007 lässt grüssen

Industrie, Formel 1, mittelständige Betriebe, Fussball, Immobilienverkauf, ...all diese Vorhaben und Unterfangen haben mit sehr viel Geld und Know-how zu tun. Geld, das leider im Extremverhältnis zu dem Kostenaufwand eines Lauschangriffes steht.

Kugelschreiber mit eingebauter Wanze.

VON ANSGAR HUTH

In einer Zeit, in der man darauf achtet, dass vertrauliche Informationen verschlüsselt werden, sind wieder die altbewährten Wanzen in unseren Büros und Privaträumen aufzufinden. Die klassische Wanze (Spionage-Minisender) hat sich jedoch im Laufe der vergangenen Jahre erschreckend schnell in zwei Richtungen weiterentwickelt. Die erste Richtung war vorhersehbar. Die heutigen Wanzen sind kleiner, leistungsstärker, bedienungsfreundlicher und schwerer zu finden als ihre früheren Artgenossen.

Die zweite verheerendere Evolutionsrichtung dieser Miniverräter konnte vor einigen Jahren noch keiner prognostizieren. Durch das mittlerweile nicht mehr kontrollierbare Internet hat jede Person Zugriff auf alle möglichen Varianten der heutigen wieder modernen Spionagetechnik. Spionageutensilien, die früher nur mit Beziehungen, grossem Zeitaufwand und viel Geld beschafft werden konnten, werden heutzutage im Internet gut sortiert, inklusive Bedienungsanleitung zu Discountpreisen angeboten. Als Aschenbecher, Handy, Taschenrechner, Kugelschreiber oder Mehrfachsteckdose getarnt, kann man diese gebrauchsfertigen Funkwanzen über das Internet beschaffen!

Die Tarnungen dieser kleinen Informationsbringer sind zum Teil genial. Mit einem Empfänger in der Grösse einer Zigarettenschachtel, kann der Lauscher die gesendeten Gespräche der Wanze mithören oder aufzeichnen. Wer würde sich nicht für die Vorhaben, Planungen und Schwächen seiner Konkurrenten interessieren? Die Bereitschaft, solche verbotenen Informationsbringer einzusetzen, ist in den vergangenen Jahre immens gestiegen!

Ansgar Alfred Huth

ist seit 15 Jahren selbständig und eigenverantwortlich in der Wirtschaft unterwegs. Er hat von der Entwicklungsphase des ersten BMW-Turbomotors für die Formel 1 über die technische Beratung von Atomkraftwerksbetreibern bis hin zur Überwachung der Castor-Transporte, einen interessanten Werdegang hinter sich. Huth verfügt über Spezialausbildungen in verschiedenen Bereichen und hat seine Fachkenntnis auf dem Gebiet der Vorbeugung und Abwehr von Lauschangriffen durch entsprechende Stellen und Behörden in der Bundesrepublik Deutschland erworben. E-Mail: huth@lauschabwehr.de. Bedenken Sie bitte, dass eine unverschlüsselte E-Mail jederzeit von Unbefugten gelesen und manipuliert werden kann.

«Warum ich, warum ausgerechnet ich?», klagt die erfolgreiche Geschäftsfrau und blickt in die ungetrübten Augen des Überbringers dieser so verheerenden und vernichtenden Information. «Wie konnte uns das nur passieren?» Auch mit dieser Aussage der gestandenen Erfolgsfrau, kann der Tatsachenüberbringer nicht viel anfangen. Jetzt heisst es erst einmal Nerven behalten und überlegt handeln.

