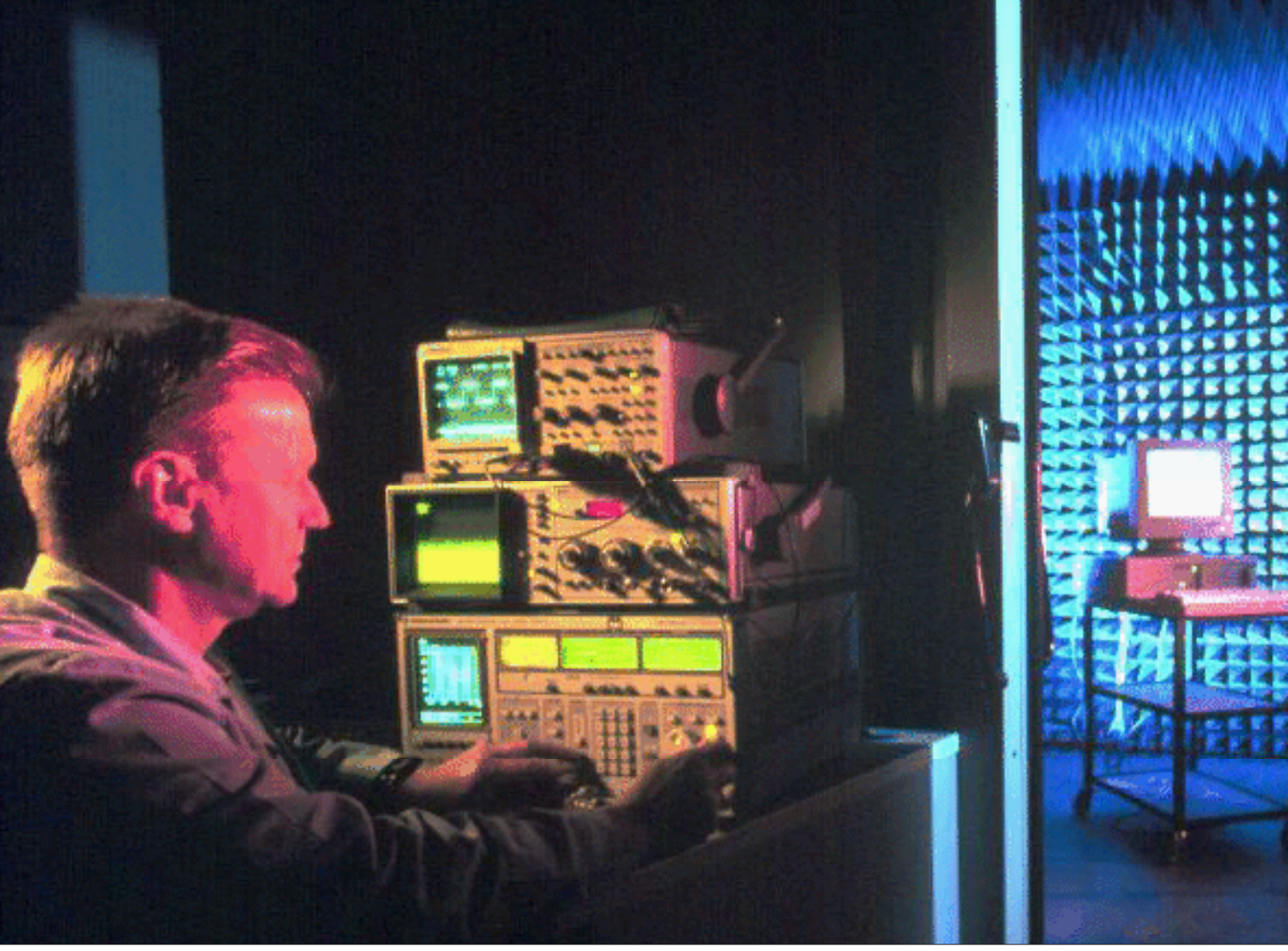


PC in der Abstrahlungs-Meßkabine (bei Siemens): Der Raubzug durch elektronische Tresore hinterläßt keine Spuren

Lauscher im Datenreich

Die Welt der Computer und der Datennetze ist ein Paradies für Spione aller Art. PC verraten vertrauliche Daten durch hochfrequente Abstrahlung. Geheimdienste überwachen den internationalen Datenverkehr und unterhöhlen zielstrebig alle Schutzvorkehrungen. Selbst das gutgesicherte Netz der Banken haben Profi-Lauscher angezapft.

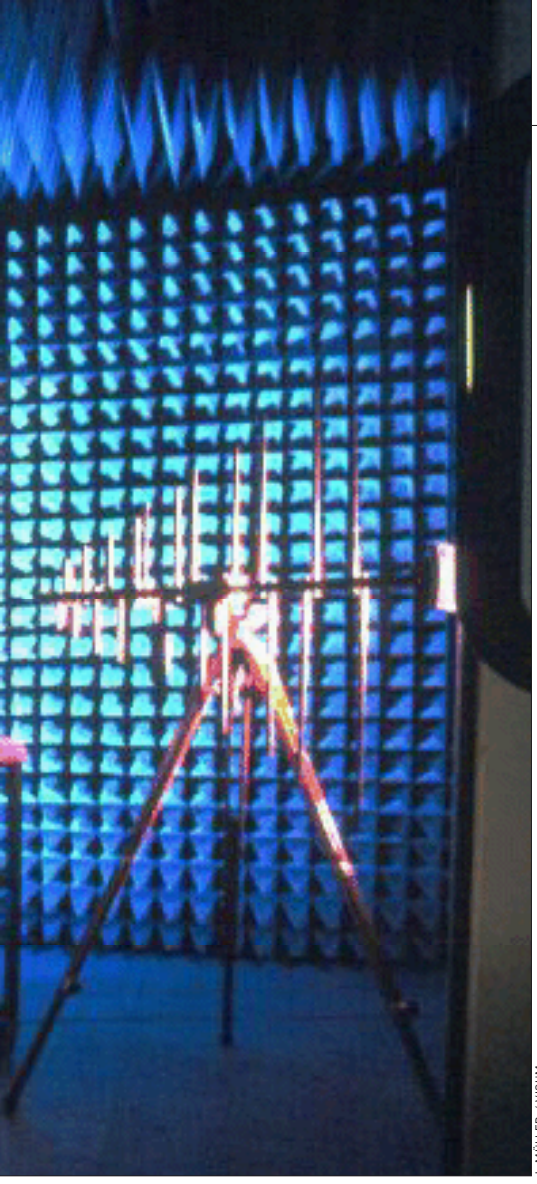
Die Männer in Overalls mit Coca-Cola-Schriftzug betraten das Bankhaus am Samstag abend. Doch Kästen mit Braunbrause hatten sie nicht dabei. Statt dessen schleppte die Gruppe schwere Metallkoffer, Kabelrollen und Antennen in das Gebäude.

„Diese Anzüge waren schon etwas lächerlich“, meint ein Elektronikspezialist. Aber er ist extravagante Wünsche seitens der Kunden gewohnt. Bei Kreditinstituten ist der Einsatz in der Nacht von Samstag auf Sonntag die Regel, denn die diskreten Banker fürchten um ihren Ruf, wenn bekannt werden sollte, daß Hochfrequenztechniker im Haus sind.

Mit Testsendern und empfindlichen Antennen vermessen die Fachleute, wie durchlässig Fenster, Decken und Wände für Radiowellen sind. Meist ist das Ergebnis eindeutig: Auf ihrem Weg durch das Gemäuer hindert fast nichts die elektromagnetischen Wellen.

Das ist angenehm für den Angestellten, der am Schreibtisch Radio hören will – äußerst mißlich jedoch für das Unternehmen, weil auch der umgekehrte Übertragungsweg weit offen steht: Jede Menge kleiner Sender stehen in den Büros und verbreiten wichtige Firmendaten. Denn als Nebenprodukt ihrer elektronischen Tätigkeit strahlen Computer Radiofrequenzen ab, die jedes Zeichen auf dem Bildschirm und jeden Tastendruck verraten.

