von Ansgar Alfred Huth

Die *Wanze im Haus* erspart den *Unternehmensberater*

Die Manager Europas haben gelernt, ihr Know-how zu verschlüsseln und nach aussen hin zu schützen. Doch jetzt feiert der klassische Lauschangriff im Inneren unserer Chef-Etagen ein verheerendes Come-back.

In einer Zeit, in der man peinlichst darauf achtet, dass vertrauliche Informationen verschlüsselt werden, und IT-Sicherheit in den Unternehmen höchste Priorität geniesst, taucht sie plötzlich wieder auf: die altbewährte „Wanze“ im Büro oder Privatgemach. Und sie ist gefährlicher denn je. Schliesslich hat sich der Spionage-Minisender 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 – noch verheerendere – Evolutionsrichtung dieser Miniverräter konnte vor einigen Jahren noch keiner voraussagen: Durch das mittlerweile nicht mehr kontrollierbare Internet hat jede Person Zugriff auf alle möglichen Varianten der heute 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 World Wide Web problemlos beschaffen. Die Tarnungen dieser kleinen Informationsbringer sind zum Teil genial. Mit einem Empfänger in der Grösse einer Zigarettenschachtel kann der Lauscher die von der Wanze gesendeten Gespräche mithören oder aufzeichnen. Und wer würde sich nicht für die Planungen und Schwächen seiner Konkurrenten interessieren? Jemand, der die Gedanken seiner Mitmenschen lesen könnte, wäre im Geschäftsleben (und nicht nur dort) unschlagbar.

Die Bereitschaft, solche verbotenen Informationsbringer einzusetzen, ist in den vergangenen Jahren immens gestiegen, da minimaler Kostenaufwand für die Lauschmittel maximalen Vorteil verspricht. Hinzu kommt, dass das Risiko des Lauschers, bei einer Abhöraktion ertappt zu werden, gegen null tendiert. Denn wer verfügt schon über eine schützende Lauschabwehreinrichtung, geschweige denn das Wissen, sich gegen diese illegalen Vorgehensweisen geschäftlich oder gar privat zu schützen?

Mannigfaltige Tarnungen

Das Platzieren der Lauschmittel erinnert an die Ausbringung von trojanischen Viren im Internet. Kleine Geschenke erhalten die Freundschaft, aber auch den Informationsfluss. Solartaschenrechner, Aschenbecher und andere vermeintlich nützliche Gebrauchsgegenstände sind beiebte Verpackungen für Wanzen. Aktenkoffer, bestückt mit einem Sender, die während der Zeit des angeblich 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 Gebrauchsanleitung für ein paar tausend Franken 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.

Das Werbegeschenk als Mogelpackung, hier: die Wanze im Kugelschreiber

ISDN-Viren, Telefonwanzen, Richtmikrofone, Körperschallmikrofone, Laser-Abhörgeräte, Lauschen per Computer, Bildschirmanzeigen in sicherer Entfernung ausspionieren und aufzeichnen: Alles das ist nur eine Frage des Geldes und der Leistungsbereitschaft krimineller Anwender. „Kugelschreiber mit eingebauter Hochleistungswanze, das macht dann 500 Franken bitte. Oder darf es noch ein bisschen mehr sein?“ Das Internet macht's möglich. Und auch die Leistungsgesellschaft fordert ihren Tribut. Das Zugehörigkeitsgefühl der einzelnen Angestellten zur Firma ist mittlerweile nicht mehr so, wie es sein sollte. Jeder kämpft für sich und mit Sicherheit erfolgreicher 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. Wer könnte dieser Tatsache widersprechen? Und wer käme da nicht in Versuchung?

Effektive Lauschabwehr

Die Gefahr ist also real. Abwehr tut not. Doch abwehren kann nur eine Person, die

Was tun im Verdachtsfalle?

eFacts

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

auch das Angreifen erlernt hat und somit realistisch die Angriffspunkte einschätzen kann. Denn zum effektiven Abwehren eines Lauschangriffes muss man sich in die technisch möglichen und finanziell gerechtfertigten Angriffsmöglichkeiten des Lauschers versetzen. Und das kann nur ein Fachmann. Auch der aktuelle Überblick über die international zu beschaffenden Spionageutensilien, ebenso der stetige Kontakt zu den Herstellern von Lauschabwehrmitteln, 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 beziehungsweise nicht bekämpfen will. Ein Lauscher, der mit einer Untersuchung seines Spionagefalles rechnet, versucht natürlich, die auffindbaren Spuren seines

