Wirtschaftsspione schrecken vor nichts zurück

Der Schaden durch diese Form der Kriminalität wird allein für deutsche Unternehmen auf 50 M

FRANKFURT, 5. Juli. Deutsche Unternehmen zählen aufgrund ihrer wirtschaftlichen und technischen Leistungsfähigkeit zur Weltspitze – und sind daher ein bevorzugtes Aufklärungsziel. Daran hat auch das Ende der bipolaren Machtverhältnisse zwischen Ost und West nichts geändert. Im Gegenteil ist eine Verschiebung der Aufklärungsbemühungen festzustellen: Stand zur Zeit des Kalten Krieges die politische und militärische Aufklärung an erster Stelle, sind heute vor allem die Wirtschaft und hier vor allem die Industrie das Ziel.

Das Thema „Spionage" wird hierzulande allerdings häufig von irreführenden Vorstellungen geprägt. Mangels einer einheitlichen Definition werden Wirtschaftsspionage, Industriespionage, Betriebsspionage und Konkurrenzspionage häufig synonym verwendet. In der Praxis der Sicherheitsbehörden hat sich die Differenzierung zwischen „Wirtschaftsspionage" als von staatlichen Geheimdiensten durch fremde Nationen und „Industriespionage" als durch nichtstaatliche Einrichtungen oder Konkurrenzunternehmen durchgeführten Maßnahmen der Informationsgewinnung durchgesetzt.

Beide sollten nicht miteinander gleichgesetzt werden, da sie von grundsätzlich unterschiedlichen Voraussetzungen ausgehen, unterschiedliche Zielsetzungen verfolgen und teilweise auch andere Methoden einsetzen. Für ein betroffenes Unternehmen bleibt die potentielle Gefährdung allerdings in beiden Fällen erheblich. Insbesondere die Ausspähversuche in- und ausländischer Konkurrenzunternehmen haben in den letzten Jahren drastisch zugenommen. Umfragen haben ergeben, daß etwa zwei Drittel aller deutschen Unternehmen bereits mit Spionageversuchen durch Konkurrenzunternehmen konfrontiert worden sind.

Die Ausspähung wirtschaftlicher und industrieller Vorgänge stellt für jeden Geheimdienst – egal welcher Nation – ein wesentliches Aufgabengebiet dar. Auch die Geheimdienste sogenannter befreundeter Nationen wenden sie an. Der Schaden, der der deutschen Industrie durch Wirtschaftsspionage entsteht, ist erheblich. Leider gibt es dazu kaum aussagefähiges Datenmaterial. Bereits 1986 vertrat das Bundesamt für Verfassungsschutz die Auffassung, daß der Schaden durch Wirtschaftsspionage in Deutschland bis zu 20 Milliarden DM beträgt. Seitdem hält sich diese Zahl hartnäckig und wird immer wieder in der einschlägigen Berichterstattung zitiert. Allerdings wäre es naiv zu glauben, daß seit 1986 (!) keine Steigerung des Volumens zu verzeichnen ist. Zahlreiche Experten gehen heute von einem geschätzten Schadensumfang von etwa 50 Milliarden DM aus.

Spionage ausländischer Geheimdienste bei deutschen Unternehmen richtet nach Angaben des Stuttgarter Wirtschaftsministeriums jährlich Schäden in Milliardenhöhe an. Der baden-württembergische Innenminister Thomas Schäuble sagte in Stuttgart bei einer Tagung, das Problembewußtsein in der Wirtschaft müsse gestärkt werden, um das Dunkelfeld der Ausspähung durch fremde Nachrichtendienste aufzuhellen. Die hochspezialisierte Wirtschaft im Südwesten sei ein beliebtes Ziel in der Wirtschaftsspionage. Kleine und mittelständische Betriebe seien besonders gefährdet, sagte der CDU-Politiker. In Stuttgart waren Politiker, Sicherheitsexperten und Manager zusammengekommen, um über die zunehmende Bedrohung deutscher Unternehmen durch ausländische Geheimdienste und Konkurrenzbetriebe zu diskutieren. Schäuble bemängelte, daß sich betroffene Firmen zu wenig an die Sicherheitsbehörden wendeten. Anders ließe sich die geringe Zahl der Hinweise nicht erklären. Experten rechneten mit einer weiteren Zunahme der Wirtschaftsspionage in den nächsten Jahren. (AP)

Ketten und Schlösser sind kein Hindernis für Spione.

