werden kann. Das Verfahren benutzt genauso wie PGP den RSA Algorithmus und MD5 zur Überprüfung. Der Haken bei der Sache ist, daß die Schlüsselpaare von Telesec erstellt und Kopien aufbewahrt werden. Das ist sicherlich eine feine Sache, falls du deine Chipkarte verlierst, aber wer noch alles Zugang zu den Daten der Telekom hat, haben wir schon weiter oben beschrieben. In der Werbung heißt es, »Auch hier gilt: Sicherheit durch Vertrauen«. Wir würden niemandem raten, jemandem zu

vertrauen, der eine Kopie deiner Schlüssel besitzt.
Manche Menschen sehen es als ihr Recht an, ihre Privatsphäre so zu schützen, wie sie es selbst für passend halten. Deshalb lehnen sie eine Staatskontrolle über die Chiffrieranwendungen ab. Sollte jemals ein Gesetz zur Reglementierung von Chiffriermethoden in Kraft treten, so gibt es für diejenigen, die behördlichen Stellen nicht allzu sehr vertrauen, dennoch einen kleinen Lichtblick. Die Gesetzgeber laufen beinahe immer der technischen Entwicklung hinterher. In den USA beschäftigen sich zum Beispiel nun bereits Leute damit, PGP unsichtbar zu machen (Stealth-PGP). Bei dieser PGP-Variante wird es schwierig werden, zu beweisen, daß eine Verschlüsselung verwendet worden ist. Oder werden sie demnächst auch verbieten, einander Rauschen oder Blödsinn zu senden? Es gibt auch noch andere Möglichkeiten, um zu verhindern, daß von Datenverschleierung die Rede ist, indem beispielsweise Nachrichten in unsinnige Texte oder in Abbildungen versteckt werden.

Nachrichten in Abbildungen

Nachrichten in Abbildungen zu verstecken geht eigentlich noch einen Schritt weiter als das Unleserlich-Machen von Kommunikation. Diese Methode wird Steganographie genannt und betrifft zugleich das Verbergen der Tatsache, daß es sich um Kommunikation handelt. Das Computerzeitalter hat die Möglichkeiten in diesem Bereich erheblich erweitert. Das Prinzip, eine Nachricht in einer Abbildung zu verstecken, läuft darauf hinaus, daß jede Farbe in einer Abbildung in eine lange Bitreihe kodiert wird. Dabei »verwendet« jedoch nicht jede Farbe jedes Bit in der Reihe. In den Bits, die nicht oder weniger wichtig sind, können nun Bits, die ein Bestandteil der Nachricht sind, versteckt werden. Nur diejenige, die weiß, um welche Bits es sich handelt, ist in der Lage, die Nachricht zu lesen. Wenn solch eine Abbildung an einem öffentlich zugänglichen Ort, wie eine Nachrichtengruppe oder ein »Schwarzes Brett« (siehe Kapitel »Computernetze und anonyme elektronische Post«), angeboten wird, kann im Prinzip jeder sich die Abbildung holen. Außenstehende können aber nicht erkennen, ob in der Abbildung eine Nachricht versteckt ist. Grundsätzlich können Nachrichten auch in Sound-Dateien verborgen werden.

Steganographieprogramme wie Stealth und Hide and Seek können über die Mailbox BIONIC 0521-68000, Login Steganographie gesaugt werden.

Kennwortsicherung von Programmen

Es gibt viele Programme, die eigentlich nicht extra zur Verschlüsselung von Texten gedacht sind, diese zusätzliche Möglichkeit aber enthalten. Bekannte Beispiele dafür sind WordPerfect, gewisse Kalkulations- und Datenbankprogramme und das Kompressionsprogramm PKzip. Diese Programme besitzen die Möglichkeit, Dateien mit einem Kennwort zu sichern. Kennwort heißt im englischen »password«, um ein sicheres »password« zu erhalten, ist es allerdings sinnvoll, ein sehr langes zu nehmen, eine »passphrase«, auch »Mantra« genannt.

Das Handbuch von WordPerfect 5.1 behauptet zur Kennwortsicherung folgendes: »WPCorp besitzt keine Möglichkeit, die Sicherung Ihrer Dateien aufzuheben, wenn Sie Ihr eigenes Kennwort vergessen haben«. Das ist aber Blödsinn. Inzwischen haben mehrere Menschen herausgefunden, wie das System funktioniert. Die erste war Helen Bergen aus Australien, die einen Nachmittag herumpuzzelte und die Rückseite eines Briefumschlags benötigte, um die Sicherung zu knacken. Als sie dies WordPerfect Pacific mitteilte, antwortete die Gesellschaft, daß »WordPerfect ein solches Programm nicht besäße und infolgedessen nicht in der Lage sei, die Sicherung zu brechen«. Ferner behaupteten sie, daß »lediglich sehr wenig Leute in der Lage seien, solch ein Programm zu schreiben«.

Inzwischen ist das Knackprogramm WPCRACK auf jedem ernstzunehmenden elektronischen »Schwarzen Brett« zu finden. WPCRACK soll für Menschen erstellt worden sein, die das Kennwort eines Dokuments vergessen haben. Das Problem mit der Kennwortsicherung bei WordPerfect ist, daß die Methode der Sicherung sehr simpel ist.[9] Außerdem sind bestimmte Schriftzeichen an bestimmten Stellen in einem WP-Dokument immer gleich. Es ist natürlich der Traum eines jeden Krypto-Experten, den Original- und den verschlüsselten Text zu besitzen. Indem das WPCRACK-

Programm diese Tatsache nutzt, kann es innerhalb weniger Sekunden das Kennwort »raten«. Andere Programme, die Kennwortsicherung von Dateien bieten, verwenden oftmals eine vergleichbare oder mitunter sogar eine noch einfachere Verschlüsselungsmethode.

Ein ernsthaftes Problem ist, daß Leute zumeist immer dasselbe Kennwort benutzen. Nehmen wir einmal an, daß du dasselbe Kennwort für deine WP-Dokumente und das Computersystem bei der Arbeit oder noch schlimmer PGP verwendest. Sobald mit Hilfe von WPCRACK das Kennwort deines WP-Dokuments geknackt wurde, ist der Rest auch bekannt.

Die meisten Kennwortmethoden taugen nicht viel, weil deren Ersteller keine Verschlüsselungsexperten sind. Einem Verschlüsselungsprogramm ist eigentlich erst zu trauen, wenn es von Menschen entwickelt worden ist, die sich auf dem Gebiet auch wirklich auskennen.

Kennwortsicherung von PCs und Festplatten

Im Handel sind eine Reihe von Programmen erhältlich, die den unerünschten Zugang zum Computer mit Hilfe eines Kennworts schützen. Manchmal ist diese Funktion sogar standardmäßig in den Computer eingebaut. Viele Menschen glauben, daß die Informationen im Computer damit auch verschlüsselt sind, was in der Regel aber nicht der Fall ist. Normalerweise wird in solchen Fällen das Starten des Computers verhindert, eine Blockade, die aber oft mit Hilfe einfacher Handlungen wieder aufgehoben werden kann. Unbefugte Neugierige können natürlich auch einfach die Festplatte aus dem Computer herausnehmen und sich diese mittels eines anderen Computers ansehen.

Für die meisten Kennwortsicherungen sind bereits Programme im Umlauf, mit denen die Sicherung aufgehoben werden kann. Computern mit einem AMI-BIOS-Chip und Programmen wie PC-Lock sind nicht zu trauen. Höchstens kann verhindert werden, daß deine Kinder auf dem Computer herumspielen.

Ein Programm, daß wohl erwähnenswert ist und auch tatsächlich die Daten auf dem Computer verschlüsselt, heißt

SecureDrive. Es benutzt IDEA und bietet sogar die Möglichkeit, (in beschränktem Maße) mit PGP zusammenzuarbeiten. Mit SecureDrive ist es möglich, Teile der Festplatte zu verschlüsseln. Auch können einzelne Disketten gesichert werden. Mit dem auf DES basierenden, jedoch weniger zuverlässigen Norton Diskreet ist dies übrigens auch möglich.

Hast du viele Daten auf einer mit SecureDrive gesicherten Festplatte, dann möchtest du sicherlich auch hin und wieder ein Backup erstellen. Das solltest du dann auf Disketten machen, die auch mit SecureDrive verschlüsselt werden. Wenn SecureDrive einmal eingeschaltet ist, funktioniert es prima mit Backup-Programmen wie MS Backup. Du mußt jedoch wohl dafür sorgen, daß die normale, MS-DOS-kompatible Backup-Methode benutzt wird. Ist dies nicht der Fall, wird SecureDrive »übergangen« und werden die Daten unverschlüsselt auf den Backup-Disketten gespeichert.

Was du nicht tun solltest

Wir haben bisher Chiffriersysteme, die zur Verschlüsselung von Dateien und Festplatten benutzt werden, und deren Sicherheit und Zuverlässigkeit behandelt. Andere Kapitel haben dir bereits ersichtlich gemacht, daß es neben Code-Knackern auch noch Eindringlinge und Bildschirm- oder Kabelabhörer gibt. Diese Methoden sind in der Praxis häufig erfolgreicher und billiger. Kein Kryptosystem ist undurchdringlich. Du wirst dir immer die Frage stellen müssen: Was ist für meinen eifersüchtigen, ehemaligen Partner, neugierigen Nachbarn, das Finanzamt oder den Geheimdienst schwerwiegender? Die besonderen Informationen, über die ich verfüge, oder der finanzielle Aufwand, den sie aufbringen müssen, um die Daten ans Licht zu bringen? Wir werden dir im Nachstehenden ein paar Tips geben, mit denen du auf jeden Fall die Kosten Unbefugter hochtreibst.

- Lasse niemals geheime Schlüssel oder Kennwörter herumliegen. Für Kennwörter gilt: Der Name eines Freundes, der Oma oder deines Hundes liegt zu nahe. Du wählst am besten ein nicht existierendes Wort. Programme, welche die Möglichkeit bieten, Kennsätze einzugeben, sind besser. Das Knacken eines Kennwortes von sechs Zeichen, kostet

einen wirklichen Hacker-Profi gerade Mal eine Minute, und entsprechende staatliche Stellen sind mit ihren Geräten womöglich noch schneller.

• Ein sicheres Kennwort zu haben ist wünschenswert. Unsichere Kennwörter sind dein Geburtsdatum, dein Name und ähnliches. Moderne Dechiffriercomputer sind in der Lage, in sehr kurzer Zeit den Wortbestand eines ganzes Lexikons als Kennwort auszuprobieren. Deshalb solltest du in ein langes Kennwort, Mantra, etwas Überlegung investieren. Einerseits solltest du das Mantra nirgends aufschreiben oder im Computer ablegen, andererseits mußt du es dir natürlich merken können.

Man kann nun Berechnungen darüber anstellen, um wieviel ein Mantra sicherer wird, wenn es verschiedene Änderungen erfährt. Mit diesen Berechnungen wollen wir euch aber nicht quälen, stattdessen ein Beispiel: »Völker hört die Signale« ist nicht sehr sicher, es ist die Anfangszeile eines bekannten Liedes. Wenn du es aber veränderst, wird es sicherer: »Völker hört die Signale, auf zum letzten PC«. Besser ist es wenn noch Schreibfehler reingemacht werden: »Fölker gört dee Signall«. Noch besser sind Leerstellen, Zahlen und Sonderzeichen: »#*1kär h˚rt diä $]gna1ä«. Letztlich sind der Phantasie keine Grenzen gesetzt.

• Bedenke, daß »Einbrecher« oder Viren die Chiffrierprogramme, Schlüssel, Kennwörter und Texte vernichten oder aus ihnen Informationen holen können. So gibt es beispielsweise die Möglichkeit, den Teil eines Chiffrierprogrammes, das nach dem Kennwort fragt (zum Beispiel PGP oder SecureDrive), mit etwas auszutauschen, das genauso aussieht und das Kennwort in einer kleinen Datei auf der Festplatte zu speichern. Ein Eindringling kann diese Datei finden und abrufen, ein »trojanisches Pferd«.

• Wenn du nur über einen Computer eines »Multiuser«-Systems oder einen Rechner, der an ein Local Area Network (LAN) angeschlossen ist, verfügst, berücksichtige, daß der Systemverwalter oder andere schlaue Nutzer sich zu deinen vertraulichen Dateien, Sicherungsprogrammen und Schlüsseln Zugang verschaffen können. Dies ist sogar möglich, während du damit arbeitest.

• Wenn du einen eigenen Computer besitzt, es jedoch nicht wünschenswert findest, daß andere sich zu Computer und Festplatte Zugang verschaffen können, so solltest du vertrauliche Dateien, Sicherungsprogramme und Schlüssel auf Disketten speichern. Auf diese Art und Weise kannst du den Zugang zu den Daten mit dir herumtragen. Diese Disketten (oder die Festplatte, wenn du sie trotzdem benutzen möchtest) kannst du wiederum mit beispielsweise SecureDrive schützen. Das Starten des Computers ohne die jeweilige Diskette ist dann nicht möglich.

• Egal welche Chiffriermethode du benutzt, für den Krypto-Experten ist es immer schwieriger, den Code zu knacken, wenn der Klartext vor dem Verschlüsseln erst komprimiert (also möglichst klein gemacht) worden ist. Bei PGP ist diese Möglichkeit integriert worden, viele im Handel erhältliche Programme machen jedoch dasselbe (PKZIP, LHARC, PKPAK). Wenn du die Code-Knacker wirklich völlig entnerven möchtest, solltest du deine Nachricht oder Datei hintereinander mit unterschiedlichen Verschlüsselungsprogrammen kodieren. Die beste Verschlüsselungsmethode ist in solchen Fällen zum Schluß zu verwenden, damit wird der verschlüsselte Text, der vorher entstanden ist, kodiert.

