Feind hört mit

Sie schummeln **WANZEN** *ins Handy, zapfen Computer an, hacken* **ISDN**-*Telefone:* **BETRIEBSSPIONE** *schädigen die Wirtschaft jährlich um* **ZWÖLF MILLIARDEN SCHILLING.** *Mit welchen Tricks* **PROFI-LAUSCHER** *agieren und was* **ABHÖRSCHUTZ** *taugt.* VON ALWIN SCHÖNBERGER

Bloß ein Feuerzeug. Ein billiges, weißes Bic-Feuerzeug, das wohl jemand vergessen hatte. Weder die Sekretärinnen im Vorstandsbüro des Wiener Pharmakonzerns schenkten ihm Beachtung noch die Direktoren. Manchmal zündete sich ein Angestellter damit eine Zigarette an und legte es wieder auf den Schreibtisch des Sekretariats, gleich neben dem Telefon.

Erst vor ein paar Wochen interessierte sich jemand näher für die scheinbar herrenlose Utensilie: Thomas Gsodam, Spezialist für Abhörschutz bei der Wiener Detektei Kusnierz & Partner, war von der Konzernleitung konsultiert worden, weil der Verdacht bestand, daß streng vertrauliche Informationen auf mysteriösen Kanälen zur Konkurrenz durchsickerten.

„Übers Pantscherl im Büro läuft noch immer recht viel." *Walter Pöchhacker, Privatdetektiv*

Gsodam, der vorsorglich mit speziellen Meßgeräten anrückte, wurde im Sekretariat fündig, gleich neben dem Telefon – im weißen Feuerzeug war eine Wanze verborgen, ein zwei Quadratzentimeter großes Elektronikbauteil.

Diskrete Recherchen belegten bald, daß ein eigener Mitarbeiter des Pharmakonzerns den Miniatursender in dem sensiblen Firmenbereich „vergessen" hatte, um an brisante Informationen zu gelangen: welche Projekte gerade aktuell waren oder wann die Vorstandsetage wegen auswärtiger Termine nicht besetzt war. Dann schlich der Mann in die verwaisten Büros, klaute geheime Forschungsdaten und verkaufte sie an die Konkurrenz.

„Die meisten Unternehmer können sich gar nicht vorstellen, daß solche Dinge tatsächlich passieren", weiß der Wiener Detektiv Walter Pöchhacker, dessen Mitarbeiter immer wieder in Büros und Konferenzräumen der Wirtschaft Wanzen aufstöbern. Allzuoft, sagt Pöchhacker, gelte Betriebsspionage noch als Stoff drittklassiger Agentenkrimis.

Verkannte Gefahr. Die Realität, sind sich hingegen Sicherheitsexperten einig, übertrifft die Fiktion bei weitem: „Nach aktuellen Erhebungen", zitiert Manfred Fink, Fachautor[1]) und Berater für Abhörschutz im deutschen Coburg, jüngste Branchenanalysen, „sind knapp 60 Prozent aller Unternehmen mit Betriebsspionage konfrontiert." Ziel von Lauschangriffen sind dabei nicht bloß Megakonzerne. „Potentiell gefährdet ist jeder, der am Markt Erfolg hat", sagt Max Burger-Scheidlin, als Leiter der internationalen Handelskammer in Wien auch mit Kriminalprävention in der Wirtschaft befaßt.

Die Fälle reichen, so Fink, „vom Handwerker, dessen Angebote ständig um ein paar Schilling unterboten werden, bis zum Großkonzern". Die Spione kommen fast immer von der Konkurrenz oder aus dem Kreis der eigenen Mitarbeiter. Deren Motive, analysiert Detektiv Bernhard Kusnierz, „sind Geldmangel, Erpressung oder schlicht Frust". Demotiviertes Personal sei leicht zu ködern, „wenn man mit ein paar Scheinen wedelt". Auf bis zu zwölf Milliarden Schilling schätzt Burger-Scheidlin den Schaden, den Wirtschaftsspione in Österreich jährlich anrichten.

