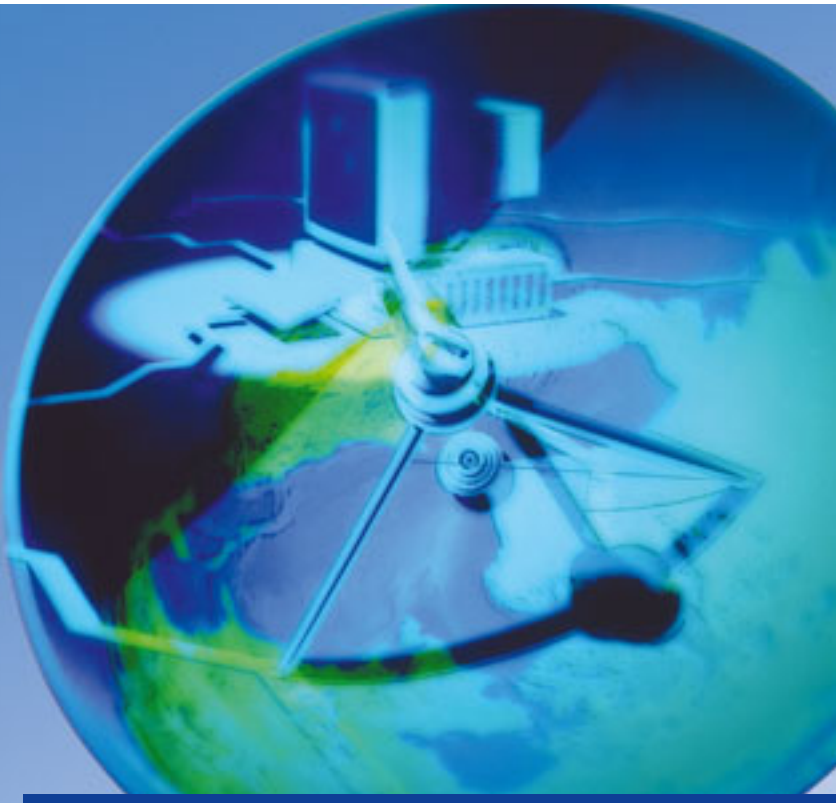
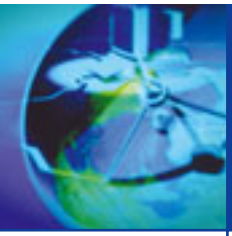


Wirtschaftsspionage

Risiko für Ihr Unternehmen

Die Verfassungsschutzbehörden des Bundes und der Länder



PRÄVENTION

Der Leitgedanke dieser Broschüre ist die Verhinderung und die Abwehr illegalen Informationsabflusses. Sie hilft dabei, die notwendige Sensibilität gegenüber den Spionagegefahren zu entwickeln und gibt erste Hinweise zur Gefahrenvorsorge.

WIRTSCHAFTSSPIONAGE

Staatlich gelenkte oder gestützte, von Nachrichtendiensten fremder Staaten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben.

KONKURRENZAUSSPÄHUNG

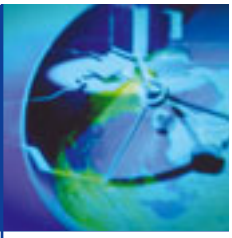
(umgangssprachlich Industriespionage)

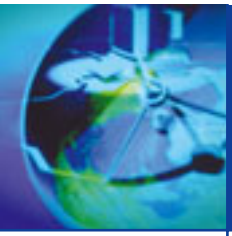
Ausforschung eines Unternehmens durch einen Wettbewerber.