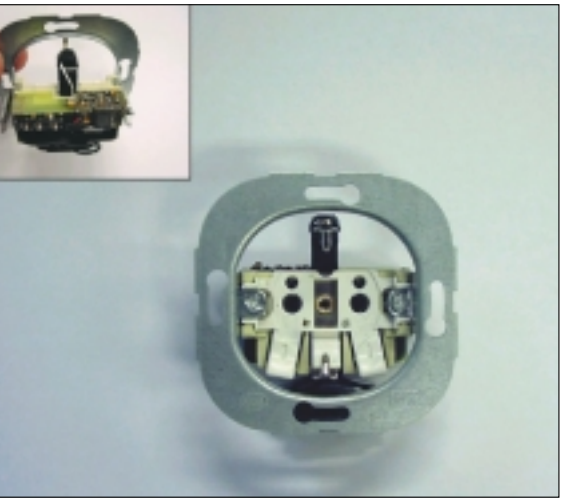
In diesem Fall explodieren innerhalb weniger Sekunden alle vertrauten Vorstellungen von Immunität, Sicherheits- und Zukunftsplanungen in dem attraktiven Kopf der betroffenen Managerin! Sie hatte schon seit Wochen so ein komisches Gefühl, wenn sie dem neuen Mitarbeiter begegnete. Als er ihr damals den tollen Design-Taschenrechner für ihren Schreibtisch schenkte, konnte sie doch nicht ahnen, was dieses harmlos gut aussehende Ding wirklich bezweckte. Ihr Büro war doch schon immer ihr bestgehüteter Raum, und gegen einen Einbruchversuch war sie doch auch gut abgesichert! All ihre Ideen, ihr Tun, ihre gesamte Unternehmensplanung, die bevorstehende Gewinnwarnung an die Aktionäre, das Unternehmen und der Imageverlust.

Spionageroman oder Realität? Insiderwissen über die betroffene AG (Gewinnwarnung usw.) enthält gegenüber der eingesetzten Technik (Design-Taschenrechner-Wanze + Scanner usw.) für lediglich 998 Euro einen extrem grossen Wert. Dies ist ein Fall aus der Realität, und er kann jedes Unternehmen betreffen. Gestohlenes Wissen ist nicht wiederbeschaffbar!

Wenn «aufgeweckte Geschäftsleute» oder «hochmotivierte Mitarbeiter» mit einem Budget in Höhe von ein paar hundert Euro in einem Unternehmen einen Millionenschaden verursachen, dann ist dies nichts Exotisches. Es ist leider allzu oft die heutige Realität.

Der Angriff

Im Zeitalter des privaten Internetanschlusses ist es jeder Person (ob Hobbyspion oder Industriespionage-Spezialist) möglich, sich mit billigen oder auch hochwertigen Abhöreinrichtungen jederzeit aufzurüsten, um etwa die Machenschaften der verhassten Ex-Ehefrau oder die Absichten und Möglichkeiten des neuen Geschäftspartners zu durchschauen. Die Palette ist beliebig erweiterbar. ►



Unterputz Stromsteckdosen sind beliebte Verstecke für Wanzen.

Im dargestellten Fall handelte es sich um das illegale Beschaffen von Insiderwissen einer Aktiengesellschaft. Die im Design-Taschenrechner eingebaute Wanze wurde von den schick integrierten Solarmodulen gespeist und war dank moderner Sprachsteuerungselektronik in der Lage, zu entscheiden wann sie «auf Sendung ging» oder besser sich zur Tarnung und Akkuschonung abschalten sollte. Das erschreckende an diesem fast schon alltäglichen Fall von profitabler Industriespionage sind nicht alleine die Konsequenzen, die ein stattgefundener Lauschangriff für das Unternehmen nach sich zieht. Das Erschreckende an solchen Fällen ist das Verhältnis Kostenaufwand der eingesetzten Spionagemittel, zum tatsächlich angerichteten Schaden für das Unternehmen.

Das Risiko des Lauschers, bei einer solchen Abhöraktion erwischt zu werden, tendiert gegen null. Wer verfügt schon über eine schützende Lauschabwehreinrichtung, geschweige denn das Wissen, sich gegen diese illegale Vorgehensweisen geschäftlich oder gar privat zu schützen? In Deutschland befinden sich laut Schätzung der Herstellerfirmen schon 500 000 bis über 1 000 000 Abhörgeräte im Besitz von Privatpersonen. Mit einer Wanze in der Grösse eines Zuckerwürfels, die nur ein paar hundert Mark kostet, werden Entwicklungsaufwand, Wettbewerbsvorsprung oder gar ganze Existenzen innerhalb kürzester Zeit vernichtet.

Die Klientel von Lauschabwehrspezialisten setzt sich mittlerweile immer mehr aus Privatleuten zusammen, die zumeist wohlhabend, prominent und somit lohnend angreifbar für jeden Lauscher ein interessantes Ziel darstellen. Informationen über solche V.I.P.s können vom Lauscher entweder zur Vorbereitung krimineller Machenschaften verwendet oder einfach an den Meistbietenden verkauft werden. Der Wert einer solchen Information kann sich schnell in fünf- bis sechsstelligen Summen darstellen.