Basierend auf 30-jähriger Forschungs- und Entwicklungszeit wurde in Deutschland ein „Lauschabwehrkoffer“ entwickelt, der als ganz normaler Aktenkoffer getarnt zu jedem zu überwachenden Einsatzort unauffällig mitgeführt werden kann. Das im Koffer untergebrachte Equipment wird durch Software-Updates immer auf dem neuesten Stand der Technik gehalten und verfügt über eine lautlose Raumüberwachung, die das Detektieren und Lokalisieren von Abhöreinrichtungen erlaubt – ohne dass der Lauscher dies bemerkt. Zudem besteht die Möglichkeit, den Lauscher zu ermitteln und ihn mit falschen Informationen zu versorgen. Dennoch: 100-prozentige Sicherheit kann und wird es 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.
Interessenten können sich informieren bei: Ansgar Alfred Huth, Sachverständiger für Datenschutz und Lauschabwehr,
Tel. 0049 - 6023 - 918700, huth@lauschabwehr.de

Angriffes zu entfernen, zu vernichten oder zumindest zu deaktivieren. Letzteres hat beispielsweise bei den bewährten fernsteuerbaren Wanzen ein Ausschalten der Sendeeinheit zufolge. Das Auffinden einer nicht-sendenden Wanze ist wesentlich aufwendiger als das Detektieren eines aktiven Minisenders.

Die vielen unterschiedlichen Wanzenarten stellen einen grossen Teil der angewendeten Angriffstechniken dar – die Vielfalt der Lauschangriffstechniken und somit die Angriffsart ist aber von dem Vorstellungsvermögen und den finanziellen Mitteln des Angreifers abhängig. Wer weiss schon, dass man die auf dem Computer-monitor

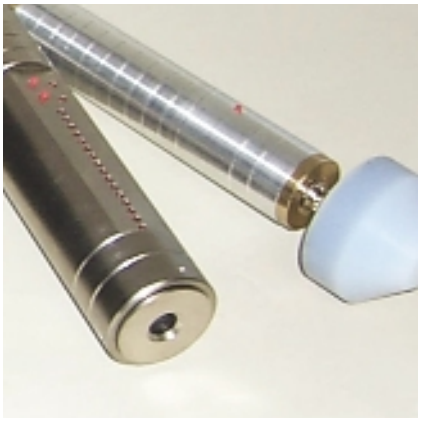
bearbeiteten Schriftstücke oder CAD-Zeichnungen zeitgleich in sicherer Entfernung nur durch das Auswerten der kompromittierenden HF-Strahlung wieder auf einem Monitor darstellen und bequem aufzeichnen kann (in CAD-Zeichnungs-Qualität versteht sich). Auf diese Art und Weise kann jeder gelernte Fernsehtechniker oder begnadete Bastler mit einem alten modifizierten Fernsehgerät die Preiskalkulationen seines Wettbewerbers 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 kennen und stetig die Weiterentwicklungen dieser Angriffsart im Auge behalten.

Zeitgemässes Equipment

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 Franken einen ernst zu nehmenden Lauschabwehreinsatz starten zu können, 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.

Lauschabwehr ernsthaft und effektiv zu betreiben ist nun mal 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 nötige Fachwissen mit dem Lesen der Bedienungsanleitung.

www.spionage.info

Mikrofone, Wanzen & Co.

Die folgende Auflistung der von jedermann zu beschaffenden Spionagemittel ist nur ein kurzer Auszug zu diesem Thema. Die Vielfalt der Lauschangriffstechniken und somit die Angriffsart ist von dem Vorstellungsvermögen und den finanziellen Mitteln des Angreifers abhängig.

„Wanzen" Minisender

Funktion

Versteckte, getarnte Raummikrofone übertragen Gespräche über Funk. Reichweite: 20 m bis 5 km. In Verbindung mit einer Scanner-Handy-Einheit: Reichweite weltweit. Energieversorgung 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.

Versteck

Die winzigen elektronischen Bauteile können in jedem Hohlraum stecken, in abgehängten Decken, Böden, Möbeln, Elektrogeräten, Zimmerpflanzen. Hier zählt Phantasie, Einfallsreichtum und Erfahrung.

Aufwand

Die Montage geht schnell und ist kinderleicht. Einfache Wanzen sind ab CHF 150,- zu haben. Wenn es sich zum Beispiel um eine getarnte Wanze handelt (Uhr, Taschenrechner, Lampe, etc.) kann sich der zukünftig Abgehörte wenigstens über ein schönes Werbegeschenk freuen und platziert das liebe „Info-Ungeziefer" eigenhändig in seinen vier Wänden.

Täter

Jeder, der Zugang zum Zimmer hat. Mitarbeiter, Besucher, Putzfrauen, Handwerker, Monteure. Letztendlich hat jeder die Möglichkeit, sich Zutritt zu einem Raum zu verschaffen.