Profi-Tricks. An die Öffentlichkeit gelangen nur spektakuläre Fälle. So flog im April 1997 bei Umbauarbeiten im Wiener Hotel Marriott auf, daß einige Zimmer verwanzt waren. Anders hätte man die Minisender wohl nie entdeckt: Unerkannt entfleuchte Abhörprofis hatten die Tapeten mit Dampfstrahlern abgelöst, stecknadelgroße Wanzen in die Wand eingebaut und die Tapeten wieder aufgebügelt.

Ähnlich geschickt agierten jene Finsterlinge, die eine infrarotgesteuerte Videokamera in einem Erdhügel am Wolfsburger VW-Testgelände deponierten. Fuhr ein Pkw vorbei, aktivierte ein Sensor den Auslöser, und die Kamera funkte Bilder von streng geheimen Prototypen an bis dato unbekannte Empfänger.

Siemens verdankt einem einzigen Versäumnis den Verlust eines 30-Milliarden-Auftrages: Weil vertrauliche Faxe aus Seoul uncodiert verschickt und von französischen Agenten angezapft wurden, konnte Siemens von der französischen Konkurrenz unterboten werden – was erklärt, warum heute TGV-Schnellzüge statt des ICE durch Korea rauschen.

Handy-Wanze. Technische Grenzen sind der Bespitzelung kaum mehr gesetzt. Erst kürzlich wurde in einem Wiener Betrieb ein Handy gefunden, in dessen Akku eine Wanze eingebaut ist. Das Anwendungsprinzip: In einem günstigen Moment tauscht der Spion den Akku seines Opfers aus und kann sowohl Telefonate als auch Raumgespräche mithören. Für nahezu unbegrenzte Funktionstüchtigkeit der Wanze sorgt der Belauschte unfreiwillig ▸

RECHTSLAGE

Paragraphen gegen Spione

Illegalen Lauschern blühen bloß matte Strafen.

■ Sechs Monate Freiheitsstrafe wegen „Verletzung des Fernmeldegeheimnisses" nach § 119 Strafgesetzbuch (StGB) riskiert, wer „Fernmeldeanlagen" anzapft. Der Täter wird nur „auf Verlangen" des Geschädigten verfolgt – nicht der Staatsanwalt ermittelt, sondern der Belauschte muß das selbst tun. Das gleiche Vergehen wird nach § 88 Telekommunikationsgesetz mit Strafen bis 50.000 Schilling geahndet.

■ Der § 120 StGB sieht Strafen von bis zu einem Jahr für „Mißbrauch von Tonaufnahme- oder Abhörgeräten" vor. Darunter fallen Wanzen ebenso wie geheimes Mitschneiden von Telefonaten. Bei diesem „Ermächtigungsdelikt" ermittelt der Staatsanwalt durch Aufforderung des Geschädigten.

■ Wer nach den §§ 122–124 StGB eine „Verletzung" oder „Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses" begeht, also geheime Daten klaut, muß mit Strafen zwischen sechs Monaten und drei Jahren rechnen. Es handelt sich ebenfalls um Privatanklagedelikte.

■ Der § 96 Arbeitsverfassungsgesetz schreibt vor, daß ein Chef, der die Telefonate seiner Mitarbeiter mithören oder aufzeichnen will, zuvor die Zustimmung des Betriebsrats einholen muß. In Firmen ohne Betriebsrat muß der Boß nach § 10 Arbeitsvertragsrechts-Anpassungsgesetz die betroffenen Mitarbeiter selbst fragen.

[1]) Manfred Fink: „Lauschziel Wirtschaft – Abhörgefahren und -techniken, Vorbeugung und Abwehr". Richard Boorberg Verlag, Stuttgart, 248 Seiten, öS 715,–.

6 In einem Kabelschacht wird eine Wanze versteckt. Der Sender zapft die Telefonleitung an und ernährt sich von der hauseigenen Stromversorgung.

1 In einem Ziergegenstand ist eine batteriebetriebene Miniwanze versteckt, die Raumgespräche und Konferenzen an einen Empfänger überträgt.

2 Die ISDN-Anlage wird wie ein Computer von außen gehackt. Der Lauscher manipuliert die Software und stellt eine Konferenzschaltung her, deren dritter Teilnehmer ein Tonbandgerät ist.