Aus Entfernungen von hundert Metern bis zu einem Kilometer können technisch versierte Lauscher verfolgen, wie vertrauliche Strategiepapiere in Vorstandsetagen zirkulieren, welche neuen Produkte in den Konstruktionsabteilungen von Elektrokonzernen entstehen oder welche diskre-



J. MÜLLER / VISUM

ten Finanztransaktionen die Machtverhältnisse in Konzernen verändern.

Zur wahren Bonanza für Spione aller Couleur haben sich auch die Datennetze entwickelt, über deren Verknüpfungen und Querverbindungen längst jeglicher Überblick verlorengegangen ist. Der Konzern Siemens erhielt jüngst eine Warnung des Verfassungsschutzes, französische Dienste hätten ein Auge auf vertrauliche Daten geworfen.

Noch ist den Managern das Debakel um die geplatzten ICE-Deals in schmerzhafter Erinnerung. Bei den Verhandlungen in Südkorea hatten die französischen Konkurrenten sämtliche Preisofferten mit hellseherischer Sicherheit unterboten. Nun durchforsten Techniker das Computernetz des Konzerns auf Informationslecks.

Kürzlich schreckte eine Meldung der *Sunday Times* das Europaparlament aus der gerade begonnenen Sommerpause. Amerikanische Geheimdienste, so will das Blatt erfahren haben, stecken tief im Informationssystem der Brüsseler Bürokraten, das auch die Korrespondenz der EU-Delegationen transportiert. Ein solcher dreister Lauschangriff würde erklären, wie die amerikanischen Verhandlungspartner die EU-Emissäre beim Ringen um das Gatt-Handelsabkommen im vorletzten Jahr über den Tisch ziehen konnten.

Richtig überraschen würde das niemanden. Warum sollten die Geheimdienste den Verkehr der Datenautobahnen an sich vorbeirauschen lassen? Schließlich hat die Phalanx der Dienste, allen voran die amerikanische National Security Agency (NSA), in seltener Einmütigkeit bisher erfolgreich verhindert, daß elektronische Nachrichten durch Verschlüsselung vor unerwünschten Mitlesern geschützt wären.

Die Tricks und Kniffe des Gewerbes behalten die verschwiegenen Herren gern in der Familie. Daß Computer ihre Daten durch Aussenden von Radiowellen verraten, in der Fachwelt „kompromittierende Abstrahlung“ genannt, wissen die Dienste schon lange. Den meisten Unternehmen wird erst jetzt so richtig bewußt, wie verletzlich sie durch die allgegenwärtigen digitalen Helfer geworden sind.

Die elektronische Überwachung ist nicht nur die Fortsetzung der altbekannten Agentenkriege mit anderen Mitteln. Das moderne Instrumentarium eröffnet den Spionen aller Lager neue Möglichkeiten, von denen die allgegenwärtigen Datensammler in George Orwells Roman nur träumen konnten.

Nicht nur, daß sich durch die drahtlosen Abhörmethoden an jedem Computerarbeitsplatz ein heimlicher Späher postieren läßt. Die riesigen Datenarchive der Rechnernetze, denen Unternehmen ihr Know-how, Behörden die persönlichen Daten ihrer Bürger und Banken intime Details ihrer Kunden anvertrauen, stehen verborgenen Mitlesern weit offen.

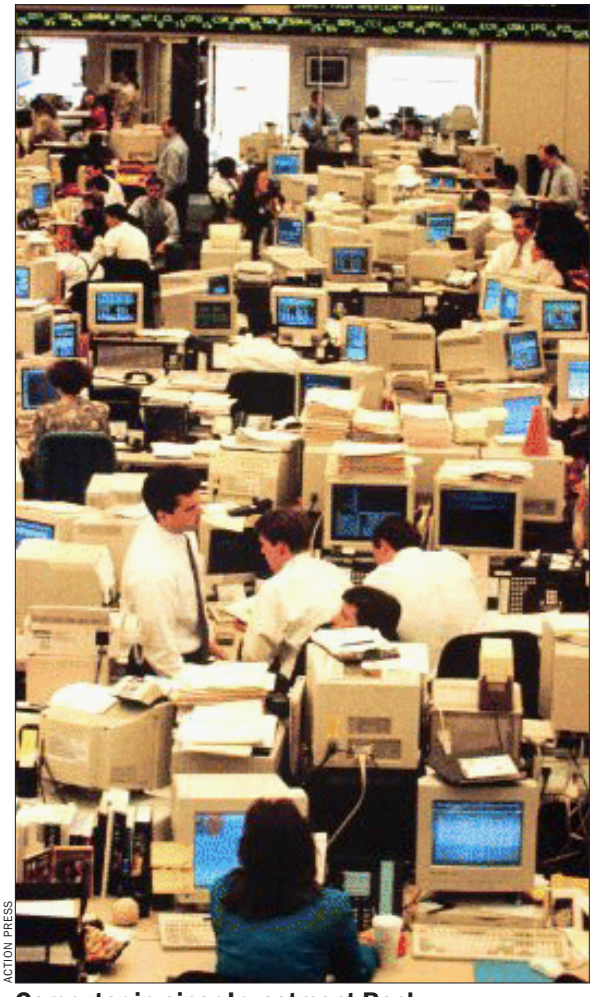
Offenbar gelingt es den Diensten immer wieder, den vermeintlich ausgefeilten Einbruchsschutz von Datenbanken zu durchbrechen. Anders als in früheren Zeiten, als noch ausgesuchte Einbrecher im Sold der Informationsbeschaffer standen, hinterläßt der professionelle Raubzug durch elektronische Tresore keine Spuren.

Während der historische Spion noch Briefumschläge in filigraner Handarbeit aufpräparierte, läßt sich der elektronische Postverkehr weltweit und in Sekundenbruchteilen filzen. Auch auf ein noch so leises verräterisches Knacken, das einst dem Belauschten einen Hinweis auf fremde Ohren in der Telefonleitung geben konnte, horcht man heute vergebens. Digitale Telefonsysteme schicken Sprache als Datenpakete durch die Leitung. Ihre Software enthält meist sogar schon Funktionen, die Dunkelmänner zur Teilnahme an privaten Unterhaltungen geradezu einlädt.

„Wer mit handelsüblichen Rechnern arbeitet, könnte seine Firmengeheimnisse ebensogut mit dem Diaprojektor auf die Wand des Nachbargebäudes werfen“, spottet ein Sicherheitsberater.

So bietet die Firma CCS mit Sitz in New York das „Computer Intercept System STG 4625“ an. „Ohne die Räume zu betreten“, wirbt das Datenblatt, könnten Interessierte die Signale von Computern auffangen. Die Abstrahlungen würden „zu einer scharfen Reproduktion der abgefangenen Daten verarbeitet“. Die kleine französische Firma Arpege Défense bietet ihren handverlesenen Kunden für ähnliche Zwecke ein ausgesuchtes Ensemble aus Standard-Labormeßtechnik und ergänzenden Eigenentwicklungen zum Paketpreis von etwa 70 000 Mark.

„Sonderelektronik“ lautet die diskrete Umschreibung für diese Art von Geräten. „Direkte Kontakte haben wir normalerweise nur mit Regierungen“, fertigt ein CCS-Angestellter unerwünschte Nachfrager ab. Doch ähnliche Elektronik dürfte längst auch in der Hand nichtbeamteter Lauscher sein. So beantragten amerikanische Drogenermittlungsbehörden die Anschaffung von abstrahlungssicheren Computern. Sie fürchte-



ACTION PRESS

Computer in einer Investment-Bank
Hinter jedem Arbeitsplatz ein Späher?

ten, daß zahlungskräftige Drogenbosse im Besitz der einschlägigen Abhörtechnik sind.

Abwehrmaßnahmen gegen drahtlose Computerspionage sind in Militärkreisen unter dem Codenamen „Tempest“ zusammengefaßt*. Seit den sechziger Jahren enthalten die geheimen und ständig aktualisierten Tempest-Handbücher Richtlinien für den Bau von abstrahlungssicheren Rechnern und die Einrichtung hermetisch abgeschirmter Räume.