Kleine Geschenke erhalten die Freundschaft und den Informationsfluss. Solartaschenrechner, Aschenbecher und andere Gebrauchsgegenstände sind beliebte Verpackungen für Wanzen. Aktenkoffer, bestückt mit einer Wanze, die während der Zeit des angeblich plötzlich dringenden Telefongespräches im Verhandlungsraum zurückgelassen werden, und das dazugehörige Handy, das als Empfänger für die Wanze im Koffer dient, um die beiden ahnungslosen Verhandlungspartner in der Zwischenzeit abzuhören, sind seit vielen Jahren inklusive Einweisung und Gebrauchsanleitung für ein paar tausend Mark zu kaufen.

Wenn ein Babyphon die Form einer handelsüblichen Mehrfachsteckdose aufweist und aufgrund des vorhandenen Netzstromes eine dauerhafte Überwachung ermöglicht, dann ist dies auch nur eine der vielen einfach zu installierenden verkaufsfertigen Möglichkeiten der Spionage, auf die ein Lauscher zugreifen kann.

ISDN-Viren, Telefonwanzen, Richtmikrofone, Körperschallmikrofone, Laser-Abhörgeräte, Lauschen per Computer, Bildschirmanzeigen, die in sicherer Entfernung ausspionieren und aufzeichnen, sind nur eine Frage des Geldes und der Leistungsbereitschaft krimineller Anwender. Kugelschreiber mit eingebauter Hochleistungswanze kosten lediglich 350 Euro.

In den letzten Jahren ist die Bereitschaft, die hier nur teilweise aufgezählten technischen Lauschangriffsmittel einzusetzen, genauso angestiegen, wie alle anderen asozialen Auswüchse unserer Leistungsgesellschaft (z.B. Mobbing). Das Zugehörigkeitsgefühl der einzelnen, vor allem auch leitenden Angestellten zur Firma ist auch nicht mehr das, was es einmal war. Jeder kämpft für sich und mit Sicherheit siegreicher als alle anderen, wenn er in Sachen Information die Nase vorn hat. Dem anderen in Sachen Wissen ein Stück voraus zu sein, ist eine siegessichere Verhandlungsposition in allen Lebenslagen.

Die Menschen, die als Lauscher enttarnt und überführt wurden, waren keine Ungeheuer oder Agenten 007. Es waren meist unauffällige Menschen, die uns tagtäglich begegnen und vielleicht noch freundlich lächeln!

Die Abwehr

Abwehren kann nur eine Person, die auch das Angreifen erlernt hat und somit realistisch die Angriffspunkte einschätzen kann. Zum effektiven Abwehren eines Lauschangriffes muss man sich in die technisch möglichen und finanziell gerechtfertigten Angriffsmöglichkeiten des Lauschers versetzen können. Auch der aktuelle Überblick über die international zu beschaffenden Spionage-Utensilien, ebenso der stetige Kontakt zu den Lauschabwehrmittel-Herstellern, gewährleistet eine realistische Einschätzung der bei dem Klienten vorgefundenen Situation. Nur der stetige Kontakt zu diesen Entwicklern und «Bastlern» verhindert, dass man von der täglich wachsenden Elektronik- und Systementwicklung in diesem Bereich ausgebremst und somit vom Lauscher, ausgespielt wird.

Effektiv Abwehren heisst auch den Lauscher im Glauben zu lassen, dass man den Lauschangriff nicht bemerkt oder erahnt hat. Ein Lauscher der mit einer Untersuchung seines Spionagefalles rechnet, versucht natürlich die auffindbaren Spuren seines Angriffes zu entfernen, zu vernichten oder zumindest zu deaktivieren.