3 Aufmerksame Geschäftspartner überreichen einen Tischkalender als Werbegeschenk. An unauffälliger Stelle in dem netten Präsent ist eine Miniaturwanze eingebaut.

4 Im Computerkabel steckt eine Leitungswanze. Sie sendet statt Sprache Bits und Bytes und macht alles, was geschrieben wird, für einen externen Lauscher lesbar.

5 Jeder Monitor strahlt elektromagnetische Felder ab. Aus 100 Meter Entfernung wird diese kompromittierende Strahlung aufgefangen und wieder in ein scharfes Computerbild verwandelt.

selbst – jedesmal, wenn er sein Handy auflädt, bekommt auch die Knopfzelle im Minisender frischen Saft. Gerade 7000 Schilling kosten derart präparierte Akkus. „Nichts im Vergleich zu dem Schaden, der damit angerichtet werden kann", staunt Experte Gsodam.

Nicht minder phantasievoll ist das Wanzenrepertoire illustrer Versand-Shops wie „Spyworld" in München oder „Gmyrek Elektronik" in Leipzig, die in Kugelschreibern, Kreditkarten oder Terminplanern installierte Sender feilbieten. Besonders fiese Spione verpacken ihre Wanzen in Tischuhren und überreichen diese großzügig als Werbegeschenke. Kabelschächte wiederum eignen sich vorzüglich, um Telefonleitungen – für Profis wegen hoher Info-Dichte das Hauptangriffsziel – unauffällig mit Miniwanzen zu spicken. Auf diese Weise können sogar Computer abgehört werden: Wanze im Kabel zwischen Tastatur und Festplatte genügt, und via Funk wird wortgetreu übertragen, was man ins Keyboard tippt.

Verräterische Strahlen. Wahre Spionagekünstler müssen ein Büro nicht betreten, um die dort verarbeiteten EDV-Daten elegant umzuleiten. Aus sicherer Distanz – zum Beispiel in einem 100 Meter entfernten Auto – fangen sie mit einer Antenne die Strahlung des Monitors auf und verwandeln die Signale mit Empfangsgeräten wieder in ein gestochen scharfes Computerbild. Als fette Beute für Betriebsspione gelten auch ISDN-Telefone. Weil es sich dabei im Grunde um Computeranlagen handelt, so Manfred Fink, bei denen „nur noch das Design ein Telefon vortäuscht", lassen sich die High-Tech-Apparate von außen über Fernwartungszugänge hacken. Der Spion von Welt stellt unbemerkt eine virtuelle Konferenzschaltung her, deren dritter Teilnehmer ein Tonbandgerät ist. Fink übersetzt ISDN daher gerne mit „Im Sinne der Nachrichtendienste".

Entsprechend gefragt sind Geräte, die sensible Firmenbereiche von der Wanzenplage befreien sollen. Vor allem im Internet bieten ausgerechnet jene Händler, die sonst mit diskretem Versand von Lauschzubehör werben, allerlei Heimelektronik für High-Tech-Kammerjäger an. Da werden unter *www.spionage.com*, *www.electron.de* oder *www.spytech.com* „Minisender-Aufspürgeräte" oder „Wanzendetektoren" verhökert.

> **„Die meisten Geräte sind purer Techno-Schrott, die ins Spielzeugregal gehören."**
> *Manfred Fink, Sicherheitsberater*

Neben Versprechungen in fetten Lettern, wonach die Produkte etwa für „anspruchsvolle Technik" stehen, erfährt der Kunde meist, daß er die oft mehrere tausend Schilling teuren Dinger bestenfalls als schicke Briefbeschwerer verwenden darf: Kleingedrucktes verrät fast immer – vorzugsweise kurz nach Erläuterung der Bezahlung „gegen Vorkasse nach Österreich" –, daß die Produkte „für den Export außerhalb der EU bestimmt" sind.

