Sicherheits- und Service-Report

EOS-Sicherheitsdienst
Friedenstraße 21 · 89555 Steinheim
Telefon (0 73 29) 72 71
Fax (0 73 29) 16 24
E-Mail: b.elsenhans@eos-online.de
www.eos-online.de

Der Lauschangriff feiert in der Wissensgesellschaft ein Comeback:

„Nicht jedes Geschenk kommt von Herzen“

Bernd Elsenhans ist Geschäftsführer der EOS-Unternehmensgruppe in Steinheim, Fachautor, Referent und Experte für Sicherheit.

Werbegeschenke wie Kulis oder Aschenbecher mit Wanze: 350 Euro, bitte. Viel später als ihre Kollegen in den USA oder Frankreich haben deutsche Unternehmer gelernt, ihr Wissen zu schützen. Kaum ist dies durch Schutzmechanismen wie Firewalls geschehen, feiert der alte Lauschangriff auf Chefetagen, Konstruktions- und Forschungsabteilungen ein Comeback. Die Gründe dafür liegen auf der Hand: Die Technik der Abhörgeräte wird immer leistungsfähiger und billiger, die „Wanzen“ (Minisender) kauft man heute anonym zu Discountpreisen übers Internet. Der Minisender hat sich in zwei Richtungen rasant entwickelt: er ist bedienungsfreundlich und kleiner – und damit schwer zu finden. Im Internet findet man ein breites Sortiment Wanzen inklusive Bedienungsanleitung zu Discountpreisen. Als Handy, Aschenbecher, Taschenrechner, Kugelschreiber oder Mehrfachsteckdose getarnt, kann man sich die Funkwanzen problemlos beschaffen, sogar genial getarnt.

Die Bereitschaft, solche verbotene Informationsbringer einzusetzen, ist gestiegen, da minimaler Kostenaufwand maximalen Vorteil verspricht. Mit einer Wanze in der Größe eines Stücks Würfelzucker werden Entwicklungsaufwand, Wettbewerbsvorsprung oder ganze Existenzen innerhalb kürzester Zeit vernichtet. Dabei tendiert das Risiko des Lauschers, ertappt zu werden, gegen null. Denn wer verfügt schon über eine Einrichtung zur Lauschabwehr, geschweige denn das Wissen, sich gegen diese illegale Vorgehensweise zu schützen?

In Deutschland befinden sich nach Schätzung der Hersteller eine Million Abhörgeräte im Besitz von Privatpersonen. Auf der Sicherheits–Fachmesse „Security“ in Essen sind die am besten besuchten Messestände die der Anbieter von Abhörgeräten. Das Platzieren der Lauscher erinnert an Troja: In kleinen Geschenkartikeln wie Solartaschenrechnern oder Aschenbechern werden die Wanzen versteckt. Oder Aktenkoffer werden mit einem Sender bestückt. Wenn ein Babyfon die Form einer handelsüblichen Mehrfachsteckdose aufweist und auf Grund des vorhandenen Netzstroms eine dauerhafte Überwachung ermöglicht, dann ist auch dies eine der vielen einfach zu installierenden verkaufsfertigen Möglichkeiten der Spionage.

ISDN-Viren, Telefonwanzen, Richt- und Körperschallmikrofone, Laser-Abhörgeräte, Lauschen per Computer, Bildschirmanzeigen in sicherer Entfernung ausspionieren und aufzeichnen: Alles nur eine Frage des Geldes und der Anwendungsbereitschaft.

Auch unsere Leistungsgesellschaft fordert ihren Tribut. Jeder kämpft für sich und mit Sicherheit erfolgreicher als alle anderen, wenn er in Sachen Information die Nase vorn hat. Wer käme da nicht in Versuchung? Die Gefahr ist real. Abwehr tut Not. Doch abwehren kann nur der, der auch das Angreifen gelernt hat und somit die Angriffspunkte realistisch einschätzen kann. Das kann nur ein Fachmann. Effektive Abwehr heißt auch, den Lauscher im Glauben zu lassen, dass man den Lauschangriff nicht ahnt. Ein Lauscher, der mit einer Gegenaktion rechnet, versucht verständlicherweise, die Spuren seines Angriffs zu entfernen, zu vernichten oder zumindest zu deaktivieren. Letzteres hat bei den fernsteuerbaren Wanzen ein Ausschalten der Sendeeinheit zufolge. Das Auffinden einer nicht sendenden Wanze ist wesentlich aufwendiger als das Detektieren eines aktiven Minisenders.

Wer weiß, dass man die auf dem Monitor bearbeiteten Schriftstücke oder CAD-Zeichnungen zeitgleich in sicherer Entfernung allein durch Auswerten der kompromittierenden HF-Strahlung wieder auf einem Monitor darstellen und bequem aufzeichnen kann? So kann jeder Fernsehtechniker oder begnadete Bastler mit einem modifizierten Fernsehgerät die Preiskalkulationen seines Wettbewerbers in Echtzeit miterleben. Die Abwehrmaßnahmen sind unspektakulär und sehr wichtig.

Was heute noch abwehrt, kann in ein paar Tagen schon überholt sein – wie bei den Programmen gegen Computerviren. Der sich in Sicherheit wiegende Geschäftsmann mit der veralteten, nicht mehr funktionierenden Abwehreinrichtung ist ein gefundenes Fressen für Lauschangriffe.

Nicht nur die Aktualität, auch die Qualität der eingesetzten Instrumente ist für die erfolgreiche Lauschabwehr von großer Bedeutung. Wer glaubt, mit Breitbanddetektor oder Feldstärkenmessgerät einen Lauschabwehreinsatz starten zu können, der sollte den Lauscher am besten gleich in seine Räume einziehen lassen.

Lauschabwehr effektiv zu betreiben, ist nun mal wesentlich kostenintensiver als einen Lauschangriff durchzuführen. Während man sich bei einem Angriff für ein Mittel oder eine Kombination aus mehreren entscheiden kann, muss der Fachmann bei einer effektiven Abwehr alle in Frage kommenden Angriffsarten detektieren und abwehren können. Das setzt nicht nur fundiertes Fachwissen voraus, sondern auch eine Ausrüstung, die in der Lage ist, ein breites Spektrum der möglichen Angriffsmethoden und -techniken zu überprüfen. Und diese Ausrüstungen ist nicht für weniger als einem fünfstelligen Betrag zu erwerben. Geschweige denn das nötige Fachwissen mit dem Lesen einer Bedienungsanleitung.

Abhilfe schaffen hier Fachfirmen und Experten, die sicherlich einen Bruchteil vom möglichen Schaden kosten. Fragen Sie uns, wir helfen Ihnen mit Sicherheit.

Miniwanzen, eingebaut in einem Startergehäuse.

Empfangsstation als Abhöreinheit mit Antenne und Netz.

Quelle:
„Sicherheits Management“ von Ansgar Alfred Huth.