CORPORATE TRUST
business risk & crisis management

Studie: Industriespionage

Die Schäden durch Spionage in der deutschen Wirtschaft

Inhalt

„Im verschärften internationalen Wettbewerb operieren unsere Konkurrenten beim Ringen um Marktanteile zunehmend mit dem Mittel der Wirtschaftsspionage. Sie ersparen sich damit eigene Forschungs- und Entwicklungskosten. Diebstahl statt Forschung senkt die Produktionskosten. Mit dem Ergebnis machen die Länder uns dann zu Dumpingpreisen Konkurrenz. Der Schaden für Exportweltmeister Deutschland wird auf über 20 Milliarden Euro im Jahr geschätzt. Das gefährdet auch unsere Arbeitsplätze.

Besonders aktiv in der Wirtschaftsspionage sind bei uns derzeit Länder aus dem asiatischen Raum. Aber auch Industrie- und Schwellenländer aus anderen Regionen betreiben nach unseren Beobachtungen in wachsendem Umfang Wirtschaftsspionage."

Dr. August Hanning,

Staatssekretär im Bundesinnenministerium und ehemaliger Leiter des Bundesnachrichtendienstes (BND) bei einem Interview am 14.10.2007.

Vorwort

Christian Schaaf
Geschäftsführer
Corporate Trust

**„Das Problem:
Es fehlt häufig an ganzheitlichen Konzepten, um sich der wachsenden Bedrohung zu stellen. Schutz gegen Informationsabfluss wird manchmal nur als EDV-Problem verstanden.“**

Die Bedrohung durch Industriespionage hat sich in den letzten Jahren für die Unternehmen geändert. Wirtschaftsspionage ist nicht mehr nur ein Betätigungsfeld der Geheimdienste, sondern leider auch zunehmend ein gebräuchliches Mittel der Konkurrenz oder die Rache eines verschmähten Mitarbeiters.

Deutschland ist Innovationsweltmeister. Die Produktion wird aus Kostengründen häufig ins Ausland verlagert, Forschung und Entwicklung bleiben im Inland. Gerade der Maschinenbau mit seinen zahlreichen Erfindungen ist eine der tragfähigsten Säulen der deutschen Wirtschaft. Dieses Wissen ist gefragt und dadurch wird Deutschland zunehmend das Ziel von illegalen Attacken.

Wie aus dem aktuellen Bericht [1] des Bundesamtes für Verfassungsschutz hervor geht, ist das Thema Wirtschaftsspionage vor dem Hintergrund des weltweiten Ringens um Marktanteile von immer höherer Bedeutung. Besonders genannt werden die Aktivitäten aus Russland und China. „Chinesische Studenten und jeder chinesische Geschäftmann, der ins Ausland gelassen wird, stehen in der Schuld der Partei. Sie müssen sich als Spitzel oder Denunzianten dafür revanchieren.“ Dies gab der Überläufer Chen Yonglin, ehemals Erster Sekretär des chinesischen Konsulats in Sydney, an, als er sich den dortigen Behörden öffnete.

Man unterscheidet zwischen Wirtschaftsspionage und Konkurrenzausspähung. Bei Ersterem handelt es sich um die durch fremde Nachrichtendienste betriebene Ausforschung eines Wirtschaftsunternehmens oder Betriebes. Die Ausforschung durch ein konkurrierendes Unternehmen oder Kriminelle bezeichnet man als Konkurrenzausspähung.

Die aktuelle Polizeiliche Kriminalstatistik (PKS) [2] benennt zwei Arten von Delikten, die dem Bereich Spionage zugerechnet werden können. Dies sind Wettbewerbsdelikte und das Ausspähen von Daten. Für das Jahr 2006 beziffert die PKS einen Anstieg bei den Wettbewerbsdelikten um

1)Verfassungsschutzbericht Der jährliche Verfassungsschutzbericht dient der Unterrichtung und Aufklärung der Öffentlichkeit über verfassungsfeindliche Bestrebungen in der Bundesrepublik Deutschland. Er beruht auf den Erkenntnissen, die das Bundesamt für Verfassungsschutz (BfV) im Rahmen seines gesetzlichen Auftrags, zusammen mit den Landesbehörden für Verfassungsschutz, gewonnen hat.

