Industrie- und Handelskammer Hannover

Wirtschaftsschutz – Gefahren der Wirtschaftsspionage und Konkurrenzausspähung

Ein Merkblatt der Industrie- und Handelskammer Hannover

Das Know-how der deutschen Wirtschaft weckt Begehrlichkeiten, denn die Bundesrepublik hat einen hohen Standard in Forschung und Technologie, große wirtschaftliche Leistungsfähigkeit, eine günstige geographische Lage sowie eine politische und wirtschaftliche Brückenfunktion.

Die Notwendigkeit, sich gegen die illegale Nutzung des eigenen Wissens durch fremde Staaten, Konkurrenten oder Einzelpersonen zu schützen, gewinnt angesichts zunehmender Globalisierung von Wirtschaft und Technologie bei gleichzeitiger Verschärfung des internationalen Wettbewerbs sowie einer ständig steigenden Abhängigkeit von moderner Informations- und Kommunikationstechnik zunehmend an Bedeutung.

Einen Überblick über die Erkenntnisse der letzten Jahre der Verfassungsschutzorgane in Deutschland soll im Folgenden die Problematik bewusst machen.

1. Wie hoch ist das Schadenssausmaß? Was ist das Kernproblem?

Wirtschaftsspionage und Konkurrenzausspähung belasten die bundesdeutsche Volkswirtschaft mit mehreren Milliarden Euro jährlich, so das Niedersächsische Landesamt für Verfassungsschutz. Einer wissenschaftlichen Studie der Uni Lüneburg zufolge beträgt das Gefährdungspotenzial für die gesamtdeutsche Wirtschaft sogar rund 50 Milliarden Euro.

Aus Studien von KPMG, Ernst & Young und PricewaterhouseCoopers der letzten drei Jahre und einer Umfrage der IHK Osnabrück-Emsland lässt sich zusammenfassen:

- Der von Wirtschaftskriminalität betroffene Kreis von Unternehmen ist größer als allgemein angenommen – jedes Unternehmen könnte in den nächsten Jahren durch Wirtschaftskriminalität betroffen sein.

- Mangelndes Problembewusstsein/Unterschätzung des Risikos bzw. Management-Sensibilisierung hätte bisherige Schäden vermeiden helfen.
- Die Täter kommen zum überwiegenden Teil aus dem eigenen Unternehmen (Innentäter) – Top-Manager eingeschlossen.

2. Begriffsbestimmung

Wirtschaftsspionage
… ist die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben.

Konkurrenzspionage (Konkurrenzausspähung, Industriespionage)
… ist die Ausforschung, die ein (konkurrierendes) Unternehmen gegen ein anderes betreibt.

Wirtschaftsspionage aufzuklären, ist Aufgabe der Spionageabwehr des Verfassungsschutzes. Sie zu verhindern bzw. zu erschweren, ist Aufgabe des Wirtschafts- und Geheimschutzes. Konkurrenzausspähung fällt in den Bereich der Polizei. Wer gegen Spionage sensibilisiert und geschützt ist, hat auch Schutz vor Konkurrenzausspähung.

3. Wer ist gefährdet? Warum besteht die Gefährdung?

Grundsätzlich ist jedes Unternehmen gefährdet, das im nationalen und/oder im internationalen Wettbewerb steht und Know-how und/oder wirtschaftliches Potenzial besitzt.

Insbesondere sind aber **kleine und mittelständische Unternehmen** mit einem erheblichen Wettbewerbsvorteil und solche mit speziellen Nischenprodukten überproportional gefährdet.

Bevorzugte Ausspähungsziele sind Wissenschaft und Technologie, schwerpunktmäßig aus den folgenden Branchen:

- Material- und Rüstungstechnik
- Computertechnologie
- Biotechnik und Medizin
- Luftfahrt- und Verkehrstechnik sowie
- Energie- und Umwelttechnik

Wie wird ein Geschäftsgeheimnis definiert:
Ein Geheimnis ist alles, dessen Verlust ein Unternehmen massiv schädigt und dem Mitbewerber nutzt. Als grobe Richtlinie gilt, dass ca. fünf Prozent aller Verfahren, Prozesse und Dokumente geheimhaltungsbedürftig sind.

