BETRIEBSSPIONAGE

Die total verwanzte Republik

In Deutschlands Konzernen wird geschnüffelt wie noch nie. Viele Unternehmen unterschätzen die Gefahr, obwohl die Schäden durch Spionage nicht selten Milliardenhöhe erreichen. Besonders ein alter Bekannter erlebt zurzeit ein Comeback: die Wanze.

von Stefan Beste

Der brisanteste Fall von Industriespionage der letzten Jahre in Deutschland ist zugleich auch einer der rätselhaftesten: Es war am 29. Juli letzten Jahres, als MLP-Chef Bernhard Termühlen, entnervt durch andauernde Berichte über angeblich dubiose Bilanzierungspraktiken des Finanzdienstleisters, sein Büro von einem Sicherheitstechniker überprüfen ließ. Wochenlang waren immer neue Interna aus dem Unternehmen nach draußen gedrungen. Der Aktienkurs des einstigen Börsenlieblings war abgestürzt.

Im Kabelschacht von Termühlens Schreibtisch förderten die Ermittler schließlich eine Wanze zu Tage. Die Gespräche waren abgehört worden – womöglich über Monate. Der Täter saß nach Darstellung des Unternehmens nur ein paar Türen weiter: Dorian Simon, bis dato Auslands-Chef des Unternehmens, hatte sich angeblich mit einer Londoner Investmentbankerin auf eine Sex-Affäre eingelassen und wurde von ihr erpresst. Ann Lawther, Übernahme-Expertin der US-Investmentbank JP Morgan Chase, soll mit Leerverkäufen auf fallende MLP-Kurse spekuliert haben. Außerdem habe sie die feindliche Übernahme des Heidelberger Unternehmens vorbereitet. Der geschasste Manager freilich bestreitet die Vorwürfe, ebenso die Bankerin. Jetzt beschäftigt der Fall die Gerichte.

Spion im Miniaturformat: Wanzen wie diese sind auch für Amateure fast problemlos erhältlich

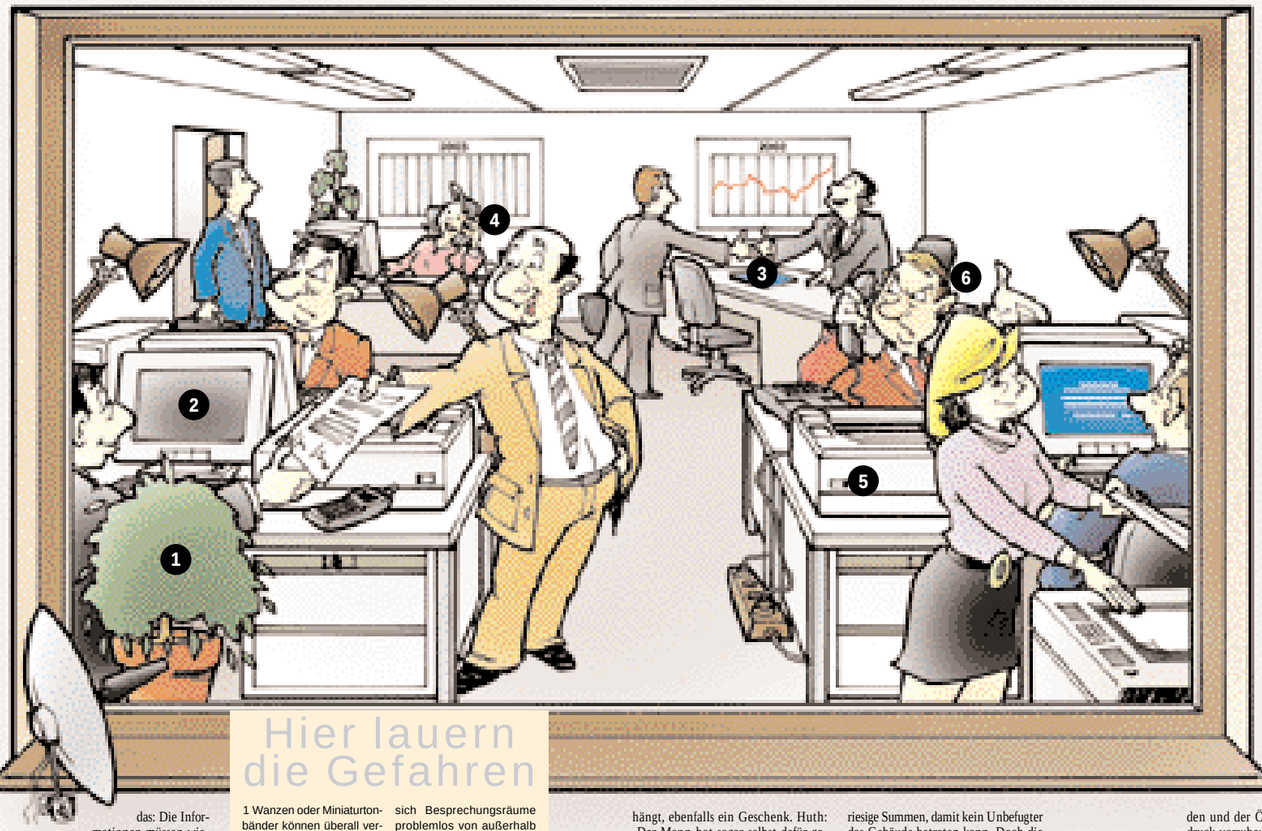
Ein Einzelfall? Im Gegenteil. In Deutschlands Unternehmen wird gelauscht, geschnüffelt und verraten wie nie zuvor. „Industriespionage nimmt explosionsartig zu“, sagt Walfried Sauer. Der 40-Jährige muss es wissen. 20 Jahre lang war er Polizeibeamter, 16 davon im Dienst einer Anti-Terror-Einheit. Heute ist er Boss der Result Group, einer Firma in Grünwald bei München, die sich auf die Sicherheit von Konzernen spezialisiert hat. Das Geschäft boomt. „Die Möglichkeit, mit relativ geringem Aufwand an wertvolle Erkenntnisse zu gelangen, ist für viele einfach zu verlockend“, sagt Sauer.