Die Aufklärungsziele gegnerischer Nachrichtendienste umfassen die gesamte Bandbreite der Industrie und Technologie. Das Hauptinteresse liegt dabei insbesondere bei den wettbewerbsintensiven Bereichen der Hochtechnologie. Dazu gehören die Informationstechnologie, die Telekommunikation, die Elektronik und Elektrotechnik, Werkstoff- und Verfahrenstechnik, Luft- und Raumfahrt, Pharmazeutik und Chemie sowie Energie und Umwelttechnik. In diesen Bereichen ist zunächst jede Information von Interesse. Das unterscheidet die langfristig ausgelegte Wirtschaftsspionage von der eher prozeß- und produktorientierten Industriespionage. Von besonderem Interesse sind Preisinformationen, Erkenntnisse aus Forschung und Entwicklung, Unterlagen zu Produktionsverfahren und zur Produktionstechnologie, Markt- und Absatzstrategien, Hersteller-, Lieferanten- und Kunden-Angaben, Verträge, Kalkulationen und Personallisten.

Zum Einsatz kommen alle traditionellen nachrichtendienstlichen Mittel und Methoden. Es werden offene Quellen (Zeitungen, Magazine, wissenschaftliche Veröffentlichungen) ausgewertet, Gespräche geführt, sogenannte Innenquellen (Informanten im Zielunternehmen) angeworben, Schein- und Tarnunternehmen (zur Einholung fiktiver Angebote, für fiktive Projektausschreibungen) gegründet, Agenten in das Zielunternehmen (als Praktikant, Zeitarbeiter, Mitarbeiter von Fremdfirmen im Zielunternehmen) eingeschleust, Gemeinschaftsunternehmen (Joint-ventures) gegründet oder technische Aufklärung betrieben einschließlich Computerspionage.

Nach vorliegenden Erkenntnissen der Verfassungsschutzämter sind insbesondere die Geheimdienste der ehemaligen Sowjetunion im Bereich der Wirtschaftsspionage in Deutschland aktiv. Die Auflösung des KGB hat keineswegs zu einer Verringerung der Bedrohung geführt. Die einzelnen Nachfolgeorganisationen des KGB (SVR, GRU, FAPSI) haben sich vielmehr neu organisiert und formiert und ihre Aktivitäten auf diesem Sektor weiter ausgebaut. Neben den Geheimdiensten der ehemaligen Sowjetunion sind außerdem Dienste aus den Ländern des Nahen und Mittleren Ostens – insbesondere Libyen, Iran, Irak und Syrien – in Deutschland aktiv. Der jüngste Spionagefall in den Vereinigten Staaten zeigt die intensiven Bemühungen Chinas bei der Aufklärung wissenschaftlicher und technischer Ziele. Auch die Vereinigten Staaten, Frankreich und Großbritannien setzen ihre Nachrichtendienste gezielt zur Gewinnung wirtschaftlicher Erkenntnisse in Deutschland ein.

Im internationalen Vergleich haben deutsche Unternehmen – mit wenigen Ausnahmen – die Bedrohung durch Wirtschafts- und Industriespionage bisher nur unzureichend zur Kenntnis genommen. Während die Industrie in Ländern wie beispielsweise den Vereinigten Staaten oder Frankreich sehr bewußt und offensiv mit Wirtschafts- und Industriespionage umgeht, sich der potentiellen Gefährdung bewußt ist und in einem hohen Maß entsprechende Schutzmechanismen aufbaut, fand das Thema in Deutschland bisher kaum Beachtung. Dies hat eine Vielzahl von Gründen.

Zum einen ist das Thema Sicherheit für deutsche Unternehmen generell ein eher unliebsames, weil es nicht zum „Kerngeschäft" des Unternehmens gehört. Wie zahlreiche andere Stabs- und Querschnittsfunktionen auch wird „Sicherheit" als zwar notwendig, aber meist störend empfunden. Verbreitet ist in diesem Zusammenhang auch die Bewertung von Sicherheitsmaßnahmen als reiner Kostenfaktor statt als wertvolle Investition in die Absicherung des operativen Geschäfts. Hinzu kommt, daß erkannte Fälle von Wirtschafts- und Industriespionage im allgemeinen kaum öffentlich bekanntgemacht werden. Während staatliche Sicherheitsbehörden aus operativen Gründen kein Interesse an einem Bekanntwerden solcher Vorgänge haben, neigen die betroffenen Unternehmen allein

Milliarden DM im Jahr geschätzt / Von Frank Schurgers

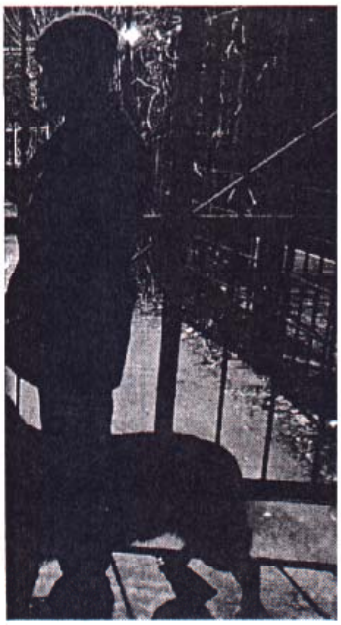

Foto ZB/Hubert Link

schon aus Gründen des Imageschutzes dazu, eine öffentliche Diskussion zu vermeiden. Wer gibt schon gerne zu, daß er das Opfer eines Wirtschafts- oder Industriespions wurde und wertvolle Unternehmensinformationen preisgegeben wurden?