• Bedenke, daß die »nicht verschlüsselten Versionen« von Dateien, die du mühevoll verschlüsselt hast, nicht von jedem Kryptoprogramm automatisch auf eine nicht wiederherstellbare Art und Weise auf der Festplatte gelöscht werden. Die Befehle der Betriebsysteme zum Löschen von Dateien (delete), erzählen dem Computer lediglich, daß der Festplattenteil, an dem sich die Dateien befanden, wieder für andere Dateien zur Verfügung steht. Es gibt eine ganze Reihe von Programmen, die den Text wieder lesbar machen. Um eine Datei wirklich zu löschen, muß sie überschrieben werden. Bei PGP ist es möglich, diese Funktion einzustellen, die Datei wird mit Zufallszeichen überschrieben, allerdings nur einmal. Angeblich gibt es Hardwarelesegeräte, die in der Lage sind, eine einmal überschriebene Datei wiederherzustellen. Hast du wirklich Gründe paranoid zu sein, besorg dir das Programm »Norton Wipeinfo«, das Dateien viele Male überschreiben kann.

• Das Gleiche gilt natürlich auch für die Dateien, die du mit einem Textverarbeitungsprogramm erstellt hast. Microsoft Word, das Dateien mit der Erweiterung ».txt« abspeichert, sichert gleichzeitig immer die letzte Version zusätzlich als ».sik«-Datei. Selbst wenn du die ».txt«-Datei überschreibst, bleibt natürlich die ».sik«-Datei erhalten.

Bei Word, das unter Windows läuft, werden die bearbeiteten Dateien in einer Auslagerungsdatei gespeichert. Diese Auslagerungsdatei ist schreibgeschützt, kann also nicht einfach so gelöscht werden. Dafür mußt du unter dem Symbol »386-erweitert« den »Virtuellen Speicher« anklicken und beim Typ Auslagerungsdatei »permanent« oder »temporär« wählen. Bei »permanent« enststehen dann die Dateien SPART.PAR und 386SPART.PAR. Diese kannst du dann überschreiben (beim Neustarten bringt Windows dann Fehlermeldungen, weil es diese Dateien nicht findet und fragt, ob es diese wieder neu einrichten soll). Bei »temporär« entsteht eine WIN386.SWP, die zwar von Windows nach Gebrauch gelöscht wird, aber eben nicht überschrieben. Außerdem legt Windows Dateien auf der Festplatte ab, die die Erweiterung ».tmp« haben, in denen immer wieder Fragmente von bearbeiteten Texten zu finden sind. Auch diese ».tmp«-Dateien solltest du regelmäßig überschreiben. Beim Überschreiben und Löschen der Auslagerungsdateien stürzt Windows auch gerne mal ab.

• Benutzt du Kryptosysteme nur für elektronische Briefe, so ist es sinnvoll, die zu verschlüsselnde Nachricht und den erforderlichen Schlüssel nie auf der Festplatte zu speichern. Das ist möglich, indem du eine scheinbare, eine »virtuelle« Platte (RAM-Platte) erzeugst, bei der ein Stück Speicher des Computers so tut, als ob es eine Festplatte wäre. Sobald du den Computer ausschaltest, verschwinden alle Informationen auf diesem Stück Speicherraum. Auf der diesem Buch beiliegenden Diskette findest du weitere Informationen.

• Egal, wie gut die Dateien gesichert sind, wenn du Nachrichten über den Computer zu einem anderen sendest, ist es immer möglich, herauszufinden, woher die Nachricht stammt und wohin sie gegangen ist. Es fällt also auf, daß du

ein Kryptosystem benutzt oder nur manchmal oder lediglich an immer die gleiche Person verschlüsselte Nachrichten sendest!

• Folgende Programme befinden sich auf der mitgelieferten Diskette: PKUNZIP, PGP, SECURE DRIVE, (IDEA-source-code).

Anmerkungen

1 Das bedeutet »modulo 10 addieren«.

2 Wenn bei dieser Methode 45 Schriftzeichen mit Zahlen ausgetauscht werden sollten, begannen die Austauschzahlen bei 5, weil ansonsten im Falle von 4 oder beispielsweise 44 Verwirrung entstehen würde. Ferner mußt du bedenken, daß bei dieser Methode vor der verschlüsselten Nachricht immer die Nummer der verwendeten Seite stand. Dies wurde dann mit einer festen Anzahl Ziffern aufgeschrieben.

3 Das ist dasselbe wie eine »modulo 2 Addition«.

4 Nehmen wir einmal an, daß du den richtigen Schlüssel-Erzeuger, der die zufälligen Schlüssel anfertigt, besitzt. Die Angriffstechniken von Code-Knackern werden sich zumeist auf den verschlüsselten Text konzentrieren. Manchmal verfügen sie durch allerlei Tricks vielleicht auch über (einen Teil des) den Klartext oder sie haben ihn erraten können. In solch einem Fall werden sie (einen Teil des) den Schlüssel herausfinden. Bei der nächsten verschlüsselten Nachricht nützt ihnen das dann aber gar nichts. Zumindest, wenn der Schlüssel nur einmal benutzt wurde.

5 Der Rest der Bits sind nämlich Paritätsbits.

6 P. Zimmermann, der Erfinder von PGP, am 12.10.93 vor dem Subcommittee for Economic Policy, Trade and Environment (Wirtschafts-, Handels- und Umweltunterausschuß) des US-amerikanischen Abgeordnetenhauses.

7 Dies ist telefonisch möglich, wenn ihr eure Stimmen erkennt. Du brauchst nicht den ganzen Schlüssel vorzulesen und zu vergleichen, sondern es genügt, die 16 Zeichen, die nach einem bestimmten PGP-Befehl auf dem Computerbildschirm erscheinen, durchzugeben.

8 Zur Sicherheit des RSA-Algorithmus: 1977 druckte die Zeitschrift Scientific American eine 129 Stellen lange Zahl ab, die das Produkt aus zwei unbekannten Primzahlen darstellte. 16 Jahre lang gelang es niemandem die zugrundeliegenden Primzahlen zu ermitteln, bis

im August 1993 es einen koordinierten Angriff auf die Zahl gab. 600 Freiwillige aus über 20 Ländern, die über das Internet verbunden waren, gelang es in acht Monaten die Primzahlen zu ermitteln. Dies konnte nur gelingen, weil die notwendige Rechenleistung auf über 600 Rechner verteilt werden konnte. Der geschätzte Rechenaufwand betrug 5000 MIPS-Jahre. Eine 129 Stellen lange Zahl entspricht einer 429-bit-Zahl. Es wurde damit gezeigt, daß eine 429-bit Zahl als nicht 100% sicher anzusehen ist.
Es muß davon ausgegangen werden, daß große finanzkräftige Geheimdienste eine solche 129-bit-Zahl in einem Zeitraum von rund vier Wochen knacken können. Nun ist es aber so, daß wenn die RSA-Zahl auf 1024 bit vergößert wird, sich der Rechenaufwand, um diese Zahl zu knacken, um etwa das 20000fache erhöht. Das wären dann 80000 Wochen oder 1538 Jahre. Wird die Bitbreite nochmals verdoppelt, kommt man zu der utopischen Rechenzeit von 450 Millionen Jahren. Die diesem Buch beiliegende Diskette enthält PGP 2.6.2 i mit 1024-bit-Schlüssel. Das in Entwicklung befindliche PGP 2.6.3 benutzt 2048-bit-Schlüssel. Fachleute gehen davon aus, daß bei der derzeitigen Entwicklung von Rechnerleistungen es jedes Jahr zu einer Verdopplung der Rechnerleistungen kommt. Selbst wenn wir dieses miteinbeziehen, können wir sagen, daß 1024-bit-Zahlen in den nächsten 10 bis 20 Jahren noch einigermaßen sicher sind.

9 Zweimal ein XOR, einmal mit einen Zähler der Position im Text und einmal mit dem Kennwort.

Literatur

FoeBuD e.V. Bielefeld, Christoph Creutzig, Abel Deuring (Hg.): PGP. Pretty Good Privacy, ISBN 3-9802182-5-2, 29,80 DM

Dr. Dob's Journal 12/93, »The IDEA Encryption Algorithm«

Internet: newsgroup sci.crypt: Frequently Asked Questions (FAQ) E. Bach, S. Bellovin, D. Bernstein, N. Bolyard, C. Ellison u.a.

Internet: anonymous FTP: Manual Pretty Good Privacy/Public Key Encryption for the Masses, Phil Zimmermann, 1993

James Bamford, The Puzzle Palace, Penguin Books 1982

Computernetze und elektronische Post

Außer den Computernetzen innerhalb eines Gebäudes oder Büros,[1] bei denen die Computer auf irgendeine Art und Weise miteinander verbunden sind, gibt es auch Computernetze, die lokal, national oder sogar weltweit miteinander verkoppelt sind.

Das sind die sogenannten Mailboxen. In der Regel besteht eine Mailbox aus einem stinknormalen PC, der mit etwas Software und einem Modem ausgerüstet ist. Du triffst nun mit dem Mailboxbetreiber eine Vereinbarung, daß du eine Mailbox benutzen darfst. Dafür kriegst du eine elektronische Adresse, eine »E-Mail«-Adresse. Außerdem sind in der Vereinbarung einige technische Dinge geregelt, wie die Software, die benutzt wird, ein Paßwort und natürlich eine Gebühr. Monatlich liegt sie zwischen 10 DM und 50 DM, je nach Service. Der Mailboxbetreiber gehört meistens zu einem Verbund weiterer Anbieter.

Angeschlossenen Benutzern (Usern) ist es möglich, elektronische Briefe, E-Mail, an andere E-Mail-Adressen zu verschicken. Reist die E-Mail über große Entfernungen, geschieht das über diverse Zwischenstationen.[2] Darüber hinaus ist es in einem solchen Netz möglich, E-Mail an ein elektronisches »Schwarzes-Brett« zu senden, das als eine Art Postfach zu verstehen ist, zu dem alle Benutzer den Schlüssel besitzen. Der Benutzer selbst bestimmt, welche Schwarze-Brett-Systeme er lesen möchte. Es kann davon sehr viele geben, die auch »newsgroups« (Nachrichtengruppen) heißen, auf denen zu bestimmten Themen Diskussionen geführt und Informationen ausgetauscht werden. Zum Beispiel werden in dem Brett /Z-NETZ/ALT/PGP/ALLGEMEIN die Vor- und Nachteile sowie Neuerungen von

PGP besprochen. Jede/r kann sich dort einmischen. Die möglichen Themen der angebotenen Nachrichtengruppen hängen von der Art des Netzes ab und davon, ob es für eine bestimmte Zielgruppe entworfen wurde. Die Association for Progressive Communications (APC) ist ein Beispiel für ein weltweites Netz, das vor allem von nichtstaatlichen Organisationen frequentiert wird. In der BRD gibt es das CL-Netz (CL steht für Computernetzwerk Linksysteme) mit Mailboxen in Leipzig, München, Nürnberg, Berlin, Esslingen, Regensburg, Straubing, Weiden, Mannheim, Göttingen und einigen anderen Orten.[3]

Die an ein solches Netz angeschlossenen Computer sind entweder permanent oder in selbst gewählten Abständen miteinander verbunden. Die Verbindung innerhalb des Netzes wird über Kabel, Funk, Satellit oder das Telefonnetz hergestellt. Ein einzelner Nutzer wird mit seinem PC zu Hause normalerweise nur ab und an mit dem nächsten Zugangscomputer (»host«) des Netzes in Verbindung treten. Dafür benötigt er Kommunikationssoftware, ein Modem und einen Telefonanschluß.

Möchte jemand die Dienste eines Netzes in Anspruch nehmen, so muß ein »account« erbracht werden, wie es in der Datennetzwelt heißt. Die Person wird vom Betreiber registriert und erhält eine eigene E-Mail-Adresse zugewiesen. Diese ist mit einer normalen Postadresse vergleichbar, sieht jedoch etwas anders aus. Wenn Ingrid Maler aus Leipzig an das CL-Netz angeschlossen ist, so sieht das beispielsweise so aus: »I.MALER@LINK-L.cl.sub.de«.[4] »LINK-L« ist die Link-Mailbox in Leipzig, »cl« steht für das CL-Netz, »sub« bezeichnet eine Untergruppe des CL-Netzes und »de« steht für Deutschland.

Wenn Ingrid nun David einen elektronischen Brief schickt, wird ihr Brief automatisch mit ihrer E-Mail-Adresse versehen. Auch die Adressen eventueller Zwischenstationen werden dem Brief hinzugefügt. Alle diese Informationen stehen in einem sogenannten »header« (Kopfzeile). Der »header« ist mit einem Briefumschlag vergleichbar, auf dem Adressat, Absender und Stempel der Postämter stehen, durch die der Brief gegangen ist. Die Zwischenstationen

sind hierbei meistens größere Rechner, die oft an Universitäten stehen. Möchten staatliche Stellen größere Mengen E-Mail überwachen, werden sie sich entweder in die Mailboxen oder in die Zwischenstationen hineinhängen.

Sogar wenn Ingrid den Brief mit einem Kryptoprogramm verschlüsselt hat, ist der »header« weiterhin lesbar. Nicht nur für David, sondern für jeden, der diesen Brief womöglich abfängt. Dritte können auf diese Art und Weise immer ermittteln, wer mit wem kommuniziert. Das Abfangen von Briefen ist auf Computer-Datennetzen in der Regel ein Kinderspiel.[5]

In einigen Mailboxen wie im FIDO-Netz ist übrigens das Verschlüsseln verboten. Einige Systembetreuer (Sysops) nehmen sich die Unverschämtheit heraus, die E-Mail mitzulesen, zu zensieren oder zu kommentieren[6].

