

URL dieses Beitrags:

Fachartikel aus PROTECTOR 1-2/2010, S. 12 bis 13

Rubriken: Sicherheitstechnik: Kommunikation, Wirtschaftsschutz: Wirtschaftskriminalität

Lauschabwehr für Besprechungsräume

"Hörschäden" vermeiden

Große Fenster, durch die viel Licht dringt, Lautsprecher in der Decke, ein Nebenstellentelefon, oder aber Handys, die im besten Falle auf lautlos geschaltet sind. Das sind Bedingungen, von denen Konkurrenzspäher und Wirtschaftsspione träumen. Dabei gibt es Schutzmaßnahmen, die selbst für kleine Unternehmen finanziell darstellbar sind.

Es muss ja nicht alles so aufwändig sein, wie der abhörsichere Raum (ASR) in der einstigen Ständigen Vertretung in Ost-Berlin. Was hier besprochen wurde, ist – aller Bemühungen zum Trotz – kein einziges Mal an unbefugte Ohren gedrungen. Ausgerechnet die auf dem Territorium der ehemaligen DDR gelegene „Laube“, so der Codename des ASR, war sicherer als 99,99 Prozent der Besprechungsräume in der Bundesrepublik Deutschland.

Einladung zum Mithören

Zu diesem Maximum an Lauschabwehr gibt es einen überaus betrüblichen Gegenpol. In den meisten Unternehmen gibt es bis heute so wenig Schutz, dass man getrost von einer Einladung zum Mithören sprechen könnte. Dabei finden Lauschangriffe häufiger statt als gemeinhin angenommen. Was Wunder, denn diese Angriffsart eröffnet fremden Diensten und Konkurrenten die optimale Möglichkeit, relevante Informationen auch ohne ein aufwändiges und riskantes Anwerben beziehungsweise Abschöpfen von Innenquellen zu gewinnen. Und das alles für ein paar tausend Euro fuffzig.

Trotz dieser Hintergründe wird in der deutschen Unternehmenswelt die Lauschgefahr nach Kräften verdrängt. Gerade bei Unternehmen kleiner und mittlerer Größe gibt es zwei, häufig zu hörende „Antithesen“, die hier beispielhaft genannt seien:

- „Weshalb sollte jemand ausgerechnet an meiner Firma interessiert sein? Es gibt doch Größere, bei denen weitaus mehr zu holen ist“ oder
- „Kein Unternehmen riskiert den massiven Imageschaden im Entdeckungsfall“

Scheinargumente

Diese Scheinargumente greifen definitiv zu kurz. Denn eines ist sicher: Da die Konzerne sich entsprechend absichern, haben Wirtschafts- und Konkurrenzspione längst die schwächer geschützten Klein- und Mittelunternehmen (KMU) ins Visier genommen. Auf den Beschaffungslisten stehen darüber hinaus die so genannten Nischenlösungen sowie Komponenten – eine Spezialität der KMU.

In die falsche Richtung führt auch der befürchtete Imageschaden: 1. ist das Entdeckungsrisiko minimal. Und 2. wäre kein Konkurrent der Welt so dumm, eigene Mitarbeiter in Marsch zu setzen. Gerade im anglo-amerikanischen Raum gibt es eine Vielzahl von Detekteien und privaten Diensten, die gerne solche speziellen Jobs übernehmen. Auftraggeber sind zwecks Spurenverwischung häufig externe Büros oder Unternehmensberatungen. Ein Beispiel ist der Spionagefall Enercon. Die Täterstruktur um Ruth Hefernan wurde zwar gefasst, doch haben sich Anbindungen an US-Konkurrenten beziehungsweise die NSA nie 100-prozentig beweisen lassen.

Ein Raum, wie die „Laube“, wäre sehr wahrscheinlich außerhalb des finanziellen Spielraums von KMU. Doch es gibt für jede Unternehmensform eine Lösung, die sich kostenmäßig darstellen lässt.