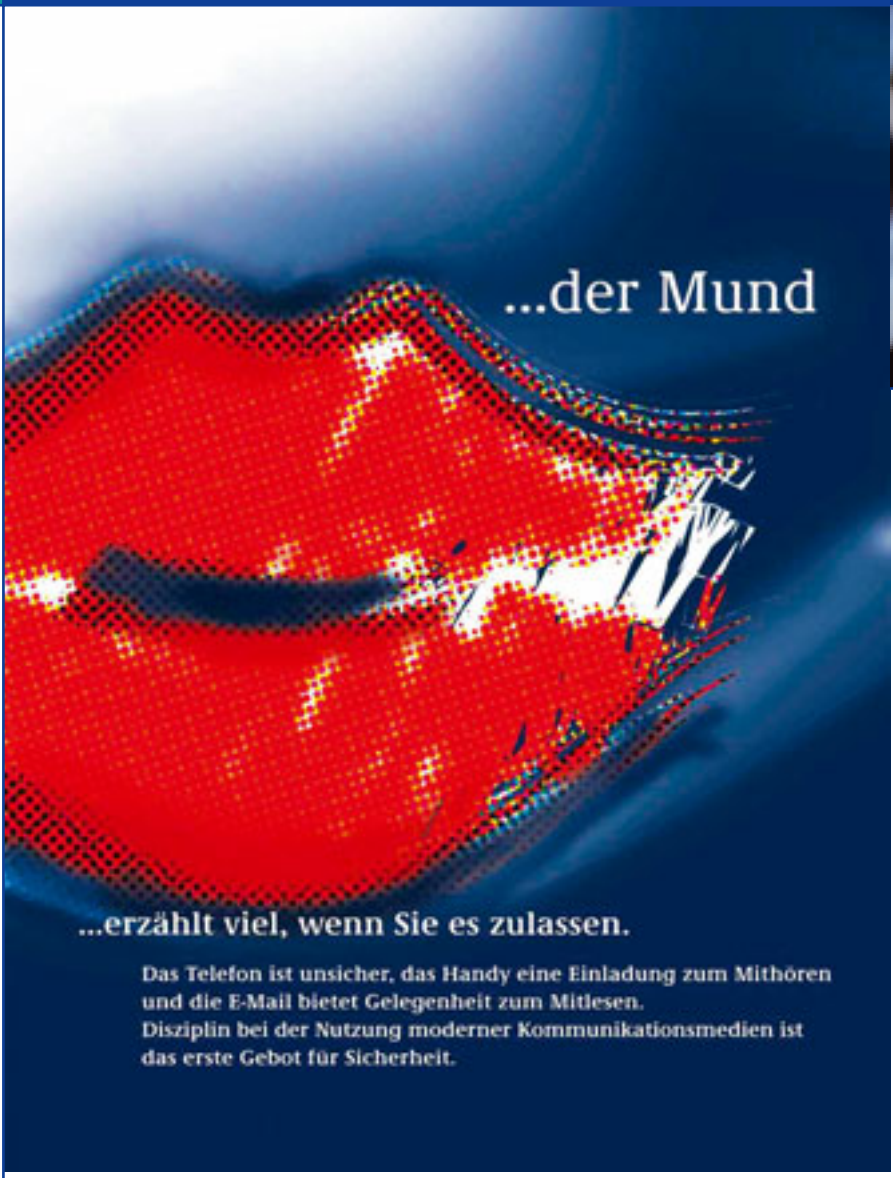
PROLIFERATION

Weiterverbreitung von Massenvernichtungswaffen bzw. der zu ihrer Herstellung verwendeten Produkte – einschließlich des dafür erforderlichen Know-hows – sowie von entsprechenden Waffenträgersystemen.

Inhalt







...erzählt viel, wenn Sie es zulassen.

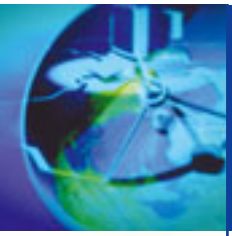
Das Telefon ist unsicher, das Handy eine Einladung zum Mithören und die E-Mail bietet Gelegenheit zum Mitlesen.
Disziplin bei der Nutzung moderner Kommunikationsmedien ist das erste Gebot für Sicherheit.

1. Wirtschaftsschutz – ein Aufgabenfeld des Verfassungsschutzes

Die Spionage im Bereich Wirtschaft gehört neben der politischen und militärischen Ausforschung zu den „klassischen“ Aufklärungszielen der Nachrichtendienste. Vor dem Hintergrund der Globalisierung der Märkte und neuer weltpolitischer Konstellationen hat die Bedeutung der Wirtschaftsspionage seit den 1990er Jahren stetig zugenommen.

Im Zentrum der Ausforschung durch fremde Nachrichtendienste stehen wegen ihres enormen ökonomischen Potenzials auch die Wirtschaftsunternehmen der Bundesrepublik Deutschland. Eine funktionierende Wirtschaft ist aber eine grundlegende Voraussetzung für die innere Stabilität von Staat und Gesellschaft. Insoweit liegt es im besonderen staatlichen Interesse, einen nicht autorisierten Wissenstransfer aus deutschen Firmen zu verhindern. Im Rahmen der staatlichen Maßnahmen zum Schutz der Wirtschaft kommt daher der Spionageabwehr eine hohe Bedeutung zu.

Zudem wirkt der Wirtschaftsschutz nicht allein der nachrichtendienstlichen, sondern auch der Konkurrenzausspähung entgegen. Das Aufgabenspektrum des Verfassungsschutzes umfasst die Beobachtung und Analyse von Operationen fremder Nachrichtendienste und die Beratung und Sensibilisierung deutscher Unternehmen und Forschungseinrichtungen.



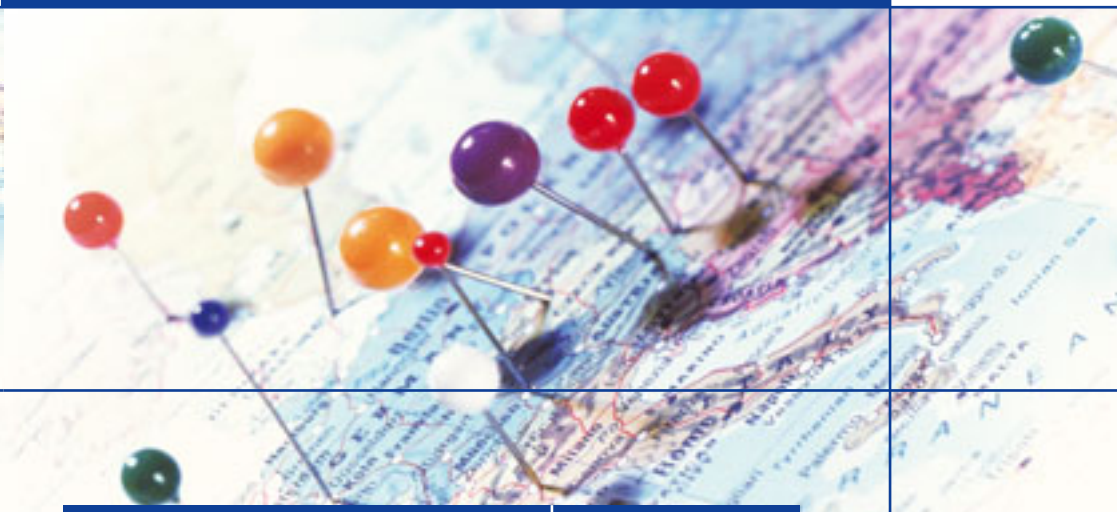
2. Das Know-how der deutschen Wirtschaft weckt Begehrlichkeiten

Fast zwanzig Jahre nach dem Ende des „Kalten Krieges“ bildet die Bundesrepublik Deutschland für ausländische Geheimdienste nach wie vor ein herausragendes Operationsgebiet.