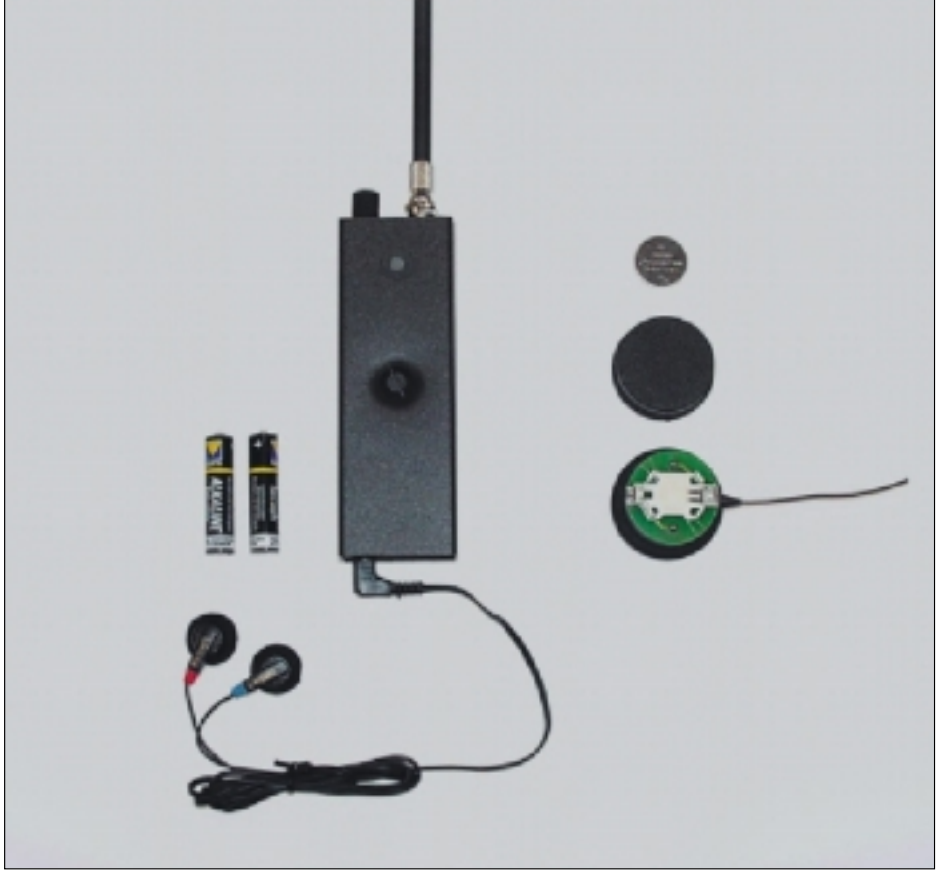
Letzteres hat zum Beispiel bei den bewährten fernsteuerbaren Wanzen ein Ausschalten der Sendeeinheit zufolge. Das Auffinden einer nichtsendenden Wanze ist wesentlich aufwendiger als das Detektieren eines aktiven Minisenders. Wobei die vielen unterschiedlichen Wanzenarten zwar einen grossen Teil der angewendeten Angriffstechniken darstellen, jedoch aber die Vielfalt der Lauschangriffstechniken und somit Angriffsart nur von dem Vorstellungsvermögen und den finanziellen Mitteln des Angreifers abhängt.

Wer weiss schon, dass man das auf seinem Computermonitor bearbeitete Schriftstück zeitgleich in sicherer Entfernung nur durch Auswerten der kompromittierenden HF-Strahlung wieder auf einem anderen Monitor darstellen und bequem aufzeichnen kann. Auf diese Art und Weise kann jeder gelernte Fernsehtechniker oder begnadete Bastler mit einem alten modifizierten Fernsehgerät die Preiskalkulationen seines Handwerkernachbarn in Echtzeit miterleben.

Diese kompromittierende Abstrahlung ist natürlich auch für Überwachungskameras ein nicht zu vernachlässigendes Informationsschlupfloch. Die Abwehrmassnahme gegen diese Spionageart ist recht unspektakulär und doch so wichtig. Man muss sie nur wissen und stetig die Weiterentwicklungen dieser Angriffsart im Auge behalten.

Was heute noch abwehrt, kann in ein paar Tagen schon überholt sein und dann ein noch grösseres Gefahrenpotenzial darstellen, als die aus Unwissenheit komplett unterlassenen Abwehrmassnahmen. Denn der sich in Sicherheit wiegende Geschäftsmann mit der veralteten nicht mehr funktionierenden Abwehreinrichtung ist ein gefundenes Fressen für die Lauschangriffe der Konkurrenten.