Außerdem, sagt Fink, „gehört das meiste davon ins Spielzeugregal". Viele Wanzen-Aufspürgeräte seien in Wahrheit simple Meßinstrumente, die bloß elektromagnetische Strahlen registrieren – die wabern freilich aus fast allen Bürogeräten. Weil moderne Wanzen mit äußerst geringer Feldstärke arbeiten, schlagen die Zeiger dieser Detektoren zwar beim Luftbefeuchter aus – die Minisender können sie in dem Strahlengewusel jedoch kaum lokalisieren. Zudem wechseln Profiwanzen laufend ihre Sendefrequenz. Gegen diese „Frequency hoppers" sind die Meßgeräte überhaupt machtlos.

Daher spüren solche Detektoren gerade noch Billigwanzen mit hoher Sendeleistung auf. Die wiederum werden oft bewußt als „Lockvögel" eingesetzt: Nach deren Fund wiegt sich der Abgehörte in Sicherheit und stellt die Suche ein – weshalb er die Profiwanze nie bemerkt, die an anderer Stelle munter weitersendet.

Wer seine Betriebsgeheimnisse nicht unabsichtlich mit der Konkurrenz teilen will, beauftragt daher einen professionellen „Sweep": Abhörschutz durch Experten. Diese verfügen meist über Spezialgerät im Wert mehrerer Millionen Schilling und ackern sich mit etwa zehn Quadratmeter pro Stunde durch verdächtige Büroareale. Gut 50.000 Schilling, so Thomas Gsodam, müsse man allerdings in einen ordentlichen Sweep investieren.

Die Detektive Thomas Gsodam und Bernhard Kusnierz rücken Wanzen mit moderner Technik zu Leibe.

Ein vergessenes Feuerzeug, ein liegengelassenes Handy – und schon hört der Feind mit.

Schwaches Fleisch. Mitunter müssen die Detektive allerdings erkennen, daß der Bespitzelte gar nicht Opfer ausgeklügelter High-Tech, sondern menschlicher Schwächen ist: „Vor allem übers Pantscherl im Büro läuft noch immer viel", weiß Detektiv Walter Pöchhacker. So etwa im Fall einer Wiener Klimatechnik-Firma, deren Geschäftsführer sich nicht erklären konnte, warum all jene seiner Kunden plötzlich günstige Angebote von einem Konkurrenzbetrieb bekamen, die er selbst per Direct-mail kontaktiert hatte. Des Rätsels Lösung: Seine Sekretärin hatte ein Verhältnis mit einem Ex-Mitarbeiter, kopierte für diesen die Mail-Postkarten und hielt die Originale zurück – exakt so lange, bis ihr Lover eigene Angebote gelegt hatte. ●

ABHÖR-TECHNIK

Zubehör für Hobby-Spione

Überwachungselektronik im Überblick: was die Geräte können, was sie kosten, wem sie nutzen.

Scrambler

Einsatzgebiet: Ein kleines Elektronikkästchen mit Telefonanschluß verschlüsselt Telefonate. Beim zweiten Gesprächsteilnehmer wird die Sprache wieder dechiffriert – deshalb sind zwei Geräte nötig.

Funktion: Analoge Gespräche werden durch Frequenz-Modulation unkenntlich, bei Digitaltelefonen wird die Sprache nach bestimmten Algorithmen zerlegt und so in Datenschrott verwandelt.

Preis/OS: 4.000,– bis 6.000,– für zwei digitale Geräte

Rechtslage: Einsatz bei uns gestattet, teils gibt es postzugelassene Geräte.

Gesamturteil: ✚ Digitals Geräte sind zu empfehlen, durchaus erschwinglich und funktionieren tatsächlich. Im Analogbereich ist die Technik äußerst kompliziert – gute Geräte sind extrem teuer.

Scanner

Einsatzgebiet: Scanner werden unter zahlreichen Markenbezeichnungen (z. B. „Multiband Receiver", „Realistic pro") angeboten und sollen Handys, Schnurlostelefone und Funkverkehr abhören oder Wanzen aufspüren können.

Funktion: Suchen Frequenzbereiche nach Signalen ab. Sollen so Sprache empfangen oder Sender orten. Weil sich aber nur recht schmale Frequenzbänder fix einstellen lassen, versagen die Dinger beim ersten Frequenzwechsel.

