Wirtschafts- und Wettbewerbsspionage

Risiken und Abwehr

Risikopotential

Der internationale Wettbewerb wird härter. Unternehmen werden immer häufiger zum Angriffsziel fremder Geheimdienste (**Wirtschaftsspionage**). Die Zahl derjenigen Unternehmen, die ihre Konkurrenz illegal ausspioniert, um sich einen Wettbewerbsvorteil zu verschaffen (**Wettbewerbsspionage**) wächst in einem atemberaubendem Tempo. Es gibt fast nichts, was nicht ausspioniert wird.
Die Auswirkungen sind dabei sehr unterschiedlich. Sie können von unbedeutenden finanziellen Schäden bis zur Existenzvernichtung reichen. Wer glaubt, seine Firma sei nicht bedroht und infolgedessen nichts unternimmt, muss später oft erkennen, dass er bereits Opfer eines Angriffs geworden ist.

Gefährdet sind keineswegs nur große Unternehmen. Auch Klein- und mittelständische Unternehmen sind lohnendes Objekt der Spionage. Meistens ist es das Ziel des Ausforschenden, genaue Informationen über Preise (Einkaufspreise, Verkaufspreise, Gewinnmargen) und Angebote sowie die Produktionstechnik und die Marketingstrategie des Konkurrenten zu erlangen. Erst in zweiter Linie geht es um Produktentwicklungen und Patente.

Die zum Ausspionieren erforderliche Hard- und Software ist sehr preiswert und regelmäßig frei käuflich. Der Kreis der potentiell Spionierenden ist daher außerordentlich groß. Neben professionell arbeitenden Spionen stellen die Hobby- und Gelegenheitslauscher ein nicht zu unterschätzendes Risiko dar, weil sie ihre Zufallsfunde skrupellos an den Meistbietenden verkaufen.

Aufgrund der modernen Kommunikationstechniken hat sich die Bandbreite der Angriffsmethoden dramatisch vergrößert. Die Risiken und die Schäden wachsen weltweit in neue Dimensionen. Allein in Deutschland schätzt man den durch Spionage jährlich entstehenden Schaden auf mehrere Milliarden Euro. Dieser Artikel zeigt Ihnen die Lücken in Ihrem Sicherheitssystem auf und erläutert, wie Sie diese schließen können.

Risikoeinschätzung

Das klassische Mittel zum Ausspionieren von Wissen sind Wanzen. Wanzen sind spezielle Abhörgeräte, die die Sprache im abgehörten Raum wie ein Mikrofon aufnehmen und die Information unter Zuhilfenahme eines Funk-Minisenders weitergeben. Daneben gibt es Laserabhörsysteme, die von außen selbst bei geschlossenem Fenster jedes gesprochene Wort auffangen. Auch Körperschallmikrofone, z.B. in Wänden eingebaut, verwandeln Ihr Büro in einen heißen Raum - ein überwachtes Zimmer.

Infolge immer kleiner und preiswerter werdender elektronischer Bauteile sinken die Preise für Abhörgeräte. Die Gefahr für den Lauscher, bei seinem Einsatz ertappt zu werden, nimmt entsprechend ab. Vergleichsweise groß geblieben sind nur die zum Betrieb der Wanzen erforderlichen Batterien. Die Gefahr des Entdecktwerdens hängt somit entscheidend von der geschickten Tarnung der Batterie ab. Besonders raffiniert sind Wanzen, die auf eine eigene Stromversorgung verzichten und statt dessen die in fast jedem Raum vorhandenen Stromquellen nutzen. Dies setzt regelmäßig eine Manipulation der Stromleitung voraus, was das Entdeckungsrisiko wiederum steigert. Auch das widerrechtliche Eindringen in eine Firma, um dort Abhörgeräte zu installieren, ist mit einem Risiko verbunden. Der Lauscher wird deshalb versuchen, die Wanze anläßlich eines Besuchs möglichst unauffällig im Raum zu hinterlassen. Achten Sie aus diesem Grund auf scheinbar zufällig vergessene Gegenstände wie Kugelschreiber, Notizbücher, Taschenrechner und dergleichen mehr. Auch bei Geschenken und unaufgefordert zugesandten Gegenständen wie Büchern, Bildern, Vasen und Blumen ist größte Vorsicht geboten.

Für den Täter wesentlich ungefährlicher ist es, den zu überwachenden Raum nicht zu betreten, sondern den Lauschangriff von außerhalb zu führen. Ihm kommt dabei zu Hilfe, dass Informationen den geschützten Einwirkungsbereich der Firma verlassen müssen, wenn sie an eine andere Firma versandt werden sollen.

Während die Briefpost keineswegs immer leicht geöffnet und unauffällig kopiert werden kann, sind Daten bei der elektronischen Nachrichtenübermittlung in anlogen und digitalen Netzwerken weitaus einfacher auszuspionieren. Dabei spielt es keine Rolle, ob die Informationen über Draht, Glasfaser, Funk oder Satelliten übertragen werden. Außerdem ist ein Abfangen der Daten kaum nachweisbar, besonders wenn die Abhörgeräte alle eingehenden und ausgehenden Nachrichten duplizieren. Telex, Fax, Datex-P, T-Online, Internet, nichts ist davon ausgenommen.

Funkverkehr, Richtfunkstrecken und Kommunikationssatelliten werden systematisch abgehört. Es gibt Hinweise, dass zumindest die landgestützte Kommunikation ins Ausland von Nachrichtendiensten komplett abgehört wird. Selbst die gewaltige Datenmenge in der Telekommunikation stellt kein Hindernis dar, seitdem modernste Hard- und Software Gespräche nach speziellen Begriffen scannen und auswerten kann.

Beachten Sie

Haben Sie den Verdacht, Opfer eines Lauschangriffs zu sein, nehmen Sie professionelle Hilfe in Anspruch. Machen Sie dem Angreifer die Arbeit schwer, indem Sie in Räumen, in denen Vertrauliches gesprochen wird, keine Gegenstände liegen lassen, die dort scheinbar zufällig vergessen wurden oder Ihnen unaufgefordert zugesandt wurden.

Abhörmethoden in Netzwerken

Galvanische Koppelung

Bei der galvanischen Koppelung wird das analoge oder digitale Kommunikationskabel mechanisch verletzt und eine feste Verbindung hergestellt, die eine äußerst hohe Abhörqualität liefert, dafür aber leichter zu entdecken ist. Solch ein Lauschangriff lässt sich meist nur im Zuge größere Wartungsarbeiten durchführen.

Beliebt ist auch das Stromnetz, weil kleine Abhörgeräte in einer Mehrfachsteckdose untergebracht werden können. Falls der Empfänger an dieselbe Phase angeschlossen wird, kann der Sender nicht nur im selben Gebäude, sondern auch außerhalb mit hoher Qualität empfangen werden.

Induktive Koppelung / Übersprechen

Bei jeder drahtgebundenen Kommunikation entsteht ein Magnetfeld um den metallischen Leiter herum, das außen am Draht abgetastet, verstärkt und wieder zurückverwandelt werden kann. Das Entdeckungsrisiko ist gering, weil das Kommunikationskabel unverletzt bleibt.