Die Täter arbeiten mit allen Tricks. Computer-Hacker durchkämmen das Internet nach brauchbaren Informationen, fangen E-Mails ab oder loggen sich in vertrauliche Firmennetzwerke ein. „Die Angreifer arbeiten zum Teil hochprofessionell“, warnt Michael Dickopf vom Bundesamt für Sicherheit in der Informationstechnik (BSI). Der einzige Schutz: hochwertige Verschlüsselungsverfahren. „Wer mit sensiblen Daten arbeitet, sollte auf keinen Fall nur auf ein Standardprodukt vom Markt vertrauen“, rät Experte Dickopf.

Hightech-Spionage durch gut ausgebildete Spezialisten ist aber nur ein Teil des Problems. Und vermutlich nicht mal der wichtigste.

In der Spionage-Szene erlebt derzeit ein alter Bekannter ein beeindruckendes Comeback: die Wanze. „Eine Zeit lang waren Wanzen so gut wie ausgestorben. Schließlich konnte man viel leichter an die Informationen herankommen, indem man zum Beispiel die ISDN-Leitung des Unternehmens anzapfte“, berichtet Ansgar-Alfred Huth, der sich auf die Abwehr von so genannten Lauschangriffen spezialisiert hat.

Mittlerweile hat die Datenverarbeitung allerdings beträchtliche Fortschritte gemacht. Und auch die Unternehmen sind vorsichtiger geworden. Elektronische Daten werden regelmäßig verschlüsselt. Für die Spione bedeutet das: Die Informationen müssen wieder dort beschafft werden, wo sie noch unverschlüsselt vorhanden sind – im Chefzimmer, im Konferenzraum oder am Telefon.



Hier lauern die Gefahren

1 Wanzen oder Miniaturtonbänder können überall verborgen sein: Die neuesten Modelle sind nur erbsengroß und passen in einen Kugelschreiber. Beliebte Verstecke sind Lüftungsschächte, Zimmerpflanzen oder Mehrfachsteckdosen. Letztere gewährleisten nebenbei noch eine unbegrenzte Stromversorgung.
2 Computerbildschime, Festplatten oder Grafikkarten verursachen elektromagnetische Strahlen, die von Profis problemlos in Originalinhalte zurückverwandelt werden können. Die Strahlung ist unter Umständen noch in mehreren 100 Metern Entfernung messbar.
3 Mit Hilfe hochempfindlicher Richtmikrofone lassen sich Besprechungsräume problemlos von außerhalb abhören.
4 Telefonate mit Handys lassen sich in der Regel leichter belauschen als Gespräche aus dem Festnetz. Vorsicht bei Mobiltelefonen, die scheinbar achtlos vom Gesprächspartner zurückgelassen werden, während er den Raum verlässt. Viele Geräte lassen sich leicht so manipulieren, dass von außen nicht erkennbar ist, ob sie eingeschaltet sind.
5 Auch Faxgeräte lassen sich anzapfen. Mit einem so genannten Monitoring-System etwa können Spione Faxe auf ihr eigenes Gerät umleiten.
6 Unzufriedene Mitarbeiter sind oft die besten Informanten der Konkurrenz.