Abwehr

Profi-Wanzenaufspürgeräte (z. B. MO 2055/II) ab ca. CHF 30.000,- (Sachverständigenwissen vorausgesetzt); Elektronisches Grossreinemachen als Dienstleistung durch einen anerkannten Sachverständigen (Sweeping) ab ca. CHF 1.500,- bis CHF 7.500,- (abhängig von Raumgrösse und Aufwand)

Mini-Tonbandgeräte

Funktion

Die Winzlinge zeichnen Sprache auf. Ein Tonbändchen in Scheckkartengrösse nimmt ca. 3 Stunden auf, selbst das allerkleinste Gerät in einem Kugelschreiber schafft 70 Minuten. Neuere Produkte erreichen sogar 4 Stunden und mehr digitale Aufzeichnung.

Versteck

Fast immer bringen Besucher die Tonbänder mit. Die Geräte werden entweder am Körper getragen, in Aktenkoffer oder anderen Konferenzutensilien eingebaut.

Aufwand

Jeder Laie kann die Mini-Tonbänder einsetzen. Ein Gerät in Scheckkartengrösse kostet ab ca. CHF 500,-.

Täter

Besucher, die das vertraulich gesprochene Wort heimlich dokumentieren wollen.

Abwehr

Sehr schwierig. Durch das geringe Magnetfeld des Löschkopfes elektronisch kaum zu orten. Profi-Wanzenaufspürgeräte mit Tonbanddetektor-Erweiterungseinheit (z. B. MO 2055/II) ab ca. CHF 30.000,- (Sachverständigenwissen vorausgesetzt)

Elektronisches Grossreinemachen als Dienstleistung durch einen anerkannten Sachverständigen (Sweeping) ab ca. CHF 1.500,- bis CHF 7.500,- (abhängig von Raumgrösse und Aufwand)

Notfalls Gepäck röntgen, Metalldetektoren einsetzen

Körperschallmikrofone

Funktion

Der Lauscher nutzt z. B. einen Heizkörper oder die ganze Wand wie ein Mikrofon. Schallwellen versetzen den Körper in Schwingungen, die das Gerät auffängt, verstärkt, filtert und hörbar macht.

Versteck

Der Lauscher sitzt unbehelligt im angrenzenden Raum. Beliebte Lauschstellen sind auch Versorgungsschächte, die vertikal durch alle Etagen führen.

Aufwand

Spitzengeräte liefern erstaunliche Hörqualität, Preis ab CHF 4.000,-. Leistungsschwächere Geräte ab CHF 500,-.

Täter

Jeder, der Zugang zum Nachbarraum hat. Funktioniert auch durch eine Glasscheibe. Betriebsinterne oder betriebsfremde Täter.

Abwehr

Rauschgeneratoren machen das Belauschen von Körperschall fast unmöglich, sind aber teuer. Rauschgeneratoren für einen kleinen Raum kosten ca. CHF 1.500,- bis CHF 4.500,-.

Drahtfunk

Funktion

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".

Versteck

In 220V-Elektrogeräte eingebaut. Oft tauschen die Lauscher vorhandene gegen präparierte Geräte aus oder implantieren das kleine Senderchen währen einer Reparatur oder günstigen Aufrüstung. Besonders beliebt: Einbau in handelsübliche Mehrfachsteckdosen.

Aufwand

Wie bei Wanzen wird ein zusätzliches Empfangssystem benötigt (wird einfach in irgendeine Steckdose im Haus eingesteckt). Das System kostet ca. CHF 750,- bis CHF 1.500,-.

Täter

Besucher, Monteure, Mitarbeiter. Der Empfang kann nur im Gebäude stattfinden.

Abwehr

Profi-Wanzenaufspürgeräte mit Netzstrom-Erweiterungseinheit (z. B. MO

2055/II) ab ca. CHF 30.000,- (Sachverständigenwissen vorausgesetzt)
Elektronisches Grossreinemachen als Dienstleistung durch einen anerkannten Sachverständigen (Sweeping) ab ca. CHF 1.500,- bis CHF 7.500,- (abhängig von Raumgrösse und Aufwand)
Netzverrauschung durch Rauschgeneratoren oder Einbau von Netzfiltern. Letztere filtern die Langwellen (zu übertragende Sprache) heraus und verhindern so die Übertragung.