Besonders gefährdet sind Leitungen, Anschlussdosen und Verteilerkästen, die über Putz verlegt wurden und somit für den Angreifer leicht erkennbar und manipulierbar sind. Noch ungeschützter sind die Verteilerkästen öffentlicher Netzwerke, die oft auf frei zugänglichem Gelände stehen.

Kabel können mit Spezialgeräten auf kapazitive Abhörung untersucht werden. Bei induktiven Lauschangriffen versagen sie allerdings meist.

Mit der induktiven Koppelung verwandt ist das Phänomen der kompromittierenden Abstrahlung (KEM), die bei allen elektronischen Geräten vorkommt.

Funk

Die drahtlose Funkkommunikation ist am leichtesten abzuhören. Betroffen sind alle Funksysteme und Funknetzwerke, wie Betriebsfunk, Bündelfunkdienste, Paging-Systeme, schnurlose Telefone, C-, D- und E-Netze.

Nationale und internationale terrestrische Richtfunkverbindungen werden in erster Linie von den Nachrichtendiensten abgehört. Gleiches gilt für die Satellitenkommunikation (z.B. Inmarsat). Interessanterweise hören Nachrichtendienste befreundeter Staaten Funkeinrichtungen zumindest in dem Maße wie Nachrichtendienste nichtbefreundeter Staaten ab.

Vorsicht ist bei betrieblichen Computerfunknetzwerken und Infrarotnetzwerken angebracht. Während bei Infrarotsystemen und bei Mikrowellenfunk wenigstens ein Sichtkontakt zwischen Lauscher und belauschtem Punkt existieren muss, können Funksysteme, vor allem wenn sie über Relaisstationen/Repeater arbeiten, von überall abgehört werden.

Allgemeine Bürokommunikationsmittel

Bei digitalen Telefonverbindungen lässt sich nur schwer ein Abhören feststellen. Anders hingegen bei analogen Leitungen, für die es spezielle Geräte zur Überprüfung gibt.

Die bei jedem Telefon und Anrufbeantworter eingebauten Lautsprecher funktionieren im Prinzip wie ein Mikrofon. Lauscher machen sich diese Eigenschaft gerne zu Nutzen.

Technische Gegenmaßnahmen sind extrem teuer und kaum wirksam. In wichtigen Besprechungs- und Arbeitszimmern sollte deshalb auf Telekommunikationsgeräte verzichtet werden.

Anrufbeantworter

Anrufbeantworter können von außen abgehört und manipuliert werden. Das Löschen echter und Aufsprechen falscher Nachrichten ist möglich.

Fax

Die Nutzung des Telefax-Dienstes der Telekom hat stark zugenommen. Damit hat sich die Wahrscheinlichkeit erhöht, bei einer versehentlich falsch eingegebenen Fax-Nummer, statt einer Fehlermeldung bei der keine Übertragung erfolgt, einen falschen Fax-Teilnehmer zu erreichen.

Möglicherweise werden die Faxe aber gezielt fehlgeleitet. Verfügt der Lauscher über ein Fax-Monitoring-Systems, kann er ankommende und abgehende Faxe gleichzeitig auf seinem Fax ausdrucken oder in Datenspeichern aufzeichnen. Denkbar ist auch, dass die Daten einfach wie ein Telefongespräch abgehört werden. Diese Gefahren werden von den Betreibern der Telekommunikationsnetzen und -diensten abgefangen.

Aufgrund der Gefährdungen darf die Übertragung sensibler Daten per Telefax nicht die Regel werden. Werden sensible Daten gefaxt, so sind sie zumindest zu verschlüsseln. Achten Sie darauf, dass alle vom Telefax-Gerät angebotenen Sicherheitsfunktionen (z. B. Anzeige der störungsfreien Übertragung, Abfrage nach Passworteingabe) genutzt werden. Sende- und Empfangsprotokolle sind vertraulich abzulegen, da sie dem Fernmeldegeheimnis unterliegen.

Verfügt Ihr Netz über Bürokommunikationssoftware, mit deren Hilfe Telefaxe gesendet und empfangen werden können, sind zusätzliche Maßnahmen zu ergreifen, da der Betrieb integrierter Telefaxlösungen wegen der verwendeten Faxmodems bzw. -karten andere Formen der Datenübertragung und des Zugriffes ermöglicht.

Stellen Sie in diesem Fall sicher, dass das verwendete Rechnersystem sorgfältig konfiguriert und gesichert ist. Dazu gehört, dass kein Unbefugter Zugang oder Zugriff zu Ihrem Netzwerk hat. Verfügen beide Seiten (Sender und Empfänger des Telefaxes) über kompatible Produkte, ist der Einsatz kryptographischer Verfahren unkompliziert und kostengünstig. Sensible Daten sind dann immer zu verschlüsseln und digital zu signieren, um das Abhören zu verhindern und Manipulationen erkennen zu können. Schon bei der Beschaffung integrierter Telefaxlösungen ist darauf zu achten, dass bei der Hard- und Software ausreichende Konfigurationsmöglichkeiten vorhanden sind, um die Anpassung an sicherheitstechnische Erfordernisse des Nutzers zu gewährleisten.

Hinweis

Am anfälligsten sind Bürokommunikationssysteme, wenn sie mit einem Computer gekoppelt sind.

Papier

Oftmals wird in modernen vernetzten Büros das Papier als Schwachstelle übersehen. Überall finden sich Listings, Probeausdrucke, Manuskripte, Entwürfe und Notizen.

Damit diese Unterlagen nicht in falsche Hände geraten, sind sie unverzüglich in einem Aktenvernichter zu entsorgen. Bei Schreibmaschinen sind außerdem die Schreibbänder, bei Druckern die Thermotransferbänder sorgfältig zu vernichten.

Aktenvernichter

Die DIN 32757 beschreibt die Anforderungen an Maschinen und Einrichtungen zur Vernichtung von Informationsträgern (Papier und Mikrofilm). Je nach dem Grad der Schutzbedürftigkeit der auf dem Datenträger gespeicherten Informationen werden fünf Sicherheitsstufen definiert. Die Sicherheitsstufe drei (Streifenbreite max. 2 mm bei beliebiger Länge) sollte eine Mindestanforderung für eine datenschutzgerechte Vernichtung sein. Für sensible Daten sollten Sie eine höhere Sicherheitsstufe wählen. Die Papierdatenträger können in der Regel mit leistungsstarken Aktenvernichtern entsorgt werden.

Für Disketten, Streamertapes und Carbonfarbbänder muss ein Schredder für die Vernichtung unter Beachtung der DIN 33858 eingesetzt werden.

Sicherheitskopierer

Der Zugang zu Kopiergeräten muss restriktiv gehandhabt werden. Ansonsten lassen sich vor der Vernichtung von Originalausdrucken noch unberechtigte Kopien anfertigen. Wenige, nur auf stark frequentierten Korridoren aufgestellte, Sicherheitskopierer mit personalisierter Chipkarte und zusätzlichem Codewort, verringern das Risiko unbefugter Benutzung.

Kopierer senden übrigens KEM aus und sind deshalb abhörbar. Zu Schutzmaßnahmen siehe KEM.

Computer

Arbeitsplatzrechner allgemein

Bei Arbeitsplatzrechnern sollten keine Diskettenlaufwerke, keine Zip-Laufwerke, CD-Brenner, DVD-Brenner und Wechselplattensysteme vorhanden sein, denn die Gefahr des unkontrollierten Kopierens ist hoch. Ungeachtet dessen lässt sich auf diese Weise das Risiko des Virenbefalls minimieren.