Ein »header«-Beispiel: Ingrid (I.MALER@LINK-L.cl.sub.de) schrieb am 8.8.1995 eine E-Mail an David (DAVID@TBX.berlinet.de) wegen »Problemen mit der E-Mail«. Der »header« könnte folgendermaßem aussehen:

Empfänger: DAVID@DOOFI.tbx.berlinet.de
MessageID: 5rUXyDNoTTB@imaler.link-l.cl.sub.de
Absender: I.MALER@LINK-L.cl.sub.de (Ingrid Maler)
ZNETZ-Absender: I.Maler%LINK-L.CL.SUB.DE@UUCP.ZER
ZNETZ-Text: Realname: Ingrid Maler
Betreff: Probleme mit der E-Mail
Erstellungsdatum: 19950808184900W+0:00
Bezug: 5rG5V9kLUsB@doofi.tbx.BerliNet.de
U-To: DAVID@TBX.BerliNet.de
Pfad: tbx.berlinet.de!zelator.BerliNet.DE!root
Mailer: CrossPoint v3.02 R/A991
GATE: RFC1036/822 U2 zelator.BerliNet.DE [UNIX/Connect v0.71]
Länge: 1452

Aus dem »header« ginge in diesem Fall unter anderem hervor, daß die Post über die Routing-Station Zelator gegangen ist.

Das Internet

Ein besonderes internationales Datennetz ist das Internet, auch als »das Datennetz der Datennetze« bekannt. Ursprünglich ist es vom Verteidigungsministerium der Vereinigten Staaten gegründet worden und wurde vor allem in akademischen Kreisen benutzt. In letzter Zeit wurde es in wachsendem Maße auch für Privatleute zugänglich. In der BRD bieten immer mehr Mailboxbetreiber gegen einen gewissen Aufpreis einen Internet-Zugang an.[6] Millionen Menschen haben weltweit schon Zugang und ihre Anzahl erhöht sich monatlich spektakulär. Das Internet scheint zu einer der größten digitalen Datenautobahnen (Text, Bild, Audio) der Welt heranzuwachsen. Es darf aber nicht unerwähnt bleiben, daß die Benutzerfreundlichkeit noch unnötig schlecht ist. Wie das Internet in Zukunft aussehen wird, hängt größtenteils davon ab, was die Nutzer selbst daraus machen. Beim Internet kann kaum noch von einer zentralen Kontrolle die Rede sein. Das Gewirr aneinander geknüpfter Computer ähnelt eher einer Ansammlung Spinnennetze, große und kleine Spinnen, die nicht immer dasselbe möchten.

Die angeschlossenen Computer kommunizieren laut eines vereinbarten Standards miteinander.[7] Unter anderem bietet das Internet auch den Service, E-Mail zu verschicken und die Möglichkeit viele Nachrichtengruppen abzufragen. Über spezielle »Schleusen«[8] können Nutzer anderer Computernetze mit Internetnutzern E-Mail austauschen. »Packet-Funk«-Netze dürften ebenfalls in absehbarer Zukunft mit dem Internet verbunden werden.

Auch auf dem Internet hat jeder eine eigene E-Mail-Adresse, die größtenteils die Identität des Nutzers bestimmt. Auch E-Mail wird zumeist, gemäß der bereits beschriebenen Methode, mit einem »header« ausgestattet. Auch auf dem Internet kann die Post einfach von Unbefugten abgefangen und, wenn die Nachricht nicht verschlüsselt ist, auch gleich gelesen werden.

Es ist natürlich von größter Wichtigkeit, daß auf Computernetzen die tatsächliche Identität eines Absenders überprüft werden kann. Diese Tatsache bildet eine der wichtigsten Sicherheiten, um den Wahrheitsgehalt der Information selbst einzuschätzen. Andererseits steht diese Identifizierungsmöglichkeit im Widerspruch zu dem Anspruch auf Privatsphäre oder sogar der Sicherheit des Briefschreibers.

Was geschieht beispielsweise, wenn eine Rechercheurin Informationen über die Korruption von Politik und Wirtschaft eines Staates in eine Nachrichtengruppe setzen möchte, aber Repressionsmaßnahmen fürchten muß? Oder wie sieht es aus, wenn eine von Repression bedrohte Opposition Informationen an Journalisten im Ausland weiterleiten möchte? Sogar wenn der Inhalt so verschlüsselt wurde, daß der Gegner ihn nicht verstehen kann, erzählt der »header« später noch genug darüber, wer mit wem kommuniziert hat und woher die unliebsamen Informationen wahrscheinlich stammen. Für manche kann es also durchaus sinnvoll sein, ohne eine Absenderangabe, Post verschicken zu können.

Die erste Infrastruktur für »anonyme Post« ist auf dem Internet bereits vorhanden. Nutzerkreise anderer Datennetze, die über eine »Schleuse« Nachrichten mit dem Internet austauschen, haben diese Möglichkeit. Bis zum heutigen Zeitpunkt ist es jedoch leider so, daß man diverse Techniken erst sehr gut studiert und sich angeeignet haben muß, bevor man auf der Grundlage der gegenwärtigen Infrastruktur wirklich sicher kommunizieren kann.

Ein Teil der NutzerInnen, die Cypherpunks[9], fördert die Idee von anonymer Post. Aus diesem Grunde haben sie sogenannte »anonyme remailer« gegründet und helfen anderen, die so etwas auch für das Internet aufbauen wollen.

Anonyme Post

Ein »anonymer remailer« ist häufig[10] nichts weiter als ein Computerprogramm, daß auf dem Rechner von jemandem mit einem Standard-»account« läuft. Dorthin kannst du Post schicken und die wirkliche Bestimmung des Briefes auf eine besondere Art und Weise mitsenden. Das Computerprogramm kann durch eine Reihe von Kennzeichen im »header« die normale Post von der anonym weiterzusendenden unterscheiden. Bei der anonymen Variante wird der

»header« so verändert, daß die Adressen des Absenders und der passierten Zwischenstationen gelöscht werden, bevor die E-Mail den eigentlichen Bestimmungsort erreicht.

Die Probleme liegen bei der Nutzung von »anonymen remailern« auf der Hand. So darf man sich fragen, wie zuverlässig die Menschen sind, die eine solche Station betreiben. Wenn sie wollen, könnten sie den ganzen Brief samt dem ursprünglichen »header« abspeichern. Dies kann bereits erfolgt sein, bevor der Brief einen »remailer« erreicht. Und auch wenn der Systemverwalter, der den Zugang zum Internet organisiert, nicht unbedingt etwas über die Existenz des »remailers« zu wissen braucht, kann er ihn dennoch entdecken, und, so er will, über Nacht einfach ausschalten.

Ähnliche Probleme gelten auch in bezug auf die Versendung anonymer Post durch den »anonymous server«. Im »header« wird die E-Mail-Adresse der Post des Absenders, die über einen solchen Server läuft, gelöscht und vor dem Weitersenden mit verschlüsselten Personalangaben versehen. Dieser Vorgang ist jedoch immer an die richtige E-Mail-Adresse des Absenders gekoppelt und alles kann in einer Datei gespeichert werden.

Um die erwähnten Schwachstellen zu umgehen, raten Cypherpunks dazu, eine Kette von anonymen »remailern« und »servern« zu verwenden und die Nachrichten mit dem Programm PGP zu verschlüsseln.[11] Die Kette funktioniert nur, wenn alle Kettenglieder dabei über einen privaten Geheim- und einen öffentlichen Schlüssel verfügen. Nehmen wir einmal an, daß Ingrid drei »anonymous remailer« benutzen will.[12] Einfachheitshalber nennen wir deren E-Mail-Adressen A, B und C. Ingrid besitzt von den drei Stationen den öffentlichen Schlüssel, die wir im weiteren AS, BS und CS nennen werden. Ingrid will, daß ihre Post über A nach B und dann von B nach C die letzendliche Bestimmung, und zwar David, erreicht. Den Inhalt des eigentlichen Briefes verschlüsselt sie mit dem öffentlichen Schlüssel von David. Die E-Mail-Adressen werden in einer Kette verschlüsselt. Das Prinzip ist vergleichbar den russischen Holzpuppen, in denen sich jeweils eine kleinere Puppe befindet. Ingrid verschlüsselt erst zusammen mit dem verschlüsselten Brief die E-Mail-Adresse von David mit Hilfe von CS. Das Ergebnis verschlüsselt sie nun zusammen mit C mit Hilfe von BS. Daraufhin verschlüsselt sie mittels AS dieses neue Resultat mit B. Das Ergebnis dieser letzten Verschlüsselung sendet sie danach an A. (Achtung: Bei den diversen Schritten müssen in Wirklichkeit auch einige Anweisungen für den »remailer« eingefügt werden).[13]

Bei A angelangt, wird die letzte Verschlüsselung entschlüsselt, und kann von B gelesen werden. Der Brief wird nun dorthin gesendet. Die E-Mail-Adresse von Ingrid und die Zwischenstationen sind nun bereist gelöscht worden. Bei B wiederholt sich dieses Verfahren, die vorletzte Verschlüsselung wird entschlüsselt, infolgedessen wird C bekannt usw.

Diese Methode, bei der verschiedene Varianten möglich sind, macht das Verknüpfen von Sender und Empfänger zu einer äußerst komplexen Angelegenheit. Wenn das Kryptosystem sicher ist, so muß die Nachricht an mehreren, vorher unbekannten Stellen von derselben Gruppe abgefangen werden, um das Puzzle zusammenfügen zu können. Ein unzuverlässiger »anonymer remailer« in der Kette kann nur wenig Unheil anrichten. Programme befinden sich in Entwicklung.

Eine völlig andere Variante für das Versenden anonymer Post wäre zu versuchen, irgendwo einen anonymen Internet-»account«, und damit eine E-Mail-Adresse, zu erhalten (und natürlich auch anonym den Mitgliedsbeitrag zu entrichten). Es gibt weltweit keine einheitlichen Regeln für den Zugang zum Internet. Werden ständig wechselnde Telefonzellen (mit Laptop und akustischem Modem) oder öffentlich zugängliche Computer verwendet, so kann die wirkliche Identität ebenfalls lange verborgen bleiben.

Anmerkungen

1 Sogenannte LANs (Local Area Networks)

2 Sogenannte »nodes«

3 Informationen über APC in den Niederlanden über: Antenna; Tel. 0031-80-235372 oder E-Mail an support@antenna.nl

4 Das »@«-Zeichen steht für »at« (dt.: zu, bei). Die Namen, die nach

diesem Zeichen stehen, weisen oft auf die Institutionen, die die jeweiligen Rechner betreiben.

5 Goldmann, Herwig, Hoofacker: Computer im Telenetz, Reinbek 1993 (Gutes Einnführungsbuch in die Datenfernübertragung mit Programmen auf Diskette)

6 Systemverwalter von »host« – oder Zwischenstationen, gewiefte andere Benutzer, Leitungsanzapfer u.ä. Siehe auch Kapitel über Abhören von Telefonverkehr.

7 TCP/IP-Protokoll

8 Sogenannte »gateways«

9 Cypherpunks (»Chiffrierpunks«): Ihr gemeinsamer Nenner ist, daß Kryptographie zum Schutz der Privatsphäre angewandt werden sollten. Sie engagieren sich dabei aktiv, um die Voraussetzungen dafür zu schaffen: Erstellung von Kryptoprogrammen, Gründung von »anonymous remailern« ...

10 Es kann jedoch auch ein Standardrechner sein, der nichts weiter macht, als »remailen«. Ein Beispiel hierfür ist der anonyme »remailer« Penet in Finnland. Einfach eine E-Mail an help@anon.penet.fi schicken und schon kriegst du die nötigen Informationen.

11 Weitere Informationen zu PGP im Kapitel über Kryptographie.

12 Die genaue Funktionsweise anonymer »remailer« und »server« kann mitunter unterschiedlich sein. Zum Erhalt einer Liste aktiver »remailer« kann E-Mail gesendet werden an: mg5n+remailer-list@andrew.cmu.edu

13 Weitere Informationen über »remailen« u.a. über: help@vox.xs4all.nl

Sprachverschleierung

Wer Telefon- oder Funkkommunikation verschleiern möchte, kann eine Vielzahl von Wegen beschreiten. Die ältesten Gerätetypen zur Sprachverschleierung sind die »scrambler«. Sie verschlüsseln das Gesprochene, indem sie die Reihenfolge des Gesprochenen durcheinander bringen (»time domain scrambling«), oder indem sie die Frequenzen, aus denen die menschliche Sprache zusammengesetzt ist, veränderm (»frequency domain scrambling«). Nach dem »scramblen« ist die verschlüsselte Nachricht nicht mehr zu verstehen, es ist allerdings möglich, durch die sonderbar verformten Geräusche eine menschliche Stimme zu erkennen.

Außerdem ist es möglich, die Sprache erst zu digitalisieren (in Nullen und Einsen umzusetzen) und die sich so ergebenden Bit-Reihen zu verschlüsseln. Die verschlüsselte Nachricht muß dann wieder in ein Tonsignal umgesetzt werden, das sich dafür eignet, über ein Telefon oder einen Sender gesendet zu werden. Dieses Verfahren mag umständlich und kompliziert klingen, bietet aber einige Vorteile. Die Bits können nämlich im Gegensatz zur Sprache selbst mit komplexeren Verschlüsselungsrezepten bearbeitet werden.

»Scrambling«-Methoden sind nur sinnvoll, wenn sie »real time« funktionieren, also die Versendung der verschlüsselten Nachrichten so schnell erfolgt, daß weiterhin die direkte Kommunikation möglich ist.

