Lauschangriff

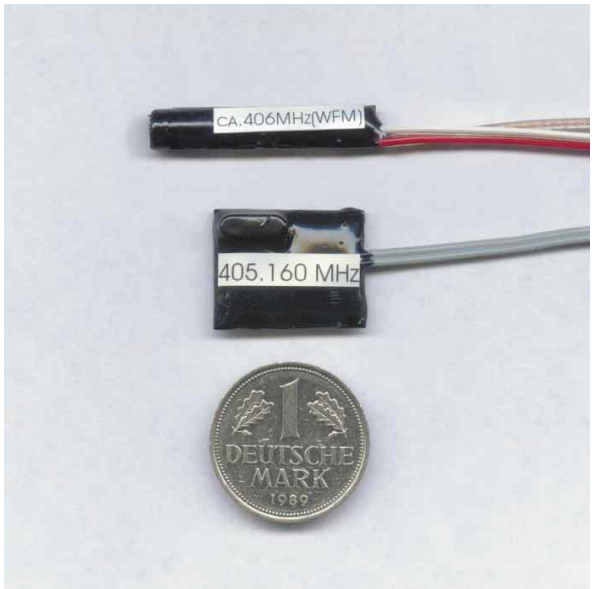
Renaissance der Wanzen

Von Ansgar Huth, Alzenau

Mehr Verschlüsselung – weniger Spionage? Leider nur bedingt... Während wichtige E-Mails und Telefonate zunehmend chiffriert durchs Netz laufen, feiert der klassische Lauschangriff im Inneren von Chef-Etagen und Entwicklungsabteilungen ein verheerendes Comeback, unterstützt durch technische Fortschritte und einfache Verfügbarkeit der Abhörtechnik.

In einer Zeit, in der man peinlichst darauf achtet, vertrauliche Informationen zu verschlüsseln, und in der IT-Sicherheit erhöhte Priorität genießt, da taucht sie plötzlich wieder auf: die altbewährte „Wanze" im Büro oder Privatgemach. Und sie ist gefährlicher denn je. Schließlich haben sich die Spionage-Minisender im Laufe der vergangenen Jahre erschreckend schnell in zwei Richtungen weiterentwickelt. Die erste Veränderung war vorhersehbar: Die heutigen Wanzen sind kleiner, leistungsstärker, bedienungsfreundlicher und schwerer zu finden als ihre früheren Artgenossen. Die zweite – noch verheerendere – Evolutionsrichtung dieser Mini-Verräter hat vor einigen Jahren noch niemand erahnt: Durch das Internet hat jede Person einfachen und relativ anonymen Zugriff auf alle möglichen Varianten der heutigen modernen Abhörtechnik.

Spionageutensilien die früher nur mit Beziehungen, großem Zeitaufwand und viel Geld zu beschaffen waren, werden heutzutage im Internet gut sortiert, inklusive Bedienungsanleitung, zu Discountpreisen angeboten. Als Aschenbecher, Handy, Taschenrechner, Kugelschreiber oder Mehrfachsteckdose verkleidet kann man gebrauchsfertige Funkwanzen über das World Wide Web problemlos beschaffen. Die Tarnung dieser kleinen Informationsbeschaffer 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? Die Hemmschwelle, sich illegal Wettbewerbsvorteile zu verschaffen, ist in unserer heutigen Gesellschaft extrem gesunken, zumal angesichts schwieriger wirtschaftlicher Bedingungen.



Funkwanzen, die ihre Stromversorgung aus vorhandenen Quellen (Telefon, Handyakku, Computerhardware, Steckdose usw.) ziehen, sind klein, leicht zu verstecken und per Internet einfach zu erwerben.

Die Investitionsbereitschaft in verbotene Informationsbringer ist in den vergangenen Jahre auch deshalb immens gestiegen, da geringe Kosten für die Lauschmittel maximalen Vorteil versprechen. 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 über das Fachwissen, sich gegen derartige illegale Vorgehensweisen geschäftlich oder gar privat zu schützen?

In Deutschland befinden sich laut Schätzung der Herstellerfirmen inzwischen 500 000 bis 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 diejenigen 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.

Geschenkter Gaul

Das Platzieren der Lauschmittel erinnert an die Ausbringung von Trojanischen Pferden: Kleine Geschenke erhalten die Freundschaft, aber auch den Informationsfluss. Solartaschenrechner, Aschenbecher und andere vermeintliche nützliche Gebrauchsgegenstände sind beliebte Verpackungen für Wanzen. Seit vielen Jahren inklusive Gebrauchsanleitung für ein paar tausend Euro zu kaufen: Aktenkoffer, bestückt mit einem Sender, die man während eines vorgeblichen, plötzlich dringenden Telefongespräches im Verhandlungsraum zurücklässt, und das dazugehörige

Handy, das als Empfänger für die Wanze im Koffer dient, um die ahnungslosen Verhandlungspartner in der Zwischenzeit zu belauschen. Wenn ein „Babyphon“ die Form einer handelsüblichen Mehrfachsteckdose aufweist und aufgrund des vorhandenen Netzstroms eine dauerhafte Überwachung über größere Distanzen ermöglicht, dann ist dies auch nur eine der vielen einfach zu installierenden verkaufsfertigen Möglichkeiten der Spionage, auf die ein Lauscher zugreifen kann.

