Vorsicht Wanzen!

Spionage ■ Die Manager haben gelernt, ihr Know-how zu verschlüsseln und nach aussen hin zu schützen. Doch jetzt feiert der klassische Lauschangriff im Inneren unserer Chefetagen ein verheerendes Comeback.

ANSGAR HUTH*

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. 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.

In Deutschland befinden sich laut Schätzung der Herstellerfirmen inzwischen 500 000 bis 1 000 000 Abhörgeräte im Besitz von Privatpersonen. Wer eine öffentliche Sicherheitsfachmesse 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 Babyphon die Form einer handelsüblichen Mehrfachsteckdose aufweist und auf Grund 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.

Lauschen per Computer

ISDN-Viren, Telefonwanzen, Richtmikrofone, Körperschallmikrofone, Laser-Abhörgeräte, Lauschen per Computer, Bildschirmanzeigen in sicherer Entfernung ausspionieren und aufzeichnen: All das ist nur eine Frage des Geldes und der Leistungsbereitschaft krimineller Anwender. «Kugelschreiber mit eingebauter Hochleistungswanze, das macht dann 350 Euro bitte, danke. Oder darf es noch ein bisschen mehr sein?» Das Internet machts 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. 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 Spionage-

- Abhörgeräte werden immer leistungsfähiger, kostengünstiger und bedienungsfreundlicher.
- «Wanzen» kauft man heute anonym und zu Discountpreisen über das Internet.
- Die Hemmschwelle, sich illegal Wettbewerbsvorteile zu verschaffen, ist in unserer heutigen Leistungsgesellschaft extrem gesunken.
- Nur sehr wenige Experten in Europa verfügen über das technische Equipment und Know-how, erfolgreiche Lauschabwehreinsätze zu realisieren.

* Ansgar Alfred Huth, Sachverständiger für Datenschutz und Lauschabwehr, 63755 Alzenau, Tel. (06023)918700 huth@lauschabwehr.de www.spionage.info

Was tun im Verdachtsfall?

- 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-/E-Mail-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.

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

Wer weiss schon, dass man die auf dem Computermonitor 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-Zeichnungsqualität 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.

Abwehren kostet

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 Lauschabwehrequipment 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 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. ■