Die Abhörmöglichkeiten sind schier unbegrenzt. Denn in jedem beliebigen Gegenstand kann sich im Prinzip eine Wanze verbergen. Ob in der unscheinbaren Dreifachsteckdose, dem achtlos auf dem Tisch abgelegten Handy oder einem Kugelschreiber – dem Erfindungsreichtum der Spione sind keine Grenzen gesetzt. „Vorsicht bei Werbegeschenken“, warnt deshalb Lauschabwehr-Experte Huth: Die kleine Aufmerksamkeit vom Konkurrenten kann sich als teures Betrugsmanöver entpuppen.

Beispiele aus der Praxis gibt es genug – auch wenn die Opfer es häufig vorziehen, die Angelegenheit unter den Teppich zu kehren. So geschah es auch bei einem mittelständischen Unternehmen aus der Auto-Zulieferindustrie: Dessen Finanzvorstand hatte über die Jahre eine Sammlung an Modellautos in seinem Büro zusammengetragen. „Der Mann fiel aus allen Wolken, als ich ihm die Wanze gezeigt habe, die im Inneren eines seiner Spielzeugautos verborgen war“, berichtet Huth. Ein anderer Unternehmens-Chef hatte in seinem Büro eine elektronische Dartscheibe aufgehängt, ebenfalls ein Geschenk. Huth: „Der Mann hat sogar selbst dafür gesorgt, dass die Wanze immer mit neuen Batterien versorgt wurde.“

Die Ausrüstung für den Lauschangriff ist für jedermann verfügbar. Das Equipment ist nicht mehr nur James Bond und Kollegen vorbehalten. Mit ein paar Klicks im Internet finden die Spione alles, was sie für ihr schmutziges Geschäft brauchen. Selbst hochempfindliche Wanzen im Miniaturformat, die sich zum Beispiel leicht in einem Kugelschreiber verstecken lassen, kosten dort nur ein paar Hundert Euro. Peanuts im Vergleich zum Wert der Informationen, die den Tätern auf diese Weise in die Hände fallen können.

Wege, die Wanzen zu platzieren, finden sich leicht. Ehemalige Geheimdienstagenten, die durch das Ende des kalten Krieges arbeitslos geworden sind, haben längst die Wirtschaftsspionage als lukratives Betätigungsfeld entdeckt. Wer es billiger haben will, besticht einfach das Reinigungspersonal. Gegen ein kleines Handgeld tauscht die Putzfrau nach Geschäftsschluss den Dreifachstecker gegen einen präparierten aus, fertig. „Viele Unternehmen investieren riesige Summen, damit kein Unbefugter das Gebäude betreten kann. Doch die eigenen Mitarbeiter können in jedem Raum frei ein- und ausgehen“, wundert sich Sicherheitsexperte Sauer.

Eine Untersuchung der Unternehmensberatung PriceWaterhouseCoopers fand heraus: In 63 Prozent der Fälle von Industriespionage saßen die Täter in der eigenen Firma. Der klassische Verräter ist männlich, älter als 35 Jahre, verheiratet, sozial integriert, hoch angesehen und nicht vorbestraft. „Das macht es so schwer, sich zu schützen“, sagt Sauer.

Die Schäden können in die Milliarden gehen – wie ein Beispiel aus dem Jahr 1994 zeigt: Damals wetteiferten die Konzerne Siemens und Alsthom aus Frankreich darum, ihre Hochgeschwindigkeitszüge ICE und TGV an Südkorea zu verkaufen. Die Deutschen unterlagen, weil Alsthom in letzter Minute ein günstigeres Angebot vorlegte. Später kam heraus, dass der französische Geheimdienst DGSE den Fax-Verkehr von Siemens überwacht hatte.

Für das Jahr 2001 hat das Bundeskriminalamt (BKA) 110 000 Fälle von Wirtschaftskriminalität ausgemacht. Schaden: 6,8 Milliarden Euro. Doch das ist bestenfalls eine grobe Schätzung. „Die Dunkelziffer ist sehr hoch“, meint etwa Heinz Hülser, Geschäftsführer der Arbeitsgemeinschaft für Sicherheit in der Wirtschaft (ASW). „Oft bemerken Unternehmen nicht einmal, dass sie Opfer von Spionage geworden sind.“

Dazu kommt, dass viele die peinliche Firmenaffäre häufig vertuschen wollen – aus Angst vor der Blamage, oder um gegenüber Kunden und der Öffentlichkeit dem Eindruck vorzubeugen, in der Firma gehe nicht alles mit rechten Dingen zu. „Opfer und Täter haben beide ein Interesse daran, dass der Fall nicht publik wird. Das macht die Aufklärungsarbeit so schwierig“, klagt Huth.