Reihenfolge zerstückeln (»time domain scrambling«)

Diese »scrambling«-Form zerteilt den gesprochenen Text etwa im halbsekündlichen Rhythmus in »Blöcke«. Das Gerät speichert diese »Blöcke«, zerteilt sie in weitere kleine-

re Stücke und vermischt sie nach einem bestimmten Muster und die zerwürfelten »Blöcke« werden gesendet. Dies ist mit der Verschlüsselung nach der Permutationsmethode vergleichbar: Nicht die Zeichen/Signale selbst werden verändert, sondern lediglich deren Reihenfolge. Bei der Entschlüsselung findet das umgekehrte Verfahren Anwendung.

Weil immer ein Stück »Sprache« zwischengespeichert werden muß, gibt es an der Sende- wie der Empfangsseite immer eine Verzögerung von etwa einer halben Sekunde, wodurch die Verzögerung der Kommunikation etwa eine Sekunde beträgt. Das ist nicht viel, bedeutet jedoch, daß diejenigen, die miteinander kommunizieren, eine gewisse Geduld aufbringen müssen. Durcheinander oder gleichzeitig zu reden, ist wenig ratsam.

Wird eine halbe Sekunde 15 mal unterteilt, ist die Anzahl der Mischmöglichkeiten mathematisch ziemlich groß, viel zu groß jedenfalls, um einfach so drauflos probieren zu können, die ursprüngliche Nachricht wieder zusammenzusetzen. Es ist aber wie gesagt möglich, in der Tonfolge der Piepser und Sprachfetzen zu hören, ob z.B. ein Mann oder eine Frau spricht. Hartnäckige Lauscher können mit der Zeit sicherlich die individuellen Gesprächspartner erkennen.

Frequenz zerstückeln (»frequency domain scrambling«)

Sprache besteht aus Schallwellen unterschiedlicher Frequenzen. Bei der Frequenzumsetzung wird die Frequenz, aus der sich die Sprache zusammensetzt, bearbeitet. Jede Frequenz wird in eine andere geändert. In den etwas älteren Systemen erfolgte dies immer nach einem festen »Schlüssel« (Umsetzungsfrequenz), dies erwies sich jedoch als leicht zu knacken.

Für modernere Systeme gilt, daß für jede zu unterscheidende Frequenz der Sprache bei der Umsetzung ein anderer Schlüssel benutzt wird. Niedrigere Frequenzen werden in höhere und höhere in niedrigere gewandelt. Augenblicklich werden vor allem Systeme benutzt, die ständig wechselnde Schlüssel benutzen. Je größer die Anzahl der in der Apparatur vorhandenen Schlüssel, desto schwieriger ist das System

zu knacken. Ein großer Vorteil ist auch, daß während der Kommunikation keine Verzögerung eintritt. Das Prinzip ist für Telefon- wie Funkkommunikationsverbindungen gebräuchlich.

Es gibt auch Geräte, die beide Methoden kombinieren. Solche Verschlüsselungen sind entsprechend schwerer zu knacken. Diese Apparate besitzen jedoch auch den Nachteil der ersteren Methode: Es entsteht eine Verzögerung von etwa einer Sekunde. Bis vor kurzem war es Privatleuten lediglich möglich, eine begrenzte Anzahl einfacher Scrambler zu kaufen. Diese garantieren allerdings noch lange keine wirkliche Sicherheit. Seit jüngster Zeit sind aber auch modernere Scrambler sowie die ersten digitalen Sprachverschlüsselungssysteme im Handel erhältlich.

Digitale Sprachverschlüsselung

Bei den modernsten Sprachverschlüsselungstechniken wird nach der Chiffrierung keine verformte Sprache mehr gesendet, sondern ein Signal, das Bits enthält. Nullen und Einsen werden mit unterscheidbaren Piepsern oder Tönen wiedergegeben. Bis vor einigen Jahren führte dieser ganze Prozeß – digitalisieren, verschlüsseln und umsetzen der Bits in ein geeignetes Signal (Modem) – noch zu Problemen. Einerseits erhielt man infolge der Digitalisierung eine (zu) große Anzahl Bits, und andererseits gelang es nicht, diese Bits in Echtzeit (»real time«) zu senden.[1] Mittlerweile gibt es Methoden der Tondigitalisierung, die weniger Bits erzeugen. Auch wurden die Techniken der Modemübertragung optimiert.[2] Die Übertragungsgeschwindigkeit hat sich enorm gesteigert. Entwicklungen, die auch den Weg zur digitalen Sprachverschleierung eröffnen.

Zur Verschlüsselung können wir im Prinzip dieselben Rezepte benutzen, die wir zuvor beschrieben haben: DES, IDEA, einen pseudozufälligen Schlüssels oder eine XOR-Operation.[3] Geräte, die pseudozufällige Schlüssel oder DES verwenden, sind am gebräuchlichsten. Nach einer digitalen Sprachverschleierung ist nur noch ein Rauschen zu vernehmen und kein Gespräch mehr zu erkennen. Die US-amerikanische Firma Motorola ist eine der ersten, die ein System

auf den Markt brachte, das sich zur (mobilen) Funkkommunikation eignet (»Digital Voice Protection«, bzw. DVP[4]). Andere Firmen wie Marconi, Ascom oder Philips liefern mittlerweile ebenfalls digitale Sprachverschlüsselungssysteme mit unterschiedlichem technischen Niveau. Zudem sind für die Funk-Kommunikation (per Telefon, Fax oder Modem) nun auch digitale Verschlüsselungssysteme erhältlich.

Selbstverständlich stellt sich bei jedem neuen Verschlüsselungssystem immer die Frage, ob nicht irgendwo eine Hintertür eingebaut wurde, die es dem Hersteller (oder staatlichen Behörden) ermöglicht, mitzuhören. Wer ein Fertigprodukt kauft, weiß nie so genau, was es alles enthält. Entscheidet man sich dennoch zur Anschaffung eines solchen Systems, so ist die britische Ascom wahrscheinlich noch die beste Wahl.

Den Preis haben wir noch nicht erwähnt, halte dich fest! Zwei Verschlüsselungseinheiten (an jeder Seite eine) kosten schnell 12 000 DM. Geräte zur Anfertigung von Schlüsseln hast du damit immer noch nicht. Ein einfaches PC-Programm mit Kabel zum Kryptotelefon kostet etwa 5000 DM.

Exkurs: Sprachverschlüsselung Marke Eigenbau

Die besseren Sprachverschlüsselungsapparate sind teuer und darüber hinaus schwer im Handel erhältlich. Man braucht jedoch kein Wunderkind zu sein, um mit den Geräten, die sich meistens bereits im Haus befinden, ein Verschlüsselungssystem für ein normales Telefon zusammenzubauen. Erforderlich sind: ein PC (zum Verschlüsseln), eine Sound-Karte (zum Aufnehmen und zur Wiedergabe des Klangs), ein Modem (zur Kommunikation mit der anderen Seite) und natürlich genügend Fachwissen und Geduld, um das ganze miteinander zu verbinden. Ein praktisches, mobiles Ganzes erhält man damit jedoch leider (noch) nicht. Die ersten Tips zu diesem Gebiet möchten wir dennoch weitergeben.

Beim ersten Schritt geht es darum, die Sprache in möglichst wenige Bits umzuwandeln. In den letzten Jahren sind im Bereich der digitalisierten Klang- und Bildgestaltung (Multimedia) große Fortschritte erzielt worden. Es sind allerlei Sound-Karten (Audiokarten) auf den Markt gebracht worden, die Bits in Klang umsetzen. Diese Karten können in den PC eingebaut werden, die erforderliche Software wird meistens zur Karte mitgeliefert. Ein bekanntes Beispiel einer solchen Sound-Karte ist der Sound Blaster. Die modernen Karten wenden ziemlich effektive Kompressionstechniken an. Solche Karten sind ab ein paar Hundert Mark erhältlich. Beim Kauf ist auf jeden Fall darauf zu achten, daß die Kompression mit Hilfe der Hardware erfolgt. Im Handel sind Karten erhältlich, bei denen in den Betriebsangaben steht, daß Komprimierung möglich ist, diese geht dann zuweilen mit Hilfe der Software vonstatten, wodurch das Verfahren zu langsam wird.

Es gibt verschiedene Techniken, mit denen Sprache in Bits umgewandelt werden kann, und zwar die Pulse-Code-Modulation (PCM), Delta-Modulation (DM) oder Delta-Sigma-Modulation, die Technik des Subband Coders/Vocoders (z. B. Mpeg Audio Coder) und die Lineais-Predictive-Kodierung (z. B. LPC-Celp). Die beiden letztgenannten Techniken erzeugen zwar im Endeffekt die geringste Anzahl Bits pro gesprochener Sekunde, LPC müßte sogar 740 bit/sek schaffen, die Techniken werden jedoch leider noch nicht standardmäßig in den gängigen Audiokarten installiert und sind also dementsprechend teuer. Leser mit elektrotechnischen Fähigkeiten können in Fachzeitschriften Schaltpläne finden und sich möglicherweise im Eigenbau etwas zusammenlöten.

Der (billigere) Chip, der häufig standardmäßig in Audiokarten eingebaut ist und für die Kromprimierung sorgt, heißt DSP. Die Kompressionsmethoden, die diesen Chip unterstützen, heißen AD-PCM, mu-Law und A-Law. Karten, die die Komprimierung mit dem DSP-Chip unterstützen, sind beispielsweise der Sound Blaster 16 MultiCD (ca. 500 DM) und das Microsoft Sound System 2.0 (ca 460 DM).

Sind die Sprachsignale in möglichst wenig Bits umgesetzt worden, dann müssen jene Bits wiederum verschlüsselt werden. Bei digitaler Sprachverschlüsselung können im Prinzip dieselben Verschlüsselungsrezepte angewandt werden, die wir bereits beschrieben haben. Nun ist jedoch die Geschwindigkeit des Algorithmus' von größerer Wichtigkeit, die selbstverständlich teilweise auch wieder von der Leistung des verwendeten Computers abhängt.

Zu Experimentzwecken eignet sich die IDEA-Blockverschlüsselung am ehesten. Diese ist durchschnittlich doppelt so schnell wie DES und scheint sicher(er) zu sein. Die Software-Ausführung ist in ursprünglicher Kodierungsform frei erhältlich, müßte jedoch grundlegend angepaßt werden, da der 128-Bit-Schlüssel, den IDEA benutzt, auf der Grundlage (eines Teils) der Nachricht angefertigt wird. Das ist zur »real time«-Sprachverschlüsselung natürlich kein guter Ausgangspunkt.

Weil die Verschlüsselung auch viel Speicherplatz erfordert, ist es

empfehlenswert, mindestens einen 386iger DX mit 4Mb Arbeitsspeicher zu verwenden.

Zum Senden der verschlüsselten Sprache ist ein Modem erforderlich. Die modernsten, nun allerdings noch sehr kostspieligen Modems, erreichen bereits Übertragungsgeschwindigkeiten von etwa 24000 bps (wirkliche Geschwindigkeit). Ein Modem mit einer Geschwindigkeit von 14000 bps und einem integrierten Fehlerkorrekturmechanismus ist jedoch bereits für 300 DM erhältlich. Solch ein Modem eignet sich im Prinzip für »real time«-Übertragungen, vorausgesetzt, daß die Digitalisierung nicht zuviele Bits ergeben hat. Die Verschlüsselung dieser Bits beansprucht nun die meiste Zeit.

Wenn du dir selbst ein System basteln willst, erhältst du mit den gegenwärtigen technischen Mitteln wahrscheinlich ein etwas unpraktisches System, das lediglich von einem festen Ort aus benutzt werden kann. Ein an das Autotelefon angeschlossenes Modem kann nicht mit allzu hohen Geschwindigkeiten arbeiten, und die zur Verfügung stehenden Audiokarten für Laptop-Computer sind, weil es sich meistens um externe Geräte handelt, nicht schnell genug.[5]

Anmerkungen

1 Mit den damals bekannten Methoden zur Umsetzung der Bitreihen in ein analoges Signal wäre, um die gewünschte Geschwindigkeit erzielen zu können, eine größere Bandbreite, als das Telefon zuläßt, erforderlich. Die Sprachfrequenzen liegen im Bereich zwischen 300 Hz und 3,4 kHz. Mit der Bandbreite der Stimme ist die Breite des Frequenzbereichs gemeint, also etwa 3 kHz. Auf dieser Bandbreite basieren die technischen Eigenschaften von Telefonapparaten. Für Funkkommunikationsgeräte ist dies noch komplizierter.

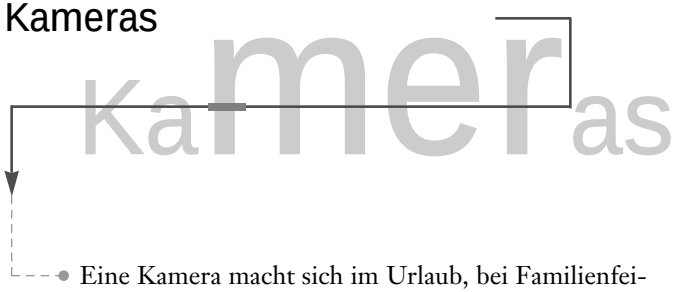
2 Wir unterscheiden 5 Methoden zur Umwandlung von digitalen Daten in ein analoges System und umgekehrt. Diese sind in der Reihenfolge des zunehmenden Komprimierungsgrads: Puls-Amplitude-Modulation, Audio-Frequency-Shift-Keying, Biphase-Modulation, Quadrature-Phase-Shift-Keying, Quadratur-Amplitude-Modulation

3 Um einen pseudozufälligen Schlüssel anzufertigen, werden in Sprachverschleierungsgeräten meistens sogenannte Schubregister verwandt. Es gibt lineare und nicht lineare Schubregister, die pseudozufällige Reihen erzeugen. Lineare Schubregister sind einfach vorherzusagen und also entsprechend leicht zu knacken. Sie sind jedoch billig und schnell und werden deshalb häufig verwendet. Zur sicheren Kommunikation eignen sich eher nicht lineare Schubregister. Aber auch diese erzeugen immer pseudozufällige Reihen und sind also auch zu knacken. Die Frage ist nur innerhalb welcher Zeit und mit welchen Mitteln.