Die zivile Welt erfuhr erst 1985 von der Gefahr. Wim van Eck, ein junger Elektrotechnikingenieur im Forschungslabor der holländischen Telefongesellschaft, war eher zufällig auf das Phänomen gestoßen. „Wir hatten damals viel mit der Nato zu tun und hörten gerüchteweise, daß das Abhören von Computern möglich sei“, erinnert sich der Techniker. „Wir haben ein bißchen herumexperimentiert und waren erstaunt, wie einfach das geht.“ Für den ersten Versuch brauchten die Fachleute eine Viertelstunde, „dann hatten wir einen normalen Fernseher so verstellt, daß er das Monitorbild eines Computers empfangen konnte“.

Erhard Möller, Professor an der Fachhochschule Aachen, versucht Unternehmen auf das Problem aufmerksam zu machen. „Lange hat sich niemand dafür interessiert“, klagt er. „Die typische Mentalität hierzulande ist: ‚Dafür ist die Post zuständig, die fährt mit dem Meßwagen rum, also wird schon nichts passieren.‘“

In seinem Labor steht ein kleiner Philips-Schwarzweißfernseher. Aus der linken Wand ragen vier zusätzliche Knöpfe. Geübt dreht Möller an den Reglern, und prompt erscheint das Monitorbild eines PC, der am anderen Ende des Labors in Betrieb ist. Das simple Gerät zeigt Spähergebnisse auf 10 bis 100 Meter Entfernung. „Es gehört wenig Phantasie dazu, sich vorzustellen, was man mit professionellem Aufwand erreichen kann“, kommentiert Möller.

Den Managern einer Landeszentralbank wollte der Professor einmal „mit der Naivität eines Ingenieurs“ eine praxisnahe Vorführung geben. In einem Hotel gegenüber dem Bankgebäude war schon ein Zimmer gemietet. Dort hätte der staunende Vorstand einen Blick auf die abgehörten Monitorbilder seiner Mitarbeiter werfen können. In letzter Minute wurde der als Mittelsmann fungierende Sicherheitschef der Bank zurückgepfiffen und gerüffelt: „Ein Vorstand geht nicht in so ein Hotel.“ Ende des Projekts.

„Ein Vorstand geht nicht in so ein Hotel“

Die verräterische Abstrahlung entsteht in fast allen Teilen der Rechenelektronik. Video- und Grafikkarten, Druckerschnittstellen, Monitore, Tastaturen und Festplatten tauschen Informationen untereinander mit hochfrequenten Impulsfolgen aus (siehe Grafik). Solche schnell geschalteten Ströme senden gemäß den physikalischen Gesetzen elektromagnetische Wellen aus.

Durch jede noch so winzige Öffnung im Gehäuse finden sie den Weg ins Freie, Kabel können als Antennen die Abstrahlung noch verstärken. Heizungsrohre und Luftschächte leiten die vagabundierenden Signale weiter, über das Stromnetz verteilen sich die streunenden Botschaften durchs Haus.

Befürworter des Großen Lauschangriffs finden solche Möglichkeiten faszinierend. „Wir denken schon darüber nach, wie wir diese Technik in unserer Arbeit anwenden können“, verrät ein Fahnder des Kölner Zollkriminalamtes. „Das soll ja nicht Jahre dauern, bis wir in die Pötte kommen, nachdem die gesetzlichen Möglichkeiten geschaffen sind.“

Jedes ungeschützte Digitalgerät gibt seine Geheimnisse über Funkwellen preis. „Aus Geldautomaten pfeifen die Daten nur so raus“, erklärt ein Schweizer Sicherheitsberater. Vielleicht liegt hier der Schlüssel für eine rätselhafte Serie von EC-Karten-Betrügereien, an denen sich zum Beispiel die Ermittler in Aachen seit Jahresanfang die Zähne ausbeißen.

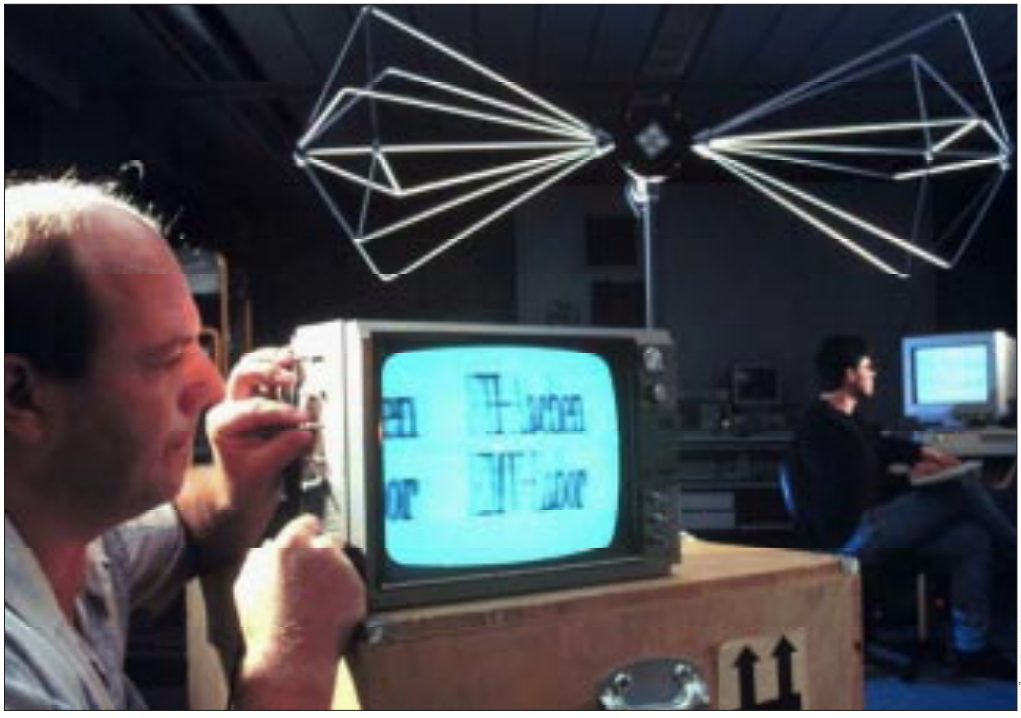
Ende letzten Jahres erleichterten technisch versierte Gauner die Konten von rund 300 Kunden der Deutschen Bank an Geldautomaten in den Niederlanden. Über 300 000 Mark erbeuteten die Diebe, offenbar mit gefälschten Karten. Deren Daten und Geheimzahl müssen sie, so ergab die Rekonstruktion, an den Automaten der Bankfilialen in Jülich und Hückelhoven abgefangen haben. „Wir haben keine Ahnung, wie das geschehen konnte. Eine heiße Spur ist nicht in Sicht“, muß der Sprecher der Staatsanwaltschaft eingestehen.

Für Möller ist der Verdacht auf drahtlosen Datenklau plausibel. „Wir haben uns noch nicht im Detail damit beschäftigt, aber wenn man die Hochfrequenzsignale einer Tastatur hörbar macht, klingen sie wie Telefonwahltöne.“ Was mit dem Ohr zu unterscheiden sei, folgert der Fachmann, müsse sich mit wenig

Verräterische Wellen

Die elektrischen Signale der Computerelektronik erzeugen elektromagnetische Wellen im Radiofrequenzbereich. Aus der Abstrahlung läßt sich zum Beispiel ein Monitorbild aus einigen hundert Metern Entfernung ausspähen. Auch Tastatur und Drucker erzeugen Radiowellen. Verbindungskabel wirken als Sendeantennen. Über die Netzleitung verbreiten sich die Signale über ganze Gebäude.

* Tempest: Abkürzung für „Transient Electromagnetic Pulse Emanation Standard“ (Grenzwerte für kurzzeitig abgestrahlte elektromagnetische Impulse).



J. MÜLLER / VISUM

Abhören eines PC-Monitors*: „Wir waren erstaunt, wie einfach das geht“

Aufwand auch computerlesbar machen lassen.

Ein Kenner der Geheimdienstszene berichtet aus eigener Anschauung, die Profis unter den Datenlauschern seien nicht einmal mehr darauf angewiesen, in unmittelbarer Nähe des angezapften Computers zu horchen. Mit einem Großrechner und findiger Analysesoftware lassen sich auch aus einem komplexen Signalgemisch die Abstrahlungen einzelner PC im Umkreis von einem Kilometer herauskitzeln.