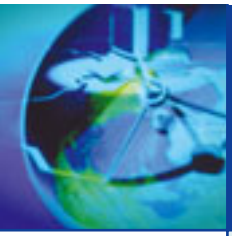
Die gewachsene politische Bedeutung des wiedervereinigten Deutschlands, seine wirtschaftliche Leistungskraft sowie das hohe Niveau der hiesigen Forschung und Entwicklung erklären das anhaltende intensive Aufklärungsinteresse fremder Staaten. Im Mittelpunkt der Ausspähungsbemühungen stehen die Bereiche Wirtschaft, Wissenschaft und Technik.

Neben ausländischen Geheimdiensten interessieren sich aber auch konkurrierende Firmen aus dem In- und Ausland für das Know-how der deutschen Wirtschaft. Überschreiten sie bei ihren Umfeld-, Konkurrenz- und Produktanalysen die vom „Gesetz gegen den unlauteren Wettbewerb (UWG)“ gezogenen Grenzen, spricht man von Konkurrenzausspähung oder Industriespionage.

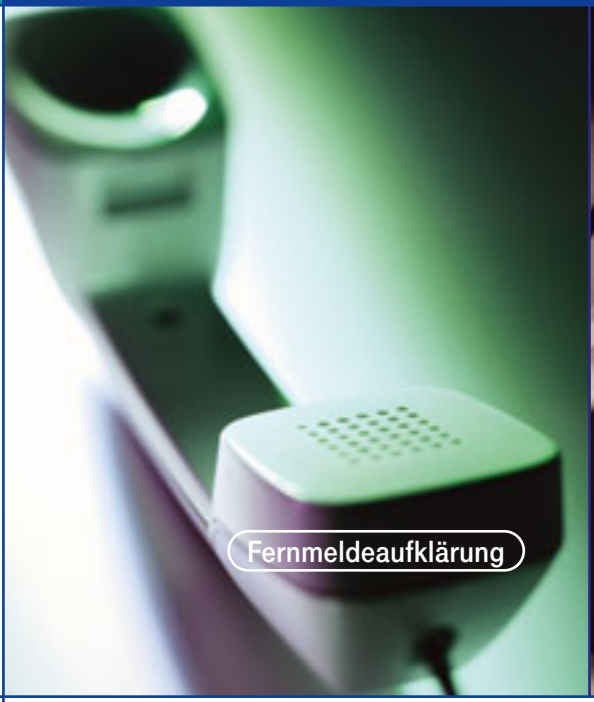
Wirtschaftsspionage und Konkurrenzausspähung vollziehen sich nicht nach einheitlichen Regeln. Staaten und Unternehmen betreiben sie in Abhängigkeit von ihren spezifischen Bedürfnissen und unter Berücksichtigung der ihnen zur Verfügung stehenden (operativen) Möglichkeiten. Staaten mit Technologierückstand sehen es eher auf wirtschaftsnahe Forschungsergebnisse und konkrete Produkte ab, während hoch industrialisierte Länder in erster Linie an wirtschaftlichen oder wirtschaftspolitischen Strategien interessiert sind. Auch bei der in aller Regel kurzfristiger angelegten Konkurrenzausspähung gibt es spezifische Interessen.

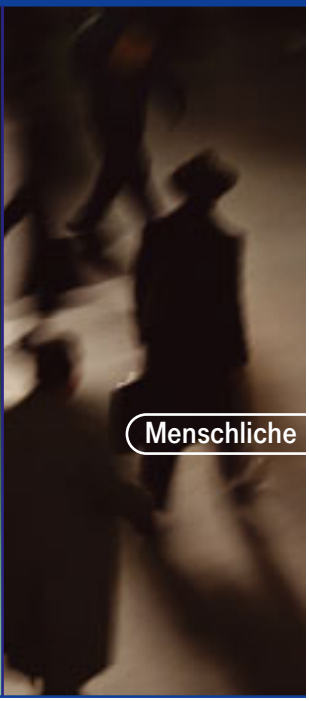


Interessen fremder Nachrichtendienste		Interessen bei der Konkurrenz-ausspähung
Technisch und wirtschaftlich hoch entwickelte Staaten	**Staaten mit Technologie-rückstand**	
■ Wirtschaftspolitische Strategien ■ Sozialökonomische und politische Trends ■ Unternehmens-, Markt- und Absatzstrategien, Zielrichtungen und Methoden der Forschung ■ Wettbewerbsstrategien, Preisgestaltung und Konditionen ■ Zusammenschlüsse und Absprachen von Unternehmen	■ Beschaffung von technischem Know-how, um Kosten für eigene Entwicklungen und Lizenzgebühren zu sparen ■ Beschaffung von Informationen über Fertigungstechniken, um auf dem Markt mit kostengünstiger gefertigten Nachbauten wettbewerbsfähig zu sein	■ Informationen über Wettbewerb, Märkte, Technologien, Kunden ■ Aktuelles Know-how zur Produktentwicklung und Produktions-technik ■ Preisinformationen ■ Kalkulationen ■ Designstudien