4 DVP benutzt zur Erzeugung des Schlüssels nicht lineare Schubregister, es können laut Werbeprospekt 2.36 x 1021 Schlüssel angefertigt werden.

5 Mittlerweile gibt es auch Online-Sprachverschlüsselungssoftware, von der wir aber nicht wissen, wie sicher sie ist. PGPFone für MAC-PCs, eine unter Windows 95 lauffähige Version soll in Vorbereitung sein. Außerdem gibt es noch das unter MS-DOS laufende Nautilus, das optional die Verschlüsselungsmethoden 3DES, Blowfish oder IDEA benutzt. Näheres über:
ftp.informatik.uni-hamburg.de /pub/virus/crypt/voice;
ftp.hacktic.nl /pub/pgp/voice;
ftp.ox.ac.uk /pub/crypto/pgp/utils

Kameras



Eine Kamera macht sich im Urlaub, bei Familienfeiern und bei einem Ausflug mit den Kleinen in den Zoo immer gut. Auch ist eine Kamera praktisch, wenn man »interessante« Menschen und ihre Treffen festhalten möchte. Für den einen ist der wohlgeformte Nachbar von gegenüber ein interessantes Objekt, und andere richten ihre Kameras auf Leute, die einer abweichenden Meinung zugetan sind. Der Sensationspresse ist es vor allem an koksenden Bürgermeistern und hohen Politikern, die im Garten nackt herumhopsen, gelegen, während die Polizei Fotos von Hausbesetzerinnnen, kritischen Studenten oder Atomkraftgegnerinnen sammelt.

Kameras können dafür verwendet werden, klammheimlich Leute zu fotografieren und um bestimmte Informationen aufzuzeichnen. Sowohl bei der klassischen Militär- als auch bei der modernen Wirtschaftsspionage gehört die Minikamera zum Standardpaket. Kommerziell erhältliche Objektschutzkameras sind im großen Maßstab verbreitet. Die modernen Kameras verbannten den herkömmlichen Nachtwächter mit Taschenlampe auf die Kinoleinwand. Die Anzahl der Videokameras, welche die Sicherheit von Personen und Objekten gewähren sollen, ist immens. Kameras werden eingesetzt, um Überfällen auf Tankstellen vorzubeugen, um den Verkehr zu überwachen, oder um dafür zu sorgen, daß auf dem Bahnhof ältere Damen nicht die Handtaschen geklaut werden. Kameras bilden einen immer normaleren Bestandteil unseres Stadtbildes.

In diesem Kapitel beschäftigen wir uns nun damit, was für Kameratypen es gibt, wie und unter welchen Umständen sie benutzt werden und was dagegen unternommen werden kann. Unter Kameras verstehen wir sowohl Foto- als Videokameras, es sei denn, daß dies im Text anders angegeben wird.

Die ersten Kameras mußten sich noch mit Kinderkrankheiten herumschlagen, die inzwischen jedoch behoben wurden: Kameras sind nun stoßfester, kleiner, lichtempfindlicher und billiger als in der Vergangenheit. Aufgenommene Bilder können auf verschiedene Arten übermittelt werden und eine Kamera kann mit einer Fernbedienung gesteuert werden. Zur Übertragung von Bildern können die gleichen Medien benutzt werden, mit denen andere digitale Daten übermittelt werden: (Koaxial) Kabel, Glasfaser, herkömmliche Telefonleitungen, ISDN[1], Autotelefon, usw. Für kurze Entfernungen eignet sich sogar Infrarotlicht. Auch Fernsehkabel sind mitunter brauchbar. Firmen senden heute bereits über die nicht sichtbaren Teile bestimmter TV-Frequenzen Nachrichten hin und her. Über die interaktive Nutzung der Kabel werden wir in Zukunft sicherlich noch viel mehr erfahren. Kameras können an Computer und High-Tech-Geräte gekoppelt werden. Aber natürlich hat alles auch seine Grenzen. Dies sollten die folgenden Passagen verdeutlichen.

Eine Kamera mit einem großen Zoom-Objektiv kann enorme Entfernungen überbrücken. Dessen war sich Brigitte Bardot vermutlich nicht bewußt, als ein Fotograf mit Teleobjektiv ein Foto von ihr schoß, als sie sich oben ohne auf ihrer Terrasse sonnte. Aufpassen also! Als grobe Grundregel kann vorausgesetzt werden, daß alles, was mit einem Fernglas wahrgenommen werden kann, auch zu fotografieren oder zu filmen ist. Mit teuren Apparaten kannst du so noch aus einer Entfernung von einem Kilometer »erkannt« werden.

Satellitenkameras regen in diesem Zusammenhang die Phantasie am meisten an. Mit ihnen ist es möglich, von der Erdumlaufbahn aus Fotos zu machen, auf denen nach ein paar Manipulationen sogar Autonummernschilder zu erkennen sind. Bevor du dich nun dafür entscheidest, keinen Schritt mehr vor die Haustür zu setzen, solltest du aber bedenken, daß solch eine Kamera nur jeweils einen bestimm-

ten Ort ins Visier nehmen kann. Und du mußt schon für enorm wichtig gehalten werden, um auf diese Art observiert zu werden.

Ist keine Kamera zu sehen, heißt das noch lange nicht, von keiner Kamera gesehen zu werden. Sogar in der eigenen Wohnung ist es möglich, fotografiert oder gefilmt zu werden. Eine Kamera läßt sich in den komischsten Dingen verstecken: Stiften, Feuerzeugen, Gürtelschnallen, Türklinken, Armbanduhren, Aschenbechern, Aktenkoffern, Nachttischlampen, Büchern oder Gemälden.[1] Doppelte Decken (die Kamera vorzugsweise neben einer Lampe installiert, da niemand dort direkt hineinsieht) und Lüftungsöffnungen sind bevorzugte Verstecke.

Kleine Kameras werden in der letzten Zeit jedoch im großen Maßstab benutzt, weil die Preise erheblich gesunken sind. Manche Geheimfotoapparate sind schon für ein paar Tausend Mark erhältlich, bessere kosten allerdings etwas mehr. Die einfachsten CCD Videokameras kriegst du ab etwa 300 DM. Die kleinsten Kameras haben ein winziges Objektiv (»pinhole«-Objektiv), das über eine dünne Röhre oder ein Kabel mit der erforderlichen Elektronik verbunden ist. Der ehemalige Bürgermeister von Washington wurde mit solch einer winzigen Kamera in einem Hotelzimmer ausspioniert. Das Objektiv befand sich in einem winzigen Loch in der Wand. So konnte dokumentiert werden, wie er sich hin und wieder dem Kokaingenuß hingab, was zu seinem Rücktritt führte. Noch raffinierter ist die »flexible« Variante, bei der die Kamera etwa durch den Lüftungskanal des Klimaanlagensystems oder eine Kabelrinne in eine bestimmte Räumlichkeit geschoben wird. Auch ist es möglich, das Objektiv in der Antenne eines Autos anzubringen. Solch eine Antenne kann über Fernbedienung gedreht werden, und es ist zugleich möglich, die Bilder andernorts zu empfangen. Das fällt weniger auf als der Typ mit Sonnenbrille, der an deinen Fersen klebt.

Es ist schwer, sich vor der Kamera-Observation zu schützen, vor allem, wenn sie kaum zu bemerken ist. In manchen Fällen hilft Vermummung. In der BRD ist es aber bekanntlich verboten, sich auf Demos zu vermummen. Eine

hübsche Mütze, eine Sonnenbrille, ein falscher Schnurrbart, oder ein Rock und etwas Busenfüllung tuns natürlich auch. Besonders wenn sich Leute in großen Menschenmengen befinden ist es häufig schwierig, die gewünschte Person zu filmen oder zu fotografieren. Blendlicht mit Halogenscheinwerfern auf die Observierer zu richten, hilft aber nicht viel, die verwendeten Kameras wissen oft, wie eine Überbelichtung zu vermeiden ist.

Nachtsichtgeräte (Restlicht-, Infrarot- und Wärmekameras)

Früher war es unmöglich, im Dunkeln zu sehen. Seit der Erfindung des Restlichtverstärkers und des Infrarotsichtgeräts ist dies nun ohne weiteres möglich. Anfänglich war die Bildqualität nicht optimal. Es konnte geschehen, daß auf dem Schirm ein grauer Fleck zu sehen war, hinter dem die Visage des Bankräubers nur vermutet werden konnte. Manchmal ist das immer noch so. Es gibt jedoch Geräte, mit denen sogar gefilmt oder fotografiert werden kann, auch wenn es zappenduster ist.

Es gibt zwei Typen von Infrarotkameras, aktive und passive. Die aktive Kamera sendet über einen Scheinwerfer, der sich auf der Kamera oder dem Sichtgerät befindet und einer schwarzen oder roten Scheibe ähnelt, Infrarotlicht. Ebenso wie nicht jeder Ton vom menschlichen Ohr gehört werden kann, ist nicht jede Sorte Licht für unsere Augen wahrnehmbar. Infrarotlicht ist ohne spezielle Hilfsmittel mit bloßem Auge nicht zu erkennen.

Um zu vermeiden, daß für den Menschen sichtbare Bestandteile des Lichts wahrnehmbar sind, muß der Scheinwerfer mit einem Filter ausgerüstet sein. Dieser Filter wird je nach der Größe des Sendebereichs des Scheinwerfers größer und dicker. Die aktive Infrarotkamera ist ein Stromfresser, infolgedessen hat auch das Speisungsgerät ein hohes Gewicht. Darum reichen die meisten mobilen Infrarotkameras nicht weiter als hundert Meter, obwohl so mancher Hersteller behauptet, daß sein Gerät mehr schaffen würde. Aktiv-Infrarotsichtgeräte dürfen keinem Sonnenlicht ausgesetzt werden.

Aktiv-Infrarot kann auch auf eine spezielle Art und Weise dazu genutzt werden, um Töne aus einem bestimmten Raum abzuhören, wobei unter anderem eine Art Kamera Verwendung findet. Bei einem Fenster im Raum werden kleine Infrarotlampen angebracht, die in einer Frequenz blinken, die dem Ton entspricht, der im Zimmer aufgefangen wird. Die Lampen müssen beim Fenster stehen, so daß die »Kamera« von draußen das Aufblinken der »unsichtbaren« Lampen registrieren kann und diese Signale wieder in Töne umgesetzt werden können. Die Kamera muß natürlich eine unbehinderte Sicht auf die Lampen besitzen, sie kann dann bis in 300 Meter Entfernung postiert sein. Dieses System kann nicht mit Hilfe von Funkwellenortern, dafür mit Infrarotortungsgeräten aufgestöbert werden und ist schon für ein paar Tausend Mark zu erwerben.

Unter einer passiven Infrarotkamera verstehen wir die Wärmekamera oder, im technischen Jargon, die Thermographiekamera. Die Funktion dieser Kamera basiert auf der Tatsache, daß Objekte mit einer Temperatur zwischen 0°C und 40°C (also auch hoffentlich dein Körper) Wärme im Infrarotbereich ausstrahlen. Eine moderne passive Infrarotkamera, die Temperaturdifferenzen bis 0,01°C registriert, setzt Wärme in ein sichtbares Bild um. Dabei ergibt das Wärmemuster kein direkt erkennbares Bild, warme Oberflächen erscheinen als helle Flecken, die kalten als dunkle. Mit Hilfe einer solchen Kamera ist aber feststellbar, ob und wieviele Menschen sich etwa an einem bestimmten Ort befinden und deren Konturen sind auch durch Wände erkennbar. Diese Kameras eignen sich auch dazu, jemanden im Freien zu orten, eine Stelle zu ermitteln, an der sich jemand noch vor kurzem befunden hat. Der Fahnder kann damit ein erst vor kurzem geparktes Auto identifizieren oder einem fahrenden PKW folgen. Die Kameraleistung wird weder von Rauch, undurchdringlichem Nebel oder absoluter Finsternis behindert. Die Wärmekamera kann einer feuchten Spur auf dem Teppich folgen und feststellen, ob gerade noch jemand im Bett lag. Alles das, was mit Temperaturunterschieden zu tun hat, kann registriert werden, allein die Interpretation der von der Kamera erzeugten Bilder ist mitunter ziemlich schwierig.

Hat der Wärmesensor dieses Kameratyps ungefähr dieselbe Temperatur wie das gesuchte Objekt, funktioniert er nicht. Deshalb liegt der Sensor besserer Geräte bei etwa -200°C.[3]

Eine weiteres Gerät, um im Dunklen beobachten zu können, ist der Restlichtverstärker. Dieser verstärkt das im Dunkeln vorhandene Licht, das vom Mond oder den Straßenlaternen stammt. Die Vertreiber solcher Geräte machen in ihren Werbeprospekten in der Regel völlig übertriebene Leistungsangaben. Ein gutes Gerät verstärkt das Restlicht in etwa um das 7000fache. Der Restlichtverstärker eignet sich nicht für die Anwendung bei Tageslicht (zu viel Licht) oder bei absoluter Finsternis (kein Licht vorhanden, das verstärkt werden kann). Um letzteres Problem zu beheben, wird der Restlichtverstärker oftmals zusammen mit einem Infrarotscheinwerfer benutzt. Dieser sendet, wie bereits erläutert, für das menschliche Auge unsichtbares Licht, mit dem der Restlichtverstärker hervorragend funktioniert.[4]

Das Gerät ist sehr teuer, besitzt jedoch ein breiteres Anwendungsspektrum, ist nicht so schwer und hat einen größeren Bereich als die Aktiv-Infrarotkamera. Regen und Nebel behindern das effektive Funktionieren des Restlichtverstärkers. Restlichtverstärker werden unter anderem von der US-amerikanischen Grenzpolizei bei der Fahndung nach MexikanerInnen, die versuchen, illegal über die Grenze in das »Land der unbegrenzten Möglichkeiten« zu gelangen, verwendet.