Arbeitsplatzrechner sollten auch keine herausnehmbaren Wechselfestplatten besitzen, da selbst abschließbare Festplatten binnen Sekunden entwendet werden können.

Bei PCs wirken die Lautsprecher wie Mikrofone. Sie lassen sich ausgezeichnet zu Spionagezwecken einsetzen. Noch einfacher ist das Abhören, wenn der PC schon mit einem Mikrofon zum Internet-Telefonieren ausgestattet ist. Ansonsten lassen sich Elektret-Kondensator-Mikrofone (ECM) schnell und unauffällig in einen Computer einbauen.

Energie

Normalerweise ist die Energieversorgung bei einem Lauschangriff das größte Problem. Neuerdings liefern Solarzellen und regenerative Energiequellen fast unbegrenzt Strom. Die Entwicklung leistungsstarker Lithium und Zink/Luft-Batterien erlauben immer längere Abhörzeiten. Einige Abhörgeräte nutzen sogar das Telefonnetz als Energiequelle. Beim PC und bei Netzwerken kommt hinzu, dass Strom an so vielen Stellen und in solch großen Mengen verbraucht wird, dass eine Abhöreinrichtung nicht leicht nachzuweisen ist. Neue oder anders als bisher verlaufende Kabel sollten Sie in jedem Fall stutzig machen.

Kompromittierende Emissionen (KEM)

Motherboards, Steckkarten (besonders die Grafikkarte), Festplatten, Scanner, Kabel und Monitore verursachen elektromagnetische Felder, die noch in großer Entfernung in Schriftzeichen zurückverwandelt werden können. Monitorkabel, Datenkabel der Tastatur, Mäuse, Scanner, Drucker, Kartenleser und die vielen Netzwerkkabel wirken wie eine Sendeantenne.

Ein sehr hohe Abhörgefahr besteht, wenn sich in der Nähe Klimaanlagen, Lüftungsanlagen, Versorgungsschächte, Wasserleitungen oder Abwasserrohre, Zentralheizungen, Kabel des öffentlichen Telefons, Telefaxkabel, Brandmelderkabel und sonstige Sprechanlagen befinden, die die KEM weiterleiten.

KEM wird sogar über das eigene Stromkabel, an das der PC angeschlossen ist, übertragen. Allerdings lässt sich ein Computer über das Stromnetz mit vertretbarem technischen Aufwand nur innerhalb eines Gebäudes abhören.

Gefährlicher sind in der Nähe des Computers verlaufende Regenrinnen, Abflussrohre und Blitzableiter, weil sie die Strahlung weiträumig außerhalb des Gebäudes weitergeben.

Hinweis

Monitore stellen alle Zeichen unverschlüsselt dar, weshalb alle Kodierungssysteme versagen.

Distanzen von mehreren hundert Metern sind leicht zu überbrücken. Mit moderner Elektronik lässt sich sogar noch aus einem ganzen Pool von gleichen Computern ein bestimmter Rechner herausfiltern, weil die Taktfrequenzen der Prozessoren sich immer etwas unterscheiden.

Beachten Sie

Mehrere dicht nebeneinander aufgestellte Computer bieten keinen Schutz vor KEM durch gegenseitige Störung.

Abhilfe für KEM

Die Ummantelung aller Geräte und Kabel mit isolierenden Materialien (z.B. Kupfer, Aluminium) macht ein Abhören mittels KEM so gut wie unmöglich. Es ist jedoch ein teures und sehr umständliches Verfahren.

In der Praxis wird das sogenannte Zonenmodell verwendet. Dabei nutzt man unter anderem die physikalische Gesetzmäßigkeit aus, dass mit größer werdendem Abstand die ausgesandte Strahlung mit dem Quadrat der Entfernung abnimmt. Server sind aus diesem Grund in Kellerräumen oder im Zentrum eines Gebäudes am besten aufgehoben. Die natürliche Dämpfung durch Wände und Böden schirmt die KEM zusätzlich ab und erschwert das Abhören beträchtlich.

Praxistipp

Bevorzugen Sie strahlungsarme Geräte. Es müssen nicht immer extrem teure Sonderanfertigungen sein.

Fast perfekt sind die erhältlichen Störgeräte gegen KEM. Diese kosten zwar vierstellige Beträge; sie lassen sich aber direkt neben dem Computer und Monitor aufstellen, wo sie eigene Überlagerungssignale erzeugen, die ein Abhören außerordentlich erschweren. Allerdings kann ein Gerät höchstens einen Raum sichern.

Alte Datenträger

Alte Disketten, Magnetbänder und Festplatten sollten zuerst formatiert und dann mechanisch zerstört werden. Probleme entstehen bei defekten Datenträgern, wenn sie sich vom Normalanwender weder löschen noch formatieren lassen. Hier kann ein starker Magnet sinnvoll sein. Wenn die Entmagnetisierung korrekt erfolgt, d. h. mit einer ausreichenden Dämpfung, kann eine Rekonstruktion der Daten ausgeschlossen werden. Dieses Verfahren bietet sich insbesondere dann an, wenn die Festplatte defekt ist. Entsprechende Löschgeräte sind im Handel erhältlich. Ist eine solche Löschung vor Ort nicht möglich, so ist hierfür ein geeigneter Auftragnehmer auszuwählen. Erst nach dem "physischen" Löschen der Daten dürfen Festplatten an eine Servicefirma zurückgegeben bzw. einer Entsorgungsfirma zur Vernichtung übergeben werden.

Die immer notwendige zusätzliche mechanische Zerstörung der Datenträger kann bei Disketten und Bändern in einem speziellen Reißwolf geschehen. Festplatten hingegen sollten geöffnet, die Magnetscheiben mittels eines Magnets behandelt und dann mechanisch zerkleinert werden. Datenträger, die sehr schutzbedürftige Daten enthalten, werden eingeschmolzen.

Hinweis

Es gibt Fachfirmen, die Daten sogar nach einem Feuer wieder von scheinbar völlig zerstörten Festplatten teilweise retten können.

Warnung

Kopieren Sie keine Dateien auf Datenträger, die schon einmal beschrieben worden sind, wenn Sie die Datenträger anschließend aus der Firma geben wollen.

Falls Sie Dateien auf Datenträgern Dritten zur Verfügung stellen müssen, sollten Sie neue, d. h. unbeschriebene Datenträger verwenden. Das einfache Löschen alter Dateien genügt nicht. Selbst das gewöhnliche Formatieren bietet keinen ausreichenden Schutz. Nur eine zerstörende

Formatierung löscht zuverlässig und unwiderrufbar alle Dateien auf einem Datenträger. Diese spezielle Formatierung muss bei den meisten Betriebssystemen extra angegeben und teilweise nochmals bestätigt werden. Nach einem logischen Löschen können hingegen ohne großen Aufwand gelöschte Dateien auf einem vermeintlich leeren Datenträger wieder lesbar gemacht werden.

Widerrechtliches Kopieren von Datenträgern

Handelt es sich um kleine Datenmengen, genügt eine Diskette um in kürzester Zeit wichtige Daten unberechtigt von einem Rechner abzuziehen. Das widerrechtliche Kopieren lässt sich nicht nachweisen, weil die Daten auf dem Datenträger nicht verändert werden. Der Datendiebstahl wird deshalb oft gar nicht entdeckt. Schutz bietet Software, die nur dem Berechtigten den Zugang zum Computer erlaubt.

