Lauschabwehr als Basisschutz

Die Abhörgefahr in der Wirtschaft wächst

Die Erfahrung zeigt, wenn es die Technik erlaubt, sich mit niedrigem Mitteleinsatz und überschaubaren Risiken illegal Wettbewerbsvorteile zu verschaffen, dann wird diese auch eingesetzt. Dass dies eine reale Gefahr ist zeigen die Schätzungen der Herstellerfirmen von Spionage-Werkzeugen. So sollen sich derzeit in Deutschland ca. 500.000 Abhörgeräte unterschiedlicher Art und Qualität in privatem, nicht-behördlichem Besitz befinden.

Von Ansgar Alfred Huth, Alzenau

Unternehmen, die sich vor dem unerwünschten Abfluss sensiblen Know-hows schützen wollen, verfügen inzwischen über mehr oder minder wirksame Informationsschutzkonzepte. Auf der technischen Seite sollte dazu neben der Verschlüsselung von Daten und Kommunikation wieder vermehrt der Schutz vor klassischen Lauschangriffen gehören, denn die Praxis des Autors zeigt: Wenn in Unternehmen der dringende Verdacht besteht, dass vertrauliche Gesprächsinhalte nach Außen drangen, dann lässt sich oft auch ein technisches Lauschmittel finden.

Industrie, Formel 1, Fußball, Immobilienverkauf, Show-Business, all dies sind Wirtschaftsbereiche, in denen Erfolg auch von Informationen über die Absichten der Mitbewerbers oder des Gegners abhängt. Mit einem Lauschgeräten, das oft nur wenige hundert Euro kosten, können Entwicklungsaufwand, Wettbewerbsvorsprung oder gar ganze Existenzen innerhalb kürzester Zeit vernichtet werden, denn gestohlenes Wissen kann nicht zurückgefordert werden. Die monetären Kosten eines Lauschangriffs im Vergleich zu den erhofften Erträgen sind in der Regel gering. Und auch das Risiko des Lauschers, bei einer Abhöraktion ertappt zu werden, liegt niedrig, denn selbst eine entdeckte Wanze lässt nicht immer Rückschlüsse auf den Auftraggeber des Lauschangriffs zu.

Die klassische Wanze (Spionage-Minisender) hat sich im Laufe der vergangenen Jahre weiterentwickelt. Heute angebotene Wanzen sind kleiner, leistungsstärker, bedienungsfreundlicher und für den vom Lauschangriff Betroffenen schwerer aufzufinden als früher. Außerdem hat dank des E-Business mittlerweile jeder Interessent Zugriff auf viele Varianten moderner Spionagetechnik. Wirksame und gefährliche Spionage-Utensilien, etwa in Kugelschreiber oder ~~in~~ Mehrfachsteckdosen versteckte Wanzen, werden in Internet-Shops inklusive Bedienungsanleitung zu niedrigen Preisen angeboten. Einen Design-Schreibtischrechner mit einer leistungsfähigen, per Solarstrom und Akku betriebenen sprachgesteuerter Wanze sowie die zugehörige Empfangstechnik gibt es schon für relativ kleines Geld.

Das Platzieren der Lauschmittel erinnert an die Ausbringung von trojanischen Viren im Internet. Kleine Geschenke wie der beschrieben Solartaschenrechner, Aschenbecher oder andere nützliche Gebrauchsgegenstände stellen attraktive Hüllen für die Wanzen dar. Auch Aktenkoffer, bestückt mit einem Sender, und das

dazugehörige Handy, das als Empfänger für die Wanze im Koffer dient, sind seit vielen Jahren inklusive Gebrauchsanleitung für dreistellige Eurobeträge zu kaufen. Diese Systeme können beispielsweise genutzt werden, um die im Raum zurückbleibenden Gesprächspartner während einer Verhandlungspause zu belauschen. Diese Systeme werden verkauft - und sie werden auch genutzt, wie der Autor bei einigen Überwachungen in der jüngsten Vergangenheit festgestellt hat.

Mindestens ebenso erfolgreich wie gefährlich ist das „Babyphone" in Form einer handelsüblichen Mehrfachsteckdose. Aufgrund des vorhandenen Netzstroms ermöglicht es eine dauerhafte Überwachung.

Die Abwehrmaßnahmen gegen Wanzen aller Art sind komplex. Notwendig sind organisatorische Maßnahmen, zum Beispiel reservierte, normalerweise verschlossene und besonders ausgestattete Räume, Handyverbot und Disziplin im Gesprächsverhalten, auch während der Pausen. Die Gewährleistung der Abhörsicherheit wird am ehesten durch eine regelmäßige Untersuchung durch Experten gewährleistet. Grundausstattung für besonders gefährdete Räume sollte ein Rauschgenerator sein.

