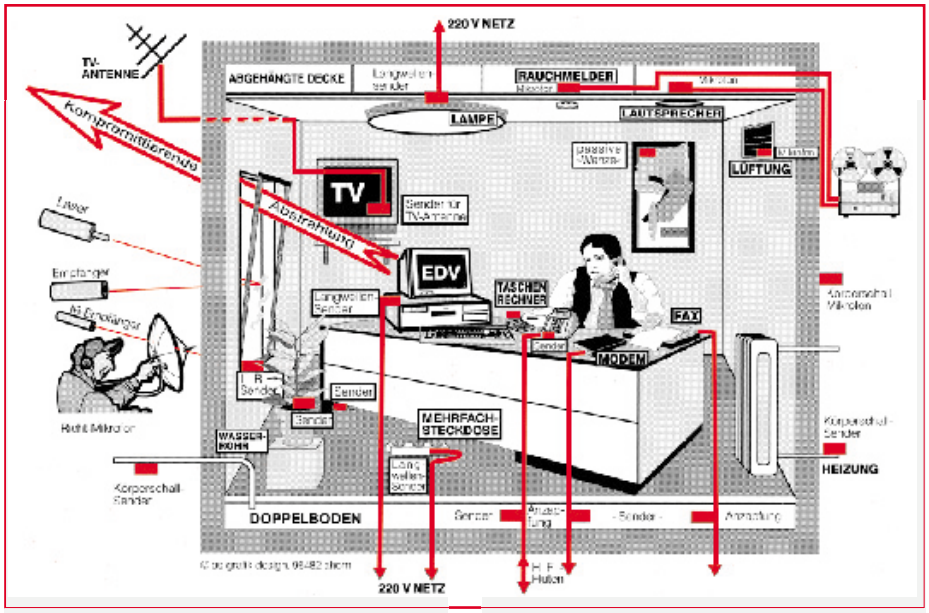

Die High-Tech-Schnüffler - sind wir noch sicher?

Nicht nur in Agentenfilmen wird fleißig spioniert, auch im wahren Leben. Und dies mit zunehmender Intensität, neuerdings zum Teil sogar staatlich sanktioniert.
Im Informationszeitalter können Informationen viel Geld wert sein, egal, ob es sich um Ihre privaten Telefongespräche handelt, Ihre Kontobewegungen oder um das Ausspionieren der neuen Entwicklungen im Betrieb - die Lauscher haben heute elektronische Ohren und sitzen warm daheim am Funkscanner.
Womit gelauscht wird und wie man sich wenigstens teilweise schützen kann, zeigt unser Artikel.

Lauschziel Wirtschaft

Der kalte Krieg ist vorbei, aber die Spione sind beileibe nicht arbeitslos. Im Gegenteil, heute tobt die Schlacht um Informationen. Wer die besitzt, hat gewonnen, wie das Beispiel ICE-Verkauf bzw. Nicht-Verkauf nach Korea recht anschaulich beweist. In diesem Falle hatte man nach Aussagen von Sicherheitsexperten schlichtweg „nur" versäumt, kryptografische Geräte zur Übermittlung der Konditionen einzusetzen, so konnte die Gegenseite wohl alles im Klartext mitlesen.

Die Industrie ist heute der Angriffspunkt Nummer 1 für Spionage, und es wird spioniert, was das Zeug hält, ob vom Satelliten aus oder am nächsten Stromverteiler, jede Information ist verwertbar. Da werden Funktelefone abgehört, ISDN-Leitungen angezapft, Computer über das Stromnetz angezapft und, und...

Jährlich gehen nach Schätzungen der Industrie Milliarden durch Wirtschaftsspionage verloren, ja sogar der Verfassungsschutz geht davon aus, daß ein nennenswerter Teil des Telekommunikationsverkehrs in Deutschland von Dritten illegal überwacht wird. Besonders im internationalen Fernsprechverkehr kann man sehr sicher davon ausgehen, daß die Nachrichtendienste immer „mittendrin" sind.

Neu im Visier - wir alle

Aber auch Lauschangriffe und Ausspionieren von Privatpersonen stehen heute hoch im Kurs. Wir wollen hier gar nicht von dem Interesse einiger Personalmanager nach dem Inhalt der geplanten Krankenversicherungskarte reden, wir hinterlassen auch so schon ausreichend elektronische Spuren im Leben, nach denen viele Leute trachten und eben neuerdings auch der Staat - für Ex-DDR-Bürger werden hier Erinnerungen wach...