2)Polizeiliche Kriminalstatistik (PKS) Zusammenstellung aller der Polizei bekannt gewordenen strafrechtlichen Sachverhalte unter Beschränkung auf ihre erfassbaren wesentlichen Inhalte. Sie soll im Interesse einer wirksamen Kriminalitätsbekämpfung zu einem überschaubaren und möglichst verzerrungsfreien Bild der angezeigten Kriminalität führen.

10,4 Prozent. Die Anzahl der Fälle erhöhte sich im Jahr 2006 auf 6.550 von 5.934 im Vorjahr. Die Fallzahlen beim Ausspähen von Daten stiegen im gleichen Zeitraum um 26,4 Prozent (2.366 Fälle für 2005 auf 2.990 Fälle in 2006).

Dies sind jedoch nur Delikte, die den Behörden bekannt geworden sind. Nach eigenen Angaben der Unternehmen wurden nur in einem Viertel der Fälle die Behörden eingeschaltet. Sie scheuen sich davor, damit an die Öffentlichkeit zu gehen. Zu groß ist die Angst vor einem Reputationsverlust. Hinzu kommt, dass vermutlich ein Großteil der Vorfälle gar nicht entdeckt wird.

Die Dunkelziffer ist damit hoch. Das Bundesinnenministerium schätzt, nach Angaben von August Hanning, Innenstaatssekretär und ehemaliger Chef des Bundesnachrichtendienstes (BND) in Pullach, den Schaden durch Wirtschaftsspionage in Deutschland auf jährlich ca. 20 Milliarden Euro.

Das Problem: Es fehlt häufig an ganzheitlichen Konzepten, um sich der wachsenden Bedrohung zu stellen. Schutz gegen Informationsabfluss wird manchmal nur als EDV-Problem verstanden. Im Vordergrund steht ein steigender Bedarf an Schutzmaßnahmen gegen Hacker. Die Anforderungen an sichere Prozesse bei der Bedienung und Vorgaben für die Mitarbeiter für den Umgang mit den sensiblen Informationen werden all zu oft außer Acht gelassen. Dabei sollte gerade dem menschlichen Faktor viel mehr Beachtung gewidmet werden.

Diese Studie zeigt, dass in den meisten Fällen eigene Mitarbeiter die Täter sind. Es ist damit fraglich, ob eine Firewall ausreichenden Schutz bieten kann, wenn die Täter mit Vollzugriff im eigenen Unternehmen sitzen.

Einen absoluten Schutz gegen Spionage gibt es nicht. Dennoch gibt es zahlreiche präventive Möglichkeiten zur Vermeidung von Informationsabfluss. Es handelt sich dabei um einen ständigen Prozess, der es erforderlich macht, immer wieder neue Lücken aufzudecken und dementsprechend zu reagieren – maßvoll und der tatsächlichen Bedrohung angepasst. Darüber hinaus kann man sich gegen das Risiko von Spionage seit kurzem auch versichern.

Corporate Trust hat zusammen mit dem Handelsblatt und dem Büro für Angewandte Kriminologie in Hamburg diese Studie erarbeitet, um eine fundierte Kenntnis über die Schäden in der deutschen Wirtschaft und die aktuelle Bedrohungssituation zu erlangen.

Ihr

Christian Schaaf

Vorwort

Hans Elmar Remberg
Vizepräsident
Bundesamt für Verfassungsschutz

„Betroffene und gefährdete Unternehmen sollten nicht davor zurückschrecken, den Verfassungschutz zu konsultieren."

Seit jeher gehört die Wirtschaft neben der Politik und dem Militär zu den „klassischen" Aufklärungszielen der Nachrichtendienste. Nicht zuletzt auch deshalb, weil eine funktionierende Ökonomie eine der Grundvoraussetzungen für die innere Stabilität von Staaten ist.

