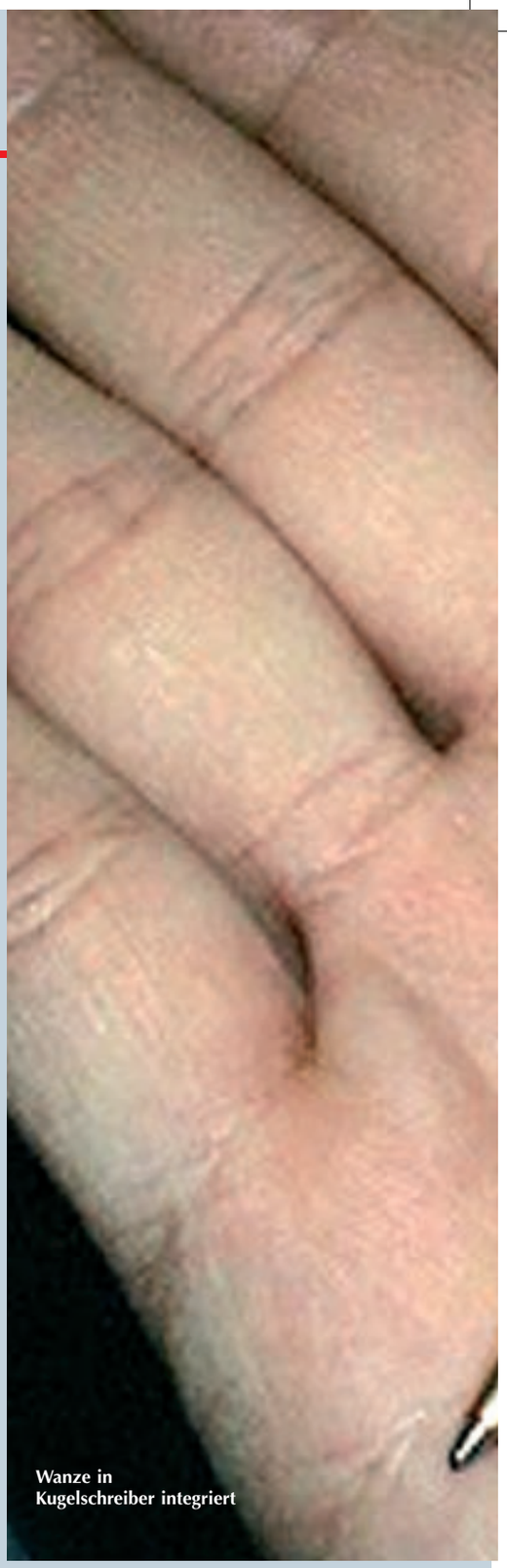
Die Wanze im Haus ...

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.



Wanze in Kugelschreiber integriert

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 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 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 gesendeten Gespräche der Wanze 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 illegale Vorgehensweisen geschäftlich oder gar privat zu schützen?

In Deutschland befinden sich laut Schätzung der Herstellerfirmen zwischen 500 000 und 1 000 000 Abhörgeräte im Besitz von Privatpersonen. Wer eine öffentliche Sicherheits-Fachmesse wie die „security" in Essen schon einmal besucht hat, der weiß, dass die mit Abstand am besten besuchten Messestände die der Anbieter von Abhörgeräten sind. Mit einer Wanze in der Größe eines Zuckerwürfels, die nur ein paar hundert Euro kostet, werden Entwicklungsaufwand, Wettbewerbsvorsprung oder gar ganze Existenzen innerhalb kürzester Zeit vernichtet.

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 vermeintliche nützliche Gebrauchsgegenstände sind beliebte Verpackungen für Wanzen.

Aktenkoffer, bestückt mit einem Sender, 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 Gebrauchsanleitung für ein paar tausend Euro zu kaufen. Wenn ein Babyfon 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 in sicherer Entfernung ausspionieren und aufzeichnen: Alles das ist nur eine Frage des Geldes und der Leistungsbereitschaft krimineller Anwender.

„Ein Kugelschreiber mit eingebauter Hochleistungswanze, das macht dann bitte 350 Euro. Oder darf es noch ein bisschen mehr sein?“ Das Internet macht’s möglich. Und auch die Leistungsgesellschaft fordert ihr 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?

Die Gefahr ist also real. Abwehr tut not. Doch abwehren kann nur eine Person die 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 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 nichtsendenden Wanze ist wesentlich aufwendiger als das Detektieren eines aktiven Minisenders. Wobei die vielen unterschiedlichen Wanzenarten zwar einen

Wanzen-Set in Modulbauweise

Empfänger mit automatischer Gesprächsaufzeichnung

großen Teil der angewendeten Angriffstechniken darstellen, die Vielfalt der Lauschangriffstechniken und somit Angriffsart aber nur von dem Vorstellungsvermögen und den finanziellen Mitteln des Angreifers abhängt.

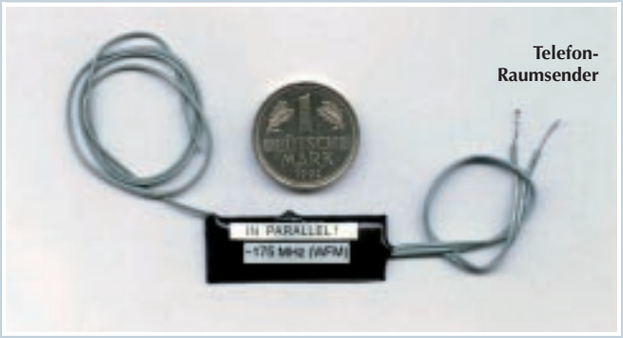
Wer weiß schon, dass man die auf dem Computermonitor bearbeitete Schriftstücke oder CAD-Zeichnungen zeitgleich in sicherer Entfernung nur durch das Auswerten der kompromittierenden HF-Strahlung wieder auf einem Monitor darstellen und bequem aufzeichnen kann (in CAD-Zeichnungs-Qualität versteht sich). 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.

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 Euro 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.

Basierend auf 30-jähriger Forschungs- und Entwicklungszeit wurde in Deutschland ein „Lauschabwehrkoffer" entwickelt, der in Sachen Detektieren und Abwehren von Lauschangriffen eine einzigartige Leistungsvielfalt aufweist und als ganz normaler Aktenkoffer getarnt

Spionage-Abwehrkoffer



Telefon-Raumsender

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 das der Lauscher dies bemerkt. Zudem besteht die Möglichkeit, den Lauscher zu ermitteln und ihn mit falschen Informationen zu versorgen.

Kleinst-UHF-Sender

Dennoch: Hundertprozentige 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.

Was tun, im Verdachtsfalle?

Nehmen Sie Kontakt mit dem Abwehrfachmann auf, aber nie von den als „abhörgefährdet“ eingestuften Räumlichkeiten aus! Benutzen Sie 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 E-Mail jederzeit von Unbefugten gelesen und manipuliert werden kann.

Der Autor: Ansgar Alfred Huth,
Sachverständiger für Datenschutz und Lauschabwehr, Alzenau,
Tel. 06023/918700, huth@lauschabwehr.de, www.spionage.info