Die heutige Überwachung ist jedoch viel perfektionierter als das frühere Spionieren der DDR-Staatssicherheit. Eines der anschaulichsten Beispiele ist das Verlangen des Staates nach dem Deaktivieren der Verschlüsselungsalgorithmen der D-Netz-Funktelefone. Gerade dieses Feature war eines der wichtigsten Werbeargumente der D-Netz-Anbieter, nun durften die mit Millionenaufwand das Ganze zum Teil wieder rückgängig machen, damit der Staat mithören kann. Und wer wird dem glauben, daß er nur die Dealer und Schlepper abhört; es ist auch nur eine Frage der Zeit, daß solcherart geöffneter Zugang auch von der Wirtschaftsspionage genutzt wird.

Wie vielfältig insbesondere in der Industrie spioniert wird, illustriert unsere Titelgrafik sehr anschaulich. Hier werden die Fortschritte der Mikroelektronik konsequent genutzt - leider wieder im negativen Sinne. Die neuen Waffen bestehen aus Silizium.

ISDN - die neue Gefahr?

Die schöne neue Welt von ISDN ist eine feine Sache - solange kein Lauscher in der Leitung sitzt. Insbesondere für Unternehmen können hier einige Gefahren lauern.

Ein ISDN-Telefon ist ja kein herkömmliches Telefon, dessen Technik nur nach Abheben von der Gabel aktiv wird. ISDN-Geräte sind kleine Computer, und die sind unter bestimmten Voraussetzungen bequem von außen steuerbar.

Gerade eines der Features von ISDN-Geräten, die mögliche Fernwartung durch den Hersteller, die bis zum Update der Gerätesoftware von ferne geht, ist schon einigen Unternehmen zum Verhängnis geworden. Und es ist anzunehmen, daß die meisten ISDN-Nutzer gerade in kleineren Unternehmen und im Privatbereich noch gar nichts wissen von der Gefahr, die hier lauert. Denn über den Fernwartungszugriff kann man das Mikrofon des Apparates freischalten, ohne daß das Gerät auch nur einen Piep von sich gibt. Es erscheint keine Displayaufschrift, kein verräterisches Knacken - nichts.

Technische Voraussetzung ist lediglich die Kenntnis der Softwarecodes des Telefonherstellers, daß die aufgrund der massenhaften Verbreitung der Technik nicht lange „top secret" bleiben, ist wohl zu denken. Und daß solch ein Zugriff tatsäch-

Bild 1: Verschlüsselung heißt das Zauberwort zum Schutz von Telekommunikationswegen vor Abhören. Hier ein Verschlüsselungsgerät für ISDN, einsetzbar vom Telefondienst bis zur Videokonferenz oder zum Versand von Computerdaten. (Foto: SIEMENS AG)

lich gelingt, bewiesen die Techniker des Datenschutzunternehmens „Biodata" im hessischen Burg Lichtenfels Anfang des Jahres im ZDF vor laufender Kamera („Mit mir nicht", Welsers Fälle). Dort wurde anschaulich demonstriert, wie man zum einen unbemerkt in die Telefonzentrale eines entfernten Unternehmens eindringen und deren Software manipulieren kann und zum anderen ebenso unbemerkt auf Kosten des anderen Teilnehmers telefonieren kann - alles über die Fernwartungsfunktion der ISDN-Telefone. Auch das Abhören einer Konferenz und das Auslesen der Nummern, die das entfernte Unternehmen selbst anruft, wurden demonstriert, dies funktionierte sogar von einem Handy aus.

Die meisten Hersteller von ISDN-Anlagen schweigen sich über dieses Thema ebenso aus wie die Telekom, deren Werbespot „alles ist möglich" so neue Bedeutung bekommt. Besonders verwerflich ist hier die fehlende Kundeninformation seitens einiger Hersteller von Anlagen, denn die meisten Kunden ahnen nichts von den „neuen Möglichkeiten" ihrer Anlage und können so auch nicht eine mögliche Gegenmaßnahme ergreifen: die Abschaltung bzw. Sperrung der Fernwartungsfunktion. Wollen Sie ganz sicher gehen, schalten Sie bei Ihrem ISDN-Telefon auch die programmierbare Möglichkeit der Raumüberwachung von ferne ab, dies gilt auch für einige Anrufbeantworter.