Optimale Angriffsoptionen

Kommen wir auf die oben genannten Risiken durch Fenster, Lautsprecher in der Decke, Nebenstellentelefone oder Handys zurück. Große, in Richtung Peripherie weisende, Fensterflächen sorgen nicht nur für gute Lichtverhältnisse, sondern auch für optimale Angriffsoptionen. Schallwellen haben bekanntlich nicht nur eine akustische Seite (Hörschall), sie versetzen auch andere (Resonanz-)Körper in Schwingungen. Prädestiniert sind dafür Glasscheiben oder Hinter-Glas-Bilder, die mittels eines Infrarot-Lasergerätes quasi abgetastet werden können. Bei geöffneten Fenstern geht es noch einfacher, da kann ein Richtmikrofon eingesetzt werden.

So einfach, wie zuweilen dargestellt, ist der Laserangriff allerdings nicht. Entscheidend ist der richtige Winkel, betont Marieluse Henneberg, Lauschabwehrspezialistin der Haverkamp GmbH. Denn es nütze nichts, wenn der Laserstrahl zwar auf die Glasscheiben auftreffe, aber nichts reflektiert wird. Kein Job also für Laien. Es ist ein offenes Geheimnis, dass namentlich osteuropäische Nachrichtendienste das Laser-Verfahren perfektioniert haben.

Lautsprecher als trojanische Pferde

Auch Lautsprecher können trojanische Pferde sein. Mit einfachsten Methoden werden sie in dynamische Mikrofone verwandelt. Vom Prinzip und Aufbau (Verstärker, Membran, Schwingspule) her sind beide Signalwandler und damit praktisch ein Spiegelbild des jeweils anderen. Das Mikrofon ist ein umgekehrter Lautsprecher – nur die (leicht zu ändernde) Schaltung der Komponenten macht den Unterschied. Ein Prinzip, das jeder kennt; in einfachen Gegensprechanlagen funktionieren Mikrofone gleichzeitig als Lautsprecher und umgekehrt.

Altbekannt ist, dass Nebenstellentelefone über die Lautsprecherfunktion beziehungsweise versteckte Funktionalitäten zu Abhörsendern umfunktioniert werden können. Ebenso wie Mobiltelefone, die auch ohne Wissen des Nutzers umprogrammiert werden können. Ein manipulierter Akku, der in Sekundenschnelle eingebaut ist, lässt auch im ausgeschalteten Zustand des Handys den Lauschangriff zu.

Spezialisten gefragt

Eine Anzahl von Gegenmaßnahmen ist im Kasten aufgeführt. Zu den Lauschabwehrprüfungen lässt sich noch ergänzen, dass diese naturgemäß nur eine Momentaufnahme darstellen. Deshalb sollte im Anschluss ein Langzeitscanner installiert werden, „der das Frequenzspektrum für eine gewisse Zeit nach dem Sweep misst und aufzeichnet“, empfiehlt Christian Schaaf von Corporate Trust in seinem Buch „Industriespionage“.



Elektromagnetische Abschirmung von Besprechungsräumen: die Realisierung sollten nur darauf spezialisierte Unternehmen vornehmen. (Bild: Emscreen)



Für Fenster bieten sich Sicherheitsfolien, die Schallwellen sowie IR- und UV-Strahlen dämpfen, an. (Bild: Haverkamp)

Ganz ohne Zweifel sind Räume mit elektromagnetischer Schirmung und akustischer Dämmung das Nonplusultra der zur Verfügung stehenden Lösungen. Die Bandbreite reicht dabei von abhörgeschützt (Schirmdämpfung bis 80 Dezibel) bis abhörsicher (bis 100 Dezibel), je nach individuellem betrieblichen Sicherheitskonzept. Dieser höchste Schutz gegen unerwünschte Informationsverluste setzt aber komplexe Detailkenntnisse voraus. Fachfremde Planer wären somit mit der Umsetzung überfordert. Die Realisierung von geschirmten Räumen gehört deshalb definitiv in die Hände von Spezialunternehmen.

Schlupflöcher stopfen

Ein Schlupfloch gibt es allerdings selbst bei den geschirmten Räumen, wie Herbert Mangstl, Leiter Vertrieb der Emscreen GmbH, berichtet. Mitschnitte von Gesprächen bleiben nach wie vor mit kleinformatigen digitalen Aufzeichnungsgeräten, die beispielsweise in Form von Kugelschreibern oder Feuerzeugen angeboten werden. Messgeräte, die Halbleiter detektieren, sind noch nicht ohne Risiken für die menschliche Gesundheit handhabbar. Ariane Wahrmann, bei Emscreen für Marketing und Kommunikation zuständig, rät deshalb zur restriktiven Benutzerbeschränkung des Besprechungsraums. Je weniger Personen Zugang haben, desto höher die Chancen bei der Suche nach der undichten Stelle. Und umso riskanter die Spionagehandlung.