Worin besteht das Problem:

- Häufig verfügen Betriebe nicht über entsprechende Sicherheitsvorkehrungen, um sich gegen den Verrat ihrer Betriebsgeheimnisse ausreichend zu schützen.

- Einerseits ist das Sicherheitsbewusstsein nicht besonders ausgeprägt, andererseits können sie nicht die finanziellen Mittel bereitstellen, um eine aufwändige Sicherheitsarchitektur zu installieren.
- Sicherheitsrelevante Vorgänge, die im Unternehmen passieren, werden
  eher verschwiegen als zum Anlass für einen besseren Schutz genommen.

4. Wer sind die Täter? Woher kommt die Bedrohung?

Grundsätzlich wird Auslandsaufklärung von fast allen Staaten der Welt betrieben, um politische Entscheidungen vorzubereiten oder weltwirtschaftliche Lagebilder zu erstellen. Allerdings nützen viele Staaten ihre Auslands- und Inlandsdienste sowie Fernmelde- und elektronische Aufklärung gezielt für Wirtschaftsspionage.

a) Länder

- **Russland und Gemeinschaft Unabhängiger Staaten (GUS)**

Zur Zeit der UdSSR stand die Verwertung politischer Informationen im Fokus der Geheimdienstaktivitäten, da den Staatsbetrieben die nötige Infrastruktur fehlte, um die über Spionage erworbenen High-Tech-Geheimnisse wirtschaftlich umzusetzen. Dies hat sich mit den neuen politischen und wirtschaftlichen Strukturen in Russland und den GUS-Staaten grundlegend geändert. Viele Teile der Wirtschaft entsprechen bereits westlichen Standards und "geklautes" Know-how zur Entwicklung von Wettbewerbsvorteilen wird zielgerichtet genutzt.

Im heutigen weltpolitischen Gefüge definiert die wirtschaftliche Stärke die politische und militärische Macht. Russland will an die Machtstellung und Stärke, die es während des kalten Krieges hatte, wieder anknüpfen.

Die unterschiedlichen zivilen und militärischen Nachrichten- und Abwehrdienste Russlands haben derzeit einen geschätzten Beschäftigtenstand von 400 000 Personen. Die Überwachungsmaschinerie hat damit wieder eine Stärke wie zu Zeiten des kalten Krieges erreicht. Zu dem sind in Russland und der Ukraine die Dienste sogar per Gesetz verpflichtet, die Wirtschaft ihres Landes zu schützen. Im Bundesgesetz der Russischen Föderation "über die Auslandsaufklärung" ist verankert: "... die wirtschaftliche Entwicklung und den wissenschaftlich-technischen Fortschritt des Landes zu unterstützen und die Sicherheit der Russischen Föderation in militärisch-technischer Hinsicht zu gewährleisten."

Außerdem wird das Know-how, das nicht von strategischer Bedeutung ist oder verwendet werden kann, an Drittländer verkauft.

- **China (Fernöstliche Staaten)**

Die dem Ministerium für Staatssicherheit MSS unterstellten Dienste in China haben fast eine Million Mitarbeiter in der In- und Auslandstätigkeit beschäftigt. Diese Mitarbeiter sammeln alles: Es gibt keine Information, die zu klein oder unwesentlich erscheint, als das sie von den eingesetzten Kräften nicht übermittelt wird. In der chinesischen Mentalität besteht kein Unrechtsbewusstsein gegenüber Know-how-Klau und Nachbau. Vielmehr wird es als eine besondere Ehrung eines Meisters gesehen, wenn er kopiert wird. Die Zielsetzung, durch wirtschaftliche Stärke politische Weltmacht zu werden, gilt auch für China.