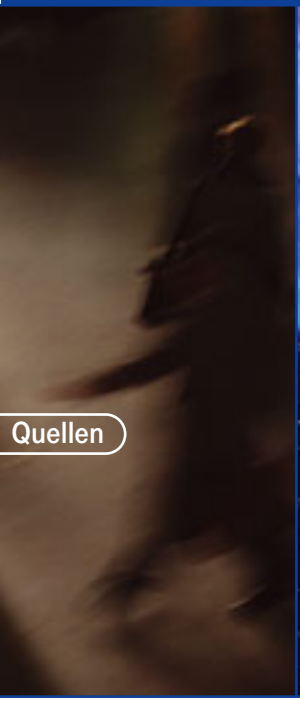


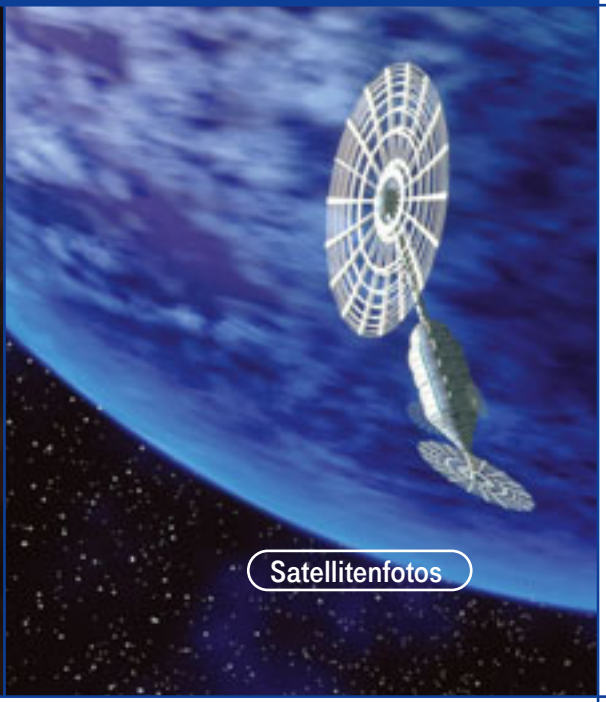
3. Fremde Nachrichtendienste





Auslandsaufklärung wird von fast allen Staaten der Welt betrieben, um politische Entscheidungen vorzubereiten oder weltwirtschaftliche Lagebilder zu erstellen.
Neben den offen zugänglichen Informationen werden hierzu auch verdeckt gewonnene nachrichtendienstliche Erkenntnisse – z. B. aus der Fernmeldeaufklärung, von Satellitenfotos sowie durch Abschöpfung menschlicher Quellen – genutzt.





Einige **Auslandsaufklärungsdienste** haben aber auch die Aufgabe, die Wirtschaft ihres Landes unmittelbar zu unterstützen, indem sie für die Unternehmen ihres Heimatlandes Informationen beschaffen, die diesen sonst nicht oder nur mit erheblichem finanziellen Aufwand zugänglich wären. In einigen Ländern sind neben den Auslandsaufklärungsdiensten auch die **Inlandsdienste** – also die klassischen Abwehrdienste – mit dieser Aufgabe betraut.

Die wichtigsten Dienste, die Wirtschaftsspionage betreiben, werden nachfolgend vorgestellt:

Chinesische Nachrichtendienste

MSS	MID	3 VBA
Guojia Anaquaanbu Ministry of State Security	**Zhong Chan Er Bu** Military Intelligence Department	**Zhong Chan San Bu** Electronic Interception Department
Ziviler Inlands- u. Auslands-nachrichtendienst	**Militärischer Inlands- u. Auslands-nachrichtendienst**	**Fernmelde-/ elektronische Aufklärung**

Die chinesischen Nachrichtendienste verfügen über ca. eine Million Mitarbeiter. Mit Sorge beobachten die Verfassungsschutzbehörden die offensive Vorgehensweise bei der Informationsbeschaffung in Deutschland.

Russische Nachrichtendienste

SWR	GRU	FSB
Slushba Wneschnej Raswedkij	**Glawnoje Raswedywatelnoje Uprawlenije**	**Federalnaja Slushba Besopasnosti**
Zivile Auslands-aufklärung	**Militärische Auslands-aufklärung**	**Ziviler & militärischer Abwehrdienst u. Fernmelde-/elektroni-sche Aufklärung**

Die russischen Nachrichtendienste verfügen über mehrere hunderttausend Mitarbeiter und sind gesetzlich verpflichtet, Wirtschaftsspionage zu betreiben. Hiervon profitiert auch die russische Wirtschaft.

Dienste von Krisenländern

Die klassische Wirtschaftsspionage hat in bestimmten Situationen auch Berührungspunkte zum Phänomenbereich „Proliferation“, d.h. zur Beschaffung von Produkten, Technologien und Know-how zum Auf- und Ausbau von Massenvernichtungswaffen bzw. deren Trägertechnologien.

Die Zuordnung einer Geschäftsaktivität birgt dann besondere Probleme, wenn es sich bei dem gehandelten Gut um ein „dual-use“-Produkt handelt, das sowohl für zivile als auch für proliferationsrelevante Zwecke eingesetzt werden kann.

Zum Thema „Proliferation“ wird auf die Broschüre der Behörden für Verfassungsschutz „Proliferation – das geht uns an!“ verwiesen.

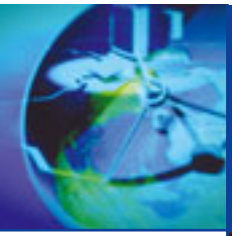

PAIS
Le Monde

Wirtschaftsspionage westlicher Dienste?

Meldungen und Berichte in den Medien sowie Äußerungen von Politikern gehen davon aus, dass auch westliche Länder Wirtschaftsspionage betreiben. Belege für eine systematische Wirtschaftsspionage westlicher Dienste liegen bisher nicht vor. Allerdings verfolgen einige westlich orientierte Staaten eine andere Philosophie vor dem Hintergrund eines strategischen Informationsmanagements.

In den USA, Großbritannien und Frankreich – so Medienberichte – könne die Wirtschaft verstärkt auf die Unterstützung der Nachrichtendienste zählen. Aus Sicht der Verfassungsschutzbehörden kann diese Mutmaßung nicht bestätigt werden. Die Spionageabwehr geht daher nach derzeitiger Erkenntnislage davon aus, dass durch westliche Nachrichtendienste keine systematische Wirtschaftsspionage gegen die Bundesrepublik Deutschland durchgeführt wird.

Allen Verdachtshinweisen wird jedoch nachgegangen.