Auch wenn die Mehrzahl der Lauschangriffe mit Wanzen erfolgt, wer sensible Informationen schützen will muss auch andere Angriffsmethoden berücksichtigen, zum Beispiel das Ausnutzen kompromittierender Strahlungen der Computermonitore. In sicherer Entfernung kann mit entsprechender Technik das aktuelle Dokument, etwa eine Konstruktionszeichnung, durch Auswerten der ausgesandten HF-Strahlung wieder auf einem Monitor in CAD-Qualität dargestellt und aufgezeichnet werden. Jeder gelernte Fernsehtechniker oder fähige Bastler könnte ein Fernsehgerät so modifizieren, dass die aktuelle Arbeit auf einem ganz bestimmten Monitor in Echtzeit mitverfolgt werden kann. Auch bei der Videoüberwachung entsteht eine kompromittierende Abstrahlung, die ausgewertet werden kann. Software, Störsender, abschirmende Tapeten oder - etwas aufwändiger - abstrahlsichere Gehäuse und Räume sind hier die einzigen technischen Gegenmaßnahmen.

Was heute als Abwehrmaßnahme geeignet ist, kann rasch technisch überholt sein und damit die Sicherheit herabsetzen. Ein Breitbanddetektor oder ein Feldstärkenmessgerät allein bedeuten nur Scheinsicherheit. Sie reichen nicht zur Aussage, ob ein Lauschangriff stattfindet oder nicht.

Effektive Lauschabwehr ist kostenintensiver als die Durchführung eines Lauschangriffs. Die Abwehr aller in Frage kommenden Angriffsarten setzt sowohl Erfahrung und fundiertes Fachwissen wie auch Messinstrumente, die in der Lage sind, das breite Spektrum der möglichen Methoden und Techniken zu überprüfen voraus. Auch wenn ein funktionierendes Lauschabwehr-Equipment (ab ca. 25.000 Euro) im Markt erhältlich ist, wird ein Experte benötigt, der den aktuellen Stand der Spionagetechnik, die im Markt erhältlichen Systeme und deren Einsatzmöglichkeiten kennt und der sein Wissen durch ständige Kontakte mit Entwicklern und „Bastlern" aktuell hält. Das kann ein hauseigener Experte sein, günstiger ist aber in den meisten Fällen ein Dienstleister.

Effektive Abwehr bedeutet auch, den Lauscher im Glauben zu lassen, dass der Lauschangriff nicht bemerkt, erahnt oder bekämpft wird. Dieser wird ansonsten versuchen, die auffindbaren Spuren seines Angriffes zu entfernen, zu vernichten

oder fernsteuerbare Wanzen etwa durch Ausschalten der Sendeeinheit zu deaktivieren. Nichtsendende Wanzen sind dann wesentlich schwerer zu detektieren als aktive Minisender.

Ein Lauschabwehreinsatz ist dann erfolgreich, wenn ein Angriff detektiert wurde oder mit hoher Wahrscheinlichkeit zu diesem Zeitpunkt ausgeschlossen werden kann. 100% Sicherheit wird es auf diesem Gebiet allerdings niemals geben.

Aktuelle Technik für Lauschangriffe:

„Wanzen": Versteckte, getarnte Raummikrofone übertragen Gespräche über Funksender mit Reichweite von 20 m bis 5 km, in Verbindung mit einer Scanner-Handy-Einheit auch weltweit. Die winzigen elektronischen Bauteile (ab 100 Euro) können in jedem Hohlraum stecken, in abgehängten Decken, Böden, Möbeln, Elektrogeräten, Zimmerpflanzen. Die Montage geht entsprechend schnell und ist ohne Fachkenntnisse durch jeden möglich, der den ausgewählten Raum betritt. Profi-Wanzenaufspürgeräte kosten mindestens ca. 25.000 Euro und setzen beim sinnvollen Einsatz langjähriges Expertenwissen vorausgesetzt. Die Kosten einer Überprüfung liegen in Abhängigkeit von Raumgröße und Aufwand zwischen ca. 1.000 bis 5.000 Euro

Mini-Tonbandgeräte: Die Geräte in Scheckkartengröße (ab 300 Euro) zeichnen bis zu vier Stunden Sprache auf, ein im Kugelschreiber untergebrachtes Gerät bis zu 70 Minuten. Meist werden die Geräte von Besuchern am Körper getragen, in Aktenkoffern oder anderen Konferenzutensilien (zum Beispiel Thermoskanne) versteckt. Jeder Laie kann diese Mini-Tonbänder einsetzen. Eine Abwehr ist sehr schwierig, da das geringe Magnetfeld des Löschkopfes elektronisch kaum zu orten ist.