- **Westliche Staaten**

Die ehemals gemeinsame Bedrohungslage des Westens während des kalten Krieges existiert nicht mehr, wohl aber die nachrichtendienstlichen Strukturen.
Politisch wird grundsätzlich nicht von einer strategischen Wirtschaftspionage westlicher Dienste ausgegangen, jedoch ist eine Weitergabe von nachrichtlich gewonnenen Informationen nicht von der Hand zu weisen.

Das global vernetzte Abhörsystem "Echelon", vom amerikanischen Nachrichtendienst NSA entwickelt und koordiniert, kann weltweit jeden E-Mail- sowie Telefon-, Fax- und Teletexverkehr ungefiltert abhören und über Satellit an die Zentrale weiterleiten. Ca. 120 000 Personen werten das Satellitenabhörprogramm aus. Die Gefahr besteht also, dass sich USA Wettbewerbsvorteile verschaffen.

In Frankreich z. B. kann auf der "Ecole de Guerre Economique" "ordentlich" studiert werden, wie man sich im "Wirtschaftskrieg" durchsetzt.

- **Sonstige**

Auch Schwellenländer und unsere östlichen Nachbarn stehen im globalen Wettbewerb. Know-how, was durch Auskundschaftung erhältlich ist, muss nicht selbst entwickelt werden.

Fazit:
Die einstigen Spionagefeinde sind nicht verschwunden, sondern vielmehr sind neue hinzugekommen. Die Verfassungsorgane haben deshalb bezüglich Wirtschaftsspionage einen „360 Grad"-Blickwinkel. Insgesamt sind in Deutschland ca. 15 000 Kräfte für Aufklärung und Abwehr zuständig.

b) Methoden

Die Aufklärungsziele und Methoden richten sich laut Bundesamt für Verfassungsschutz nach dem jeweiligen technologischen Stand der handelnden Staaten.

Interessen hochentwickelter Staaten richten sich insbesondere auf:
- Unternehmens- und Marktstrategien
- Wettbewerbsstrategien, Preisgestaltung und Konditionen, insbesondere bei großen Ausschreibungen
- Zusammenschlüsse und Absprachen von Unternehmen
- Informationen über Entscheidungsprozesse im Unternehmen
- Informationen über Manager und deren unmittelbare Mitarbeiter

Die Ziele technisch weniger entwickelter Staaten liegen eher in den folgenden Bereichen:

- die Beschaffung von technischem Know-how, um Kosten für die eigenen Entwicklungen oder Lizenzgebühren zu sparen
- Beschaffung von Informationen über Fertigungstechniken, um auf dem Markt mit kostengünstigeren Nachbauten konkurrenzfähig zu sein

5. Welche Methoden nutzen die Ausspäher? Was können Sie dagegen tun?

a) Offene Quellen und offene Beschaffung

Es wird geschätzt, dass ca. 80 Prozent der Erkenntnisse von Nachrichtendiensten aus offenen Quellen stammen. Diese Infos helfen, um ein Gesamtbild über ein Aufklärungsziel zu erstellen.

- **Internet, Fachbeiträge aus öffentlichen Bibliotheken und Datenbanken**
  Diese Quellen sind für jedermann so gut wie unbemerkt zugänglich. Bei der Recherche über das Internet können z. B. längst nicht mehr aktuelle Sachstände gefunden werden, die dennoch interessante Rückschlüsse auf aktuelle nicht veröffentliche Tatbestände zulassen.

- **Besuch von öffentlichen Veranstaltungen (z. B. Messen, Kongresse, Symposien etc.) sowie Teilnahme an Studiengängen oder wissenschaftlichen Projekten**
  Die Teilnahme an diesen Veranstaltungen erfolgt unter dem Aspekt der Produktvermarktung, der Geschäftsanbahnung oder der Produkt- bzw. Technologieentwicklung – eine Nabelschau von Leistung und Wissen.