Einer Passiv-Infrarotkamera kannst du dich möglicherweise dadurch entziehen, daß du isolierende Kleidung anziehst, die dazu führt, daß die Körpertemperatur nicht von den Wärmekameras »gesehen« wird. Die Außenseite des Anzugs wird (nach einer gewissen Zeit) die Temperatur der Umgebung angenommen haben. Gesicht und Hände müssen ebenfalls bedeckt sein, da sie sonst weiterhin die verräterische Wärme ausstrahlen. Guerillas in El Salvador wickelten sich manchmal in Alufolie und zogen darüber nasse Kleidung an, damit sie von mit Wärmeinfrarotkameras ausgerüsteten Militärflugzeugen nicht so leicht entdeckt werden konnten. Damit konnte zumindest eine gewisse Wär-

meisolation erzielt werden, die die Interpretation der Bilder erschwerte.

Gegen Aktiv-Infrarot hilft jedoch keine Isolierung. Das einzige, was dagegen unternommen werden kann, ist zu versuchen, daß die »unsichtbaren« Lichtbündel einen nicht erreichen. Jemand, der selbst über ein Infrarotsichtgerät verfügt, kann andere Aktiv-Infrarot-Scheinwerfer entdecken. Noch simpler zur Ortung von Infrarotstrahlen sind kleine Karten im Format von Kreditkarten, die grün aufleuchten, wenn eine Infrarotquelle auf sie gerichtet ist. Solch eine Karte kostet ein paar Mark, für einige Hundert Mark sind Geräte zu erwerben, die mit Ton-, Vibrations- oder sichtbaren Signalen vor infraroten Lichtbündeln warnen. Auch einige Ferngläsern der Bundeswehr oder NVA sind mit Infrarotentsuchern ausgestattet.

Überwachungskameras

Einige Betriebe und Behörden verwenden Kameragehäuse, die nichts weiter als billige Kamera-Imitationen sind, mit allem drum und dran wie blinkenden Lämpchen, die den Menschen signalisieren sollen, sie würden beobachtet. Attrappen sind schwer von echten Kameras zu unterscheiden. In einer modernen Stadt ist dieses sogenannte »Closed Circuit Television« überall zu finden: in der U-Bahn, auf Bahnhöfen, bei Banken, Tankstellen, in Einkaufszentren, Parkhäusern, an Botschaften und Hauptverkehrsstraßen. Manchmal absichtlich und drohend sichtbar, manchmal jedoch kaum bemerkbar, im Auge einer Modepuppe versteckt, hinter einer verspiegelten Glaswand, durch die von der anderen Seite hindurchgeschaut werden kann,[5] in einer Kugel an der Decke usw. Die vielen Bilder sieht sich möglicherweise nie jemand an, geschweige denn, daß sie gespeichert werden. In anderen Fällen ist dies aber sehr wohl gang und gäbe. Du könntest dich fragen, auf wievielen Videobändern oder Computerfestplatten dein Gesicht festgehalten wird, wenn du durch die Stadt spazierst oder radelst. Die meisten Banken machen Videobilder von dir, wenn du mit einer EC-Karte Geld abhebst. Und womöglich finden wir eines Tages in unserer Post einen Prospekt von Karstadt, weil wir dort

10 Minuten lang vorm Schaufenster über den Sinn des Lebens sinniert haben.

Nicht jeder kann permanent unter Beobachtung stehen, das ist allein schon wegen des finanziellen Aufwands nicht machbar. Andererseits sind durch die Möglichkeit, daß Kameras an Computer gekoppelt werden können, viele neue technische Möglichkeiten entstanden. So sinken die Preise für digitale Speichermedien (Festplatten, überschreibbare CD-ROM-Disketten). Speicherkapazität kann weiter erhöht werden mit Hilfe moderner effizienter Datenkomprimierungstechniken, wodurch ein Bild in weniger Bits (Nullen und Einsen) gepreßt werden kann. Es ist kein Problem mehr, 20000 Aufnahmen auf einen Gigabyte zu bekommen. Auch können Kameras so eingestellt werden, daß sie zwar ständig Aufzeichnungen machen, jedoch nur während fester zeitlicher Intervalle (»time-lapse«) ein Teil davon auf Videorecorder (»time-lapse-recorder«) aufgenommen wird. Andere Kameras nehmen ihre Dreharbeiten erst auf, wenn der zu observierende den Raum betritt oder dort bestimmte Bewegungen stattfinden (die von speziellen Sensoren geortet werden). Moderne, mit Computern gesteuerte Überwachungssysteme können so programmiert werden, daß sie nur Objekte ab einer bestimmten Größe, die sich mit einer bestimmten Geschwindigkeit in eine bestimmte Richtung bewegen, orten und gegebenfalls Bilder festhalten.

Sollte die Aufnahme aus irgendeinem Grunde eine schlechte Qualität haben, beispielsweise wegen eines verschmutzten Objektivs oder eines zu oft verwendeten Bandes, so kann mit Hilfe von Computertechniken nachträglich noch ein überraschend scharfes Bild erzeugt werden. Die neuesten Kameratypen machen nur noch »digitale Fotos«. Die Kamera, an der nichts besonderes zu sehen ist, speichert das Bild sofort in Form von Einsen und Nullen. Das so festgelegte Foto wird später direkt in den Computer eingegeben, der die eigentliche Abbildung auf den Schirm zaubert.[6] Solch eine Kamera ist zusammen mit Computerprogrammen, die eigens dafür entwickelt wurden, in der Lage, eine Reihe charakteristische Maße wie die Entfernung zwischen

Mund- und Augenwinkel zu speichern. Werden diese Daten mit anderen Maßen kombiniert, so ergibt sich ein einzigartiges Identifikationssystem. Diese Programme sind vor allem bei polizeilichen Stellen sehr beliebt.

Wie preiswert mittlerweile der Einstieg in einfache Überwachungstechniken ist, zeigt der Blick in einschlägige Fachzeitschriften. Dort werden einfache schwarz/weiß Überwachungskameras inklusive Langzeitvideorecorder und Monitor schon ab 1500 DM angeboten.

Polizei und Kameras

Kameras in Einkaufsläden, an Gebäuden und entlang den öffentlichen Straßen können für die Polizei aus verschiedenen Gründen äußerst praktisch sein. Die Aufklärungsrate von Überfällen auf Geschäfte mit Überwachungskameras ist natürlich ziemlich hoch. Kameras sind nicht immer auf das Objekt gerichtet, wie es einem erscheinen mag. Eine »Verkehrskamera« im niederländischen Arnheim war tatsächlich auf die Hausbesetzer des »Hotel Bosch« gerichtet.[7] Verkehrskameras eignen sich im Zusammenspiel mit der neueren Computertechnik hervorragend dafür, um zu ermitteln, wo sich jemand mit seinem Fahrzeug gerade befindet.

Was geschieht mit all diesen Bildern von Leuten, die an öffentlichen Orten von Überwachungs- oder Verkehrskameras festgehalten werden? Wer verwaltet den zunehmenden Informationsstrom? Wer hat Zugang dazu? Für welche Zwecke werden die Bilder benutzt?

Die polizeiliche Verwendung von Kameras zur Observation ist gesetzlich nicht verboten. Auch werden die Geräte immer billiger. Die meisten Polizeieinheiten und gewiß die technischen Dienste, die den Observierungseinheiten zur Seite stehen, verfügen sicherlich auch über Minikameras (zum Beispiel die Videoantenne), große Teleobjektive, Nachtsichtgeräte usw. Auch der getarnte Beobachtungsbus mit eingebauten Foto- und Videogeräten eignet sich hervorragend dafür, ein Objekt zu observieren. In welcher Größenordnung derlei Methoden Verwendung finden, läßt sich schwer sagen. Das Ausmaß der technischen Ermittlungsmethoden wird vor Gericht kaum einmal behandelt.

1980 versteckte die bundesdeutsche Polizei fünf Kameras an der Villa von F.J. Kroesen, dem damaligen Oberbefehlshaber der US-Armee in Westeuropa, gegen den die Rote Armee Fraktion (RAF) später einen Anschlag verübte. Die Kameras registrierten die Personen und Autokennzeichen in der Umgebung der Villa. Das aufgezeichnete Material wurde elektronisch gespeichert. Schließlich erfolgte der Anschlag etwa 800 Meter von der Observierungszone entfernt. Durch Kameraaufzeichnungen und Computerauswertung gerieten danach ca. 200 Menschen in die Rasterfahndung der Polizei.

1987 installierte das Berliner Landesamt für Verfassungsschutz eine Überwachungskamera in einem Hinterhof. Ein Verfassungschutzagent hatte den Keller gemietet, dessen Zugang über diesen Hinterhof erfolgte. Fast ein Jahr lang wurden alle Menschen, die sich tags wie nachts durch diesen Hinterhof bewegten, auf Band aufgenommen. Nach zehn Monaten waren endlich zwei Autonome auf Band zu sehen, wie sie mit einem Rucksack durch den Hinterhof marschierten. Grund genug, die beiden neun Monate einzusperren, denn in dem Keller des Agenten befanden sich mehrere Zeitzünder, die dann beschlagnahmt wurden. Das Verfahren wurde später eingestellt, die Verhafteten erhielten ihren Rucksack zurück und mußten sang- und klanglos entlassen werden.

Wie funktionieren Kameras und Ferngläser?

Der nahezu wichtigste Faktor bei einer Kamera ist die Belichtung. Um zu verhindern, daß ein Bild über- oder unterbelichtet wird, befindet sich gegenwärtig in jeder Kamera ein Belichtungsmesser, so daß die richtige Belichtung eingestellt wird. Diese wird von der Blendengröße und der Verschlußzeit bestimmt. Die Blendengröße ist der Durchmesser der Öffnung im Verschluß. Der Verschluß trennt den Film vom zu fotografierenden Objekt. Je größer die Blendenöffnung ist, desto mehr Licht fällt auf den Film. Ein zweiter Faktor ist die Zeit, die der Verschluß geöffnet ist: die Verschlußzeit. Je länger der Verschluß geöffnet ist, desto mehr Licht fällt auf den Film. Verschlußzeit und Blendengröße

stehen miteinander im Zusammenhang. Je länger die Verschlußzeit dauert, desto kleiner wird die Blendengröße. Bei einer langen Verschlußzeit entsteht ein verwackeltes, unscharfes Bild, wenn sich das Objekt bewegt oder die Kamera nicht völlig still gehalten wird.

Es gibt noch etwas, das diejenige, die jemanden fotografieren möchte, berücksichtigen muß. Je kleiner die Verschlußgröße (beziehungsweise je höher die Blendenzahl) ist, desto größer wird der Bereich, innerhalb dessen die Kamera ein scharfes Bild erzeugt (die sogenannte Tiefenschärfe). Diese dürfte im Prinzip eigentlich nie groß genug sein. Die Gefahr, daß ein Foto unscharf wird, verringert sich dadurch, und es ist nicht so wichtig, wie weit die Kamera vom zu fotografierenden Objekt entfernt ist.

Ist genug Licht vorhanden, sollte es also keine Probleme geben. Es wird eine hohe Blendenzahl gewählt (der Verschluß also nicht weit geöffnet), dies ergibt eine angemessene Verschlußzeit und eine gute Tiefenschärfe. Bei wenig Licht wirst du gezwungen, die Blende weit zu öffnen, um eine noch akzeptable Verschlußzeit zu erhalten. Die Tiefenschärfe nimmt damit ab. Gelingt es nicht, ein Objekt scharf zu stellen, so wirst du dir eine Spezialkamera anschaffen müssen.

Auch die Filmsorte ist wichtig. Die Lichtempfindlichkeit eines Films wird in ISO beziehungsweise mit der alten Bezeichnung DIN/ASA ausgedrückt. Ein häufig verwendeter Film ist der ISO 21/100 (21 DIN beziehungsweise 100 ASA). Für weniger lichtempfindliche Filme (z.B. 50 ASA) ist mehr Licht erforderlich, um dieselbe Kombination zwischen Blendenzahl und Verschlußzeit und der sich daraus ergebenden guten Tiefenschärfe zu erhalten. Der Vorteil bei diesen Filmen liegt darin, daß sie eine feinere Körnung besitzen, das Foto also aus kleineren Punkten zusammengesetzt ist. Auf einer normalen Vergrößerung sieht das menschliche Auge keine Punkte, sondern ein zusammenhängendes Bild. Lichtempfindlichere Filme (z.B. ein 1600-ASA-Film) besitzen eine viel gröbere Körnung. Einzelheiten können dadurch verloren gehen, infolge dessen ist solch ein Film nicht für alle Zwecke geeignet. Es ist also nicht so, daß ein stark vergrößertes Foto immer mehr Einzelheiten sichtbar macht.

Film- und Videobilder bestehen aus Linien. Je mehr Linien, desto schärfer wird das Bild. Die Punkte, an denen sich die horizontalen und vertikalen Linien kreuzen, werden Pixel genannt. Je mehr Pixel, desto besser das Bild. Es heißt, daß das Bild bei mehr Pixeln einen größeren Auflösungsgrad besitzt.

Schließlich gibt es noch ultraviolett-empfindliche Filme. Diese Filme werden zum Beispiel dafür benutzt, um berühmte Gemälde zu untersuchen oder herauszufinden, ob in einem wichtigen Dokument Wörter gestrichen worden sind. Wenn du solch einen Film verwenden möchtest, genügt eine normale Kamera vollkommen.