Große Datenmengen werden meist mittels extern angeschlossener Festplatten kopiert. Bei technisch möglichen Datentranferraten von über 30 MB/sek. von Festplatte zu Festplatte lassen sich extrem große Datenbestände in nur wenigen Stunden kopieren. Für 30 GB beispielsweise benötigen Fachkräfte samt Auf- und Abbau der Hardware-Verbindung weniger als eine halbe Stunde.

Netzwerke

Kabelschächte

Am verwundbarsten ist das Netzwerk bei seinem Kabelnetz. Die in langen Kabelschächten verlegten Kabel lassen sich nur mit großem Aufwand auf Beschädigungen, die von Manipulationen herrühren, kontrollieren. Ein besonders großes Risiko bilden zusätzlich verlegte aber unbenutzte Kabel. Ein Angreifer kann einen Sender direkt an ein unbenutztes Kabel galvanisch koppeln. Durch die parallele Verlegung zu den anderen Netzwerkkabeln findet eine qualitativ sehr gute induktive Koppelung statt.

Falls es nötig ist, verlegen Lauscher auch neue Kabel von der Dicke eines menschlichen Haares oder benutzen elektrisch leitende Farbe!

Gegenmaßnahmen

Überflüssige Kabel in den Schächten sollten Sie entfernen. Ist das nicht möglich, klemmen Sie die Kabel einfach ab oder schließen Sie sie kurz und erden sie anschließend.

Das Phänomen der induktiven Koppelung tritt vor allem bei asymmetrischen Koaxleitungen auf. Die vielfach verwendeten twisted Pair-Kabel neigen seltener zu diesem Effekt. Das Überkoppeln ist messtechnisch nachweisbar.

Findet der Lauscher keine freien parallelen oder nur twisted Pair-Kabel, wird er versuchen, einen Sender mit induktiver Koppelung in den Kabelschacht einzubringen. Das Einbringen wird erschwert, wenn alle Verteiler abschließbar sind und zusätzlich versiegelt und plombiert sind.

Um die Gefahr der induzierten Überkopplung zu reduzieren, sollten Sie nur hochwertige, mehrfach abgeschirmte Kabel verwenden. Noch besser ist es, wenn die Isolierungsschichten zusätzlich mit einem Rauschsignal überlagert und kapazitiv überwacht werden.

Abhörgeräte können auch seriell in das Netzwerkkabel eingebaut werden. Hierfür benutzt man kleine Verbindungsstücke an den Kupplungen der Kabel oder baut sie an schlecht einsehbaren Stellen der Schächte in das Kabel ein. Die eingesetzten Geräte arbeiten teilweise sehr raffiniert, weil sie sich erst beim Senden von Daten im Kabelstrang selbst aktivieren.

Glasfaser

Glasfaserkabel können gleichfalls abgehört werden. Manchmal ist das sogar leichter als bei metallischen Leitern.

ISDN

ISDN erlaubt durch Software-Manipulation das unbemerkte Abhören. Insbesondere die ISDN-Schaltung, bei der mehrere Personen gleichzeitig in Kontakt treten können, kann von Dritten missbraucht werden, um sich unbemerkt in eine Zweierkommunikation aufzuschalten. Vor allem Nebenstellenanlagen sind gefährdet.

FTP-Server

Schlecht gewartete FTP-Server stellen ein Risiko dar, da in älteren Versionen des FTP-Server-Programms Sicherheitslücken existieren, die zur Erlangung von Administratorrechten führen können. Vorsicht ist schon deshalb geboten, weil viele Beschreibungen zur Installation und Konfiguration von Anonymous-FTP-Servern sicherheitsbedenkliche Fehler enthalten. So kann es bei einer Fehlkonfiguration einem Angreifer gelingen, die Datei mit den verschlüsselten Passwörtern aller Benutzer auf seinen Rechner zu laden und dort zu entschlüsseln.

Netzwerkanwendungen

Alle Anschlüsse an das öffentliche Telefon-/Daten-Netz (Modem, ISDN, Standleitung, Datex-L/P, Btx, DSL) außerdem alle LANs und WANs sind gefährdet.

Trojanische Pferde

Bei Trojanischen Pferden handelt es sich um scheinbar harmlose Programme, die von außen in Ihr System eingeschleust werden und etwas ganz anderes tun, als sie vorgeben. Trojanische Pferde vermehren sich nicht und sind in der Regel nur einmal wirksam. Die von ihnen ausgehende Bedrohung ist aus diesem Grund nicht sehr groß. Gefährlich sind sie allerdings deshalb, weil sie meist nicht zufällig, sondern gezielt eingesetzt werden, um innerhalb eines Netzwerkes bestimmte Aufgaben auszuführen. Sie können beispielsweise Passwörter abfragen und diese an einen außenstehenden Empfänger senden.

Die größte Gefahr der Einschleppung besteht bei der Nutzung fremder Software (Shareware, Publicdomain-Software, Demonstrationsprogramme) unabhängig vom Speichermedium (Diskette, CD). Ein weiteres Bedrohungspotential stellen externe Netze dar, von denen ein Trojanisches Pferd als Attachement zur E-Mail oder als unaufgeforderte Datei mittels FTP und zunehmend auch über das World Wide Web als Java-Applet oder JavaScript bzw. VisualBasic in das eigene Netz eingeschleust werden kann.

Modeme und ISDN

Modeme und ISDN-Schnittstellenkarten sind verwundbar, weil sie bei ankommenden Daten selbständig eine Verbindung zum Computer herstellen können. Dies ist bei der Fernwartung sogar unabdingbar.

Fernwartung

Es macht kaum einen Unterschied, ob vor Ort oder von fern gewartet wird. Die Fernwartung erfreut sich allerdings regen Zuspruchs, weil sie eine schnelle Hilfe bietet, mit geringeren Kosten verbunden ist und Spezialisten zur Verfügung stehen. Die Fernwartung erlaubt einen sehr weitreichenden Zugriff auf die Ressourcen des ferngewarteten Arbeitsplatzrechners. Es muss also uneingeschränkt sichergestellt werden, dass sich am anderen Ende der Leitung tatsächlich ein Wartungsmitarbeiter bzw. eine Wartungsanlage befindet.

Beachten Sie

Moderne Sicherheitssysteme wie Firewalls erlauben die Fernwartung aus sicherheitstechnischen Gründen nicht!

Falls Sie eine Fernwartung in Ihrem LAN benötigen, sollten Sie zunächst die Ankopplung der einzelnen Arbeitsplätze erst auf vorhergehenden telefonischen Kontakt und nach erfolgreicher Berechtigungskontrolle mechanisch durchführen lassen und nach Beendigung der Arbeiten wieder unterbrechen.

Zur Kontrolle der Zugangsberechtigung gibt es entsprechende kryptografische Methoden. Die Verschlüsselungstechnik bietet Abhilfe gegen das Abhören auf den beim Warten verwendeten Leitungen. Verschlüsselte Daten kann der Wartungstechniker zwar wahrnehmen, aber er kann sie nicht verstehen.