- **Gesprächsabschöpfung**
  In zumeist lockerer Atmosphäre, z. B. am Abend beim Essen oder in der Hotelbar, auf Tagungen oder auch auf Urlaubsreisen wird versucht, die Zielperson in eine freundliche Gesprächsatmosphäre zu verwickeln, um Geschäftsgeheimnisse herauszubekommen. Diese Methode hat den Vorteil, dass der als "Quelle" missbrauchte Gesprächspartner nie das Gefühl hat, etwas Unerlaubtes zu tun, und der Empfänger braucht sich nicht als Nachrichtendienstler zu

enttarnen. Strategie ist dabei meist, über Teilinformationen zu einem Gesamtbild zu gelangen.

Einige Tipps:

- Untersuchen Sie Ihr Internetangebot unter dem Aspekt "Sicherheit" und prüfen Sie, ob Ihre Firma z. B. im Hinblick auf Produkte, Produkteigenschaften oder Verfahren zuviel offenbart.
- Prüfen Sie auch Diplomarbeiten oder Dissertationen, die Werksstudenten in Ihrer Firma fertigen, auf sicherheitsrelevante Inhalte.
- Überlegen Sie, welche Details über Ihr Privatleben und über Ihre privaten Aktivitäten bzw. das Ihrer Führungskräfte an die Öffentlichkeit gelangen können bzw. was über das Internet recherchiert werden könnte (Bsp.: Teilnahme an einem Golf-Turnier mit Teilnehmerliste im Internet aus der Ihre Abwesenheit in der Firma ableitbar ist).
- Abfall – Sorgen Sie bei Rechnern und elektronisches Datenmaterial sowie Papieren und Akten, die sicherheitsrelevante Informationen enthalten, für eine entsprechende Entsorgung.
- Prüfen Sie alle Präsentation unter dem Aspekt sicherheitsrelevanter Informationen. Versetzen Sie sich in die Lage eines Konkurrenten.
- Sprechen Sie mit Ihren Mitarbeitern, die mit sicherheitsrelevanten Informationen zu tun haben, und weisen Sie sie darauf hin, dass auch außerhalb ihres eigentlichen Arbeitsbereiches und der Firma, z. B. in Freizeit und im Urlaub, Geheimes auch geheim bleiben muss.

b) Geheime Beschaffung

- **Überwachung von Telekommunikation, Eindringen in Informationssysteme**
  Die Informations- und Kommunikationstechnik ist heute einer der Hauptangriffspunkte, wenn es um die Beschaffung von Informationen geht. Ob gespeicherte Dateien oder der Kommunikationsverkehr, mit moderner IT und Spyware wird versucht, in die internen Systeme einzudringen. Beispielsweise kann jede E-Mail, die verschickt wird, von Dritten zum Zweck der Spionage ausgewertet werden. Ebenso können eingehende E-Mails als so genannte Trojaner vertrauliche Daten abschöpfen oder Passwörter ausspähen.

- **Legalresidenturen, Journalisten, Geschäftsleute**
  Bei diplomatischen oder konsularischen Vertretungen sowie bei Presseagenturen können Mitarbeiter mit nachrichtendienstlichen Aufgaben betraut sein bzw. sind grundsätzlich dazu angehalten, alle Informationen aus ihren Geschäftskontakten weiterzuleiten. Zunehmend werden diese Personen auch als Mitarbeiter in privatwirtschaftlichen Unternehmen eingesetzt.

- **Agenten**
  Geheime Mitarbeiter werden als Agenten für eine Verrats- oder Aufklärungstätigkeit angeworben oder Spione vor Ort mit einem falschen Persönlichkeitsprofil eingesetzt.