Diese Erkenntnis hat natürlich im Zeitalter der Globalisierung einen noch höheren Stellenwert erfahren. Gerade im Zeichen verschärfter Konkurrenz auf dem Weltmarkt ist Wirtschaftsspionage und ihre Abwehr noch wichtiger geworden. Dies gilt in besonderem Maße für ein Land wie Deutschland, das seinen Reichtum nicht in erster Linie Rohstoffen und Bodenschätzen verdankt, sondern der innovativen Fähigkeiten seiner Menschen und Unternehmen.

Deshalb hat der Staat ein elementares Interesse daran, einen illegalen Wissenstransfer zu verhindern sowie technologisches und unternehmerisches Know-how zu schützen. Die Verfassungsschutzbehörden tragen dieser Aufgabenstellung seit Jahren Rechnung, auch durch eine enge Zusammenarbeit mit Institutionen und Verbänden sowie mit den Unternehmen selbst.

Sie verstehen unter Wirtschaftsspionage ausschließlich die staatlich gelenkte und unterstützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben. Dabei ist die oftmals identische Vorgehensweise durch die „bloße" Konkurrenzausspähung unverkennbar. Die Spionageabwehr gehört zu den Kernkompetenzen des Verfasssungsschutzes. Erkenntnisse und Analysen politischer und militärstrategischer Spionage sind von hohem Nutzen auch für Abwehr von Wirtschaftsspionage.

Produktideen, Fertigungstechniken, Patente sowie Unternehmens- und Marktstrategien sind als strategische Potenziale eines Unternehmens besonders schutzbedürftig. Ihnen gilt das Interesse von Konkurrenten und fremden Nachrichtendiensten. Sie sind die wesentlichen Angriffsziele.

Das Internet spielt dabei eine herausgehobene Rolle. Und zwar nicht nur bei der Auswertung offen verfügbarer Informationen, sondern auch im Zusammenhang mit neuartigen Angriffs- und Ausspähungstechniken. Ein wirkungsvoller Schutz gegen derartige Angriffe ist aufwändig. An Stelle eines wenig effizienten punktuellen Vorgehens gilt es auf der Basis methodischen Wissens ein ganzheitliches Schutzkonzept zu entwickeln, eine Kombination sorgfältig abgestufter und abgestimmter Entscheidungen personeller und materieller Art. Das Bundesamt für Verfassungsschutz steht als koordinierende Zentralstelle für die Angriffsanalyse und den gezielten Informationsrückfluss zur Verfügung. Über die Analyse erkannter Schadsoftware können bspw. Ausspähungsziel und potenzielle Angreifer eingegrenzt werden.

Eine erfolgreiche Abwehr wirtschaftlicher Ausspähung bedarf der Sensibilität gegenüber den Angriffsgefahren, der Kenntnis über Methoden und Ziele der Angreifer sowie schließlich geeigneter Schutzmaßnahmen. Vor allem aber braucht sie die vertrauensvolle Zusammenarbeit zwischen Sicherheitsbehörden und Unternehmen. Nicht nur fremde Nachrichtendienste tragen eine Fülle unterschiedlicher Informationsbruchstücke zusammen, um so Gesamtbilder ihrer Aufklärungsziele zu erstellen. Auch die Spionageabwehr braucht Detail-Informationen, um einzelne Teile zusammenzufügen und auf der Basis tragfähiger Analysen geeignete Abwehrstrategien zu entwickeln.

Betroffene und gefährdete Unternehmen sollten nicht davor zurückschrecken, den Verfassungsschutz zu konsultieren. Die Verfassungschutzbehörden stehen selbstverständlich für Beratungsgespräche, insbesondere auch bei fragwürdigen Kontakten und Vorkommnissen zur Verfügung. Entsprechende Angaben werden vertraulich behandelt, denn anders als Polizei und Staatsanwaltschaft unterliegen sie nicht dem Strafverfolgungszwang.

Ihr
Hans Elmar Remberg

Ergebnisse in kürze

- Die Ergebnisse dieser Studie verdeutlichen die massive Bedrohung der deutschen Wirtschaft durch Industriespionage. So hatten bereits 18,9 Prozent der Unternehmen einen Spionagefall im eigenen Unternehmen oder waren von Informationsabfluss betroffen.