Systembedingte Risiken

Leider wurde bei der Netzwerkentwicklung der Datensicherheit nicht von Anfang an die notwendige Aufmerksamkeit geschenkt. Netzwerke leiden deshalb unter systembedingten und schwer schließbaren Sicherheitslücken!

Bereits aus dem Umstand, dass z. B. die einfache IP-Adresse der Netzwerkkarte für die Adressierung ausreicht, ergeben sich eine Reihe von Risiken:

Innerhalb des eigenen LANs kann eine Person durch Manipulation der IP-Adressen und Routing-Einträge E-Mail oder andere Daten umleiten, weil das ARP (Adress Resolution Protocol) es erlaubt. Dies funktioniert innerhalb eines LANs mit Wirkung nach außen. So nimmt die falsche PC-Adresse im LAN die Post und Daten auch von außen an. Hier hilft dann selbst eine Firewall nicht mehr.

Um einem Spion, der innerhalb der eigenen Firma falsche ARP-Adressen versendet, das Handwerk zu legen, genügt es, das RAM-Cache abzuschalten, weil die Adressen regelmäßig im RAM-Cache gespeichert werden. Zusätzlich müssen Sie verhindern, dass weitere Einträge hinzugefügt werden. Verwenden Sie nur ein statisches Cache.

Berücksichtigen Sie, dass das Hinzufügen weiterer Einträge unter Windows nicht verhindert werden kann. Ein weiterer Grund, auf ein etwas sichereres Netzbetriebssystem wie Unix / Linux umzusteigen.

Desgleichen erlaubt das ICMP (Internet Control Message Protocol) Manipulationen. TCP/IP-Rechner versenden Statusmeldungen, damit Router die Post so umleiten, dass der schnellste Weg gefunden wird. Gibt ein Datenspion seinen Rechner als schnelles Gateway aus, erfolgt eine Redirection aller Nachrichten über ihn! Hier hilft eine Firewall, weil sie keine ICMP-Pakete in Ihr LAN hinein lässt.

Internet

Am schlechtesten sieht es mit der Datensicherheit im Internet aus. Beim Internet kann der Lauscher irgendwo auf der Erde sitzen. Er hat Zeit für seine Angriffe und wird, wenn er vom Ausland agiert, nur selten enttarnt.

Firewalls

Falls Sie ständig ans Internet angeschlossen sein wollen, sollten Sie eine Firewall (eine Art Brandschutzmauer) zwischen Ihrem LAN und der Außenwelt einbauen. Am besten wird dazu ein eigener Server eingesetzt, auf dem sich die Firewall-Software befindet. Die Firewall filtert nicht nur alle eingehenden, sondern auch alle ausgehenden Daten.

Nutzen Sie diesen Firewall-Rechner nicht gleichzeitig als Proxy für das Internet. Hierfür empfieht sich ein seperater PC. Ein Proxy speichert alle häufig abgefragten Daten des Internets für den schnellen Zugriff zwischen. Nur dort - oder besser auch auf einem separaten Rechner - sollten die eigenen Werbeseiten für das Internet liegen. Keinesfalls darf ein Internet-Surfer mittels Browser direkt auf Ihr LAN zugreifen können.

Unter einer Firewall ("Brandschutzmauer") wird eine Schwelle zwischen zwei Netzen verstanden, die überwunden werden muss, um Systeme im jeweils anderen Netz zu erreichen. Die Hauptaufgabe einer Firewall besteht darin, zu erreichen, dass jeweils nur zugelassene netzübergreifende Aktivitäten möglich sind und dass Missbrauchsversuche frühzeitig erkannt werden.

Die Stärke der Firewall hängt wesentlich von der eingesetzten Technik und ihrer korrekten Administration ab. Entscheidend für ihre Sicherheit sind die Staffelung und die organisatorische Einbindung der Firewall in die Informations- und Kommunikationsinfrastruktur.

Besteht innerhalb Ihrer Firma ein einheitliches Sicherheitsniveau und ist eine Kontrolle der internen Verbindungen durch die Firewall nicht erforderlich, bietet sich eine zentrale Firewall an. Diese unterstützt nicht eine Differenzierung nach Teilnetzen. Dementsprechend muss sich der Grad des gewährleisteten Schutzes nach den sensibelsten Daten richten. Für Bereiche Ihrer Firma, die mit weniger sensiblen Daten umzugehen hat, hat dies den Nachteil, dass unnötig hohe Schranken errichtet werden. Somit besteht latent die Gefahr, dass von diesen Bereichen weitere Zugänge zum Internet geschaffen werden, wodurch der gesamte Zweck der Firewall ad absurdum geführt wird.

Bei der zentralen Lösung besteht zudem die Gefahr, dass Ihr gesamtes Netz als eine Einheit betrachtet wird und Zugriffe von oder nach außen beschränkt werden.

Der Einsatz einer zentralen Firewall ist nur vertretbar, wenn alle angeschlossenen Teilnetze über ein gleiches Sicherheitsbedürfnis bzw. -niveau verfügen und zudem nicht die Gefahr des internen Missbrauchs besteht.

Haben Sie in Ihrer Firma Subnetze mit besonderem Schutzbedarf und soll innerhalb der Subnetze jeweils ein einheitliches Sicherheitsniveau erreicht werden, kommt eine gestaffelte Firewall in Betracht. Es handelt sich dabei um eine Kombination zentraler und dezentraler Komponenten, wobei durch die zentrale Firewall ein Mindestschutz für das Gesamtnetz gewährleistet wird. Die Kombination zentraler und dezentraler Schutzmechanismen erlaubt den autonomen Schutz aller Subnetze.

Für die dezentralen Firewalls bieten sich prinzipiell die gleichen Mechanismen wie bei einer zentralen Firewall an. Bei sorgfältiger Konfiguration bleiben geschützte Subnetze auch dann gesichert, wenn die zentrale Firewall durch einen Eindringling überwunden wird.

Gestaffelte Firewalls sind gleichfalls mit einem hohem Administrations- und Pflegeaufwand verbunden, der jedoch auf die zentrale Firewall und die jeweiligen Bereiche verteilt ist.

Warnung

Firewalls sind keineswegs absolut sicher. Es halten sich hartnäckig Gerüchte, wonach sich alle Geheimdienste in den jeweiligen Firewalls ihrer nationalen Hersteller Hintertüren einbauen ließen! Dass die Firewall-Hersteller laufend neue Versionen ihrer Produkte herausgeben, verstärkt zusätzlich den Eindruck vieler Skeptiker, dass es manchen Hackern doch gelingt, Eingang zu finden.

Um den Schutz vor unberechtigtem Eindringen zu erhöhen, sollte außerhalb der Arbeitszeiten die Verbindung eines LANs zur Außenwelt physikalisch unterbrochen werden.

Passwörter

Passwörter, die über die Tastatur eingegeben werden, können aufgrund der KEM noch in einigen Metern Entfernung aufgefangen werden.

Passwörter dürfen nicht aus dem sozialen Umfeld des Anwenders entnommen werden, weil der Datenspion zuerst diese Passwörter ausprobieren wird. Der Namen der Ehefrau oder der Kinder, das Kfz-Kennzeichen, die Automarke, die eigene Telefonnummer sind unbrauchbar.