Einige Tipps:

- IT-Sicherheit ist eines der wichtigsten Themen im IT-Bereich. Mehr oder weniger beschäftigt sich jedes Unternehmen damit, allerdings sollte dieses Thema strategisch und umfassend angegangen werden. Neben Datensicherung, Back-up oder Rechnerausfall sollte die Strategie auch die Abwehr von Angriffen von außen enthalten.
- Sie sollten sich bewusst sein, dass, wenn Sie private oder geschäftliche Kontakte zu Personen von diplomatischen oder ähnlichen Institutionen pflegen, Ihr Gesprächspartner auch ein Nachrichtendienstoffizier sein könnte. Solche Tarndienstposten werden mehr und mehr auch in staatlichen Handelsvertretungen und Firmenniederlassungen eingerichtet.

6. Die größte Gefahrenquelle – der Innentäter

Innentäter sind konspirativ auftretende Mitarbeiter im Unternehmen, die in Anbetracht ihrer legalen Zugangsmöglichkeiten und ihres Insiderwissens über innerbetriebliche Schwachstellen in der Lage sind, den Unternehmen mehr Schaden zuzufügen, als externe Täter es je könnten.

Der Verfassungsschutz sowie Studien rechnen mit einer über 80-prozentigen Innentäterschaft. Innentäter kann jeder sein. Die Delikte reichen von Spionage, Sabotage, Korruption, Diebstahl oder IT-Kriminalität. Als Motive lassen sich Unzufriedenheit am Arbeitsplatz,

Geldgier, Abenteuerlust, das Gefühl, etwas Besonders zu sein, ausmachen. Im Zusammenspiel von Entfremdung der Arbeit und sinkender Hemmschwelle für Straftaten entwickelt sich mangelndes Unrechtsbewusstsein.

Tipp:
Verhaltensweisen, die bei Mitarbeitern in sicherheitsrelevanter Weise als auffällig gelten können:

- Frustration, Unzufriedenheit am Arbeitsplatz/im Beruf
- besondere Neugier/auffälliger Arbeitseifer
- nicht gerechtfertigtes Interesse an Unterlagen
- Nutzung von Spionagehilfsmitteln wie private Film-, Foto- und Textaufzeichnungsgeräte
- auffällige und nicht plausible Verbesserung der finanziellen Situation
- Auffälligkeiten im persönlichen Umfeld
- Anzeichen für Alkoholsucht, Drogenabhängigkeit oder Spielsucht
- nicht eindeutig geklärter beruflicher Werdegang
- Überqualifikation
- fehlende Identifizierung mit dem Unternehmen
- nicht nachvollziehbare Kontakte zu Vertretungen ausländischer Staaten/Konkurrenzunternehmen
- auffällige und verdächtige Verbindungen ins Ausland
- Auftauchen von Teilinformationen bei Wettbewerbern

Oftmals sind im Kollegenkreis Verhaltensweisen dieser Art von den entsprechenden Personen bekannt. Es gilt jedoch als unkollegial, andere anzuschwärzen.

Innentäter können auch sein:

- Wachmänner
- Putzfrauen
- Austausch-/Gastwissenschaftler/Praktikanten
- Delegationsmitglieder
- Dolmetscher
- Messebesucher
- ausländische Geschäftspartner
- Fremdfirmen

Einige Tipps:

- Achtung Fremdfirmen: Wenn Sie Fremdfirmen zur Bewachung und zum Objektschutz eingestellt haben, sollten Sie sich über das jeweilige Schutzpersonal ausreichend informieren.

- Mitarbeiter: Wenn Sie Personal für sicherheitsrelevante Positionen neu einstellen oder versetzen, sollten Sie einen umfassenden Hintergrund-Check machen.

- Clean desk: Leiten Sie Ihre Mitarbeiter dazu an, dass sie, wenn sie Feierabend haben, sich unbekannte Besucher anmelden oder für längere Zeit das Büro verlassen, alles das, was keinen Außenstehenden etwas angeht, wegzuräumen und sicher aufzubewahren. Dies sollte so beliebte Plätze wie unter der Schreibtischschutzauflage oder in Schreibtischablagekörben beinhalten.