GEGENMASSNAHMEN

- Den Besprechungsraum nach dem Muster von Rechenzentren in das Gebäudeinnere verlegen.
- Fenster in Richtung Peripherie vermeiden. Ist dies aus baulichen Gründen nicht möglich, präventiv gegensteuern:
 - schwere, dunkle Vorhänge,
 - Aufbringen einer speziellen „Signal Defence“ Fensterfolie, die nach Herstellerangaben dank einer Beschichtung aus 21 unterschiedlichen Metallen (Verminderung des Durchlassfaktors auf 0,01 Prozent in erheblichem Maße vor dem Abhören von Handys, D-Tect Telefonen, Laptops, PDAs, PCs und anderen, auf Funkwellen basierenden Geräten (WLAN, Bluetooth) schützt. Ist allerdings nur in Kombination mit weiteren Maßnahmen sinnvoll.
 - geeignete Rolläden.
- Kein Telefon im Besprechungsraum.
- Verbot von Mobiltelefonen: Die Handys könnten in Wertfächern im unkritischen Flurbereich deponiert werden. Zur erweiterten Sicherheit: Handydetektor, der in einem definierten räumlichen Nahbereich jede Sendeaktivität eines Mobiltelefons signalisiert.
- Klare Prioritäten: weniger relevante Besprechungen können andernorts stattfinden.
- Eindeutige Zugangsregelungen: kein Dauerzugangsrecht für Hausmeister, Handwerker, Putzkolonnen. Kein Zugang von Dritten ohne Beaufsichtigung.
- Lauschabwehrprüfung (Sweep) der relevanten Räumlichkeiten durch anerkannte Experten (zum Beispiel Manfred Fink Security Consulting), um eingebrachte Miniatursender und andere Lauschtechnik zu detektieren.

Klaus-Henning Glitza, freier Autor in Harsum.

Mehr zum Thema

Suchbegriffe: Lauschabwehr, Lauschangriff, Abhören, Wirtschaftsspionage, abhörsicher, ASR

Lesezeichen



[Hilfe zu Lesezeichen](#)

TOOLBOX



pdf-Datei des Artikels
kostenlos herunterladen



Diese PROTECTOR-Ausgabe
bestellen



PROTECTOR-Abonnement
bestellen

Sicherheit.info im Überblick

Sicherheitstechnik

Videoüberwachung
Zutrittskontrolle
Brandschutz
Gefahrenmeldetechnik
Freilandsicherung
Warensicherung

Dienstleistungen

Bewachungsgewerbe
Detektive
Notrufzentralen/
Leitstellen
Personenschutz

Wirtschaftsschutz

Sicherheitskonzepte
Risk Management
Branchenlösungen
Wirtschaftskriminalität
Versicherungen

Öffentliche Sicherheit

Sicherheitspolitik
Kriminalitäts-
bekämpfung
Organisierte
Kriminalität
Terrorismus-
bekämpfung

Private Sicherheit

Brandschutz
Mechanische Sicherheit
Elektronische Sicherheit
Mobile Sicherheit
Videoüberwachung
Tipps & Tricks

Arbeitssicherheit

IT-Sicherheit

Netzwerksicherheit
Malware-, Spam- und
Virenabwehr
Identitäts-
management
Verschlüsselung
Backup und Storage
Mobile Sicherheit
RZ-Sicherheit

Branche intern

Personen
Firmen
Verbände
Messen und
Veranstaltungen
Meinung
Stellenanzeigen

Tools & Datenbanken

Branchenverzeichnis
Errichter vor Ort
Sicherheitsdienstleister
vor Ort
Terminkalender
Marktübersichten
Tests
E-Mail-Newsletter
RSS-Feed
Videos

PROTECTOR

Heftarchiv
Mediadaten
Abonnement
Einzelhefte

W&S

Heftarchiv
Mediadaten
Abonnement
Einzelhefte

Service

Kontaktformular
Mediadaten
Media Kit (engl.)
Presse
Impressum
Hilfe