Kameras sind mit allen möglichen Objektiven zu bestücken. Mit Hilfe eines 50-mm-Objektivs entsprechen die gemachten Fotos ziemlich genau dem, was mit dem bloßen Auge wahrgenommen wird. 50mm bezieht sich auf die Brennweite des Objektivs. Eine kleinere Zahl betrifft ein Objektiv mit einem kleineren Winkel, die sogenannten Teleobjektive, mit denen Objekte herangeholt werden können. Ein 50-mm-Objektiv ist mindestens 50mm lang, extrem lange Teleobjektive können bis zu 2 Meter lang sein, was den Gebrauch natürlich nicht gerade sehr praktisch macht. Mit allerlei Spiegeln können sie wohl in ein handlicheres Format umgewandelt werden. Dies geht aber wieder auf Kosten der Lichtstärke.

Auf einem Fernglas stehen immer zwei Nummern (z.B. 10 x 50). Die erste Nummer bezieht sich auf den Vergrößerungsfaktor des Fernglases, die zweite Nummer gibt an, bei welcher Lichtstärke das Fernglas noch sichtbare Bilder erzeugen kann. Je höher diese zweite Zahl ist, desto lichtempfindlicher ist der Apparat.

Anmerkungen

1 Integral Service Digital Network. Über ISDN ist eine viel schnellere digitale Datenübertragung möglich als über die gewöhnliche analoge Telefonleitung.

2 Die japanische Firma Watec hat sich beispielsweise auf Miniaturkameras mit Maßen von 36 x 34 x 68 mm für Schwarzweißbilder und

42 x 44 x 50,5 mm für Farbfilme verlegt. Ein anderes Unternehmen, das sich gut mit kleinen Kameras auskennt, ist P3 (Personal Protection Products) in Hamburg.

3 Die Kühlung erfolgt auf thermo-elektrischem Wege oder mit Hilfe eines Argon-Verdunsters. Ein Beispiel einer Wärmekamera ist die Thermovision 110. In groben Zügen beschrieben, besteht diese Kamera aus einem Objektiv, einem beweglichen Spiegel, einem Sensor mit 48 empfindlichen Elementen, einer winzigen Kathodenstrahlenröhre und einem Okular. Das Wärmebild, das in das Objektiv gelangt, wird ähnlich wie bei einem Fernsehbild horizontal und vertikal abgetastet. Die Auflösung ist bei dieser Kamera jedoch etwas geringer. Jedes der 48 Sensorenelemente sorgt zusammen mit dem beweglichen Spiegel für das Abtasten einer Bildlinie. Auf diese Art und Weise werden 30 Wärmebilder auf dem Schirm der Monochrom-Kathodenstrahlenröhre erzeugt (Preventie 8/9 1990, Nr. 105).

4 Restlichtverstärker sind in drei Phasen entwickelt worden. In Prospekten werden diese häufig als Generationen beschrieben. Die erste Generation benutzt zur Umwandlung des vorhandenen Lichtes in Elektronenenergie, die danach auf einen mit Phosphor beschichteten, elektronen-empfindlichen Schirm prallen, eine Fotokathodenröhre. Dadurch erhält man ein grünes Bild. Das vorhandene Licht wird 5000 bis 7000fach verstärkt. Bei der zweiten Generation (teurer, kleiner, besser zu hantieren, geringere Verzerrung) werden die Elektronen erst durch eine sogenannte MCP (Microchannel Plate) geleitet. Osteuropäische Geräte der zweiten Generation sind für relativ wenig Geld in westlichen Armee-Dumpshops erhältlich. Die modernste, die dritte Generation der Restlichtverstärker, die mit einer »gallium-arsenide«-Fotokathode funktionieren, wird im normalen Handel kaum angeboten. Sie werden allerdings bereits in Schiffahrtskreisen benutzt. Restlichtkameras, wie sie die US-amerikanische Grenzpolizei verwendet, kosten bei der Firma P3 etwa 30000,– DM, ein zusätzlicher Infrarotscheinwerfer noch mal 6000,– DM.

5 Ob durch einen Spiegel von der anderen Seite aus hindurchgesehen werden kann, läßt sich einfach feststellen, indem du darauf eine starke Taschenlampe richtest. Wenn es sich um einen Beobachtungsspiegel handelt, werden der dahinter befindliche Raum und eventuell die erschreckten Gesichter sichtbar.

6 Zum Beispiel von HAL Peripherals: Dycam Model 1

7 Antwort auf Fragen an den Bürgermeister und das Ratskollegium von Arnheim

Wissenswertes vom Lauschen

Nachwort von Otto Diederichs

Zwar garantiert das Grundgesetz der Bundesrepublik von 1949 in seinem Artikel 10 die Unverletzlichkeit des Brief-, Post- und Fernmeldegeheimnisses. Doch bereits der zweite Absatz des Artikels relativiert dies wieder: »Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden.«[1] Diese gesetzliche Grundlage besteht seit 1968 und wird mit steigender Tendenz genutzt.[2] Im Gegensatz zum »Großen Lauschangriff«, der seit gut zwei Jahren wieder in aller Munde ist, bestehen hier bereits Erfahrungen. Sie können einen Eindruck von dem vermitteln, was zu erwarten sein wird, wenn der »Lauschangriff« mit seinen erweiterten Möglichkeiten (z.B. Einsatz von »Wanzen« und Video) einmal gesetzlich erlaubt sein wird. Erste Schritte auf diesem Weg sind mit dem sog. OrgKG[3] von 1992 und dem Verbrechensbekämpfungsgesetz[4] von 1994 bereits getan.

Während die Abhörbefugnisse für den Verfassungsschutz in einem eigenen Gesetz geregelt wurden,[5] hat man die Grundlagen für die Polizei lediglich in der Strafprozeßordnung (StPO) verankert.[6] Für die BürgerInnen hat dies einen ganz entscheidenden Nachteil: Wo für den Geheimdienst noch eine, wenngleich nachträgliche und zudem höchst unzulängliche, Kontrolle durch die G-10-Ausschüsse der Parlamente zumindest vorgesehen ist, gibt es im polizeilichen Bereich nichts dementsprechendes. Die »Kontrolle« beschränkt sich allein auf die Staatsanwalt- und Richterschaft. Diese jedoch sind zugleich auch die Anordnungsinstanzen.

Katalogstraftaten

Die Delikte, bei denen eine Telefonüberwachung (TÜ) durchgeführt werden kann, sind in 100a StPO abschließend

genannt. Bei diesen handelt es sich zunächst um den Bereich, der den politischen Straftaten zuzuordnen ist, wie Hoch- und Landesverrat, Straftaten gegen die Landesverteidigung oder die Sicherheit der NATO-Truppen und ähnliches. Im weiteren dann um die sog. Katalogstraftaten: Geldfälschung, Mord, Menschenhandel, Geiselnahme, Bandendiebstahl, Raub und Erpressung sowie Verstöße gegen das Waffen- und das Betäubungsmittelgesetz. In allen polizeilichen Ermittlungsverfahren, denen eines oder mehrere der genannten Delikte zugrundeliegen, ist damit eine *Telefonüberwachung* grundsätzlich möglich und rechtmäßig. Der regulär hierfür vorgesehene Weg sieht einen entsprechenden Antrag der Polizei vor, der von einem Richter bestätigt werden muß. Eher als Ausnahmeregelung für Fälle, in denen eine richterliche Anordnung nicht schnell genug zu erreichen ist (z.B. an Wochenenden), sieht die StPO eine Eilanordnung durch die Staatsanwaltschaft vor.[7] Diese muß allerdings binnen drei Tagen von einer RichterIn bestätigt werden, ansonsten ist sie unverzüglich abzubrechen und evtl. Bandaufnahmen wären zu vernichten. Für ganz dringliche Fälle sehen die Polizeigesetze ebenso wie in anderen Lagen, auch hier die »Gefahr im Verzuge« vor, also eine Situation, in der unverzügliches Handeln gefordert ist, z.B. um eine Gefahr abzuwenden oder sonst unwiderbringliche Beweise zu sichern. »In der Praxis hat sich (...) herauskristallisiert, daß die Polizei Gefahr im Verzuge sehr großzügig begründet und so den Richtervorbehalt umgehen kann (...)«, bilanziert hierzu die Bundesarbeitsgemeinschaft kritischer Polizisten und Polizistinnen.[8]

Hintertür §129 StGB

Gleichwohl sind durchaus Fälle denkbar, in denen das rechtliche Instrumentarium dennoch nicht ausreicht. So gelten z.B. Diebstahl, Hehlerei und Betrug nicht zu den Katalogstraftaten. »Organisierte Kriminalität spielt sich in einem großen Maße in den Bereichen Diebstahl und Hehlerei ab. Aufgrund dieser Straftaten ist die Anordnung einer Telefonüberwachung aber nicht zulässig. Schlüssel zum Erfolg kann hier der durch entsprechende Ermittlungen untermauerte Verdacht einer kriminellen Vereinigung (§129 StGB) sein,« lautet die Anwort des Staatsanwaltes Michael Füllkrug, der hierzu auch gleich einige (zumindest recht fragwürdige) Beispiele liefert.[9] Dabei kommt es nach Füllkrug »für die Verwertbarkeit der Telefonüberwachungserkenntnisse nicht darauf an, ob sich der Verdacht eines Vergehens nach §129 StGB durch die weiteren Ermittlungen bestätigt«.[10] Gleiches gilt, so bleibt hinzuzufügen im politischen Bereich für die Verwendung des §129a StGB (Bildung einer terroristischen Vereinigung.[11]

Viele Zahlen ohne konkrete Aussage

Nach einer Berechnung des Referenten für Strafverfolgung im nordrhein-westfälischen Innenministerium, Andreas Dickel, liegt das statistische Risiko eines Bundesbürgers, Opfer einer Telefonüberwachung zu werden, bei 1:10000.[12] Solche Rechenbeispiele sind ebenso problematisch wie der von PolizeikritikerInnen gern gezogene Vergleich zwischen den Telefonüberwachungszahlen der Bundesrepublik und den USA.[13] Doch nicht nur im internationalen Vergleich fehlt es an gesichertem, nach einheitlichen Kriterien erhobenem Zahlenmaterial. Auch für die Bundesrepublik allein ist es ausgesprochen schwierig, Informationen über den tatsächlichen Umfang der jährlichen Telefonüberwachungen zu gewinnen. Finden lassen sich, wenn auch mit etwas Mühe, Zahlen. Nur sind diese, um die Sprache des Computerzeitalters zu benutzen, untereinander nicht kompatibel. Zu verschieden sind die Berechnungsgrundlagen. Schon bei der allgemein gebräuchlichsten Form, der Zählung von Fällen entsprechend der Befugnisnorm nach §100 StPO sind Unterscheidungen zwischen richterlicher und staatsanwaltschaftlicher Anordnung möglich.[14] Ebenso die Trennung nach Ermittlungsfällen und/oder überwachten Anschlüssen[15]; nach Bundesländern und/oder Oberpostdirektionen/Generaldirektionen der Telekom[16], deren Zuständigkeit nicht unbedingt gleichbedeutend ist mit den Grenzen der Bundesländer. Bis 1992 wurden Telefonüberwachungsmaßnahmen in den Bundesländern der ehemaligen DDR zudem von den Direktionen der alten Länder in »Paten-

schaft« mitübernommen.[17] »Abhöraktionen gingen erstmals zurück«, meldete jedoch Mitte Februar 1995 überraschenderweise die Presse. Im weiteren war dann zu lesen, daß die Zahl der richterlichen und staatsanwaltschaftlichen Anordnungen 1994 im Vergleich zum Vorjahr um rund 250 gesunken war.[18] Der Eindruck, daß tatsächlich weniger Telefone abgehört werden, gibt Anlaß zum genaueren Hinschauen. So beziehen sich die Zahlen richterlicher oder staatsanwaltschaftlicher Lauschanordnungen nicht notwendigermaßen nur auf Telefonanschlüsse, sondern können auch andere Datenweitergaben über das Telefonnetz (z.B. Fax) umfassen. Da weiterhin eine Anordnung auch mehrere Anschlüsse betreffen kann, bedeuten weniger Anordnungen nicht, daß auch weniger Apparate abgehört wurden: In Baden-Württemberg wurden in den Jahren 1990–92 im Durchschnitt 1,3 Anschlüsse pro Anordnung überwacht.[19] Werden Anordnungen nach ihrer maximalen Geltungsdauer von drei Monaten weiter verlängert, so tauchen diese Verlängerungen in der Statistik nicht mehr auf. Über neun Monate wurde bspw. in Göttingen die Gruppe »Antifa M« überwacht. Während dieser Zeit wurden 13929 Telefonate mitgeschnitten und ausgewertet.[20] Endgültig gesprengt werden die Dimensionen, wenn öffentliche Fernsprecher abgehört werden: Im November 1987, auf dem Höhepunkt der Auseinandersetzungen um die Hamburger Hafenstraße, wurden dort auch die Telefonzellen in der Umgebung überwacht;[21] oder im Zuge der Fahndung nach dem bundesweit bekanntgewordenen Berliner Kaufhauserpresser Dagobert zeitweise bis zu 3000 Telefonzellen in der Stadt abgehört.[22]

Richterliche und staatsanwaltliche Anordnungen zur Telefonüberwachung gem. §§ 100a, 100b StPO

	1973	1974	1975	1976	1977	1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994
Baden-Württemberg									162	169	162	135	286	234	305	362	390	421	503	559	759	
Bayern									120	132	131		120	188	201	276	301	342	446	560		
Berlin																		8	46	72	100	
Brandenburg																				6	59	
Bremen									7	20	19		16	15	32	40	31	34	140	206		
Hamburg									64	46	60		51	79	101	85	124	122	172	224	206	
Hessen									147	209	187		247	254	238	291	335	366	402	443	562	
Mecklenburg-Vorpommern																				0	18	
Niedersachsen									56	69	69		144	176	265	246	283	127	182		475	
Nordrhein-Westfalen									133	243	265		315	393	500	555	531	630	729	912	888	
Rheinland-Pfalz									44	40	42		100	77	66	117	156	167	110	195	172	
Saarland									12	4	1		3	1	37	46	44	35	30	30		
Sachsen																				26	30	
Sachsen-Anhalt																				11		
Schleswig-Holstein									17	27	28		41	51	48	65	77	30	51	51		
Thüringen																				19		
Bund (BKA)													98	171	155	162	173	173				
Gesamt	104	252	432	511	526		443	727	766	968	964	1.124	1.308	1.532	1.805	2.191	2.247	2.494	2.797	3.499	3.964	3.730

Quellen: Monatsschrift f. Kriminologie und Strafrechtsreform 2/79, S. 72; BT-Drs. 10/2395, S. 7; 11/1255, S. 30; 12/5269, S. 6ff.; 12/7116, S. 18; 12/8306, S. 2 u. 6; 13/618, S. 4ff. BT-Protokolle 1991, S. 2354; 1993, S. 13359ff.; Der Spiegel 18/91, S. 20ff.; die ungezeitene v. 25.10.92 und 4.8.93 (Lokalteil HH); Pressemitteilung des MdB von Essen v. 29.4.92; Brief des BMJ-SS Funke an MdB Köppe v. 4.8.93; Der Tagesspiegel v. 22.11.93; IM Baden-Württemberg, Pressemitteilung v. 8.12.93; 13/555, S. 2ff.; LT-Baden-Württemberg Drs. 11/4888, S. 100 u. S. 222ff.