Computern die Abstrahlung abzugewöhnen ist extrem aufwendig. Nur eine Handvoll Firmen beherrscht diese Kunst. Siemens fertigt in seinem Werk für Kombinationstechnik in Fürth Kleinserien von Tempest-konformen PC. Etwa 20 000 Mark inklusive Monitor, fast das Zehnfache der zivilen Variante, kostet ein PC, dessen Verschwiegenheit der strengen Nato-Richtlinie AMSG 720B genügt. Ein „tempestierter“ Laserdrucker ist für rund 10 000 Mark zu haben.

Der Umbau geschieht in Handarbeit. Siemens-Techniker weiden Seriengeräte der Tochterfirma Siemens-Nixdorf aus. Die ausgeschlachteten Originalgehäuse kommen gleich zur Entsorgung. „Die sind überhaupt nicht abzudichten mit all den Löchern für Lüfter und Steckverbindungen“, kommentiert der zuständige Produktmanager Walter Kräutlein.

Um sie gegen ungebetene Lauscher abzuschirmen, wird die gesamte Rechnerelektronik in ein zweischaliges Stahlgehäuse eingebaut. Der Lüfter darf nur noch durch ein feinporiges Lochblech atmen, mehrere Dutzend Schrauben sichern die Gehäusedeckel, alle nach außen führenden Leitungen müssen Filterschaltkreise durchlaufen. Rund 1000 Mark kostet allein die Spezialglasscheibe, die den Bildschirm hochfrequenzsicher abdeckt.

Vor dem Diskettenlaufwerk des Tempest-PC sitzt eine massive Metallschiebetür, deren Öffnen einen nervenden Signalton auslöst. Er soll den Benutzer zum baldigen Schließen bewegen, denn schon der Schlitz zum Einschieben der Diskette vermindert die Schutzwirkung des Gehäuses, das nach Art eines Faradayschen Käfigs alle Radioquellen innerhalb der metallischen Hülle gegen die Außenwelt abschirmt.

Nur einige hundert Stück der Hochsicherheits-PC produziert Siemens pro Jahr. Die meisten Geräte gehen an geheimhaltungsbedürftige Behörden. Sie erhalten die versiegelten PC in einzeln verplombten Kartons.

Bis vor einigen Jahren war der Verkauf von Tempest-PC an Kunden außerhalb von Militär und Behörden ein hochsensibles Geschäft. „Vor der Wende mußten wir beim Bundesamt für Sicherheit in der Informationstechnik zurückfragen, bevor wir einen PC der höchsten Schutzklasse ausliefern konnten“, erklärt Kräutlein das Verfahren.

Auch heute noch meldet die Firma die Namen aller Käufer von Hochsicherheitsgeräten an das Bonner Bundesamt für Sicherheit in der Informationstechnik (BSI). „Eine freiwillige Maßnahme“, betont BSI-Sprecher Michael Dickopf, das sei „so eine Sitte aus alten Tagen“.

Das BSI, Nachfolger der BND-nahen „Zentralstelle für das Chiffrierwesen“, wacht über die Einhaltung der elektronischen Verschwiegenheit. Das Amt berät Behörden, die mit Verschlußsachen hantieren, und die „geheimschutzbetreute Wirtschaft“, umgangssprachlich auch Rüstungsindustrie genannt.

Jeder PC, der zur Verarbeitung von Verschlußsachen zugelassen ist, hat einen bis mehrere Tage in der Meßkabine des Bundesamtes verbracht. Prüfgeräte horchen während dieser Prüfung in diverse Frequenzbereiche hinein und vergleichen Pegel mit geheimen Grenzwerten. „Wir suchen nach bestimmten Signalen, aber die Kriterien sind nicht öffentlich“, erläutert ein Mitarbeiter, der „gut damit leben kann, daß mein Name nicht in der Zeitung steht“.

Geheimdienste spielen in der Datenwelt eine merkwürdige Doppelrolle. Als Bock und Gärtner in einer Person basteln die Geheimniskrämer einerseits an ausgeklügelter Spionagetechnik und definieren andererseits die Sicherheitsstandards. Da die Schutzvorschriften naturgemäß Aufschluß über die ei-

S. HUSCH / TERZ

Geldautomat: „Da pfeifen die Daten nur so raus“

* Experiment an der Fachhochschule Aachen.

recht auf eine Privatsphäre wahrzunehmen. Auch die elektronische Post sollte Briefumschläge haben, und das geht nur durch Verschlüsselungsmethoden.

SPIEGEL: Viele Gesetzentwürfe sehen Verschlüsselungsmethoden vor, durch die Strafverfolgungsbehörden eine Art Nachschlüssel erhalten. Das wäre doch so etwas wie ein Briefumschlag, Ihr Nachbar kann Ihre Liebesbriefe nicht lesen, aber die Polizei kann bei Verdacht den Umschlag öffnen. Warum ist Ihnen das auch nicht recht?

Zimmermann: Was heute eine verfassungstreue Ermittlungsbehörde ist, kann morgen etwas Schreckliches sein. Demokratien verwandeln sich mitunter in Polizeistaaten. Ihr Land hat die Erfahrung vor etwas über einem halben Jahrhundert gemacht. Wenn wir jetzt eine Infrastruktur schaffen, die die totale Überwachung der Bürger ermöglicht – was passiert mit so einem System, wenn es in die falschen Hände fällt?

SPIEGEL: Was ließe sich konkret mit dem Nachschlüsselsystem anstellen?

Zimmermann: Es ist heute schon ein leichtes, jeden Tag Millionen von elektronischen Nachrichten auf politisch subversiven Inhalt zu untersuchen. Es wäre durch das Anzapfen von Reisebuchungssystemen oder Kreditkartenunternehmen sehr einfach, jeden Schritt von politischen Gegnern zu verfolgen. Eine weniger wohlmeinende Regierung, die im Besitz dieser technischen Möglichkeiten ist, könnte die letzte sein, die wir je gewählt haben. Schon aus Gründen der gesellschaftlichen Hygiene sollten wir nicht zulassen, daß so eine technische Infrastruktur entsteht.

SPIEGEL: Werden Firmen, die Kryptoprogramme herstellen, von Geheimdiensten unter Druck gesetzt?

Zimmermann: Sicher, das passiert dauernd. In den USA bekommen alle Firmen, die Verschlüsselungsprogramme herstellen, Besuch von der National Security Agency (NSA). In einem vertraulichen Gespräch legt man ihnen nahe, den Schutz dieser Programme abzuschwächen.

SPIEGEL: Wer garantiert mir, daß PGP sicher ist?

Zimmermann: Bevor es PGP gab, existierte kein Verschlüsselungsprogramm für Privatleute, das Geheimdienste nicht hätten brechen können. Natürlich wissen wir nicht, was die NSA wirklich kann, aber ich habe die besten Verfahren benutzt, die in der akademischen Literatur zu finden sind. Ich habe den Algorithmus von PGP veröffentlicht. Er ist von Kryptologen in aller Welt gründlich untersucht worden und hat bisher allen Attacken standgehalten.

genen Horchfähigkeiten geben könnten, sind die Schutzmaßnahmen ihrerseits geheim. Der Rest der Welt kann so nur rätseln, vor wessen elektronischen Ohren dieser Schutz tatsächlich Bestand hat.

Die Geheimniskrämerei mag ein Grund dafür sein, warum sich in der Privatwirtschaft bisher noch niemand so recht für das Sicherheitsmodell des BSI interessiert, das geprüfte Geräte in die vier Klassen der Zone 0 bis 3 einteilt.

Die Beratungsprozedur ist aufwendig: BSI-Techniker vermessen die Durchlässigkeit der Gebäude, ermitteln die Entfernung zu Standpunkten möglicher Spione und empfehlen danach für den jeweiligen Rechnerstandort einen Schutzgrad. Die Kriterien, nach denen das geschieht, erfährt der Beratene nicht.

Der Berliner Sicherheitsberater Hans-Georg Wolf will elektronische Spione mit

J. MÜLLER / VISUM

Erfinder Wolf mit Schutzgerät
Tarnkappe für Geheimnisträger

ihren eigenen Waffen schlagen. Er hat zusammen mit den Aachener Abstrahlungsforschern ein patentes Kästchen entwickelt, das Computerlauschern das Handwerk legen soll.

