Lauschangriff

Auf der Lauer: Wanzen

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.

In einer Zeit, in der IT-Sicherheit erhöhte Priorität genießt, taucht die „altbewährte“ Wanze gefährlicher denn je wieder auf - im Büro oder zu Hause. Die heutigen Wanzen sind kleiner, leistungsstärker, bedienungsfreundlicher und schwerer zu finden als ihre früheren Artgenossen. Noch gravierender: Durch das Internet hat jede Person einfachen und relativ anonymen Zugriff auf alle möglichen Varianten der heutigen modernen Abhörtechnik. Spionageutensilien werden dort 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 ist zum Teil genial. Mit einem Empfänger in der Größe einer Zigarettenschachtel kann der Lauscher die gesendeten Gespräche der Wanze mithören oder aufzeichnen. Die Hemmschwelle, sich illegal Wettbewerbsvorteile zu verschaffen, ist in unserer heutigen Gesellschaft extrem gesunken - angesichts schwieriger wirtschaftlicher Bedingungen. Auch ist das Zugehörigkeitsgefühl der einzelnen Angestellten zur Firma mittlerweile geringer. Jeder kämpft für sich und nur der ist erfolgreich, wer in Sachen Information die Nase vorn hat.

Die Investitionsbereitschaft in verbotene Informationsbringer ist in den vergangenen Jahre auch deshalb immens gestiegen, weil geringe Kosten für die Lauschmittel maximalen Vorteil versprechen. Hinzu kommt, dass das Risiko des Lauschers, bei einer Abhöraktion ertappt zu werden, gegen Null tendiert. 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, 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. Die Gefahr ist real. Abwehr tut not. 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.

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 oder 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.

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

Kompromittierende Abstrahlung bei Bildschirmarbeitsplätzen oder bei Netzwerkleitungen und Überwachungskameras ist 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.

Eine funktionierende Lauschabwehrausstattung ist nicht unter einer fünfstelligen Summe zu erwerben – und wie so oft bei Sicherheitstechnik ist es mit dem Lesen der Bedienungsanleitung auch nicht getan, sondern die eigentlichen Kosten entstehen durch das eingesetzte Personal. Mit einem erfahrenen Partner an der Seite kann man Informationsdiebstähle im Verdachtsfall wirksam und solide bekämpfen oder mit hoher Wahrscheinlichkeit ausschließen.

Ansgar Alfred Huth
Sachverständiger für Datenschutz und Lauschabwehr
Hanauerstr. 58, 63755 Alzenau
Tel.: +49 (0) 6023-918700; Fax.: +49 (0) 6023-918701;Handy: +49 (0) 179-1958282 ; http://www.spionage.info; Email.: huth@spionage.info

Zum Autor: Ansgar Alfred Huth ist ein anerkannter und erfahrener Datenschutz- und Lauschabwehr-Sachverständiger, der in den Bereichen Abhörsicherheit und detektieren von Lauschangriffen einen nicht gerade alltäglichen Erfahrungsschatz nachweisen kann.