Auch ist es eine ebenso verbreitete wie irrige Annahme, daß nur Großunternehmen einer Bedrohung durch Wirtschafts- und Industriespionage unterliegen. Im Gegenteil: Gerade in Deutschland gibt es eine hohe Zahl kleinerer und mittlerer Unternehmen, die in innovativen Produkt- und Technologiebereichen forschen, entwickeln und produzieren und weltweite Geschäftsbeziehungen unterhalten. Gerade diese Unternehmen sind am meisten gefährdet. Zum einen besitzen sie technisch und wirtschaftlich im höchsten Maße wettbewerbsfähige und innovative Produkte und Kenntnisse, gleichzeitig verfügen sie im Vergleich zu Großunternehmen in der Regel über nur

unzureichende Schutzkonzepte. Sie sind damit das ideale Ziel der Ausspähung.

Letztendlich kann jedes Unternehmen Ziel von Wirtschafts- und Industriespionage werden. Weder die Größe eines Unternehmens noch die Branche sind ein Indikator für die Gefährdung. Nur die Verfügbarkeit relevanter Informationen zählt. Und die ist in ausnahmslos jedem Unternehmen gegeben. Während die staatlich gesteuerte Wirtschaftsspionage durch fremde Nachrichtendienste nach Prioritäten erfolgt, kann nahezu jedes Unternehmen Ziel von Ausspähversuchen durch Konkurrenzunternehmen werden. Die Gefahr wächst, je innovativer und forschungsintensiver das Produkt oder die Branche und je internationaler die Geschäftsbeziehungen des Unternehmens sind.

Unbestritten haben deutsche Sicherheitsbehörden ein relativ klares Bild über den aktuellen Stand der Bedrohung der deutschen Sicherheit durch Wirtschaftsspionage. Festzuhalten bleibt aber, daß der verfassungsmäßige Auftrag deutscher Sicherheitsbehörden sich auch nur auf den Bereich der staatlich gesteuerten Angriffe fremder Nachrichtendienste erstreckt und Ausspähversuche im Bereich der Industriespionage nicht umfaßt. So bleibt die konkrete Vorsorge dem Unternehmen selbst und die Unterstützung einzelner Unternehmen in diesem brisanten Problembereich spezialisierten Experten und Beratungsunternehmen vorbehalten, die über entsprechende Erfahrung verfügen. Nur sie sind letztlich in der Lage, im konkreten Einzelfall erforderliche Schutzmaßnahmen zu empfehlen und die vitalen Interessen des Unternehmens zu wahren.

In der öffentlichen Diskussion finden insbesondere technische und computergestützte Angriffe (Hacking) gegen Unternehmen große Beachtung. Die Möglichkeiten der modernen Technologie haben dem versierten Angreifer hier bisher ungeahnte Wege und Methoden eröffnet. So tätigen deutsche Unternehmen auch beträchtliche Investitionen zum physischen Schutz ihres Betriebsvermögens (Zutrittskontrollsysteme, Wachdienste, Video-Überwachung) oder zum Schutz ihrer DV-gestützten Informationssysteme (Firewalls). Unbeachtet bleibt weitestgehend die verwundbarste Stelle eines Unternehmens: der einzelne Mitarbeiter als Träger des Wissens. Sowohl Wirtschafts- als auch Industriespione werden immer versuchen, über Mitarbeiter eines Unternehmens relevante Informationen abzuschöpfen. Warum sollte man den aufwendigen und mitunter riskanten Weg eines technischen Eindringversuchs nehmen, wenn ein gut vorbereitetes Gespräch mit einem unbedarften Mitarbeiter des Zielunternehmens nicht nur harte Fakten, sondern gleich auch noch die Bewertung und Interpretation der Daten liefern kann? Und darüber hinaus ist dies in den meisten Fällen noch nicht einmal strafrechtlich zu verfolgen.

Das Wissen in den Köpfen der Mitarbeiter läßt sich eben nicht durch technische Maßnahmen vor unberechtigtem Zugriff schützen. Um so wichtiger ist es, Mitarbeiter zu sensibilisieren und sie im Umgang mit relevanten Unternehmensinformationen zu trainieren. Dazu sollte ein integriertes Schutzkonzept entwickelt werden und in entsprechenden Verfahren und Prozeduren umgesetzt werden. Der Aufwand für solche Maßnahmen ist im allgemeinen deutlich geringer als die Implementierung technischer Systeme. Der Schutz, der dadurch erreicht wird, ist allerdings enorm.