Laut Telekom soll ein solches Eindringen nur in private ISDN-Nebenstellenanlagen möglich sein, das einzelne ISDN-Telefon im Privathaushalt wäre nicht angreifbar. Eine solche Aussage kann man glauben, aber angesichts der ungeheuren Funktionsvielfalt der umfangreichen Programmierbarkeit der neuesten Telefongeneration könnten vielleicht aber doch Zweifel auftauchen. Analoge Endgeräte innerhalb von ISDN-Nebenstellenanlagen sind auf diesem Wege nicht manipulierbar.

Leider bietet der graue Markt schon komplette Gerätekonfigurationen für den Angriff auf ISDN an, die für einige tausend Mark alle bei o. g. Test genannten Angriffsmöglichkeiten realisieren.

Der sicherste Abhörschutz für ISDN-Anlagen wird durch Verschlüsselungsgeräte (Abbildung 1) geboten, die zwar teuer sind, aber dieses Geld allemal wert, wenn man an die möglichen Verluste durch Abhören denkt.

Aber nicht nur ISDN-Telefone sind von Lauschangriffen betroffen, auch unsere inzwischen allgegenwärtigen Funktelefone nach CT1-und DECT-Standard sind keinesfalls sicher vor dem Abhören. CT1-Telefone machen dies sogar besonders leicht, denn ein einfacher Funkscanner aus dem Elektronikhandel genügt bereits, Gespräche ungestört zu belauschen.

Aber auch DECT ist nicht mehr sicher trotz Frequenzhopping und Sprachverschleierung. Die einheitliche Luftschnittstelle GAP ist hier der Angriffspunkt. Mit entsprechender Empfangstechnik, die GAP „versteht", sind auch DECT-Apparate, wenn auch mit hohem technischem Aufwand, abhörbar.

Immer hinterher

Haben Sie ein Handy? Dann haben Sie es zumindest bei beruflichen Fahrten wohl auch immer eingeschaltet. Und genau das ist für Schnüffler genauso interessant wie das Abhören der damit geführten Gespräche.

Ein Handy „hangelt" sich bei Bewegung durch An- und Abmelden automatisch von Funkzelle zu Funkzelle. Diese Funkzellen sind nicht sehr groß, die Vermittlungssysteme arbeiten computergestützt und speichern so auch über eine gewisse Zeit, vor allem aus statistischen Zwecken, wer wann welche Funkzellen passiert hat. Damit ist bequem ein komplettes Bewegungsprofil des Handy-Besitzers erstellbar, und es ist wieder nur eine Frage der Zeit, daß auch andere als die staatlichen Schnüffler Zugriff auf diese Daten haben. Denn wer mag heute schon den Versicherungen irgendeines Dienstleisters glauben, daß Ihre Daten bei ihm sicher sind.

Am Rande in diesem Zusammenhang bemerkt, man male sich nur aus, was uns in Zukunft blüht, wenn das digitale Fernsehen kommt. Hier geben wir unsere Vorlieben, Neigungen und Konsumgewohnheiten direkt über das Kabel an die Sendezentrale weiter, die dann diese schon computerlesbaren Daten beliebig weiterverwerten kann, vor allem für Marketingzwecke und zur Erstellung von Persönlichkeitsprofilen. Doch das nur, um zu illustrieren, wie weit wir schon elektronische Spuen hinterlassen.

Um auf das Thema Handy zurückzukommen, von außen ist einem digitalen Funknetz kaum beizukommen, der Rechenaufwand zur Ermittlung der aktuellen Funkzelle wäre zu groß, zumal auch von Zelle zu Zelle je nach freier Frequenz eine ebensolche für das Handy gewählt wird.

Der elektronische Lauschangriff gilt dennoch schwerpunktmäßig den Unternehmen. Denn die Informationen über die Vorhaben der Konkurrenz sind Geld wert, da scheut man keine Mühen. Kein Büro ist vor dem Lauschangriff sicher (siehe Titelgrafik).