Preis/OS: Ab 2.000,–, Spitzenscanner um 10.000,–

Rechtslage: Nach dem Telekommunikationsgesetz ist der Besitz gestattet, der Einsatz jedoch verboten.

Gesamturteil: ➖ Gehören ins Spielzeugfach, spüren bestenfalls taiwanische Schnurlostelefone auf oder stoipern unabsichtlich über ein D-Netz-Telefonat. Wenn ein „Abhörschutz-Profi" damit arrückt: rausschmeißen.

Wanzendetektor

Einsatzgebiet: Die Geräte, angeboten in unüberblickbarer Modellzahl mit klingenden Namen („Wanzen-Aufspürgerät", „Protector", „Buc Detactor"), sollen Wanzen und Minisender aufspüren können.

Funktion: Registrieren die elektromagnetischen Felder (EMF), die elektronische Geräte emittieren. Moderne Wanzen haben jedoch geringe Feldstärke, weshalb sie im Strahlengewusel eines modernen Büros untergehen.

Preis/OS: Ab 1.500,–, im Schnitt zirka 5.000,–

Rechtslage: Legal, wenn es sich um reine Meßgeräte handelt. Verboten, wenn sie selbst als Empfänger fungieren können.

Gesamturteil: ➖ Finden praktisch alles: Kopierer, Ventilatoren, Luftbefeuchter – außer Wanzen. Nur bei Uraltmodellen, die auf einer Frequenz fixiert sind, ist die Sendeleistung dafür hoch genug. Fazit: Finger weg.

Spektrum-Analyzer

Einsatzgebiet: Die Geräte, die zur Standardausrüstung von Spezialisten für Abhörschutz gehören, sind Breitbandempfänger, die Frequenzen messen und auf einem kleinen Monitor als Kurven anzeigen.

Funktion: Arbeiten mit speziellen Filtern, die eine Vielzahl von Frequenzbereichen selektiv analysieren und unerwünschte, starke Störquellen – z. B. Radio oder Monitor – erkennen und ignorieren. Können so gezielt auf Wanzensuche gehen.

Preis/OS: Ab 100.000,–

Rechtslage: Zugelassene Meßgeräte, stellen lediglich Frequenzbereiche optisch dar.

Gesamturteil: ✚ Hochsensible Profi-Technologie, die grundsätzlich von geschulten Experten bedient werden sollte – die können die Meßergebnisse nämlich auch interpretieren.

Wanze

Einsatzgebiet: Batteriebetriebene oder drahtgebundene Minisender werden in Kugelschreibern, Feuerzeugen oder sogar Kreditkarten versteckt. Andere Modelle werden ins Telefon oder in Kabelschächte eingebaut.

Funktion: Suchen Frequenzbereiche nach Signalen ab. Sollen so Sprache empfangen oder Sender orten. Weil sich aber nur recht schmale Frequenzbänder fix einstellen lassen, versagen die Dinger beim ersten Frequenzwechsel.

Preis/OS: Professionelle Wanzen ab zirka 7.000,–

Rechtslage: Fällt juristisch unter „nicht genehmigte Sendeanlagen" – damit verboten.

Gesamturteil: ⚪ Wer eine Strafverfolgung wegen Betriebsspionage riskieren will, findet zu gemessen am möglichen Informationsgewinn – moderaten Preisen ein breites Angebot effizienter Wanzen.

Empfänger

Einsatzgebiet: Mit Geräten wie „Interceptor", „Uniden Pro 30" oder „Transceiver" kann aus sicherer Distanz – manchmal in noch zwei Kilometer Entfernung – empfangen werden, was eine Wanze überträgt.

Funktion: Gleicht im Grunde einem Radio, nur daß man nicht geeichte Frequenzen benutzt. fängt Signale von einem Sender bzw. einer Wanze auf, die auf einer definierten Frequenz übertragen werden.

Preis/OS: Ab zirka 1.500,–

Rechtslage: Hängt vom Frequenzspektrum ab, geheimes Mithören ist jedoch grundsätzlich strafbar.

Gesamturteil: ⚪ Es gilt dasselbe wie bei Wanzen: Der Einsatz ist strafbar. Nur Empfänger der gehobenen Preisklasse bieten ungestörten Empfang.