4. Methoden der Wirtschaftsspionage

Zu den Arbeitsmethoden der Aufklärungsdienste gehören sowohl die offene Informationsgewinnung als auch die konspirative, verdeckte Nachrichtenbeschaffung. Heute lassen sich aus den weltweit zur Verfügung stehenden Quellen Informationen beschaffen, die früher nur über Agenten zu erlangen waren.

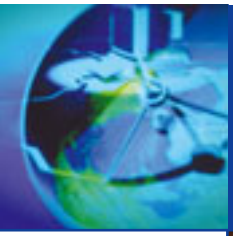
In unserer offenen Gesellschaft ist eine große Fülle auch sensibler Informationen frei zugänglich: in Fachzeitschriften, Dissertationen oder Produktbeschreibungen; man findet sie in öffentlichen Bibliotheken, in Datenbanken, auf Industriemessen oder im Internet. Oft schon versetzt eine gründliche Auswertung informativer Veröffentlichungen die Nachrichtensammler jeglicher Couleur in die Lage, Gesamtbilder ihrer Ausforschungsziele zu erstellen.

Bei ihren konspirativen Beschaffungsaktivitäten verschleiern die Geheimdienste ihre wahren Absichten und versuchen, z. B. unter der Tarnung ihrer Mitarbeiter als Diplomaten, Geschäftsleute oder Journalisten, an nachrichtendienstlich interessantes Material zu gelangen. Zusätzlich erfolgt die verdeckte Informationsbeschaffung in Deutschland durch geheime Mitarbeiter, die als Agenten für eine Verrats- oder Aufklärungstätigkeit angeworben wurden, oder es werden Nachrichtendienstmitarbeiter eingesetzt, die unter einer falschen Identität als so genannte Illegale in Deutschland

eingeschleust wurden. Die Informationsbeschaffung mit menschlichen Quellen wird ergänzt durch moderne Nachrichtentechnik, die bei der Fernmelde- und elektronischen Aufklärung sowie als Kommunikationsinstrument bei der Agentenführung eingesetzt wird.

Offene Beschaffung		Geheime Beschaffung	
Auswertung von Veröffentlichungen, Internet und Datenbanken		Einsatz von Agenten. „Quelle im Objekt“	
Besuch von öffentlichen Veranstaltungen (z. B. Messen, Kongresse, Symposien etc.)		Überwachung von Telekommunikation	
Teilnahme an Studiengängen oder wissenschaftlichen Projekten: Praktikanten, Gast-/Austauschwissenschaftler		Eindringen in Informationssysteme	
Abschöpfung im Gespräch; „social engineering“❶			

❶ „social engineering“ ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch „Aushorchen“ zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen Angst oder Respekt vor Autorität ausgenutzt. Dadurch können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln.



5. Gefahrenpotenziale

5.1 Gefahrenpotenzial: Mensch

Auch wenn Ausspähungsgefahren durch technische Schutzmaßnahmen eingeschränkt werden können, bleibt der Mensch als möglicher Risikofaktor bestehen.

Der „Innentäter“ spielt bei der Wirtschaftsspionage auch heute noch eine bedeutende Rolle. Verschiedene Studien von führenden Unternehmensberatungen, Fachzeitschriften und Wirtschaftsprüfungsgesellschaften belegen, dass in der Gesamtbreite der Wirtschaftskriminalität die größte Gefahr von den eigenen Mitarbeitern ausgeht. Dies zeigt, dass die „klassische“ Arbeitsweise, das Anwerben eines mit guten Zugängen ausgestatteten Firmenangehörigen, nach wie vor eine sehr effiziente Methode für fremde Nachrichtendienste (und Konkurrenzunternehmen) darstellt, um an Insiderinformationen zu gelangen.

Vielfach erwachsen auch Risiken aus der Tendenz, spezielle Prozesse aus dem Unternehmen auszulagern („outsourcen“) oder Fremdpersonal in den Unternehmen einzusetzen. Unter Umständen begeben sich Unternehmen so in Abhängigkeiten und verlieren die nötige Kontrolle über ihr Wissen.

5.2 Gefahrenpotenzial: Technik

Ein Leben ohne moderne Informations- und Kommunikationstechnik ist heute nicht mehr vorstellbar. Riesige Datenmengen werden in elektronischer Form vorgehalten und Informationen erreichen in Sekundenbruchteilen ihren Empfänger am anderen Ende der Welt. Das globale Dorf ist Realität geworden. Es eröffnet der Wirtschaft ungeahnte Möglichkeiten, beinhaltet aber auch bisher nicht gekannte Risiken. Nachrichtendiensten bieten sich vielfältige Angriffsmöglichkeiten, um an geheime Informationen aus Wirtschaft und Wissenschaft zu gelangen.

Dabei spielt eine wesentliche Rolle, dass erforderliche Sicherheitsmaßnahmen zur Datensicherung häufig unter dem Aspekt der Wirtschaftlichkeit bewertet und nicht den örtlichen Anforderungen angepasst werden. Spionage via Internet kennt keine zeitlichen und sprachlichen Barrieren, sie ist effizient und kostengünstig zugleich. Zudem birgt sie für den Angreifer, aufgrund der geografischen Unabhängigkeit, auch nur ein geringes Entdeckungsrisiko.

Die zunehmenden elektronischen Attacken auf Computernetze stellen mittlerweile eine größere Gefahr dar als traditionelle Ausspähungsversuche. Es dürfte heute wohl kein Unternehmen mehr geben, das nicht an das Internet angebunden und davon in mehr oder weniger großem Maße abhängig ist. Der wirtschaftliche Erfolg eines Unternehmens hängt daher heute auch davon ab, wie gut es gelingt, sensible Datenbestände und die elektronische Kommunikation vor Datenverlust und Datenmissbrauch zu schützen.