Lauschangriff über alle Wege

Da kommt auch heute noch die traditio

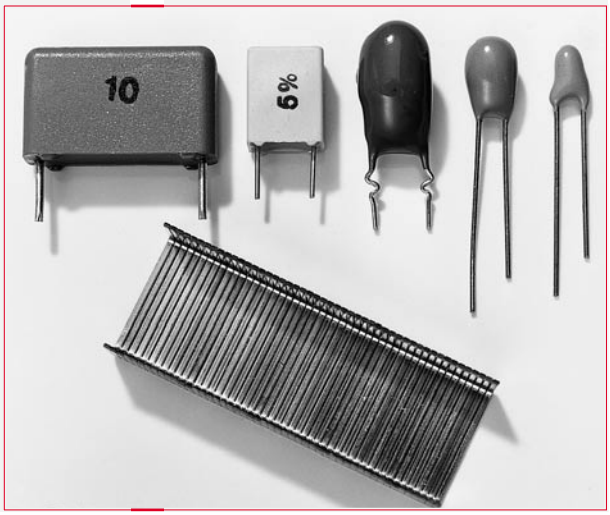

Bild 2: Sehen aus wie ein Kondensatorsortiment - moderne Wanzen zum Einbau in elektronische Geräte (Foto: Fink Security Consulting)

Bild 3: Professionelles Werkzeug für das Wanzen-„Sweeping" - der Cerberus-Nahfeld-empfänger mit zugehöriger Computer-Auswertesoftware (Foto: Fink Security Consulting)

nelle Wanze in Heerscharen zum Einsatz, ein Mini-Sender mit eingebautem hochempfindlichem Mikrofon. Diese werden immer kleiner, langlebiger und leistungsfähiger und sind z. B. von normalen elektronischen Bauelementen nicht zu unterscheiden. So kann es sein, daß dem Unternehmen schon beim Kauf einer Telefonanlage mit jedem Telefon eine Wanze mitgeliefert wird, die sich als harmloser Kondensator auf der Platine tarnt und Ihre Betriebsspannung direkt aus dem Gerät bezieht (Abbildung 2).

Auch mit Solarzellen versehene, vom Wasser im regelmäßig gegossenen Blumentopf versorgte und mit eigener Stromversorgung arbeitende Wanzen sind in den verschiedensten Bauformen gang und gäbe und für den Laien überhaupt nicht als solche zu erkennen. Die Wanzen sind ohne großen, professionell geplanten Aufwand kaum zu finden, sie sind heute schon für ein paar Mark bei Spezialversendern zu haben.

Das Auffinden durch Spezialfirmen ist teuer, langwierig und von hohem technischen Aufwand begleitet. Dazu werden spezielle Nahfeld-Empfänger wie der bei Security-Firmen beliebte „Cerberus-2" (Abbildung 3) eingesetzt, die bereits im Rechnerverbund für Langzeit- und Spezialauswertungen arbeiten. Solche Nahfeldempfänger, die beim „Sweeping" genannten professionellen Aufspüren von Wanzen bereits sehr erfolgreich sind, sind auch entsprechend teuer. Sie kosten schnell mehrere zehntausend Mark und sind so den Profis vorbehalten, denen man die Suche nach Wanzen auch überlassen sollte.

Um eine gefundene Wanze über ihre eventuell noch vorhandene Aktivität zu untersuchen, gibt es preiswertere Nahfeld-Frequenzzähler, die vor allem zum Aufspüren der Sendefrequenz der Wanze dienen (Abbildung 4). Diese sind bereits für unter 1000 DM erhältlich.

Von Lasern und großen Ohren

Es braucht gar nicht sooo kompliziert zu sein, einen Raum abzuhören. Immer noch beliebt ist das Abhören per extrem bündelndem Richtmikrofon. Hier sind in geeigneter Umgebung Abhörentfernungen bis zu 1000 m möglich. Solche Technik kommt darum vorwiegend im Freien zum Einsatz, wenn an die überwachten Personen nicht anders heranzukommen ist.