- Das Risiko von Industriespionage wird deutlich unterschätzt. Obwohl über 80 Prozent der Befragten glauben, dass das Risiko für Industriespionage weltweit ansteigen wird, glauben nur 33,7 Prozent, dass die Gefahr auch für ihr eigenes Unternehmen steigen wird.

- Für die deutsche Wirtschaft entstehen durch Spionage jährlich Schäden in Milliardenhöhe. Insgesamt 64,4 Prozent aller geschädigten Unternehmen hatten auch einen finanziellen Schaden zu verzeichnen. Die Schäden reichten von 10.000,- Euro bis über 1 Million Euro je Schadensfall. Rechnet man dies hoch auf alle Unternehmen in Deutschland, ergibt sich eine Schadenssumme von mindestens 2,8 Milliarden Euro.

- Das Ziel der Spionage waren meistens technische Innovationen bzw. das Know-how bei den Produktionsabläufen.

- Bei den geschädigten Unternehmen sind die Branchen Automobil- / Luftfahrzeug- / Maschinenbau mit 26,9 Prozent sowie Eisen / Stahl / Metallverarbeitung mit 21,8 Prozent am häufigsten betroffen.

- Der Informationsabfluss durch eigene Mitarbeiter scheint eine der größten Gefahren zu sein. Von den geschädigten Unternehmen hatten 20,3 Prozent im eigenen Betrieb einen Verrat von Interna an Unberechtigte zu beklagen.

- Der Hackerangriff [3] ist die zweithäufigste Form der illegalen Attacken auf Unternehmen. Hier meldeten 14,9 Prozent der geschädigten Unternehmen, dass ihre IT–Systeme bereits von einem eingeschleusten Spionageprogramm bzw. einem Hackerangriff betroffen waren.

- Die wenigsten Unternehmen achten darauf, ihre vertraulichen Gespräche an einem geschützten Ort durchzuführen. So war das Abhören von Besprechungen mit 10,7 Prozent eine weitere sehr häufige Form der Spionage. Die geschädigten Unternehmen hatten damit einen Informationsabfluss durch einen sogenannten Lauschangriff [4] zu verzeichnen.

- In vielen Fällen ist es relativ einfach, an Details von Neuentwicklungen zu gelangen: durch Aushorchen argloser Mitarbeiter. Der richtige Ansprechpartner sowie ein paar geschickt formulierte Fragen genügen und schon gelangen die streng geheimen Informationen ungefiltert an die Konkurrenz. Durch die immer noch höchst gebräuchliche Form des „Social Engineering" [5] kamen 8 Prozent der betroffenen Unternehmen zu Schaden

3)Hackerangriff Unerlaubtes Eindringen in fremde Computer- oder Netzwerksysteme, meist durch Überwinden der Sicherheitsmechanismen.

4)Lauschangriff Nachrichtendienstlicher Sprachgebrauch für die akustische Überwachung bzw. das Abhören von Gesprächen.

5)Social Engineering Ausspionieren über das persönliche Umfeld, durch zwischenmenschliche Beeinflussungen und meist durch geschickte Fragestellungen. Social Engineering hat das Ziel, unberechtigt an Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen.

- Bemerkenswert ist, dass nicht Forschung & Entwicklung, sondern der Vertrieb der am stärksten durch Spionage betroffene Unternehmensbereich ist. Exakt 20 Prozent der Vorfälle fanden hier statt. Forschung & Entwicklung kam mit 16,1 Prozent auf Rang 2, der Bereich Personal mit 14,7 Prozent auf Rang 3.

- Die Spionagehandlungen finden in gut einem Viertel der Fälle durch die eigenen Mitarbeiter statt. Sie waren in 24 Prozent aller Fälle, bei denen ein Täter ermittelt werden konnte, verantwortlich für den Know-how-Abfluss im Unternehmen und stellen damit die größte Tätergruppe dar. Über ein Drittel der Unternehmen wollte gar keine Angaben zu den Tätern machen.