Nicht nur die Aktualität, auch die Qualität der eingesetzten Lauschabwehrinstrumente ist für einen erfolgreichen Lauschabwehreinsatz von entscheidender Bedeutung. Wer im Glauben lebt, mit einem Breitbanddetektor oder Feldstärkenmessgerät für ein paar hundert Mark einen ernst zu nehmenden Lauschabwehreinsatz zu starten, der sollte den Lauscher am besten gleich in seine Privaträume einziehen lassen. Denn so sparen sich beide die Kosten für die Technik, und der Lauscher bekommt auch was er will.



Stethoskop-Wanzen mit Empfänger im Set.

Lauschabwehr ernsthaft und effektiv zu betreiben ist wesentlich kostenintensiver als einen Lauschangriff durchzuführen. Während man sich bei einem Lauschangriff für ein Mittel oder eine Kombination der sinnvoll einzusetzenden Hilfsmittel entscheiden kann, muss man bei einem effektiven Lauschabwehreinsatz alle in Frage kommenden Angriffsarten abwehren beziehungsweise detektieren können.

Das setzt nicht nur fundiertes Fachwissen voraus, sondern auch eine Gerätschaft, die in der Lage ist, ein breites Spektrum der möglichen Spionageangriffsmethoden und -techniken zu überprüfen. Ein funktionierendes Lauschabwehr-Equipment ist nicht unter einer fünfstelligen Summe zu erwerben, geschweige denn das Fachwissen mit dem Lesen der Bedienungsanleitung.

Der Lauschabwehrkoffer besitzt in Sachen Detektieren und Abwehren von Lauschangriffen eine einzigartige Leistungsvielfalt und kann als ganz normaler Aktenkoffer getarnt zu jedem zu überwachenden Einsatzort unauffällig mitgeführt werden. Dieser in einem deutschen Labor von Hand gefertigte Spionageabwehrkoffer ist per Software-Update immer auf dem neuesten Stand der Technik und verfügt über eine lautlose Raumüberwachung, die das Detektieren und Lokalisieren von Abhöreinrichtungen (ohne dass dies der Lauscher bemerkt) erlaubt. Die Möglichkeit den Lauscher zu ermitteln und ihn zukünftig mit falschen Informationen zu versorgen, ist bei dieser getarnten Abwehrmethode gegeben. Ein Lauschabwehreinsatz ist erfolgreich, wenn man entweder einen Lauschangriff detektiert hat oder mit hoher Wahrscheinlichkeit einen Lauschangriff zu diesem Zeitpunkt ausschliessen kann. Hundertprozentige Sicherheit wird es auf diesem Gebiet niemals geben, jedoch kann man mit einem erfahrenen Partner an seiner Seite den Daten-GAU und somit die immer häufiger in unserer Gesellschaft vorkommenden Informationsdiebstähle wirksam und solide bekämpfen.

Der Schutz

Es gibt viele Möglichkeiten in Sachen Lauschangriffe. Der Angriff kann drahtlos oder drahtgebunden erfolgen. Für den Täter bietet sich so oder so die Möglichkeit, Wort und Bild unbemerkt zu übertragen, aufzuzeichnen, auszuwerten und weiterzugeben.

Grosse Gefahren ergeben sich nicht nur durch getarnte Minisender im Aschenbecher, Kugelschreiber und Mehrfachsteckdosen, sondern auch durch das Anzapfen von Daten- und Telefonleitungen. Auch Videowanzen werden immer beliebter. Schwachstellen in Ihren Räumlichkeiten finden sich überall.

Gerade in der heutigen Zeit, in der sich immer mehr Geschäftsleute zum sinnvollen Verschlüsseln ihrer Telefongespräche, Faxe, E-Mails und Videokonferenzen entschlossen haben, hat ein Lauscher meist nur noch die Möglichkeit, über die interne Informationsschiene an die «noch nicht verschlüsselten» kostbaren Daten und Gespräche heranzukommen. Es ist in vielen Fällen sehr einfach, ein Unternehmen oder eine Privatperson auf Dauer zu überwachen!