7. Prävention – das Bundesamt für Verfassungsschutz rät

Hier einige Hinweise, wie Sie Ihren Wirtschaftsschutz strategisch ansetzen:

- Nicht warten bis ein Spionagefall eingetreten ist.
- Aktuelle Informationen bei kompetenten Partnern einholen.
- Informationsschutz als wichtigen Bestandteil der Firmenphilosophie und Firmenstrategie verankern.
- Sicherheitsstandards regelmäßig analysieren.
- Ganzheitliches Sicherheitskonzept realisieren und permanent fortschreiben.
- Schutzmaßnahmen auf den Kernbestand zukunftssicherer Informationen konzentrieren.
- Einhaltung und Erfolg der Sicherheitsvorkehrungen kontrollieren, Sicherheitsverstöße sanktionieren.
- "Frühwarnsystem" zur Erkennung von Know-how-Verlusten installieren.
- Auffälligkeiten und konkrete Hinweise konsequent verfolgen, professionelle Hilfe in Anspruch nehmen.
- Informationsschutz ist ein strategischer Erfolgsfaktor.

Das Wesentliche:

- Versetzen Sie sich in die Lage eines unternehmerischen Gegners: Was wurde er beschaffen, um einen Wettbewerbsvorteil zu erringen, wo würde dieser ansetzen und wie würde er vorgehen.

- Machen Sie alle Mitarbeiter zu Sicherheitsbeauftragten. Eine sensibilisierte und aufmerksame Belegschaft ist der beste Schutz.

Unterstützung/Adressen:

- **Niedersächsischer Verfassungsschutz**
  Der Verfassungsschutz, Bereich Wirtschaftsschutz, bietet Hilfestellung und steht Unternehmen für Beratungen kostenlos zur Verfügung. Die Arbeit ist vertraulich. Der Verfassungsschutz unterliegt nicht dem Zwang, Straftaten polizeilich bzw. staatsanwaltlich verfolgen zu lassen. Kontaktaufnahme für eine Beratung oder bei einem Sicherheitsvorfall:

  Niedersächsisches Ministerium für Inneres und Sport
  Verfassungsschutz, Wirtschafts- und Geheimschutz
  Tel. (0511) 6709-247
  Fax: (0511) 6709-393
  E-Mail: wirtschaftsschutz@verfassungsschutz.niedersachsen.de
  www.verfassungsschutz.niedersachsen.de

- **Sicherheitspartnerschaft gegen Wirtschaftskriminalität in Niedersachsen**
  In der Sicherheitspartnerschaft sind das Land Niedersachsen, vertreten durch Innen-, Wirtschafts- und Justizministerium sowie dem Landespräventionsrat und die niedersächsischen Industrie- und Handelskammern und Handwerkkammern sowie der Verband für Sicherheit in der Wirtschaft e.V. vertreten. Zielsetzung ist, den durch Wirtschaftskriminalität in den verschiedensten Erscheinungsformen verursachten Schaden zu reduzieren, das wechselseitige Verständnis zwischen Staat und Wirtschaft zu fördern sowie die gegenseitige Kooperationsbereitschaft zu entwickeln. – s. auch IHK Hannover unter www.hannover.ihk.de, Rubrik Sicherheit

- **IT-Sicherheit**
  erste Hilfestellung finden Sie bei:

  Bundesamt für Sicherheit in der Informationstechnik (BSI)
  www.bsi.de

  Beratungszentrum für elektronischen Geschäftsverkehr
  der IHK Hannover (begin)
  www.begin.de

  Niedersächsisches Landesamt für Verfassungsschutz
  www.verfassungsschutz.niedersachsen.de

Stand: Oktober 2008

Autor:
Sabine Hillmer
Abteilung Industrie und Verkehr
Tel. (0511) 3107-272
Fax (0511) 3107-430
E-Mail: hillmer@hannover.ihk.de

Industrie- und Handelskammer Hannover
Schiffgraben 49
30175 Hannover
www.hannover.ihk.de