Festverdrahtete Raummikrofone

Funktion
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.
Versteck
Diese Raummikrofone finden sich vor allem in Deckenverkleidungen und Mauerhohlräumen.
Aufwand
Nur mit hohem Aufwand machbar, aber dann unbegrenzte Betriebs- und Nutzungszeit.
Täter
Profi-Lauscher in Botschaften und Auslandsvertretungen, Hotels und besonders in Konferenzzentren und 1. Klasse Kabinenplätze in Flugzeugen bestimmter Airlines, etc.
Abwehr
Extrem aufwendig. Abhören kann durch Rauschgeneratoren erschwert werden.
Ausweichen ins Freie ist nur sinnvoll, wenn niemand in Sichtweite elektronisch mithören kann.

Richtmikrofone

Funktion
Der Schall wird durch ein Parabol-Richtmikrofon oder Standard-Richtmikrofon eingefangen. Die Schallwellen werden wie bei einer Körperschall-Auswertung mehrfach verstärkt, gefiltert und ausgewertet.
Versteck
Der Lauscher lauert z. B. im Freien auf einer Parkbank und richtet die Spitze seines Regenschirmes unbemerkt auf eine Person oder ein geöffnetes Bürofenster. Diese Regenschirmspitze, die während des Spazierens durch eine kleine Hülse geschützt ist, stellt das Richtmikrofon dar.
Aufwand
Jeder Laie kann diese Richtmikrofone ansetzen. Einfache Bedienung. Leistungsfähige Geräte kosten ab ca. CHF 600,-.
Täter
Ob Laie oder Profi, jeder kommt in Frage.
Abwehr
Wichtige Gespräche nicht im Freien in Sichtweite anderer Personen führen. In Chef- und Besprechungsräumen Fenster geschlossen halten.

Telefonwanzen

Funktion
Die Täter klemmen sie z. B. direkt an die Telefonleitung, die dann auch den Strom liefert. Der Sender wird aktiviert, wenn der Hörer abgenommen wird, überwacht permanent den Raum in Sachen Schallwellen oder wird von aussen aktiviert.
Versteck
Telefon, Telefonanschlussdose, innerhalb oder ausserhalb der Telefonleitungen des Hauses (Verteilerkasten, Vermittlungsstelle der Telefongesellschaft)
Aufwand
Ein versierter Laie kann die zuckerwürfelgrossen Telefonwanzen leicht einbauen. Preis ab ca. CHF 200,- inkl. Bedienungsanleitung.
Täter
Servicetechniker, Ehemänner, letztendlich jeder, der im Internet einkaufen kann. Bei einer Installation in Verteilerkästen muss man jedoch bei dem Täter eine hohe kriminelle Energie voraussetzen.
Abwehr
Professionelle Telefon-Leitungsüberwachung durch einen erfahrenen anerkannten Dienstleitungsbetrieb, der den Telefonanschluss permanent in Sachen Funktionsfähigkeit und Anomalien überwachen kann. Kosten ca. CHF 50,- pro Monat.
Profi-Wanzenaufspürgeräte mit Telefonleitungs-Erweiterungseinheit (z. B. MO 2055/II) ab ca. CHF 30.000,- (Sachverständigenwissen vorausgesetzt)
Elektronisches Grossreinemachen als Dienstleistung durch einen anerkannten Sachverständigen (Sweeping) ab ca. CHF 1.500,- bis CHF 7.500,- (abhängig von Raumgrösse und Aufwand)
Daten- und Gesprächsverschlüsselungstechnik einsetzen.

Fax-Monitoring-System

Funktion
Das System protokolliert zusätzlich alle ein- und ausgehenden Faxnachrichten auf Papier oder Festplatte. Die Teilnehmer merken davon nichts.
Versteck
Das Gerät wird direkt an die Faxleitung (Telefonleitung) angeschlossen, wie die festinstallierte Telefonwanze.
Aufwand
Fax-Monitoring-Systeme sind ab ca. CHF 6.000,- zu erwerben.
Täter
Profis, die gezielt vorgehen und sich die Bespitzelung etwas kosten lassen.
Abwehr
Professionelle Telefon-Leitungsüberwachung durch einen erfahrenen anerkannten Dienstleitungsbetrieb, der den Telefonanschluss permanent in Sachen Funktionsfähigkeit und Anomalien überwachen kann. Kosten ca. CHF 50,- pro Monat.
Profi-Wanzenaufspürgeräte mit Telefonleitungs-Erweiterungseinheit (z. B. MO 2055/II) ab ca. CHF 30.000,- (Sachverständigenwissen vorausgesetzt)
Elektronisches Grossreinemachen als Dienstleistung durch einen anerkannten Sachverständigen (Sweeping) ab ca. CHF 1.500,- bis CHF 7.500,- Daten- und Gesprächsverschlüsselungstechnik einsetzen.