Viel zeitgemäßer und interessanter ist das Abhören über die Fensterscheibe (siehe Titelgrafik). Dabei wird diese mit einem konstanten Laserstrahl angestrahlt und der reflektierte Strahl durch einen Empfänger ausgewertet. Eine Glasscheibe wirkt wie eine Mikrofonmembrane, sie schwingt im Takt des Schalldrucks, der durch Geräusche, Sprache und Laute entsteht. Dieses Schwingen ist optisch nicht sichtbar und auch mechanisch kaum auswertbar. Der Laserstrahl dagegen wird durch das feine Schwingen der Scheibe moduliert.

Strahlende Elektronik

Das derzeit wohl in fast allen Unternehmen dunkelste Kapitel in puncto Datensicherheit ist die Vernachlässigung der kompromittierenden Abstrahlung. Was heißt das?

Jedes elektronische Gerät, das Daten verarbeitet, transportiert oder intern Schwingungen erzeugt, muß dies über Leitungen und Kabel tun - und wenn es nur die Leitung vom Taschenrechnerprozessor zu dessen Display ist. Selbst auf Netzkabeln sind auch in größerer Entfernung zum Gerät noch die Datenströme nachweisbar. Nachweisbar heißt dann auch lesbar (zumindest teilweise). Durch Spezialantennenanordnungen in Nebenräumen oder außerhalb des Gebäudes ist der Lauscher in der Lage, Bildschirminhalte oder die Ausdrucke des Bürocomputers zu empfangen. Das Problem liegt zum einen in der Überkopplung der Bussignale auf die Netzteile bzw. Netzkabel der Geräte und zum anderen in der Abstrahlung der Bildschirmkabel bzw. Monitore.

Ein Lauscher muß sich im letzteren Falle nur die Frequenz des Taktes der Bildschirmkarte suchen, dazu die passende Synchronisierung finden, und schon kann er, unter Umständen sogar über die Oberwellen des Pixeltakts, das Bild decodieren - und das gleich online auf den Videorecorder!

Auch die Abstrahlung der Videokarte selbst bei ungenügend abgeschirmtem Computergehäuse und die Abstrahlung der Datenkabel der Schnittstellen sorgen für weithin lesbare Signale. Ein nicht mehrfach geschirmtes Netzwerk- oder Druckerkabel, im Kabelschacht fein parallel zu den Netzkabeln verlegt, läßt den Schnüffler vor Freude in die Hände klatschen.

Selbstversuch gefällig? Versuchen Sie doch einmal, neben einem x-beliebigen Computer störungsfrei eine Funkuhr, einen Funkkopfhörer oder ein Funkthermometer zu betreiben - der Störnebel wird dies, sofern Sie nicht über originales Apple-Equipment oder besonders sorgfältig geschirmte Computergehäuse, Monitore und Kabel verfügen, zu verhindern wissen. Und warum darf in so manchem Haushalt nicht der Rechner laufen, wenn ferngese-

Bild 4: Nahfeld-Frequenzzähler für das Analysieren von Wanzenaktivitäten (Foto: Fink Security Consulting)

Bild 5: Abhörsichere Standleitungsverbindungen im firmeneigenen Computernetz bietet ein Datenschutz mit dem DSM Link von Siemens. Damit ist nicht nur Abhören verhindert, sondern auch Datenfälschung (Foto: SIEMENS AG)

hen wird? Eben, weil der Rechner so in die Netzleitung auf der gleichen Phase einstreut, daß seine Oberwellen noch im Netzteil des Fernsehgerätes ihr Unwesen treiben können.

Denn die meisten Rechner, Monitore und Kabel sind nicht ganz dicht - strahlungsmäßig gesehen. Da gibt es Riesen-Plastikblenden an der Vorderseite, die nichts abschirmen, da werden lackierte Bleche verschraubt, ohne daß sie metallischen Kontakt bekommen, da werden Billigkabel ohne Schirmung verwendet und, und, die Sündenliste ist lang. Sogar die Tastaturleitung strahlt oftmals so gut, daß ein Auswertungsgerät jeden Tastenanschlag mitbekommt.

Deshalb sollte man im Büro Maßnahmen ergreifen, die die kompromittierende Abstrahlung wesentlich mindern bzw. ganz unterbinden. Beim Computerkauf sollte man auf ein allseitig geschirmtes Gehäuse achten, das weitestgehend HF-dicht ist. Wie so etwas aussieht, kann man sich bei Apple ansehen. Hier sorgen federnde Bleche an allen Klappen und Blenden für einen zuverlässigen HF-Kurzschluß.