Fest steht: Jeder kann Opfer eines Lauschangriffs werden. Doch während sich die großen Konzerne längst auf die Gefahr eingestellt und mit viel Aufwand eigene Sicherheitsabteilungen aufgebaut haben, sind viele Mittelständler weiterhin völlig arglos. „Sicherheitsmanagement ist für die Verschwendung. Bis es mal richtig kracht“, beklagt Ex-Kripo-Mann Sauer.

Und ASW-Mann Hülser ergänzt: „Besonders gefährdet sind Firmen aus Hightech-Branchen.“ Berühmtheit erlangte das Beispiel des ostfriesischen Windkraftanlagen-Herstellers Enercon. Die Firma hatte ein neues Produkt entwickelt, hoffte auf ein Millionengeschäft in den USA. Doch der US-Rivale Kenneth Windpower beanspruchte das Patent der Windräder für sich und ließ Enercon den Verkauf seiner Anlagen per Gericht verbieten. Ein Agent der amerikanischen National Security Agency (NSA) hatte Faxe der Firma abgefangen und die Baupläne an die heimische Industrie weitergeleitet. Bis heute wehrt sich Enercon vergeblich gegen die Folgen des Spionageangriffs. Allein die Anwaltskosten sollen sich inzwischen auf mehrere Millionen Euro belaufen.

„Das Verhältnis von Aufwand und Ergebnis ist erschreckend. Schließlich können die Informationen, die mit Hilfe einer billigen Wanze beschafft werden, Millionen wert sein“, sagt Hülser. Oder Milliarden an Wert vernichten, wie der Absturz von MLP an der Börse gezeigt hat. Die Heidelberger Firma hat inzwischen übrigens Konsequenzen gezogen und die Sicherheitsmaßnahmen erheblich verstärkt. <<

Internet-Adressen

www.bsi.de Internet-Seite des Bundesamts für Sicherheit in der Informationstechnik. Bietet unter anderem gute Broschüren zu Fragen der IT-Sicherheit und Unternehmensspionage zum Herunterladen.

www.asw-online.de Die Arbeitsgemeinschaft für Sicherheit in der Wirtschaft versteht sich als Scharnierstelle zwische Sicherheitsbehörden und Unternehmen. Viele hilfreiche Links zu Landesverbänden, Behörden, Polizei und Verbänden.

www.bhe.de Webseite des Bundesverbands der Hersteller und Errichter von Sicherheitssystemen. Viele technische Informationen und Adressen.

Schutz vor Spionage

Das raten Experten

Ein 100-prozentiger Schutz vor Spionage kann auch durch den Einsatz der besten und teuersten Abwehrmaßnahmen nicht erreicht werden, warnt das BSI. Doch mit einiger Vorsicht lässt sich die Gefahr der Ausforschung von Betriebsgeheimnissen zumindest eindämmen.

1 Wichtige Räume wie Vorstandsbüros oder Konferenzräume sollten regelmäßig von Spezialisten auf Wanzen untersucht werden.

2 Auch danach können noch Wanzen in einen Raum geschmuggelt werden. Mit moderner Technik lassen sich aktive Minisender jedoch elektronisch aufspüren.

3 Netz, Telefon- und Datenleitungen sollten regelmäßig auf Manipulationen überprüft werden.

4 Vorsicht bei Geschenken. In allem, was ins Büro geschafft wird, kann eine Wanze versteckt sein.

5 Mobiltelefone haben in Konferenzen nichts zu suchen. Es gibt Möglichkeiten, die Geräte in Betrieb zu halten, ohne dass das von außen bemerkt werden kann.

6 Alarmsignale beachten: Verfügt ein Konkurrent plötzlich über eine ähnliche Technik wie das eigene Unternehmen, kann das auf eine undichte Stelle hinweisen.

7 Noch ein Alarmsignal: Die Qualität der eingekauften Waren sinkt auffällig – oft sind verbotene Preisabsprachen der Grund.

8 Gab es vor kurzem Entlassungen oder Umstrukturierungen in der Firma? Sind viele Mitarbeiter unzufrieden, ist erhöhte Wachsamkeit vonnöten. Die meisten Fälle von Geheimnisverrat werden von den eigenen Mitarbeitern begangen.

9 Besteht der Verdacht, dass spioniert wird, ist fachkundige Hilfe nötig. Andernfalls können womöglich Beweise für den Verrat vernichtet werden.

10 Über aufgedeckte Betrugsfälle sollte offen informiert werden. Das schreckt zumindest Nachahmer ab.