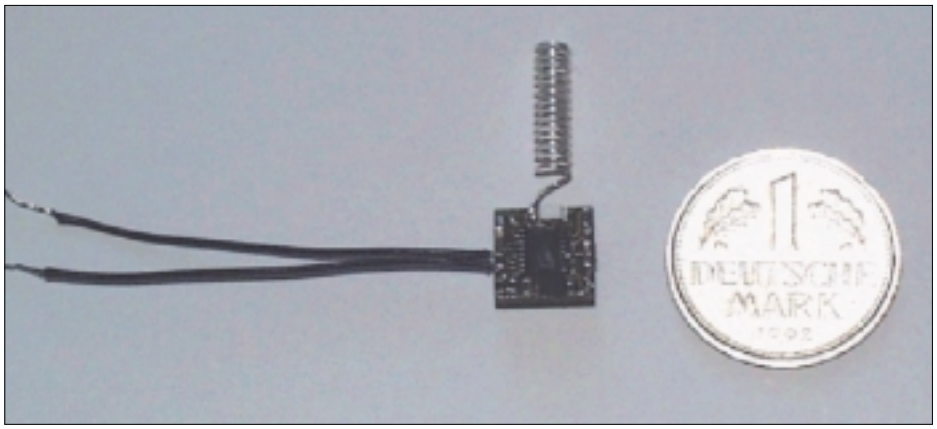
Die hier vorgestellten Möglichkeiten sind nur eine grundlegende Auswahl an Überwachungsmethoden oder elektronischen Angriffsmethoden, da die Möglichkeiten von Tag zu Tag erweitert und weiterentwickelt werden.

Es erscheint schier unmöglich, alle Kombinationsmöglichkeiten der Mittel in Sachen Spionageangriff aufzuzeigen, denn die Grenzen der Machbarkeit werden lediglich von Ihrer Vorstellungskraft und dem Fachwissen abgesteckt.

«Wanzen» Minisender: Dies sind versteckte, getarnte Raummikrofone, die Gespräche über Funk übertragen. Die Reichweite beträgt 20 Meter bis 5 Kilometer. In Verbindung mit einer Scanner-Handy-Einheit ergibt sich eine weltweite Reichweite. Die Energieversorgung erfolgt meist über Batterie, aber auch über Netzstrom- und Telefonnetz oder Solarzellen. Passive Wanzen benötigen keine angebaute Energieversorgung. Die benötigte Energie wird einfach von aussen eingestrahlt.

Die winzigen elektronischen Bauteile können in jedem Hohlraum stecken, in abgehängten Decken, Böden, Möbeln, Elektrogeräten und Zimmerpflanzen. Hier zählt Fantasie, Einfallsreichtum und Erfahrung. Die Montage geht schnell und ist kinderleicht. Einfache Wanzen sind ab 100 Euro zu haben. Wenn es sich zum Beispiel um eine getarnte Wanze handelt (Uhr, Taschenrechner, Lampe usw.) kann sich der zukünftig Abgehörte wenigstens über ein schönes Werbegeschenk freuen und platziert das liebe «Info-Ungeziefer» eigenhändig in seinen vier Wänden.

Als Täter kommt jeder in Frage, der Zugang zum Zimmer hat: Mitarbeiter, Besucher, Putzfrauen, Handwerker und Monteure. Letztendlich hat jeder die Möglichkeit, sich Zutritt zu einem ►



Der Kleinsender ist nicht grösser als eine Münze.

Raum zu verschaffen. Die Abwehr ist durch Profi-Wanzenaufspürgeräte (z.B. MO 2055/ II, ab ca. 20 000 Euro) möglich. Für die Bedienung ist Sachverständigenwissen vorausgesetzt. Elektronisches Grossreinemachen als Dienstleistung durch einen anerkannten Sachverständigen (Sweeping) kostet 1000 bis 5000 Euro (abhängig von Raumgrösse und Aufwand).

Mini-Tonbandgeräte: Die Winzlinge zeichnen Sprache auf. Ein Tonbändchen in Scheckkartengrösse kann rund drei Stunden aufnehmen. Selbst das allerkleinste Gerät in einem Kugelschreiber schafft 70 Minuten. Neuere Produkte erreichen sogar vier Stunden und mehr digitale Aufzeichnung. Fast immer bringen Besucher die Tonbänder mit, die das vertrauliche gesprochene Wort heimlich dokumentieren wollen. Die Geräte werden entweder am Körper getragen, in Aktenkoffer oder in anderen Konferenzutensilien eingebaut. (Die Thermoskanne lässt grüssen!)