Der Monitor sollte einer der ganz strahlungsarmen Sorte nach TCO sein, das Monitorkabel mehrfach geschirmt und mit HF-Drosseln versehen sein. Hier scheidet jeder Selbstbau unweigerlich aus.

Dies gilt auch für das Druckerkabel, das ebenfalls doppelt geschirmt sein muß, um nicht alle Daten an die Netzleitung zu „verraten".

Ihr Twisted-Pair-Netzwerkkabel mußte mal wegen eines Druckers auf zwei Adern getauscht werden? Nichts einfacher als das: Abisolieren, Adern abschneiden, vertauscht klemmen oder löten, isolieren und wieder rein in den Kabelschacht - der Spion freut sich und kann gar nicht allen Datenverkehr Ihrer Firma so schnell mitschreiben. TCP/IP kann bald jeder Computer mit irgendeiner Kommunikationssoftware an Bord, das Signal muß nur noch aus der Netzleitung herausgefischt werden.

Letzter Tip dazu: Verlegen Sie Datenkabel immer möglichst weit entfernt von Netzkabeln. Wenn sich das nicht vermeiden läßt, achten Sie wenigstens auf perfekte Schirmung der Datenkabel.

Bleibt nur noch zu erwähnen, daß auch Faxgeräte, Modems, ISDN-Karten etc. Daten über ein Netz versenden, das vor Zugriff sicher sein muß. Es nutzt also nichts, im Büro alles zur Datensicherheit zu unternehmen, wenn der Telefon-Anschlußverteiler außen am Gebäude hängt.

Bild 6: Das neuartige Datensicherungsmodul DSMLord stellt die Vertraulichkeit von Gesprächen in Verbindung mit fast allen Telefonendgeräten sicher, auch auf Reisen. (Foto: SIEMENS AG)

Wirksamste Methode - Verschlüsseln

Verschlüsseln heißt das Zauberwort, um sich gegen den direkten Angriff auf das Firmenkabelnetz und alle anderen Übertragungskanäle zu wappnen. Solche professionellen Geräte arbeiten mit anerkannten kryptologischen Verfahren, die nur mit unverhältnismäßigem Aufwand zu entschlüsseln sind.

Bereits bei der Diskussion der ISDN-Problematik tauchte diese Technik auf (Abbildung 1). Solche Verschlüsselungsgeräte, wie sie z. B. Siemens und Bosch anbieten, beherrschen sowohl das Gebiet der vertraulichen Datenübertragung per ISDN wie auch per firmeneigenem Netz (Corporate Networks, Abbildung 5) und Betriebsfunkverkehr. Netzwerk-Verschlüsselungsgeräte bieten zusätzlich auch einen wirksamen Schutz gegen Datenfälschungen.

Und der Datenversand? Hier bieten selbst preiswerte Programme, wie „Steganos" einen wirksamen Schutz gegen Datenklau, denn ohne Krypto-Paßwort ist nichts zu machen, man sieht es der Datei auch nicht an, womit sie verschlüsselt wurde.

Damit auch auf Reisen keine wichtigen Informationen an fremde Ohren gelangen, gibt es mobile Verschlüsselungsgeräte, die mit fast allen Telefonen zusammenarbeiten (Abbildung 6).

Machen Sie es, ob privat oder geschäftlich, den Schnüfflern schwerer, ihren Job zu tun.

Wer noch tiefer in die Problematik einsteigen will, dem sei abschließend das Buch „Lauschziel Wirtschaft" (Abbildung 7) von Manfred Fink, erschienen im Richard Boorberg-Verlag Stuttgart, zur Lektüre empfohlen.

Hier legt ein renommierter Sicherheitsfachmann, den wir auch für das Zustandekommen von Teilen dieses Artikels gewinnen konnten, detailliert Abhörgefahren und -techniken, ihre Vorbeugung und Abwehr dar. ELV

Bild 7: „Lauschziel Wirtschaft" - in diesem Buch findet der weiterführend Interessierte fundierte Fakten, Daten und Hinweise zum Thema Lauschangriff und Abwehr (Boorberg-Verlag Stuttgart).