In den letzten zehn Jahren hat sich beispielsweise in den Vereinigten Staaten eine eigenständige Disziplin entwickelt, die die Gewinnung von kritischen Unternehmensinformationen zum Gegenstand hat. „Business Intelligence" zählt in Amerika heute zu den Branchen mit den höchsten Zuwachsraten. In diesem Bereich sind in erster Linie Unternehmen und Personen aktiv, die ihr Handwerk bei Militär und Geheimdienst gelernt haben und diese Methoden jetzt ebenso erfolgreich wie gewinnbringend in der Wirtschaft einsetzen. Auch wenn einschlägige Unternehmen oder Interessenverbände immer wieder betonen, daß die Informationsgewinnung nur unter Beachtung der rechtlichen Bestimmungen und strikter ethischer Regeln erfolgt, bleibt die potentielle Gefahr des Unternehmens bestehen. Ziel ist und bleibt es, die kritischen und vitalen Unternehmensinformationen eines Konkurrenten zu erlangen, um daraus einen eigenen Wettbewerbsvorteil zu ziehen.

Auch in Frankreich wird die offensive Ausspähung von Konkurrenzunternehmen mittlerweile systematisch betrieben – und gelehrt. Unter Leitung des ehemaligen Leiters des französischen Auslandsgeheimdienstes DGSE wurde 1997 in Paris eine private Hochschule für Wirtschaftsspionage, die „Ecole de Guerre Economique", gegründet. Es wäre naiv zu glauben, daß die deutsche Industrie, die zu den besten in der Welt zählt, von solchen Erscheinungen und Angriffen verschont bliebe.

Die Erfahrung in der Beratungspraxis zeigt, daß die meisten Unternehmen in Deutschland bedauerlicherweise erst dann bereit sind, aktive Maßnahmen zum Schutz gegen Wirtschafts- und Industriespionage durchzuführen, wenn sie bereits das Opfer eines Spionageangriffs geworden sind. Dies setzt voraus, daß ein Spionageangriff auch als solcher erkannt wurde, was häufig nicht der Fall ist. Präventive Schutzmaßnahmen haben noch nicht den erforderlichen Stellenwert. Ausgangspunkt und Kern eines wirkungsvollen Schutzmechanismus für das Unternehmen ist die Entwicklung eines „Integrierten Schutzkonzepts", das alle Aspekte der materiellen und immateriellen Sicherheit umfaßt und unternehmensweit in Struktur und Abläufe eines Unternehmens integriert wird. Ein integriertes Schutzkonzept umfaßt organisatorisch-strukturelle Maßnahmen ebenso wie personelle, rechtliche und physische (baulich-technische) Maßnahmen sowie solche zum Schutz der Informationstechnologie.

Frank Schurgers ist General Manager Strategics der Control Risks Deutschland GmbH, Siegburg.

Die hundert Größten auf Diskette

F.A.Z. FRANKFURT, 5. Juli. Die Frankfurter Allgemeine Zeitung veröffentlicht zum 41. Mal die Rangfolge der größten deutschen und internationalen Unternehmen. Diese Übersicht dient immer mehr Unternehmen als Grundlage für Werbemaßnahmen. Eine erweiterte Fassung wird daher bereits im fünften Jahr auf Diskette angeboten. Die Diskette enthält neben sämtlichen Berichten dieser Beilage alle Tabellen mit Umsatz, Jahresüberschuß und Beschäftigtenzahlen von mehr als 400 deutschen Unternehmen sowie den größten Unternehmen Europas. Spezielle Auswertungen informieren über die Unternehmen mit den meisten Beschäftigten, den höchsten Umsatzzuwächsen, Umsatzrenditen und Jahresüberschüssen. Ebenso enthalten sind Tabellen mit den größten Industrieunternehmen der Welt nach Umsatzstärke und nach Marktkapitalisierung sowie den größten deutschen Unternehmen nach Marktkapitalisierung. Zusätzlich zur Zeitungsversion enthält die Diskette mehr als 450 vollständige Anschriften aller in den Branchenranglisten enthaltenen deutschen und europäischen Unternehmen. Sie eignet sich für individuelle Mailings und Auswertungen von Kennzahlen der großen deutschen und europäischen Unternehmen. Die Diskette im Format MS-DOS 3,5" enthält die Daten in den gängigen Formaten zur Übernahme in die Textverarbeitung, Datenbank oder Tabellenkalkulation und kostet 59 DM zuzüglich Versandkosten. Sie kann über den F.A.Z.-Versandservice (Schulstr. 12, 65468 Trebur, Telefon: 06147/697, Telefax: 06147/3275) oder direkt über das Internet-Angebot der F.A.Z. unter www.FAZ.de/archiv, erworben werden.