Das „Secudat"-Gerät, nicht größer als ein Buch, analysiert die Streustrahlung des PC und erzeugt nach Art eines Störsenders in der Nähe des Computers zusätzliche Radiowellen, die verräterische Impulse des Rechners überdecken. Auf diese Weise verschwindet, wie unter einer elektronischen Tarnkappe, das Bild auf dem Monitor eines Abhörgeräts hinter undurchdringlichem Schneegestöber.

Wolf kennt das Milieu der Geheimniskrämer aus seiner Arbeit für das damalige DDR-Außenministerium. 1986 begann er, die Lohnbuchhaltungen in DDR-Botschaften zu computerisieren. Die Innovation bereitete den Geheimdienstlern des Arbeiter-und-Bauern-Staates große Probleme, denn die Streusignale der Robotron-PC 1715 und 1834 konnten die eigenen Meßtrupps noch in 1800 bis 2000 Meter Entfernung registrieren – ein Geschenk für den Klassenfeind.

„Die Computer galten als äußerst unsicher", erinnert sich Wolf, „das MfS forderte von uns, daß wir entweder die gesamte Buchhaltung mit umständlichen Codesystemen führten oder die Räume, in denen die Rechner standen, mit Metallfolien und Drahtgeflechten gegen Abstrahlung abschirmten."

Die Faraday-Käfige, die die Botschaftsangehörigen im Do-it-yourself-Verfahren improvisierten, waren oft fensterlose stickige Zellen von wenigen Quadratmetern Grundfläche. Solch beschwerliche Arbeitsverhältnisse brachten Wolf auf die Idee einer eleganteren elektronischen Lösung. Zudem ist der kleine Störsender wesentlich billiger als die aufwendige Tempestierung.

Das BSI hat das Secudat-Gerät im Februar getestet und bescheinigt dem Apparat, er sei „für den Schutz sensitiver, mittels PC-Systemen bearbeiteter Informationen geeignet". Die Zulassung für Verschlußsachen nach Behördenstandard jedoch verweigert das Amt. Die Gründe sind wie immer geheim. So bleibt nur die Spekulation, ob die Einstufung formalen Kriterien folgt, die keine andere Schutzmaßnahme außer der Abschirmung vorsehen, oder ob das heimliche Gewerbe nicht vielleicht über Methoden verfügt, die im Labor normalsterblicher Elektrotechniker fehlen.

Spionagetechnik zu entwickeln gehört nicht zu den offiziellen Aufgaben der Bonner Behörde, wohl aber die „Entwicklung von Verfahren und Werkzeugen für die Prüfung" der Abhörsicherheit.

Im Rahmen dieser Forschungstätigkeit entstand offenbar auch das „KOR5". Dieses Gerät wird von der Bosch-Tochter ANT vertrieben. Es dient zur „Feststellung und Eingrenzung kompromittierender Abstrahlung", so der Firmenprospekt, „wo sich sein Vorgängermodell schon vielfach bewährt hat und wofür es nach wie vor konkurrenzlos ist".

Das Gerät kann durch „Kreuzkorrelation" verräterische Signale selbst aus einem eine Million mal stärkeren Rauschen heraushören. Um die streunenden Botschaften wieder lesbar zu machen, wäre nur ein simpler Zusatz nötig. Die zugrunde liegende Technik ist mit den Patenten DE 4301701 C1 und DE 3911155 C2 geschützt. Gemeinsame Erfinder sind drei Diplomingenieure – Beschäftigte der ANT und des BSI.

Die Datenwelt ist heute der Kampfplatz für das Kräftemessen der Geheim-

dienste. Die amerikanische NSA betreibt sogar eine eigene Chipfabrik, um jederzeit über Bauteile aus absolut vertrauenswürdiger Quelle für ihre geheimnisvollen Rechner zu verfügen.

In der Szene gilt als sicher, daß die Elektronikspezialisten in diesen Fabriken aber auch Schaltkreise herstellen, die – in Aussehen und Funktion nicht von den Originalen zu unterscheiden – in die Hardware gegnerischer Computernutzer eingeschmuggelt werden. Solche Digitalwanzen könnten in unbewachten Momenten interne Daten per Funk aussenden oder auf ein Signal von außen den eventuell strategisch wichtigen Rechner lahmlegen.

Diese Möglichkeiten bereiteten den Verantwortlichen des DDR-Ministeriums für Staatssicherheit (MfS) seinerzeit erhebliche Sorgen. Sie konnten sich nie sicher sein, was ihnen westliche Computer möglicherweise an solchem elektronischen Kroppzeug ins Haus schleppten. Denn trotz Embargo schafften zahlreiche kleine Schieber auf zum Teil abenteuerlichen Wegen begehrte Rechner, etwa des Typs Vax der US-Firma DEC, in die DDR.

Die Hauptabteilung XVIII zum Beispiel meldete im Januar 1988 in einem internen Bericht stolz die erfolgreiche Installation eines Convex-Großrechners im Wert von 5,7 Millionen Dollar, geliefert über „die bewährte Embargolieferlinie Sunny“.

Konnten sich die westlichen Dienste diese Chance zum elektronischen Schnüffeln entgehen lassen? Horst Männchen, bis 1989 Chef der MfS-Hauptabteilung III und zuständig für die Funkabwehr, erinnert sich an die Beunruhigung.

„Wir haben unsere Rechner auseinandergenommen und alle Bauteile mit den Originalschaltplänen verglichen“, verrät er heute. „Wir bekamen laufend Warnungen des KGB über drahtlose Abhörvorrichtungen in Computern, aber wir haben bei unseren Messungen nie etwas gefunden.“

Männchen hatte allen Grund zur Vorsicht, denn – kaum zu glauben – seit etwa 1986 stand in der Datenverarbeitungszentrale des MfS-Hauptquartiers Normannenstraße ein Siemens-Rechner. Der Oberbeschaffer Alexander Schalck-Golodkowski, dessen Kommerzielle Koordinierung über die Intrac GmbH intensive Geschäftsbeziehungen zum Münchner Elektronikkonzern pflegte, brachte die Hardware ins Land.

Der 1,5 Millionen Mark teure Rechner, so gab Schalck später bei seiner Vernehmung an, sei „nach den Ordnungsprinzipien der Siemens AG legal geliefert und eingesetzt worden“.

„Natürlich haben wir uns gefragt, warum bekommen wir diese Rechner“, berichtet Männchen. In der Abteilung XIII, der „zentralen Rechenstation“ des MfS in Berlin-Köpenick, gingen gar regelmäßig Siemens-Techniker ein und aus. „Zwei- bis dreimal pro Jahr“ seien die westlichen Wartungstrupps angerückt.

Schwer vorstellbar, daß kein westlicher Geheimdienst davon wußte und niemand seine elektronischen Finger nach den Datenbeständen ausstreckte. Für Männchen war die argwöhnisch beäugte West-Hardware dennoch das kleinere Übel: „Unsere Robotron-Rechner waren ja eher Sendeanlagen als Computer. Selbst mit einer doppelten Abschirmung haben wir die kaum dicht bekommen.“

BPK

„Enigma“-Chiffrierer im Zweiten Weltkrieg*
Kräftemessen der Geheimdienste

Auch in geschlossene Räume reicht das Ohr der elektronischen Lauscher. Dabei müssen sie heute nicht einmal mehr heimlich durchs Gebäude schleichen, um etwa Wanzen zu verstecken. Viel bequemer ist es, die modernen Telefone zum Komplizen zu machen.

Längst stehen in den Telefonanlagen von Behörden und Firmen keine Schaltschränke mehr, in denen Relais und motorgetriebene Wählgeräte die Verbindungen herstellen. Digitale Nebenstellenanlagen sind Computer. Schon im Apparat auf dem Schreibtisch steckt ein Rechner, er verwandelt die Sprache in einen Datenstrom, dessen Weg durch das Telefonnetz durch ein Ensemble von Vermittlungscomputern bestimmt wird.