Einstmals Sonderfall: Berlin

Einen Sonderfall bildete jahrzehntelang Berlin, wo die §§ 100a/100b StPO durch eine Alliierte Anordnung (Berlin Kommandatura Order, BK/O) im Juli 1969 außer Kraft gesetzt waren[23] und Überwachungsmaßnahmen über die Alliierten abgewickelt wurden.[24] Erst im Zuge der deutsch-deutschen Vereinigung wurde die BK/O geändert und die Zuständigkeit in deutsche Hände gelegt – zunächst allerdings noch mit der Beschränkung, daß die schriftliche Zustimmung der alliierten Behörden, in deren Sektor die Maßnahme stattfinden soll, einzuholen ist, »bevor ein Staatsanwalt oder ein Gericht (...) die Überwachung der Maßnahme unmittelbar anordnet«.[25] Am heftigsten betroffen vom Rückzug der Allierten aus dem Telefonkabel waren Berlins Verfassungsschützer, die wegen nun plötzlich fehlender technischer Einrichtungen zunächst keine Gespräche mehr abhören konnten[26] und erst eigene Kapazitäten aufbauen

mußten. Doch auch Berlins Polizei hatte anfänglich noch Beschränkungen ihrer neuen »Freiheiten« hinzunehmen: Von vier Anträgen wurde im ersten halben Jahr seit Inkrafttreten der Neuregelung lediglich einer genehmigt.[27] Unterdessen jedoch haben auch in Berlin die Abhörzahlen durchaus »Bundesniveau« erreicht.

Neue Forderungen ...

»Mir – und damit sehe ich mich in Übereinstimmung mit der Mehrzahl der Bürger und Bürgerinnen – liegt eine effektive Kriminalitätsbekämpfung heute und auch in Zukunft am Herzen, und für diesen Zweck ist die Telekommunikationsüberwachung – auf gesicherter rechtlicher Grundlage – ein unverzichtbares Instrument«,[28] meldete sich im Herbst 1994 der hessische Innenstaatssekretär Heinz Fromm mit der Sorge zu Wort, die Sicherheitsbehörden könnten den Anschluß an die moderne Technik verlieren. Neben Telefax, Btx und Mailbox sind es insbesondere die Digital- und Mobilfunknetze, die dem früheren Chef des hessischen Landesamtes für Verfassungsschutz Kummer bereiten. Dies nicht etwa, weil eine Überwachung hier technisch nicht möglich wäre, sondern weil die staatlichen Investitionskosten in die neuen Techniken immens sind und z.B. allein für die D-Netze ca. 40–50 Millionen DM betragen.[29] Daher sollte seiner Ansicht nach »verstärkt Einfluß auf die Systemhersteller genommen werden, damit sie bereits bei der Entwicklung neuer Telekommunikationssysteme entsprechende Überwachungskomponenten mit vorsehen.«[30] Eine Analyse der polizeilichen Bedürfnisse ist von der AG Kripo der Innenministerkonferenz bereits erarbeitet.[31] Im Frühjahr 1995 war es dann soweit. Von der Öffentlichkeit weitgehend unbemerkt verabschiedete das Bundeskabinett eine neue Fernmeldeanlagen-Überwachungs-Verordnung (FÜV), die seit dem 18. Mai 1995 in Kraft ist;[32] sie gilt neben dem herkömmlichen Telefon zugleich auch für das ISDN-Netz der Telekom und für den Bereich der Computer-Mailboxen. Binnen eines Jahres müssen die Netzbetreiber nun die für eine Überwachung notwendigen technischen Voraussetzungen schaffen.

... und Begrenzungen

Einhalt gebieten angsichts solcher omnipotenten Vorstellungen in der Überwachungspraxis lediglich die personellen und technischen, insbesondere aber finanziellen Ressourcen. Nach Informationen aus den mit solchen Maßnahmen befaßten Fachdienststellen des Bundeskriminalamtes (BKA) kostet eine Telefonüberwachung je nach Umfang und Dauer bis zu 500000 DM. Für das Abhören der D1- und D2-Mobilfunknetze sind weitere Kostensteigerungen zu erwarten. Hier geht man von Beträgen zwischen 700000 und einer Million DM aus.[33]

Wenig versprechen sollte man sich von der Vorstellung, den Richtervorbehalt auszudehnen.[34] Zurecht mahnt Werner Sack, Mitglied der Neuen Richtervereinigung hier zur Vorsicht, denn »Richtervorbehalte verhindern keine Grundrechtsverletzungen, sie kontrollieren lediglich deren Anlaß und Ausmaße.«[35]

(Otto Diederichs ist Redakteur und Mitherausgeber des in Berlin erscheinenden Informationsdienstes Bürgerrechte & Polizei/Cilip)

Anmerkungen

1 Art. 10 GG, Absatz 2
2 siehe auch: Bürgerrechte & Polizei/Cilip Nr. 49 und Nr. 50, S. 78–79
3 Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKg), in BGB1 Nr. 34 (Teil I) v. 22.7.92
4 Gesetz zur Änderung des Strafgestzbuches, der Strafprozeßordnung und anderer Gesetze (Verbrechensbekämpfungsgesetz), in: BGB1 Nr. 76 (Teil I) v. 4.11.94
5 7. Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses v. 13.8.68 (sog. G-10-Gesetz)
6 §100 a StPO
7 §100 b StPO, Abs. 1, Satz 2
8 Unbequem Nr. 17, März 1994, S. 23
9 Kriminalistik 7/90, S. 352–353
10 ebd.

11 vgl. BT-Drs. 12/8306 v. 20.7.94
12 Kriminalistik 2/94, S. 88
13 vgl. Unbequem Nr. 16/93, 17/94; Der Spiegel 33/93
14 vgl. BT-Plenar-Protokoll 12/157 v. 12.5.93, S. 13.353
15 Kriminalistik 2/94, S. 88
16 vgl. BT-Drs. 12/8306 v. 20.7.94
17 BT-Drs. 12/7116, S. 18
18 Berliner Zeitung, 16.2.95
19 Pressemeldung Innenministerium Baden-Württemberg, 8.12.93
20 die tageszeitung, 22.2.95
21 Der Spiegel, 18.1.88; Frankfurter Rundschau, 3.2.88; Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten, Hamburg 1989, S. 100–104
22 Der Tagesspiegel, 24.1.93; die tageszeitung 23.4.94
23 BK/O (69)6, Juli 1969 und (74)2, März 1974
24 Der Spiegel, 25.10.95
25 BK/O (89)7, Juni 1989
26 Der Tagesspiegel, 14.10.90
27 Der Tagesspiegel, 31.1.90
28 der kriminalist 10/94, S. 485
29 ebd.
30 ebd., S. 487
31 ebd.
32 die tageszeitung, 23.6.95
33 Deutsches Allgemeines Sonntagsblatt, 16.9.94
34 Der Spiegel, 16.8.93
35 Unbequem 17/94, S. 23

Programme auf Diskette

Programme
auf Diskette

Zu diesem Buch gehört eine Diskette für PCs. Auf der findet sich eine Reihe von Programmen und Algorithmen, die im Kapitel über die Verschleierung von Daten beschrieben sind.

Auf der Diskette steht eine »READ.ME«-Datei. Diese Datei ist im ASCII-Format gespeichert und kann mit nahezu jedem Textverarbeiter und Editor eingesehen werden. Hier finden sich weitere Anweisungen, wie die Programme installiert und benutzt werden können.

Eine Reihe der Programme sind sogenannte »Sharewa-re«-Pakete. Das heißt, daß diese Programme nicht kostenlos sind! Es ist gestattet, sie auszuprobieren und sie in ihrer kompletten Form weiterzuverbreiten, wenn dafür kein Geld verlangt wird. Solltest du dich jedoch dafür entscheiden, das Programm zu verwenden, mußt du dich registrieren lassen. Du zahlst dann dem/den Autor(en) ein geringes Entgelt, für das du in vielen Fällen auch Anspruch auf Unterstützung, Neufassungen usw. erhältst. Für die genauen Informationen, wie du dich je Programm registrieren lassen mußt, verweisen wir auf die Dokumentation der jeweiligen Programme.

Die Herausgeber:

Backslash

Die Stiftung Backslash unterstützt fortschrittliche Gruppen und Organisationen beim Gebrauch moderner Computerkommunikation. Backslash gibt Tips und Kurse, wie aus der täglichen Informationsfülle, die relevante Information herauszufinden ist.

Postfach 6681, 1005 ER Amsterdam

E-Mail: oortjes@backslash.xs4all.nl

Hack-tic

Zeitschrift für Techno-Anarchisten und freie Technauten; Niederlandens erstes und farbenfrohestes Hackerblatt berichtet regelmäßig über: Knackbare Computersysteme, unsichere Telefonnetze, Privatsphäre, Computernetzwerke, sichere Kommunikation und die Gesetzgebung zur Computerkriminalität.

Tel 0031-20-6222699, Fax 0031-20-622753

E-Mail: redaktie@hacktic.nl

Xs4all: Internet für Alle!

Die Stiftung Xs4all ist aus der niederländischen Hackerszene hervorgegangen. 1992 unter dem namen Hack-tic Netwerk als ein uucp-Netzwerk angefangen, hat es im März 1993 die Flügel ausgebreitet und ließ die User online über das Internet ausschwärmen. Damit waren die Zeiten vorüber, in denen der Internetzugang nur das Privileg einer handvoll Glücklicher war. Am 1. September 1994 änderte Hack-tic Netwerk seinen Namen in Xs4all.

Tel 0031-20-6200294, Fax 0031-20-6222753

E-Mail: helpdesk@xs4all.nl

Jansen & Janssen

Das Büro Jansen & Janssen archiviert und recherchiert Information zu Polizei und Geheimdiensten in den Niederlanden. Die Daten, welche aus Presse, Fachliteratur oder weniger zugänglichen Quellen stammen, sind über Computer abrufbar - zumindest für diejenigen, die Polizei und Geheimdiensten kritisch gegenüberstehen.

Jansen & Janssen haben bislang folgende Publikationen herausgegeben: »Regenjassen Demokratie« (dt., Regenmantel Demokratie), war eine Untersuchung zur Infiltration des niederländischen Verfassungsschutzes in der linken Szene. Den Praktiken des Geheimdienstes gegen Asylsuchende war die Broschüre »De Vluchteling Achtervolgd« (Die verfolgten Flüchtlinge) gewidmet. 1993 wurde »Opening van Zaken« (Taschen öffnen) veröffentlicht, ein alternativer Verfassungsschutzbericht. Hier kommt vor allem die Jagd des Staates nach der RARA (Radikale Anti-Rassistische Aktion) ausführlich zur Sprache. Die RARA trat erstmals 1985 in Erscheinung und beging Anschläge gegen Unternehmen wie Shell, die mit dem südafrikanischen Apartheidsaat kooperierten.

Postfach 10591, 1001 EN Amsterdam

AutorInnenkollektiv Keine Panik

Weit draußen in den unerforschten Einöden eines total aus der Mode gekommenen Ausläufers des westlichen Spiralarms der Galaxis leuchtet unbeachtet eine kleine gelbe Sonne. Um sie kreist in einer Entfernung von ungefähr achtundneunzig Millionen Meilen ein absolut unbedeutender, kleiner blaugrüner Planet, dessen vom Affen stammende Bioformen so erstaunlich primitiv sind, daß sie Handys noch immer für eine unwahrscheinlich tolle Erfindung halten.

Viele von den BewohnerInnen dieses Planeten waren unglücklich, weil ihre Telefongespräche, Redaktionskonferenzen und alle möglichen anderen Aktivitäten von anderen immerzu belauscht wurden. Damit das nicht so bliebe, begann eine kleine Gruppe, die sich AutorInnenkollektiv Keine Panik nannte, dieses Buch aus dem holländischen zu übersetzen, den deutschen Verhältnissen anzugleichen und zu aktualisieren, damit ein paar Leute in Zukunft weniger unglücklich sein sollten.

Kontakt über die Edition ID-Archiv, Postfach 360205, D-10972 Berlin