ISDN-Mitschnitt, Telefonwanzen, Richt- und Körperschallmikrofone, Laser-Abhörgeräte, Lauschen mit Computerhilfe, um Bildschirmanzeigen in sicherer Entfernung auszuspionieren und aufzuzeichnen: Alles 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 macht's möglich.

Und auch die Leistungsgesellschaft fordert ihren Tribut. Das Zugehörigkeitsgefühl der einzelnen Angestellten zur Firma ist mittlerweile oft nicht mehr so, wie es sein sollte. Jeder kämpft für sich und ist mit Sicherheit erfolgreicher als alle anderen, wenn er in Sachen Information die Nase vorn hat. Dem anderen Wissen voraus zu haben, 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 derjenige, der auch das Angreifen erlernt hat und somit realistisch die möglichen Angriffspunkte und-arten abwägen kann. Zur effektiven Abwehr eines Lauschangriffes muss man sich in alle technisch möglichen und finanziell gerechtfertigten Angriffsmöglichkeiten eines Lauschers versetzen. Das kann nur ein Fachmann. Erst 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.

Stiller Alarm

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

Obwohl die vielen unterschiedlichen Wanzenarten einen großen Teil der verwendeten Attacken darstellen, hängt doch die Vielfalt der Lauschangriffstechniken nur vom Vorstellungsvermögen und den finanziellen Mitteln des Angreifers ab. Mit entsprechendem Einsatz lassen sich auf dem Computermonitor bearbeitete Schriftstücke oder CAD-Zeichnungen zeitgleich in sicherer Entfernung durch das Auswerten der kompromittierenden HF-Strahlung wieder auf einem Monitor darstellen und bequem aufzeichnen (weiterhin in CAD-Zeichnungs-Qualität, versteht sich).

Textdarstellungen auf vereinzelten Bildschirmarbeitsplätzen erfordern weniger Aufwand und ermöglichen schon gelernten Fernsehtechnikern oder begnadeten Bastlern mit relativ wenig Hardware-Aufwand die Preiskalkulationen seines Wettbewerbers in Echtzeit

Ein in Deutschland entwickelter Lauschabwehrkoffer vereint Suchempfänger, Codetonsender, Sound-Korrelator, Bildschirm, Empfangsantennen, Handsonden, Druckerschnittstelle und Expansionsport in einem unauffälligen „Gehäuse“. Der Empfangsbereich erfasst Frequenzen zwischen 1 und 6000 MHz mit FM-, AM-, NFM-, NAM-Modulation.

Was tun im Verdachtsfall?

Kontaktieren Sie einen Abwehrfachmann oder die Behörden niemals aus den als „abhörgefährdet“ eingestuften Räumlichkeiten heraus.

Benutzen Sie am besten eine öffentliche Telefonzelle oder einen Telefon-/E-Mail-Anschluss eines **nicht im normalen Umfeld** gelegenen Kommunikationsmittels und Teilnehmers. Schalten Sie während des Telefongespräches ihr Handy aus oder lassen Sie es am besten im Auto oder Büro (manipulierte Handys lassen sich ggf. ohne jede Display-Meldung ferngesteuert zum Abhören aktivieren).

Bedenken Sie zudem, dass eine unverschlüsselte E-Mail immer die Gefahr birgt, von Unbefugten gelesen und manipuliert zu werden.

mitzuerleben. Kompromittierende Abstrahlung ist übrigens auch bei Netzwerkleitungen und Überwachungskameras ein nicht zu vernachlässigendes Informationsschlupfloch. Abwehrmaßnahmen gegen diese Spionagemethode sind verfügbar und reichen von besonderer Software über abschirmende Tapeten bis hin zu Störsendern sowie aufwändigen abstrahlsicheren Gehäusen und Räumen.

Abhörempfänger mit automatischer Gesprächsaufzeichnung

Auch hier gilt es, die aktuelle Entwicklung zu verfolgen, die von der (auch Fach-)Öffentlichkeit eher unbeobachtet vonstatten geht. Was heute noch abwehrt oder zu aufwändig ist, kann in ein paar Wochen schon überholt sein und dann vielleicht ein noch größeres Gefahrenpotenzial darstellen als aus Unwissenheit komplett unterlassene Abwehrmaßnahmen. Denn wer sich als Geschäftsmann mit seiner (veralteten) Abwehreinrichtung in Sicherheit wiegt, wird leicht zum gefundenen Fressen für die Lauschangriffe eines Konkurrenten.

Eine funktionierende Lauschabwehrausstattung ist nicht unter einer fünfstelligen Summe zu erwerben – und wie so oft bei Sicherheitstechnik ist es mit dem Lesen der Bedienungsanleitung nicht getan, sondern die eigentlichen Kosten entstehen durch das eingesetzte Personal. 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 ermöglicht eine lautlose Raumüberwachung zum Detektieren und Lokalisieren von Abhöreinrichtungen – ohne dass der Lauscher dies bemerkt. Somit besteht die Möglichkeit, den Lauscher zu ermitteln und ihn mit falschen Informationen zu versorgen. „Natürlich" wird man auch damit keine 100-prozentige Sicherheit erreichen, jedoch kann man mit einem erfahrenen Partner an seiner Seite Informationsdiebstähle im Verdachtsfall wirksam und solide bekämpfen oder mit hoher Wahrscheinlichkeit ausschließen. ◆

Ansgar Alfred Huth ist Sachverständiger für Datenschutz und Lauschabwehr (www.spionage.info).