Die Kontrolle über diese Anlagen übt eine hochkomplexe Software mit Millionen von Programmzeilen aus. Immer neue „Leistungsmerkmale“, die den Telefonkomfort steigern sollen, denken sich die Hersteller aus. Die auf individuelle Firmenbedürfnisse zugeschnittenen Software-Varianten wechseln oft sogar mehrmals im Jahr.

„In diesen Programmen findet sich ein Wust von Zusatzfunktionen, die in früheren Versionen benutzt wurden oder später einmal integriert werden sollen“, stellte der Frankfurter Sicherheitsberater Klaus-Dieter Matschke bei der Untersuchung von ISDN-Systemen fest und mahnt: „Der Schutz vor Software-

ADN / BUNDESARCHIV KOBLENZ

PC-Fertigung bei Robotron (1986): Geschenk für den Klassenfeind

* Mit Panzergeneral Heinz Guderian in Frankreich, 1940.

mißbrauch spielt offenbar kaum eine Rolle."

„Die Software von Telefonanlagen enthält in der Regel auch Funktionen, die in Deutschland verboten sind, etwa zum unbemerkten Mithören", warnt Olaf Erber vom BSI.

Solche Überwachungsmöglichkeiten gehörten in manchen Ländern zu den Exportschlagern. Zwar seien diese unappetitlichen Features in der deutschen Installation abgeschaltet, in den Tiefen der Systeme könne ein findiger Hacker diese Funktionen jedoch wieder aktivieren und sich unbemerkt in beliebige Gespräche einklinken.

Die „Dreierkonferenz" zum Beispiel gehört zum Standard der Komfortanlagen. Ein Eindringling muß nur herausfinden, wie man den Warnton unterdrückt, der das Einschalten signalisiert. In den USA, so Erber, verursachen Telefonhacker jährlich Schäden von zwei Milliarden Dollar, indem sie trotz aller Abwehrmaßnahmen Nebenstellenanlagen mißbrauchen, um auf Kosten des Unternehmens zu telefonieren.

Wer das System so weit überlistet, so fürchten Experten, findet auch Wege, Gesprächsdaten abzuzapfen oder mit den praktischerweise integrierten Freisprechmikrofonen der Telefonapparate komplette Büros abzuhören.

„Wenn wir Schweizer Bankauszüge verlangten, bekamen wir sie"

Auf digitalem Weg findet sich so mancher heimliche Zugang, an wohlgehütete Geheimnisse zu kommen. Wenn es die weltumspannenden Datennetze nicht schon gäbe, ein Geheimdienst müßte sie erfinden.

Das gekonnt bediente Computerterminal liefert die gewünschten Informationen viel bequemer als Dietrich und Brechstange. Als sich die Regierung des US-Präsidenten Reagan Anfang der achtziger Jahre den Kampf gegen Korruption und Drogen auf die Fahne schrieb, wurde die aggressive Recherche in fremden Datenschätzen zum zentralen Hilfsmittel.

Norman Bailey, Reagans Direktor für die Sicherheitsplanung im Weißen Haus, gab die Direktive „Follow the money" aus. Wer den Weg schmutziger Gelder durch das Bankensystem verfolgen kann, findet auch die Hintermänner. „Ich war erstaunt, daß noch niemand auf die Idee gekommen war, die Zahlungen zu verfolgen. Wir fingen an, diese Suche systematisch zu betreiben", erläutert Bailey und räumt ein, daß „neben menschlichen Quellen die elektronische Aufklärung eine wichtige Rolle spielte".

„Ich habe mich nie für die Methoden interessiert, aber wenn wir über eine Finanztransaktion Bescheid wissen wollten, hat die NSA uns präzise Daten geliefert", so ein ehemaliges Mitglied der Reagan-Regierung. „Wenn wir Schweizer Bankauszüge verlangten, haben wir sie von dem Dienst auch bekommen."

Diese Unterwanderung sei nicht so schwer gewesen, denn der elektronische internationale Zahlungsverkehr konzentriere sich auf eine Handvoll Abrechnungsstellen, sogenannte Clearinghouses. Diese strategischen Knotenpunkte habe die NSA planmäßig angezapft.

Doch wie kann der US-Geheimdienst so scheinbar mühelos in die Datenfestungen eindringen? Experten vermuten, daß es der NSA über ein Netz von Tarnfirmen gelungen ist, heimliche Hintertüren in der Bankensoftware zu verstecken. Über diese verborgenen Einlässe öffnen sich den Lauschern Wege, die an den elektronischen Burgwächtern vorbeiführen.

Eine zentrale Rolle in den Rochaden der amerikanischen Dienste spielt ein Softwarepaket namens Promis. Das „Prosecutors Management Information System", ein Datenmanagementsystem für Strafverfolger, wurde von dem ehemaligen NSA-Mitarbeiter Bill Hamilton konzipiert. Seit 1969 befaßte er sich mit der Software – zunächst mit staatlichen Forschungsgeldern. Schließlich wurde Promis das Hauptprodukt der von ihm gegründeten Firma Inslaw.

Hamilton baute das Datenbankprogramm zu einer universellen Spürmaschine aus. Durch geniale Algorithmen ist Promis in der Lage, nach Art einer Rasterfahndung in kurzer Zeit Daten aus verschiedensten Quellen zusammenzupuzzeln. So können Ermittlungsbehörden etwa die Informationen von Telefongesellschaften, Kreditkartenunternehmen, Finanzämtern und Polizeibehörden miteinander verknüpfen, um Verdächtige aufzuspüren.

Promis wurde zur Standardsoftware an amerikanischen Gerichten zur Verwaltung von Prozeßkarteien. Das System war jedoch so vielseitig, daß Inslaw es mit geringen Änderungen auch an Versicherungen oder Steuerbehörden verkaufen konnte. 1983 war Hamilton gut im Geschäft: Seine Firma unterhielt die Rechenzentren der zehn größten US-Strafverfolgungsbehörden. Im April lieferte er eine Spezialversion von Promis an das Justizministerium in Washington.

Doch von einem Tag auf den anderen fiel Hamilton in Ungnade: Das Justizministerium war mit der Software angeblich nicht zufrieden und verweigerte die Bezahlung der lukrativen Serviceverträge. Mit immer neuen bürokratischen Schikanen trieb das Ministerium Inslaw an den Rand des Bankrotts.

Das Justizministerium habe die Software Promis durch „üble Tricks, Täu-

to AG im August 1975 anläßlich der Demonstration eines neuen Chiffriergerät-Prototypen nennt als Teilnehmer die NSA-Kryptologin Nora Mackebee.

Bob Newman, ein Ingenieur des Chipherstellers Motorola, mit dem Crypto in den siebziger Jahren bei der Entwicklung einer neuen Generation von elektronischen Verschlüsselungsmaschinen kooperierte, kennt Mackebee gut. Ihm wurde die Frau als „Beraterin“ vorgestellt.

„Die Leute kannten sich gut aus in Zug und haben den Motorola-Leuten Reisetips für den Besuch bei der Crypto AG gegeben“, berichtet Newman. Auch Polzer erinnert sich an die amerikanische „Aufpasserin“, die nachdrücklich die Verwendung bestimmter Verschlüsselungsverfahren forderte.

Je nach Einsatzgebiet seien die Manipulationen an den Schutzgeräten mehr oder weniger subtil gewesen, berichtet Polzer. Manchen Abnehmern sei schlicht abgemagerte Codetechnik verkauft worden, nach dem Motto „für diesen Kunden genügt das, der braucht nicht so was Gutes“.

In heikleren Fällen hätten die Spezialisten tief in die kryptologische Trickkiste gegriffen: Die so präparierten Maschinen hätten dem verschlüsselten Text „Hilfsinformationen“ beigefügt, mit denen all jene, die Bescheid wußten, den ursprünglichen Schlüssel rekonstruieren konnten. Das Ergebnis war stets dasselbe: Was für den gutgläubigen Benutzer der Crypto-Maschinen wie ein undurchdringlicher Geheimcode aussah, war für die eingeweihten Lauscher mit kaum mehr als einer Fingerübung wieder lesbar zu machen.

Die Crypto AG bezeichnet solche Berichte empört als „altes Hörensagen“ und „reine Erfindung“. Doch ein Prozeß, den die Firma gegen ihren Ex-Angestellten Bühler anstrengte, weil dieser geäußert hatte, an dem Verdacht seiner iranischen Vernehmer sei möglicherweise etwas dran gewesen, fand im November letzten Jahres ein überraschendes Ende.