Die Passwörter bei Bildschirmschonern der gängigen grafischen Betriebssysteme lassen sich mit moderner Elektronik binnen Sekunden knacken. Dennoch sollten Sie sie mit kurzem Zeittakt (1 Minute) aktivieren, damit nicht eine kurze Abwesenheit vom Arbeitsplatz von Fremden zum Ausspionieren genutzt werden kann.

Einen besseren Passwortschutz bieten gute UNIX-/Linux-Systeme.

Praxistipp

Denken Sie sich einen langen Satz aus und nehmen Sie jeweils den ersten oder letzten Buchstaben jedes Wortes. Bestimmte Wörter kann man auch durch Zahlen ersetzen (Nichts z.B. durch 0 oder Nein durch 9).

Beispiel: "Nein! Niemand ist so dumm, dass er nicht etwas dazu lernen könnte". Die ersten Buchstaben ergeben: 9Nisdde0edlk, die letzten 9dtomsr0sune. Das lässt sich leicht merken und ist erstaunlich schwer zu knacken.

Viele Systeme erlauben die Eingabe von Groß- und Kleinbuchstaben, so dass man dies ausnutzen sollte.

Verschlüsselung

Wichtige Daten sind zu verschlüsseln!

Nachrichtenverschlüsselung

Es sind alle Daten zu verschlüsseln, die über das öffentliche Netz verschickt werden. Neben E-Mail und FTP zählen dazu auch der Postversand und Kurierdienste.

Vertrauen Sie keinesfalls der von der Standardsoftware (Betriebssystem, Anwenderprogrammen) angebotenen Verschlüsselung. Diese lässt sich binnen Sekunden knacken.

Ausschließlich RSA-Systeme mit mindestens 2048- besser 4096-bit-Schlüsseln gelten als sicher.

Es gibt symmetrische und asymmetrische Verschlüsselungsverfahren. Bei den symmetrischen muss der einzige Schlüssel an die Empfängerstelle gebracht werden. Hierzu zählt der weit verbreitete DES-Standard, der in Fachkreisen als sehr unsicher gilt.

Asymmetrische Verschlüsselungsverfahren werden auch Public-key-Verfahren genannt, da es zwei Schlüssel gibt, einen privaten für den Erzeuger und einen öffentlichen, den Sie jedem anderen geben können, damit dieser Ihnen Nachrichten verschlüsselt zusenden kann.

Der sicherste Algorithmus hierzu heißt RSA nach den US-Mathematikern Rivest, Shamir und Adleman. Er gilt als online-sicher, wenn er eine Schlüssellänge von mindestens 2048 Bit hat. D. h. während einer Online-Sitzung von gewönlicher Dauer ist er von Normalsystemen kaum knackbar. Besser ist jedoch ein 4096-Bit-Schlüssel.

Das Faszinierende an diesem Prinzip ist, dass man aus dem öffentlichen Schlüssel nicht den privaten herausbekommen kann. Jede Nachricht mit dem einen Schlüssel erzeugt, lässt sich nur mit dem anderen wieder entschlüsseln. Jeder kann somit gefahrlos seinen öffentlichen Schlüssel auf Internet-Servern weltweit verteilen.

Datenverschlüsselung und Authentifizierung. sind garantiert. Wenn ein Empfänger eine Nachrichtenunterschrift mit dem Public-key des Absenders decodiert, weiß er sofort, ob sie vom richtigen Absender stammt, denn sie kann nur von dessen Private-key erzeugt worden sein.

Zur Sicherheit sollten die öffentlichen Schlüssel dennoch nicht beliebig veröffentlicht werden, sondern nur einzelnen Partnerfirmen ausgehändigt werden. Es ist Lauschern nämlich möglich, sich dazwischen zu hängen. Der Datenspion entfernt einfach Ihren Public-key vom Internet-Server und stellt dafür seinen eigenen öffentlichen Schlüssel dort hin, den er dann für Ihren Schlüssel ausgibt. So etwas findet man selbst meist nur zufällig heraus. Dann nämlich, wenn der Lauscher Nachrichten nicht schnell genug weiterleitet.

Da auch 4096-Bit-Schlüssel decodierbar sind, sollten Sie Ihren Schlüssel in regelmäßigen Abständen ändern! Experten gehen davon aus, dass Geheimdienste für das Decodieren eines Schlüssels höchstens einen Monat benötigen.

Transferkontrolle

Selbst bei kodierter E-Mail kann ein Lauscher bereits aufgrund einer Analyse der Datenmenge, der Häufigkeit des Datenversendens, der Sendezeit und den Namen der Adressaten erstaunliche Rückschlüsse ziehen.

Als preiswerten Schutz bieten sich hier mehrere E-Mail-Adressen für ein und denselben Benutzer an, die zusätzlich codiert sind (z.B. "user194@Firma.de" statt den Namen des Geschäftsführers). Ebenso bietet die gebündelte Übersendung der gesamten E-Mail en bloc einen gewissen Schutz.

Festplattenverschlüsselung

Wichtige, schutzbedürftige Daten auf Festplatten müssen ebenfalls verschlüsselt werden, dies gebietet bereits der Datenschutz.

Auslagerungsdateien

Eine Schwachstelle bildet der Cache-Speicher. Fast alle modernen Betriebssysteme (z.B. alle Windows-Versionen) benutzen sogenannte Auslagerungsdateien, die den RAM-Speicher bei Bedarf um Festplattenspeicher (mit virtuellem RAM-Speicher) ergänzen. Dort sind alle Daten unverschlüsselt zu finden!

Haben Sie einen permanenten Auslagerungs-Speicher eingerichtet, können Sie diesen Bereich der Festplatte regelmäßig mit Spezialprogrammen löschen. Bei einer temporären Auslagerungsdatei können die Daten über die gesamte Festplatte verstreut sein.

Speichern in Clustern

Über die gesamte Festplatte verstreute Dateifragmente entstehen übrigens auch durch Sicherungsspeicherungen. Aus Sicherheitsgründen ist das regelmäßige Zwischenspeichern erwünscht. Leider kann dieser positive Aspekt von Spionen missbraucht werden. Bei Sicherungsspeicherungen wird die alte Datei weder gelöscht noch von der neuen Datei überschrieben. Bei jedem Speichervorgang wird die neue Dateiversion auf den nächsten freien Cluster der Festplatte geschrieben und die Speicherstelle der vorherigen Version zum potentiellen Überschreiben freigegeben. Aber erst wenn das Ende der gesamten Partition/Festplatte erreicht ist, fängt der Schreibkopf der Festplatte wieder vorne an, die freigegebenen Cluster zu überschreiben.

Dateien füllen selten den gesamten Cluster völlig aus. Meist bleibt am Ende des letzten Datei-Clusters Speicherplatz frei. Daraus folgt, dass alte Daten nie wirklich völlig überschrieben werden.

Angenommen, ein Cluster kann 4.096 Byte Daten speichern und Sie speichern darauf nur eine Datei mit der Größe von 800 Byte ab, so bleibt ein unbenutzter Speicherraum von 3.096 Zeichen übrig. In diesem Speicherraum können noch Daten von einer schon überschriebenen Datei stehen, die mit einem speziellen Editor gelesen werden können!

Leider wird beim Kopieren einer Datei auf andere Datenträger (z.B. Diskette) der gesamte Cluster kopiert, so dass Sie unbewusst einem Außenstehenden erstaunliche Interna liefern können.