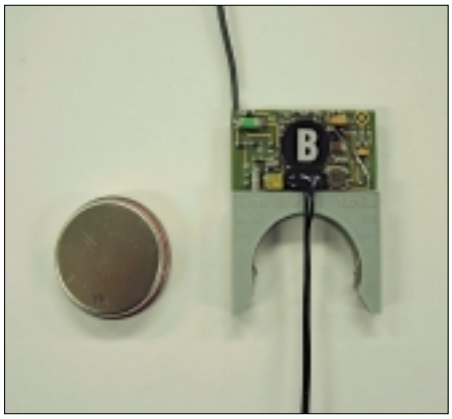
Jeder Laie kann die Mini-Tonbänder einsetzen. Ein Gerät in Scheckkartengrösse kostet ab 300 Euro. Die Abwehr gestaltet sich sehr schwierig. Durch das geringe Magnetfeld des Löschkopfes sind die Geräte elektronisch kaum zu orten. In Frage kommen Profi-Wanzenaufspürgeräte mit Tonbanddetektor-Erweiterungseinheit. Auch hier ist Sachverständigenwissen vorausgesetzt.

Körperschallmikrofone: Der Lauscher nutzt zum Beispiel einen Heizkörper oder die ganze Wand wie ein Mikrofon. Schallwellen versetzen den Körper in Schwingungen, die das Gerät auffängt, verstärkt, filtert und hörbar macht. Der Lauscher sitzt dabei unbehelligt im angrenzenden Raum. Beliebte Lauschstellen sind auch Versorgungsschächte, die vertikal durch alle Etagen führen. Spitzengeräte liefern erstaunliche Hörqualität. Diese Methode funktioniert auch durch eine Glasscheibe. Der Preis für Körperschallmikrofone beträgt 2500 Euro, leistungsschwächere Geräte sind ab 250 Euro zu haben. Als Täter kommen alle in Frage, die Zugang zum Nachbarraum haben. Es sind betriebsinterne oder betriebsfremde Täter.

Rauschgeneratoren machen das Belauschen von Körperschall fast unmöglich, sind aber teuer. Rauschgeneratoren für einen kleinen Raum kosten rund 1000 bis 3000 Euro.

Drahtfunk: Funktioniert innerhalb des Gebäudes. Der Langwellensender nutzt die 220-Volt-Stromleitung als Antenne und bezieht den Strom aus dem Netz. Diese Netzstromwanzen benötigen somit keine Batterie. Sie eignen sich hervorragend für eine dauerhafte «Datenverbindung». Diese Babyphone-Technik ist jedem Papa bestens bekannt. Gute Verstecke bieten 220-V-Elektrogeräte.

Oft tauschen die Lauscher vorhandene gegen präparierte Geräte aus oder implantieren das kleine Senderchen während einer Reparatur oder günstigen Aufrüstung. Besonders beliebt: Einbau in handelsübliche Mehrfachsteckdosen. Solche werden seit Jahren gebrauchsfertig inklusive Bedienungsanleitung im Internet angeboten. Tipp: Schauen Sie mal die Verteilerdosen im Zimmer an.



ISDN-Telefon-Wanze.

Wie bei Wanzen wird ein zusätzliches Empfangssystem benötigt (wird einfach in irgendeine Steckdose im Haus eingesteckt). Das System kostet so um die 500 bis 1000 Euro. Als Täter kommen Besucher, Monteure und Mitarbeiter in Frage. Der Empfang kann nur im Gebäude stattfinden. Die Abwehr erfolgt mit Profi-Wanzenaufspürgeräten mit Netzstrom-Erweiterungseinheit. Sachverständigenwissen wird für die Abwehr vorausgesetzt. Netzverrauschung erfolgt durch Rauschgeneratoren oder Einbau von Netzfiltern. Letztere filtern die Langwellen (zu übertragende Sprache) heraus und verhindern so die Übertragung.

Festverdrahtete Raummikrofone: Die klassische Stasi-Wanze wird oft schon bei der Errichtung eines Gebäudes fest installiert. Gespräche werden von einer festen Abhörstation im Haus belauscht, ausgewertet oder weitergeleitet.