Noch vor der Verhandlung, in der womöglich peinliche Details ans Licht gekommen wären, stimmte die Firma einem außergerichtlichen Vergleich zu. Seitdem schweigt Bühler eisern zu dem Fall. „Der hat wohl finanziell ausgesorgt“, vermutet ein Szenekenner.

„In der Branche weiß doch jeder, wie das läuft“, meint Bühlers Ex-Kollege Polzer. „Natürlich schützen solche Geräte davor, daß unbefugte Dritte mithören, wie es im Prospekt steht. Die interessante Frage ist aber doch: Wer ist der befugte Vierte?“

G. MATHIESON / MAI

Horchposten der NSA: Angriff auf strategische Knotenpunkte des Geldverkehrs

schung und Betrug gestohlen“, urteilte Richter George Bason vier Jahre später in einem Prozeß gegen Hamiltons einstige Auftraggeber. Die juristischen Auseinandersetzungen um Schadensersatz dauern bis heute an.

Warum stiehlt eine Bundesbehörde Software? Offenbar hatten Hamiltons ehemalige Kollegen von der NSA ein Auge auf das Superprogramm geworfen und Bedarf im Namen der nationalen Sicherheit angemeldet. Mehrere Zeugen bestätigten vor einem Inslaw-Untersuchungsausschuß, daß Promis nach dem Raubzug bei Hamilton in der Geheimdienstszene auftauchte. Dort versahen es Programmierer mit geheimen Zugängen, sogenannten Trap Doors, durch die

Durch geheime Zugänge vorbei an den Burgwächtern

NSA-Schattenmänner jederzeit unbemerkt in Promis-Datenbanken eindringen konnten.

Die NSA habe gezinkte Promis-Versionen in den folgenden Jahren an Behörden in aller Welt verteilt, so die Informanten. Offenbar paßte der Inslaw-Coup auch Reagans Finanzdatenjägern exakt ins Konzept: Im Herbst 1983, nachdem Inslaw außer Gefecht gesetzt war, tauchte Promis plötzlich in der Washingtoner Weltbankzentrale auf. Das bezeugt Stephen McCallum, der seinerzeit bei der Servicefirma Control Data beschäftigt war. Die Firma war damit beauftragt, ein damals frisch eingerichtetes System von Vax-Rechnern zu warten.

Auf diesen Rechnern wurde gerade Promis installiert, und zwar, so McCallum, „als Kernstück eines Nachrichtensystems, das Daten sammelte und an die Mitgliedsbanken weiterverteilte“.

Den Nachrichtenknoten unterhielt die Weltbankabteilung für Entwicklung und Wiederaufbau – ein lohnendes Ziel für Reagans Sonderermittler, die den Verdacht hegten, korrupte Politiker in Drittweltstaaten würden Hilfsgelder auf private Konten umleiten.

Eine Unterwanderung der Weltbank-Datenzentrale könnte der gelungene Auftakt für den Einbruch in die Datenschätze der Geldwelt gewesen sein. William Casey, seinerzeit CIA-Chef und Gebieter über alle US-Geheimdienste, rühmte sich später, einer seiner größten Erfolge sei „die Penetration des internationalen Bankensystems“ gewesen.

Soviel elektronische Raffinesse ist jedoch nur selten erforderlich. Die meisten Informationen liegen offen auf den Datenstraßen herum. Wer heute eine elektronische Nachricht durch eines der großen Online-Systeme oder Internet verschickt, kann fast sicher sein, daß die NSA bei Interesse einen Blick darauf wirft.

Die Wege der Datenpakete im Internet sind unergründlich. Die Vermittlungsrechner im Netz, sogenannte Router, wählen nicht nach Art des Telefonnetzes eine direkte Verbindung zwischen Sender und Empfänger, sondern suchen für jedes eingehende Datenpaket die aktuell am wenigsten verstopfte oder die für den Betreiber billigste Reiseroute für den Sprung zum nächsten Netzknoten. Nach diesem Prinzip ist es durchaus nicht ungewöhnlich, daß Nachrichten von Krefeld nach Winsen über New York reisen.

Wayne Madsen, Koautor einer aktualisierten Version des NSA-Klassikers „The Puzzle Palace“, glaubt, daß sich die Lauscher längst Abzweigungen zu den Hauptstraßen des Internet gebaut haben. Die großen Knotenpunkte mit Namen wie „Fix East“ oder „Mae West“, die immense Datenströme kanalisieren, seien

angezapft. „Seit etwa drei Jahren sind Techniker damit beschäftigt, im Auftrag der NSA in die Software der Vermittlungsrechner zusätzliche Programme einzubauen, die Datenpakete je nach ihrem Ursprungs- und Zielort ausfiltern und zur Auswertung abzweigen“, beschreibt Madsen das Verfahren.

Der amerikanische Supergeheimdienst für elektronische Aufklärung, zu dessen knapp 40 000 Bediensteten die Elite der Codeknacker gehört, will sich dieses Geschäft nicht vermiesen lassen und versucht seit Jahren zu verhindern, daß sich Verschlüsselungsverfahren verbreiten, die er nicht entwirren könnte.

Bislang mit Erfolg: Die amerikanischen Exportgesetze behandeln Verschlüsselungstechnik oberhalb einer bestimmten Güte als „Waffen“, deren Ausfuhr verboten ist. Wie gefährlich diese Waffe ist, richtet sich nach der Komplexität der verwendeten Schlüssel, gemessen an der Anzahl der Stellen der Schlüsselzahl, ausgedrückt in Bit.

Mehr als 40 Bit dürfen es nach dem Willen der NSA nicht sein. Das ist vermutlich die Grenze, bis zu der die Großrechner des Geheimdienstes den Buchstabensalat durch heftiges Herumprobieren noch bequem entziffern können. Jedes weitere Bit verlängert die Suchzeit; Schlüsselbandwürmer von mehreren hundert Bit würden die Computer bis zum Ende des Universums rattern lassen.

Ein Drogendealer frustrierte die Telefonfahnder

Die Anhänger der Kryptokontrolle werden nicht müde zu betonen, wie wichtig der Zugriff des Staates auf die Daten sei. „Der unkontrollierte Gebrauch von Kryptografie durch Kriminelle und Terroristen stellt ein unakzeptables Risiko dar“, erklärte FBI-Direktor Louis Freeh letzten Monat vor einem Senatsausschuß.

Er hatte auch gleich Beispiele parat: Ein Mann, der wegen der Planung von Anschlägen auf Flugzeuge vor Gericht stehe, habe auf seinem Computer verschlüsselte Daten verwahrt, die das FBI bisher nicht knacken konnte. Ein mutmaßlicher Drogendealer habe durch ein Sprachverschlüsselungsgerät die Fahnder frustriert, die sein Telefon abhörten.

FBI-Chef Freeh und die Geheimdienste geraten mit ihrer harten Haltung immer mehr in die Defensive. An die Proteste von US-Bürgerrechtlern, die in der Datenverschlüsselung einen Bestandteil ihrer verfassungsmäßig garantierten Privatsphäre sehen, haben sie sich schon gewöhnt. Nun aber machen auch die Vertreter der Softwareindustrie Druck, deren Kunden endlich ihre Geschäftsgeheimnisse auf dem Weg durch die Datennetze wirksam vor Industriespionen schützen wollen.