Körperschallmikrofone: Der Lauscher nutzt dabei zum Beispiel einen Heizkörper oder die Wand als Mikrofon. Schallwellen versetzen den Körper in Schwingungen, die das Gerät auffängt, verstärkt, filtert und hörbar macht. Der Lauscher sitzt dazu in angrenzenden Räumen oder lässt sich per Funk, GSM, oder ISDN die abgehörten Gespräche liefern oder aufzeichnen. Die Preise liegen je nach Qualität zwischen 250 und 2.500 Euro. Abgewehrt werden sie durch Rauschgeneratoren (1.000 bis 3.000 Euro), die ein Belauschen stark erschweren.

Netzstrom-Wanzen: Der Langwellensender der den „Babyphones" ähnelnden Systeme nutzen die 220-Volt-Stromleitung als Antenne und beziehen den Strom aus dem Netz. Diese meist in Elektrogeräte eingebauten Wanzen benötigen somit keine Batterie und können für dauerhaftes Abhören, allerdings nur innerhalb des Hausnetzes, verwendet werden. Der Angriff erfolgt meist über den Austausch des Originals gegen ein präpariertes Gerät. Häufig erfolgt der Einbau in Mehrfachsteckdosen oder auch Verteilerdosen. Das System (Sender und Empfänger) kostet ca. 500 bis 1.000 Euro. Rauschgeneratoren zur Netzverrauschung oder der Einbau von Netzfiltern, zum Herausfiltern der Langwellen, erschweren solche Angriffe.

Fest verdrahtete Raummikrofone: Die klassische „Stasi-Wanze" wird oft schon bei der Errichtung eines Gebäudes oder Fahrzeugs fest installiert, oft in Deckenverkleidungen und Hohlräumen. Gespräche werden von einer festen Abhörstation belauscht, ausgewertet oder weitergeleitet. Der Installationsaufwand ist hoch. Meist handelt es sich bei den Tätern um Profi-Lauscher der Nachrichtendienste~~n~~. Eine Abwehr ist extrem aufwändig, allerdings kann das Abhören auch hier durch Rauschgeneratoren erschwert werden.

Richtmikrofone: Der Schall wird durch ein Parabol- oder Standard-Richtmikrofon eingefangen, die Schallwellen danach mehrfach verstärkt, gefiltert und ausgewertet. Untergebracht werden sie beispielsweise in der Spitze eines Regenschirms. Richtmikrofone ab 400 Euro sind auch von technischen Laien einzusetzen. Die wirksamste Abwehr ist, sensible Gespräche nicht im Freien in Sichtweite anderer Personen zu führen, in Chef- und Besprechungsräumen die Fenster während wichtiger Gespräche geschlossen zu halten.

Telefonwanzen: In Apparaten, in- oder externen Verteilerdosen und -kästen klemmen die Täter die Wanzen direkt an die Telefonleitung an. Der Sender wird aktiviert bei Abnehmen des Hörers, anderen Geräuschen im Raum oder durch ein Schaltsignal von Außen. Die zuckerwürfelgroßen Telefonwanzen (Preis ab ca. 150 Euro) lassen sich auch von versierten Laien einbauen. Verwandt damit sind die Fax-Monitorring-System (Preis ca. 4.000 Euro), die alle ein- und ausgehenden Faxnachrichten, ohne dass die Teilnehmer etwas davon merken, zusätzlich auf Papier oder Festplatte protokollieren. Die Abwehr erfolgt auch hier über einen qualifizierte Dienstleister. Auch Daten- und Gesprächsverschlüsselungstechnik verhindern den Informationsabfluss.

Was tun im Verdachtsfall?

Nehmen Sie Kontakt mit einem Abwehrfachmann oder Sicherheitsbehörden auf, aber nie aus den als „abhörgefährdet" eingestuften Räumlichkeiten
Benutzen Sie am besten eine öffentliche Telefonzelle oder einen Telefon-Anschluss eines nicht im normalen Umfeld liegenden Kommunikationsmittels
Schalten Sie während des Telefongesprächs Ihr Handy aus oder lassen Sie es am besten im Auto oder zu Hause.
Bedenken Sie, dass eine unverschlüsselte E-Mail jederzeit von Unbefugten gelesen und manipuliert werden kann.

Über unseren Autor:
Ansgar Alfred Huth ist ein anerkannter Sachverständiger für Datenschutz und Lauschabwehr. Seit 17 Jahren selbstständig in der Industrie- und Bankenwelt unterwegs, bietet er Dienstleistungen zum Thema Konferenzschutz und Lauschabwehr an.
Seine Academy bildet 2003 Personenschützer, Sicherheitsexperten und Manager auf dem Gebiet des alltäglichen Informationsschutzes aus. Kontakt zum Autor: Tel. 06023-918700, Internet: www.spionage.info