5.2.1 Internet

Grundsätzlich unterliegt jedes IT-System einer Gefährdung durch Viren- oder Trojanerattacken. Diese Formen von Schadsoftware sind in der Lage, alle Arten von Login-Daten, Netzwerkinformationen, Datenmaterial und Dokumenten Unbefugten zugänglich zu machen, Dateien zu verändern oder andere Netzwerkcomputer zu manipulieren oder zu „kapern“. Trojanisierte E-Mails, denen ein „social engineering“ vorausgehen kann, spähen zunächst die Systemumgebung der angegriffenen Rechner aus, um im Weiteren auch Daten abzuziehen.

Die Vorgehensweise bei Angriffen auf fremde IT-Systeme mittels Trojanern hat mittlerweile eine neue Qualität erreicht. Während der klassische Verbreitungsweg über Datenträger immer noch eine nicht zu unterschätzende Gefahr darstellt, erfolgen Angriffe immer häufiger mit spezieller, auf das Opfer zugeschnittener Spionagesoftware.

Zunächst wird ermittelt, welche Vorlieben, Interessen oder Hobbys die Zielperson haben könnte, um sie mit einer entsprechenden E-Mail zu konfrontieren. Beim Öffnen dieser Mail wird dann unbemerkt ein Trojaner platziert. Aktuelle Trojaner werden teilweise von marktgängigen Schutzprogrammen nicht detektiert.

5.2.2 Telekommunikationsanlagen

Die TK-Anlagen bieten eine Vielzahl von Funktionen, die auch zur unrechtmäßigen Informationsbeschaffung genutzt werden können. Hierunter fallen:

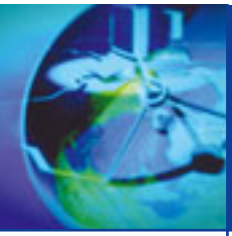
- Aufschalten (auf Verbindungen Dritter)
- Konferenzschaltung (unbemerkter Aufbau im Hintergrund)
- Automatischer Rückruf
- Freisprechen / Lauthören (Abhören von Raumgesprächen)

Das besondere Risiko erwächst daraus, dass heutige TK-Anlagen hochkomplexe Rechnersysteme darstellen. Wesentliche Gefährdungen ergeben sich aus dem Abhören von Informationen innerhalb des Systems, unbefugten Zugriffen auf Administration und Datenspeicher sowie durch Missbrauch des „remote access“ bzw. Fernzugriffes.

5.2.3 Drahtlose Verbindungen

Ob bei der Fahrt mit dem ICE, im Flughafenterminal, vom heimischen Arbeitsplatz aus oder direkt vor Ort beim Kunden – immer mehr Mitarbeiter sind heutzutage über mobile Anschlüsse mit ihrem Unternehmen verbunden. Die Funkanbindung von stationären, besonders aber von mobilen Endgeräten eröffnet jedoch nicht nur den berechtigten Nutzern, sondern auch Hackern, Konkurrenten oder fremden Nachrichtendiensten völlig neue Zugangsmöglichkeiten zu IT-Netzwerken und angeschlossenen Systemen. Nach wie vor wird die hohe Verwundbarkeit drahtloser Kommunikationsverbindungen vielerorts nicht erkannt bzw. nicht genügend ernst genommen. Anders ist es nicht zu erklären, dass selbst professionell betriebene Netze in der Wirtschaft lediglich mangelhaft oder überhaupt nicht abgesichert sind. Risikobehaftet sind praktisch alle auf drahtloser Verbindung basierenden Techniken bzw. IT-Komponenten. Als besonders anfällig haben sich erwiesen:

- WLAN-Technologie
- Bluetooth-Schnittstelle



- DECT-Standard
- Funktastaturen und -mäuse
- GSM-Mobiltelefone

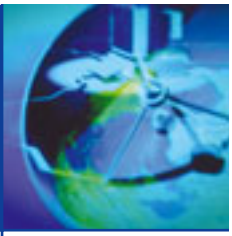
Soweit ein Verzicht auf den Einsatz drahtloser Kommunikationselemente nicht möglich sein sollte, ist es umso wichtiger, sich sachgerecht zu schützen. Dies ist nicht immer durchführbar, z. B. bei Funktastaturen und -mäusen. Im Hinblick auf WLAN-Verbindungen bietet eine Verschlüsselung jedoch einen adäquaten Schutz; sie sollte daher auf jeden Fall aktiviert und die voreingestellte Werks-Codierung gewechselt werden.

5.2.4 Mobile Endgeräte

Ebenso hohe Risiken wie drahtlose Verbindungen an sich, bergen die diversen mobilen IuK-Endgeräte (z. B. Laptops, Mobiltelefone, Smartphones, Personal Digital Assistants / PDA's und USB-Sticks), mit deren Hilfe die Kommunikation zwischen den im Außeneinsatz befindlichen Mitarbeitern und dem Unternehmen abgewickelt wird. Kaum jemand aus dem Kreis der Nutzer macht sich darüber Gedanken, dass sich unbefugte Dritte gezielt – durch Diebstahl oder im Wege des zufälligen Gerätezugriffes – Zugang zu vertraulichen Firmendaten verschaffen könnten.

Die heute in vielen Unternehmensnetzen gebräuchlichen Standard-Sicherheitsmaßnahmen wie etwa Virenschutz, Verschlüsselung und Firewalls werden viel zu selten eingesetzt. Häufig wiederkehrende Risiken im Zusammenhang mit mobilem Firmen-Equipment sind der missbräuchliche private Einsatz bis hin zur Überlassung an Dritte (Familienangehörige, Bekannte etc.), der Anschluss an ungesicherte (drahtlose) Verbindungen und die eigenmächtige Installation ungeprüfter Software.

6. Gefährdung deutscher Unternehmen im Ausland



In der globalisierten Wirtschaftswelt sind Geschäftsreisen und Aufenthalte im Ausland unabdingbar und gehören zum gewohnten Bild des Arbeitsalltages in den Unternehmen. Insofern kommt auch dem Faktor Sicherheit auf Reisen eine besondere Bedeutung zu.