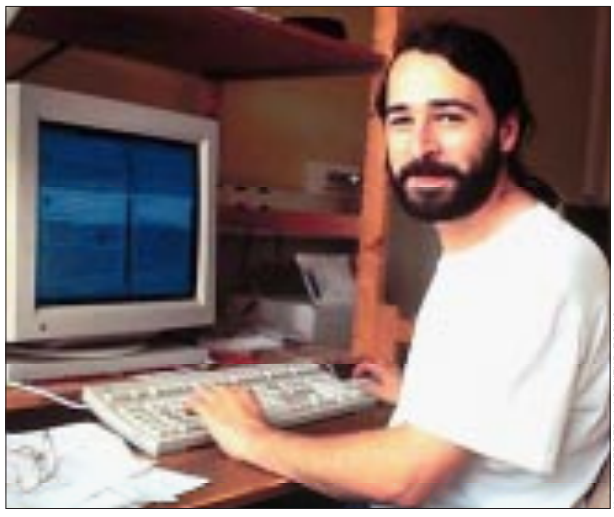
Steuerzentrale der AT&T-Telefonnetze: Die Wege der Datenpakete im weltweiten Netz

Die Exportbeschränkungen hätten bislang vor allem einen Effekt gehabt: Die Hersteller von Kommunikationsprogrammen ließen lieber gleich ganz die Finger von Verschlüsselungsmethoden, weil es viel zu umständlich sei, getrennte Versionen für In- und Ausland zu entwickeln und etwaige Gesetzeskonflikte zu riskieren, wenn die falsche Version in die falschen Hände fällt.

Die Firma Lotus hatte Anfang des Jahres den Balanceakt gewagt und eine Sonderregelung mit der NSA ausgehandelt. Das Programm Notes schützt die elektronische Korrespondenz serienmäßig mit einem 64 Bit langen Schlüssel.

In der Exportversion, dazu verpflichteten sich die Lotus-Manager, werden nun 24 Bit dieses Schlüssels mit einem Sonderschlüssel geschützt, wenn die geheime Nachricht übermittelt wird. Ein Nachschlüssel gibt der NSA den Zugriff auf diese 24 Extrabit, so daß der Geheimdienst sich bei Bedarf nur noch mit dem Brechen des 40 Bit langen Schlüssels abzugeben braucht.

Der normale Untergrundhacker ohne Nachschlüssel, so versicherte Lotus, rackere sich an dem hochsicheren 64-Bit-Code nach wie vor vergebens ab. Doch trotz aller Beteuerungen bleibt bei den nichtamerikanischen Notes-Kunden das Gefühl, sie seien mit zweitklassigem Schutz abgespeist worden. „Das kann nur eine Zwischenlösung sein“, gibt auch Notes-Entwickler Ray Ozzie zu, „wir wollen, daß sich die Kryptografiegesetze grundlegend ändern.“



H. BAMBERGER / AGENTUR FOCUS

Codeknacker Doligez: Acht Tage lang geknobelt

Auch die Firma Netscape war gezwungen, den Verschlüsselungsmechanismus der populären Internetsoftware Navigator zur Verwendung außerhalb der USA zu verschlechtern. Netscapes Image trug schweren Schaden davon, als der französische Informatikstudent Damien Doligez am 14. Juli letzten Jahres der Internetwelt verkünden konnte, er habe eine mit der Exportversion des Navigators verschlüsselte Nachricht entziffert.

Doligez hatte 120 Computer seiner Universität acht Tage lang knobeln lassen. Geheimdienste, so darf man vermuten, bringen das Kunststück mit Hilfe von

C. PSIHOYOS / MATRIX / AGENTUR FOCUS

sind unergründlich

Superrechnern in einem Bruchteil der Zeit fertig.

Mit dem 128 Bit langen Originalschlüssel, so rechnete Netscape vor, wäre der Firma die Blamage erspart geblieben. Den zu knacken hätte eine Billion mal länger gedauert.

Wie absurd Exportbeschränkungen für Software in einer global vernetzten Welt sind, zeigt eine Regelung, die Netscape Mitte letzten Monats mit den US-Behörden traf: Künftig dürfen sich Computernutzer auch die US-Version des Navigators aus dem Internet auf ihre Festplatte laden. Die Interessenten müssen nur per Mausklick erklären, daß sie amerikanische Staatsbürger sind.

Indes denken sich die professionellen Geheimniskrämer immer neue Varianten aus, wie sie Computerbenutzern zwar ein gewisses Sicherheitsgefühl vermitteln können, aber dennoch die Oberhoheit im Reich der Codes behalten könnten.

1994 versuchte die US-Regierung die Industrie auf den Clipper-Chip, eine NSA-Entwicklung, einzuschwören. Der Schaltkreis, so die frohe Botschaft, ermögliche die Entwicklung preiswerter abhörsicherer Telefone und Modems, ein neuer Massenmarkt tue sich auf.

Mit einer unwesentlichen Einschränkung: Eine noch einzurichtende Behörde werde Nachschlüssel zu jedem Chip verwalten und sie auf berechtigtes Verlangen an Strafverfolger aushändigen.

Für diese Art von Sicherheit sahen die Firmen jedoch keine Marktchancen, und der Clipper verschwand wieder in den Schubladen. Als jüngsten Kompromißvorschlag bietet die US-Regierung an, die Reglementierungen zu lockern, wenn sich die Hersteller von Software einer konzertierten Aktion zur Schlüsselverwaltung anschließen. „Vertrauenswürdige Dritte“ sollten künftig die Codezahlen verwahren.

Programmiererin Machado
Papstporträt oder Bombenrezept?

Auch dieser Vorschlag stößt bislang auf wenig Gegenliebe. Eine Horrorvision der Geheimdienste wird wahr: Die Pandora-Büchse der Kryptografie steht weit offen. Zentrales Haßobjekt der Spione ist der amerikanische Informatiker Phil Zimmermann, Erfinder des Verschlüsselungsprogramms PGP. Sein Credo lautet: „Geheimnisse gegenüber dem Staat zu haben, gehört zur Demokratie“ (siehe Interview Seite 200).

Im Handumdrehen verbreitete sich Zimmermanns Programm per Datennetz um die Welt. In fast jedem Land findet sich ein Internet-Server, der „internationale“ PGP-Versionen anbietet.

Drei Jahre lang ermittelten die US-Behörden gegen den Programmierer, der zwangsläufig in den Verdacht geraten war, gegen die Exportgesetze verstoßen zu haben. In einer Solidaritätsaktion sammelte der Zimmermann-Verteidigungs-Fonds Geld für die horrenden Anwaltskosten des Kryptologen. Im Januar schließlich gaben die Strafverfolger auf und stellten das Verfahren ein.

Nachrichten nicht mehr lesen zu können und womöglich ausgerechnet am Beginn des Informationszeitalters aus den globalen Datenbörsen ausgesperrt zu werden, muß bei den Geheimdiensten das Gefühl existentieller Bedrohung auslösen. In Frankreich etwa ist der private Gebrauch von Verschlüsselungstechnik gleich grundsätzlich verboten.

„Es wird bald kaum noch unverschlüsselte Informationen geben“, warnte der damalige BND-Chef Porzner im Februar vergangenen Jahres in einem vertraulichen Brief an Kanzleramtsminister Bohl und forderte, endlich dafür zu sorgen, daß Justiz-, Wirtschafts- und Außenministerium ihren Widerstand gegen eine Reglementierung der Verschlüsselungstechnik aufgeben. „Ein solches Gesetz“, so Porzner, „ist für die Sicherung einer erfolgreichen Erfüllung des Aufklärungsauftrages des Bundesnachrichtendienstes auch in Zukunft dringend erforderlich.“

Das Argument, Verschlüsselungstechnik müsse kontrolliert werden, um kriminellen Aktivitäten auf die Spur zu kommen, ist den Geheimdiensten längst entglitten. Wer wirklich Übles im Schilde führt, kann sich im Internet inzwischen Programme besorgen, die auch gleich das Vorhandensein jeglicher Nachricht verschleiern.

Die sogenannte Steganografie, in verschiedenen Spielarten schon seit der Antike gebräuchlich, läuft im Computer zu wahrer Höchstform auf. Problemlos kann der Rechner in scheinbar harmlosen Daten durch die Änderung einiger unbedeutender Bit Informationen verstecken, ohne daß ein heimlicher Lauscher mitbekommt, was da an ihm vorbeizieht.

Die Programmiererin Romana Machado, die auch in ihrer Zweitkarriere als Aktmodell recht erfolgreich ist, hat beispielsweise ein subversives Prográmmchen namens Stego entwickelt, das Daten in beliebigen elektronischen Bildern versteckt.

Die geheime Fracht verändert die Helligkeit einzelner Bildpunkte so subtil, daß der Betrachter völlig ahnungslos bleibt, ob das Papstporträt nicht vielleicht in Wirklichkeit eine Anleitung zum Bombenbau ist. ❑