Dieses Problem nimmt mit steigender Clustergröße moderner Festplatten zu. Cluster mit einer Größe von 4.096 und 8.182 Byte sind keine Seltenheit! Dies ist genügend Platz für einen Geschäftsbrief.

Sicherheitsmaßnahme

Schutz bieten nur spezielle Löschprogramme, die den gesamten freien Speicher auf einer Festplatte löschen, indem sie ihn mehrfach mit bestimmten Zeichen überschreiben. Gute Werkzeuge löschen gezielt den unbenutzten Clusterbereich einer Datei. Einzelne Werkzeuge kombinieren das Löschen mit einer Festplattenoptimierung.

Personelle Angriffe

Neben allen technischen Abhörgefahren sollten Sie das Risikopotential Mensch nicht unterschätzen.

Mitarbeiter

Beim eigenen Personal sollten Sie bereits bei der Einstellung von Führungskräften in wichtigen Positionen sorgfältige Überprüfungen mit Einwilligung der Betroffenen durchführen.

Manche Mitarbeiter stellen sich trotz vieler Jahre loyaler Zusammenarbeit später als Wirtschaftsspione heraus. Die Motive hierfür sind vielfältig. Manchmal lassen allerdings äußere Anzeichen auf eine Veränderung des Mitarbeiters schließen. Um diese rechtzeitig wahrzunehmen, sollte sich ein Vorgesetzter in regelmäßigen Abständen mit seinem Personal ausführlich unterhalten.

Turnusmäßige Sicherheitsschulungen des Personals bieten die Chance, Mitarbeiter zu sensibilisieren und das Verständnis für notwendige Sicherheitsmaßnahmen zu wecken.

Praxistipp

Es ist jedem Mitarbeiter zu verdeutlichen, dass Datensicherheit Sicherung des eigenen Arbeitsplatzes bedeutet.

Es ist im einzelnen genau zu regeln, welche Mitarbeiter sich wann und in welchen Bereichen der Firma aufhalten dürfen. Besondere Regelungen sind für Besucher zu erlassen. In unregelmäßigen Zeitabständen ist zu überprüfen, ob die Vorschriften eingehalten werden.

Der Personenkreis, der hochsensible Bereiche betreten darf, ist in jedem Fall klein zu halten.

Die Zugangsberechtigung sollte nicht auf Räume beschränkt bleiben, sondern auch die virtuellen Zugänge durch Datennetzwerke einschließen. Hierzu sind verschiedene Zugriffshierarchien notwendig.

Gäste

Unbedingt erforderlich sind Regelungen für Besucher, insbesondere für diejenigen, die unangemeldet erscheinen. Es ist erstaunlich, wie frei und unkontrolliert sich nicht angemeldete Besucher, nur aufgrund der Vorlage einer falschen Visitenkarte, manchmal in einer Firma bewegen können. Nicht nur, dass sie ohne Kontrolle in das Büro geführt werden, sie werden dort auch noch allein gelassen, obwohl sensible Daten für jeden frei zugänglich sind. Unter falschem Namen eingelassenen Besuchern wurden auch schon mal die Produktionsanlagen oder sogar das Herzstück des neuen Computernetzwerkes in der EDV-Abteilung gezeigt.

In die Firma eingedrungene Personen können die Zieladressen von Faxen und am Computer die Zieladressen der E-Mail ändern. Falls der unberechtigte Empfänger die erhaltenen Nachrichten unverzüglich an die richtige Adresse - mit oder ohne gefälschter Absenderkennung - weiterleitet, fällt dies oftmals erst spät und dann meist nur zufällig auf.

Ungebetene Besucher schleusen gerne Abhörgeräte als Gast- oder Werbegeschenke ein. Machmal entpuppt sich ein scheinbar versehentlich liegengelassener Gegenstand als eine Wanze. Vor allem bei Gebrauchsgegenständen ist größte Aufmerksamkeit geboten. Auch induktive Geräte muss man nur in der Nähe eines Telefons oder PCs aufstellen, um die Kommunikation abzuhören.

Größte Vorsicht ist geboten, wenn Sie diese Geschenke an ein Netz anschließen sollen. Abhörsysteme sind in der Lage, ihre Energie nicht nur aus dem Stromnetz, sondern auch aus einem Telefonnetz zu beziehen.

Manchmal schleust der Belauschte selbst unbewusst eine Wanze in sein Büro ein. Die heutige Miniaturisierung macht sogar auf den ersten Blick völlig unbedenkliche Objekte gefährlich. So wurden schon Kugelschreiber, Bücher, Vasen, Blumentöpfe, Bilder und sogar Trinkgläser zur Spionage benutzt. Dem Einfallsreichtum, wie Objekte zur Spionage getarnt werden können, sind keine Grenzen gezogen.

Outsourcing von Wartungsarbeiten

Angesichts des zunehmenden Outsourcing von Wartungsarbeiten nimmt die Gefahr zu, durch Fremdfirmen ausgelauscht zu werden.

Fremdfirmen sind vor der Auftragserteilung mittels Referenzen zu überprüfen. Das Fremdpersonal ist bei der Auftragsdurchführung in der Firma während der gesamten Arbeitszeit ständig zu überwachen.

Bei Wartungsarbeiten gilt besondere Vorsicht. Vor allem unvorhergesehene Wartungsarbeiten (beispielsweise nach Sabotage, Einbruch) können fingiert sein. Sie bieten dem Spion außerdem die Chance, größere Abhöranlagen fest einzubauen.

Falls möglich, sollten Sie Hardware- und Software-Arbeiten vom eigenen Personal durchführen lassen. Zumindest die Systemadministration ist selbst durchzuführen.

Manchen Service-Technikern wird sogar das Supervisor-/Master-Passwort zum Netzwerk verraten. Einige externe Servicefirmen wiederum teilen dieses Passwort noch nicht einmal dem Netzwerkinhaber mit.

Praxistipp

Nach der Wartung des Netzwerks oder des Einzelarbeitsplatzes durch eine externe Servicefirma sollten diejenigen Passwörter geändert werden, die der Servicefirma zur Verfügung gestellt wurden. Wenn für die Wartung die höchste Zugangsberechtigung erteilt wurde, sollten die Paßwörter aller Ebenen geändert werden!

Austauschen von Geräten und Gegenständen

Dies ist ein für den Laien tückischer Bereich, da er die Notwendigkeit des Austauschs eines Computer- oder Netzwerkteiles nur schwer überprüfen kann. Angesichts der fortgeschrittenen Miniaturisierung elektronischer Bauteile lassen sich ganze Abhörsysteme auf einer Netzwerk- oder Grafikkarte zusätzlich einbauen, ohne dass dies sofort auffällt. Sie werden über den PC-Stromkreis gespeist und können mittels der Kabel mit enormer Feldstärke die Daten über Kilometer hinweg nach außen senden.

Praxistipp

Zusätzliche Steckkarten, deren Funktion nicht sichtbar/nachweisbar ist oder die angeblich zur Zeit nicht funktionieren, sollten Sie sofort wieder entfernen lassen.

Einbruch

Jeder Einbruch sollte Sie misstrauisch machen. Hierbei lassen sich leicht Netzwerke manipulieren oder Abhörgeräte einbauen.