Die Gefährdungen für Firmenvertreter sind vielfältig. Sie können dabei durch Terrorismus, Entführung, Erpressung, Geiselnahme, Krieg, Bürgerkrieg, Naturkatastrophen, aber auch durch Spionagetätigkeiten der Nachrichtendienste des Gastlandes sowie durch Know-how-Verlust geprägt sein.
Die Verfassungsschutzbehörden geben deshalb für Reisen ins und Aufenthalte im Ausland folgende Verhaltensempfehlungen:

- Vor Reiseantritt möglichst genaues Bild vom Gastland erarbeiten, allgemeine Gefährdungs- u. Sicherheitslage eruieren und mit den Gebräuchen und Gesetzen des Landes vertraut machen.[2]
- Vorherige Prüfung der Geschäftsverbindung und des Geschäftspartners.
- Keine missverständlichen oder abweichenden Angaben zur Person bzw. zum Arbeitgeber im Visumantrag.
- Aktuelle Ein- und Ausfuhrverbote oder -beschränkungen beachten.
- Im Gastland auf keinen Fall kompromittierende Situationen schaffen.
- Abwägung von Nutzen und Risiken einer Zusammenarbeit bzw. von Vereinbarungen mit ausländischen Service- u. Sicherheitsfirmen.
- Misstrauen bei ungewöhnlichen und intensiven Fragestellungen in Gesprächen.
- Niemals Gespräche mit Fremden über Reisezweck und Arbeitgeber führen.

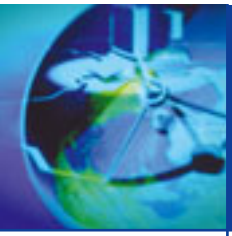
[2] Länder- und Reiseinformationen des Auswärtigen Amts beachten www.auswaertiges-amt.de

- Kritische Betrachtung von privaten Kontakt- oder Begegnungsversuchen.
- Kein persönliches Votum gegenüber Gesprächspartnern mit politischen oder berufsbezogenen Inhalten.
- Sensible Firmenunterlagen nie unbeaufsichtigt im Hotelzimmer, Tagungs- oder Büroraum belassen, Gepäck nie unbeaufsichtigt stehen lassen.
- Möglichst vollständige Vernichtung von nicht mehr benötigten Unterlagen – Abfall kann wertvolle Informationen enthalten.
- Vorsicht bei Geschenken von Geschäftspartnern in Form von USB-Sticks – mögliche Verbreitung von Trojanern.
- Nur gesicherte Kommunikationswege für sensible Informationsübermittlung nutzen – sämtliche unverschlüsselte Kommunikation (Fax, Telefon und E-Mail) ist gefährdet.
- Zum Schutz von PC und Notebook: Passwörter sowie Virenschutz- und Verschlüsselungsprogramme einsetzen (hierbei sind spezifische Ländergegebenheiten zu beachten).
- Vorsicht bei der Nutzung von Mobiltelefonen: Abhörgefahr! Nie unbeaufsichtigt lassen – manipulierte Mobiltelefone können als Mikrofon dienen.
- Geschäftliche Daten auf USB-Stick oder DVD speichern und am Körper mitführen, nie aus der Hand geben, auch nicht im Hotelsafe aufbewahren.
- Auf Notebooks möglichst nur das Betriebssystem aufspielen, minimale Konfiguration nur für Reisezwecke.

7. Instrumente zur Bekämpfung von Wirtschaftsspionage und Konkurrenzausspähung

Die Abwehr von Wirtschaftsspionage und Konkurrenzausspähung ist schwieriger geworden, doch sie ist nicht aussichtslos. Voraussetzungen einer erfolgreichen Abwehr sind: Sensibilität gegenüber den Angriffsverfahren, Kenntnisse über die Methoden und Ziele der Nachrichtendienste, der Einsatz geeigneter Schutzmaßnahmen und die Einsicht in deren Notwendigkeit. Sie sind unverzichtbar, denn sie helfen, erhebliche wirtschaftliche Schäden zu vermeiden.

- Fordern Sie uns bei Ihren Fragen zur Sicherheit.
- Vereinbaren Sie einen regelmäßigen Informationsaustausch in Sicherheitsfragen mit uns.
- Nehmen Sie bei Sicherheitsvorfällen unsere Hilfe an.



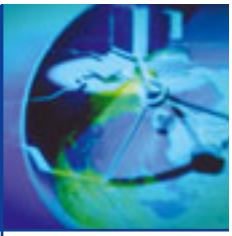
8. Die „10 Goldenen Regeln“ der Prävention

Die nachfolgenden Merksätze fassen abschließend kurz und prägnant die wesentlichen Aspekte des Informationsschutzes zusammen. Bei Bedarf können sie durch unternehmensspezifische Gesichtspunkte ergänzt werden.

1. Nicht warten, bis der Spionagefall eingetreten ist!
2. Aktuelle Informationen bei kompetenten Partnern einholen!
3. Informationsschutz als wichtigen Bestandteil der Firmenphilosophie und Firmenstrategie verankern!
4. Sicherheitsstandards regelmäßig analysieren!
5. Ganzheitliches Sicherheitskonzept realisieren und permanent fortschreiben!
6. Schutzmaßnahmen auf den Kernbestand zukunftssichernder Informationen konzentrieren!
7. Einhaltung und Erfolg der Sicherheitsvorkehrungen kontrollieren, Sicherheitsverstöße sanktionieren!
8. „Frühwarnsystem“ zur Erkennung von Know-how-Verlusten installieren!
9. Auffälligkeiten und konkrete Hinweise konsequent verfolgen, professionelle Hilfe in Anspruch nehmen!
10. Informationsschutz als strategischen Erfolgsfaktor nutzen!

Nehmen Sie das Angebot einer kostenlosen Beratung durch den Verfassungsschutz an.