Diese Raummikrofone finden sich vor allem in Deckenverkleidungen und Mauerhohlräumen. Sie sind nur mit hohem Aufwand installierbar, bieten aber dann unbegrenzte Betriebs- und Nutzungszeit. Profi-Lauscher verwenden sie in Botschaften und Auslandsvertretungen, Hotels und besonders in Konferenzzentren und sogar in Erstklasse-Kabinenplätzen in Flugzeugen bestimmter Airlines. Eine Abwehr ist extrem aufwendig. Das Abhören kann durch Rauschgeneratoren erschwert werden. Ausweichen ins Freie ist nur sinnvoll, wenn niemand in Sichtweite elektronisch mithören kann.

Richtmikrofone: Der Schall wird durch ein Parabol-Richtmikrofon oder Standard-Richtmikrofon eingefangen. Die Schallwellen werden wie bei einer Körperschallauswertung mehrfach verstärkt, gefiltert und ausgewertet. Der Lauscher lauert im Freien auf einer Parkbank und richtet die Spitze seines Regenschirmes unbemerkt auf das Ziel oder das geöffnete Bürofenster. Diese Regenschirmspitze, die während des Spazierens durch eine kleine Hülse geschützt ist, stellt das Richtmikrofon dar. Regenschirme eignen sich nun mal zum Abhören, Schiessen und Nässeabhalten.

Jeder Laie kann diese Richtmikrofone auf Sie ansetzen. Die Bedienung ist einfach. Leistungsfähige Geräte kosten ab 400 Euro. Als Täter kommen Laien und Profis in Frage. Wichtige Gespräche sollten nicht im Freien in Sichtweite anderer Personen geführt werden. In Chef- und Besprechungsräumen sollten Fenster geschlossen bleiben. Wichtige Gespräche führt man auch aus anderen Gründen grundsätzlich nicht in Räumen, die über Fenster ins Freie verfügen.

Telefonwanzen: Die Täter klemmen sie zum Beispiel direkt an die Telefonleitung, die dann auch den Strom liefert. Der Sender wird, aktiviert, wenn der Hörer abgenommen wird oder überwacht permanent den Raum in Sachen Schallwellen oder wird von aussen aktiviert. Als Versteck dienen Telefon, Telefonanschlussdose, innerhalb oder ausserhalb der Telefonleitungen des Hauses (Verteilerkasten, Vermittlungsstelle der Telefongesellschaft).

Ein versierter Laie kann die zuckerwürfelgrossen Telefonwanzen leicht einbauen. Preis: ab 150 Euro, inklusive Bedienungsanleitung. Als Täter kommen Servicetechniker und Ehemänner in Frage, letztendlich aber jeder, der weiss, wie man im Internet einkaufen kann. Bei einer Installation in Verteilerkästen muss man jedoch im Täter eine hohe kriminelle Energie voraussetzen.

Als Abwehr dient eine professionelle Telefon-Leitungsüberwachung durch einen erfahrenen anerkannten Dienstleitungsbetrieb, der den Telefonanschluss permanent in Sachen Funktionsfähigkeit und Anomalien überwachen kann. Die Kosten belaufen sich auf rund 35 Euro pro Monat. Profi-Wanzenaufspürgeräte mit Telefonleitungs-Erweiterungseinheit können ebenfalls erfolgreich sein.

Fax-Monitoring-System: Das System protokolliert zusätzlich alle ein- und ausgehenden Faxnachrichten auf Papier oder Festplatte. Die Teilnehmer merken davon nichts. Das Gerät wird direkt an die Faxleitung (Telefonleitung) angeschlossen, wie die festinstallierte Telefonwanze. Fax-Monitoring-Systeme sind ab 4000 Euro zu erwerben. Täter sind Profis, die gezielt vorgehen und sich die Bespitzelung etwas kosten lassen.

Als Abwehr dient die professionelle Telefon-Leitungsüberwachung durch einen erfahrenen anerkannten Dienstleistungsbetrieb, der den Telefonanschluss permanent in Sachen Funktionsfähigkeit und Anomalien überwachen kann. Kosten rund 35 Euro pro Monat. Auch ein Profi-Wanzenaufspürgerät mit Telefonleitungs-Erweiterungseinheit kann erfolgreich sein.

Dies ist nur eine kleine Auflistung der von jedermann zu beschaffenden Spionagemittel und stellt nur einen kleinen überschaubaren Auszug zu diesem Thema dar. ■