Beschriften Sie die sensiblen Bereiche nicht: Hinweisschilder an den Türen (z.B. "Server-Raum") erleichtern den einbrechenden Lauschern die Arbeit. Halten Sie alle Räume nach Dienstschluss verschlossen.

Stellt sich nach dem Einbruch heraus, dass nichts entwendet wurde, kann dies daran liegen, dass etwas zurückgelassen wurde! Wurden wertlose Gegenstände entwendet, könnte der Einbruch fingiert sein.

Abwehr

Vorbeugung / Vorsorgeuntersuchung

Führen Sie regelmäßig Routinekontrollen der wichtigsten Systeme und deren Verkabelung durch. Wenn Sie dabei bereits als Laie eine Abhörvorrichtung entdecken (sogenannte Lockvögel), können Sie mit hoher Wahrscheinlichkeit davon ausgehen, dass sich ein weiteres Gerät irgendwo in Ihren Räumen befindet. Finden sich zwei Abhörgeräte in Ihrer Firma, dürften bereits ganze Abteilungen verseucht sein. Dann hilft nur noch ein spezialisierter Suchtrupp.

Meist ist es kein Zufall, wenn sich Ihre Konkurrenz, nachdem Sie wichtige interne Entscheidungen getroffen haben, plötzlich ganz unerwartet verhält. Nehmen Sie vage Ahnungen durchaus ernst. Es kam bereits öfters vor, dass sich bei einem Sweep (Säuberung eines Areals von Abhörgeräten) Wanzen gefunden wurden, deren Batterien schon seit Jahren leer waren.

Ein Sweep einer Fachfirma kann schnell fünfstellige Beträge erreichen, aber Ihre Firmengeheimnisse sind wesentlich mehr wert.

Die Auswahl der richtigen Firma ist schwierig. Allein ein Tagespreis von 5.000 Euro ist keine Garantie für eine erfolgreiche Arbeit.

Die Fachfirma sollte folgende Mindeststandards erfüllen:

- Analyse Ihrer Firma (Branche, Produkte, Firmengelände)
- Ausarbeitung der zu erwartenden Angriffe
- Lösungskonzepte
- Säuberung eines mit Ihnen festgelegten Areals mit einem mehrköpfigem Team von Spezialisten für jedes Gebiet (Funk/Radiotechnik, Netzwerke) mit aufwendiger Elektronik (u.a. einem hochwertigen Spectrum Analyzer).

Warnung

Einmannfirmen, die einen 100% igen Schutz versprechen, aber nicht über sehr gute elektronische Geräte verfügen, sollten Sie kein Vertrauen schenken.

Selbsthilfe

Es ist sinnlos, sich selbst Spezialgeräte zur Spionageabwehr anzuschaffen. Erstens sind die guten Geräte sehr teuer und zweitens nur vom Spezialisten mit langjähriger Erfahrung zu bedienen (z.B. Spectrum Analyzer, Wärmebildkameras). Auch die Interpretation der von den Geräten gelieferten Messdaten ist eine Kunst für sich und dem Spezialisten vorbehalten.

Billige Messgeräte aus dem Versandkatalog sind ihr Geld nicht wert und wiegen den Anwender nur in einer trügerischen Sicherheit, wenn das Gerät nichts angezeigt hat.

Grundstück

Es ist von Vorteil, wenn Sie ein Gebäude auf einem Firmengelände besitzen, das abgezäunt ist. Denn je größer der Abstand zum Lauscher ist, desto höher und teurer wird der Lauschaufwand.

Gefährdet sind Büroetagen, wenn sich der Lauscher innerhalb Ihrer Firma befindet, weil er Sie leicht von der Etage darüber oder darunter abhören kann.

Gebäude

Die Zugänge zum Firmengebäude sind zu kontrollieren. Die wichtigsten Räume sollten im Innern des Hauses oder im Keller liegen. Hierfür existieren ganze Zonenmodelle.

Das BSI

- Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63

53133 Bonn

Tel. 0228/9582-0

Fax 0228/9582-400

- **http://www.bsi.de**

erteilt Auskünfte.

Bei Schallisolationen und Hochfrequenz-Schirmungsmaßnahmen sollten Sie sich Gedanken machen, ob diese nur für einzelne Räume oder für das ganze Gebäude sinnvoll sind. Im Prinzip handelt es sich hierbei um einen Faraday-Käfig.

Einen hohen Schutzwert erzielen Sie mit dem Raum-im-Raum-Prinzip des BSI. Entweder werden Ganzmetallkäfige oder Metallfolien verwendet. Allerdings müssen dann alle Zuleitungen in diesen Raum mit besonderen HF-Filtern versehen werden.

Netzwerke

Es ist keineswegs notwendig, alle PC miteinander zu vernetzen. Es ist zu prüfen, ob alle Abteilungen auf alle Daten der anderen Bereiche zugreifen müssen. Gehen Sie der Frage nach, ob alle Daten sogar auf demselben Server abgelegt werden müssen.

Vor allem die Abteilungen Personal, F und E, Produktion und Marketing sollten über eigene, unabhängige Netze verfügen.

Darüber hinaus sollten genaue Nutzerrechte vergeben werden, so dass nur die Personen auf Daten Zugriff haben, die sie benötigen. Alle Zugriffe müssen mittels Chipkarte und zusätzlichem Passwort (beides auf RSA-Basis mit mindestens 2.048-bit-Schlüssel) personalisiert werden. Mit einem Zugriffsprotokoll lassen sich zudem unberechtigte Zugriffe besser nachweisen.

Arbeitsplätze von Mitarbeitern, die aufgrund von Krankheit, Urlaub oder Außendienst abwesend sind, müssen für diese Zeit gesperrt werden. Nur in Ausnahmefällen dürfen Aushilfskräfte an diesen Arbeitsplätzen arbeiten.

Alle Zugriffsrechte von außerhalb der Firma sind zu unterbinden, da sie in der Regel unkalkulierbare Sicherheitslücken darstellen.

Data-Warehouse

In den letzten Jahren kam es in vielen großen Firmen zu einem Aufbau von Data-Warehouses - gigantischen zentralen Firmendatenbanken. Es mag aus Controlling-, Vertriebs- und Marketing-Sicht sinnvoll sein, die gesamten Daten aller Kunden und Geschäftsvorfälle in einer einzigen Datenbank zu führen und diese dort mit Data-mining-Instrumenten zu analysieren. Aus Sicherheitsgesichtspunkten ist es untragbar. Jeder Spion wird versuchen, an diese - im Übrigen oft sehr schlecht geschützten - Systeme heranzukommen. Völlig unmöglich ist jeglicher Schutz, wenn an diesen Systemen auch noch externe Spezialisten über das normale Intranet arbeiten. So muss sich niemand wundern, wenn die Konkurrenz die eigenen Kunden besser kennt als das eigene Toppmanagement.

Resümee

Einen hundertprozentigen Schutz gibt es nicht. Die zur Spionage und Sabotageabwehr zu treffenden Gegenmaßnahmen basieren auf Ihrer individuellen Kosten-Nutzen-Analyse. Der Aufwand für einen potentiellen Lauscher ist so hoch zu treiben, dass bei ihm die Kosten und das Risiko der Entdeckung seinen erwarteten Nutzen übersteigen.

Lesen Sie zu diesem Thema auch **VPN - Virtual Private Network**