9. Ihre Ansprechpartner



Bundesamt für Verfassungsschutz
Merianstr. 100
50765 Köln
Tel: 0221-792-3838 • Fax: 0221-792-1247
E-Mail: bfvinfo@verfassungsschutz.de • http://www.verfassungsschutz.de

---

Landesamt für Verfassungsschutz Baden-Württemberg
Taubenheimstr. 85 a
70372 Stuttgart
Tel: 0711-9544301 • Fax: -9544444
E-Mail: wirtschaftsschutz@lfvbw.bwl.de • http://www.verfassungsschutz-bw.de

---

Bayerisches Landesamt für Verfassungsschutz
Knorrstr. 139
80937 München
Tel: 089-31201-500 • Fax: -31201-380
E-Mail: wirtschaftsschutz@lfv.bayern.de • http://www.verfassungsschutz.bayern.de

---

Senatsverwaltung für Inneres und Sport – Abteilung II –
Potsdamer Str. 186
10783 Berlin
Tel: 030-901290 • Fax: 90129844
E-Mail: info@verfassungsschutz-berlin.de • http://www.verfassungsschutz-berlin.de

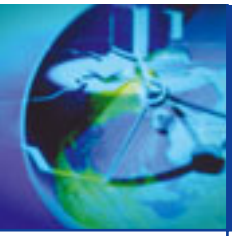
---

Ministerium des Innern des Landes Brandenburg
- Abteilung V -
Henning-von-Tresckow-Str. 9-13
14467 Potsdam
Tel: 0331-8662500 • Fax: -8662599
E-Mail: info@verfassungsschutz-brandenburg.de •
http://www.verfassungsschutz-brandenburg.de

Landesamt für Verfassungsschutz Bremen
Flughafenallee 23
28199 Bremen
Tel: 0421-53770 • Fax: -5377195
E-Mail: office@lfv.bremen.de • http://www.bremen.de/innensenator

---

Freie und Hansestadt Hamburg
Behörde für Inneres
Landesamt für Verfassungsschutz
Johanniswall 4 III
20095 Hamburg
Tel: 040-244443 • Fax: -338360
E-Mail: poststelle@verfassungsschutz.hamburg.de •
http://www.verfassungsschutz.hamburg.de



Landesamt für Verfassungsschutz Hessen
Behördenzentrum Wiesbaden
Konrad-Adenauer-Ring 41 – 43
65187 Wiesbaden
Tel: 0611-720406 • Fax: -720179
E-Mail: lfv-hessen@t-online.de • http://www.verfassungsschutz-hessen.de

---

Innenministerium des Landes Mecklenburg-Vorpommern
- Abteilung II/5 -
Johannes-Stelling-Str. 21
19053 Schwerin
Tel: 0385-74200 • Fax: -714438
E-Mail: info@verfassungsschutz-mv.de • http://www.verfassungsschutz-mv.de

---

Niedersächsisches Ministerium für Inneres und Sport - Abteilung 6 -
Büttnerstr. 28
30165 Hannover
Tel: 0511-67090 • Fax: -6709393
E-Mail: wirtschaftsschutz@abt6.mi.niedersachsen.de •
http://www.verfassungsschutz.niedersachsen.de

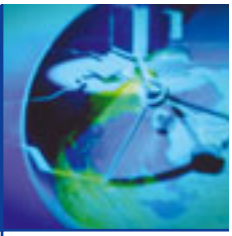
Innenministerium des Landes Nordrhein-Westfalen
- Abteilung 6 -
Haroldstr. 5
40213 Düsseldorf
Tel: 0211-8712821 • Fax: -8712980
E-Mail: info@mail.verfassungsschutz.nrw.de • http://www.verfassungsschutz.nrw.de

---

Ministerium des Innern und für Sport Rheinland-Pfalz
- Abteilung 6 -
Schillerplatz 3 - 5
55116 Mainz
Tel: 06131-163772 • Fax: -163688
E-Mail: abteilung6@ism.rlp.de • http://www.verfassungsschutz.rlp.de

---

Landesamt für Verfassungsschutz Saarland
Neugrabenweg 2 – 3. Etage
66123 Saarbrücken
Tel: 0681-30380 • Fax: -3038109
E-Mail: referat2-4@lfv.saarland.de • http://www.saarland.de/verfassungsschutz.htm



Landesamt für Verfassungsschutz Sachsen
Neuländer Straße 60
01129 Dresden
Tel: 0351-85850 • Fax: -8585500
E-Mail: verfassungsschutz@lfv.smi.sachsen.de • http://www.verfassungsschutz.sachsen.de

Ministerium des Innern des Landes Sachsen-Anhalt
- Abteilung 5 -
Zuckerbusch 15
39114 Magdeburg
Tel: 0391-5673900 • Fax: -5673999
E-Mail: ref54@mi.sachsen-anhalt.de • http://www.mi.sachsen-anhalt.de/verfassungsschutz

Innenministerium des Landes Schleswig-Holstein
- Abteilung IV / 7 -
Düsternbrooker Weg 92
24105 Kiel
Tel: 0431-9883500 • Fax: -9883503
E-Mail: IV7-zentrale@im.landsh.de •
http://www.verfassungsschutz.schleswig-holstein.de

Thüringer Landesamt für Verfassungsschutz
Haarbergstr. 61
99097 Erfurt
Tel: 0361-44060 • Fax: -4406251
E-Mail: kontakt@tlfv.thueringen.de • http://www.verfassungsschutz.thueringen.de

Braucht Ihr Sicherheits-bewusstsein ein Update?

IMPRESSUM

Herausgeber:

Bundesamt für

Verfassungsschutz für die

Verfassungsschutzbehörden in

Bund und Ländern

Druck:

Vereinigte Verlagsanstalten,

Düsseldorf

Stand: Juni 2008