- Bei den beteiligten Mitarbeitern sind vor allem Sachbearbeiter (31,4 Prozent der Fälle), gefolgt von Facharbeitern (22,9 Prozent der Fälle) und dem Management (17,1 Prozent der Fälle), für den Informationsabfluss im Unternehmen verantwortlich.

- Nur in knapp einem Viertel der Vorfälle wurden die Behörden eingeschaltet. Die Unternehmen suchten jedoch in etwa 40 Prozent der festgestellten Spionagefälle Hilfe bei externen Spezialisten.

- Bei der Frage nach Sicherheitsvorkehrungen gaben 27,1 Prozent aller befragten Unternehmen an, keinen ausreichenden Passwortschutz auf Ihren IT-Geräten zu haben.

- Der Abhörschutz wird völlig vernachlässigt, obwohl er eine zentrale Stellung beim Schutz gegen Industriespionage hat. Nur in jedem zehnten Unternehmen sind die zentralen Belange des Abhörschutzes zur Chefsache ernannt. In fast 60 Prozent aller Unternehmen gibt es gar keinen Verantwortlichen für diesen Bereich.

- Nur gut ein Viertel aller Unternehmen überprüft die Mitarbeiter mit einem Background-Check [6] auf verdächtige Hinweise, bevor sie diese an sensible Positionen setzen. Integritätstests [7] für neue Bewerber lässt sogar nur jedes zehnte Unternehmen durchführen.

- In Zukunft wollen 73 Prozent aller Unternehmen mehr Maßnahmen in punkto Schutz gegen Industriespionage durchführen. Ganz oben auf der Liste steht dabei der Wunsch nach mehr Sensibilisierung [8] der Mitarbeiter für dieses Thema.

6)Background-Check Überprüfung von Mitarbeitern bezüglich ihren früheren Arbeitgeber, finanziellen Verhältnisse, Firmenbeteiligungen bzw. verdächtigen Lebensumstände.

7)Integritätstest Psychologisches Testverfahren zur Überprüfung der Integrität am Arbeitsplatz. Der Test prüft vor allem die Bereiche „Persönlicher Arbeitsstil" und „Allgemeine Wertvorstellungen" ab.

8)Sensibilisierung Unterweisung der Mitarbeiter zu einer bestimmten Gefahrenlage mit Bezugnahme auf eine aktuelle Bedrohung.


1 160 428
70 607
10 647
10 875
189 673
48 640
253 694
1 744 564
1 741 670
-75 874
-298 745
0
108 323
15 249
20 034
24 064
4 571
1 017
9 960
736
402
12 946
11 524
2 446
45 953
37 539
165 841
-36 429
-36 827
91
-31 825
82

Methodik der Studie

Diese Studie wurde in Zusammenarbeit mit dem Handelsblatt und der Diplom-Kriminologin Bärbel Bongartz auf Grundlage einer Befragung von 7.486 deutschen Unternehmen erstellt. Dafür wurde ein repräsentativer Querschnitt aus ca. 60.000 Unternehmen ausgewählt und nach dem Zufallsprinzip befragt.

Es wurde großer Wert darauf gelegt, dass die Befragung branchenübergreifend angelegt war und sowohl Konzerne als auch mittelständische Betriebe und kleinere Unternehmen (jeweils gemessen nach dem Umsatzvolumen und der Mitarbeiterzahl) befragt wurden.

Die Befragung erfolgte in Form eines standardisierten Fragebogens, der sowohl in Druckform als auch auf einer Webseite online beantwortet werden konnte. Befragt wurden jeweils die Geschäftsleitung bzw. die Sicherheitsverantwortlichen der Unternehmen. Die Beteiligung war bei einzelnen Branchen sehr unterschiedlich. Anhand der festgestellten Schäden ist jedoch davon auszugehen, dass Spionage vor allem in diesen Branchen ein großes Problem darstellt und daher auch eine höhere Bereitschaft vorhanden war, sich mit der Thematik auseinanderzusetzen.

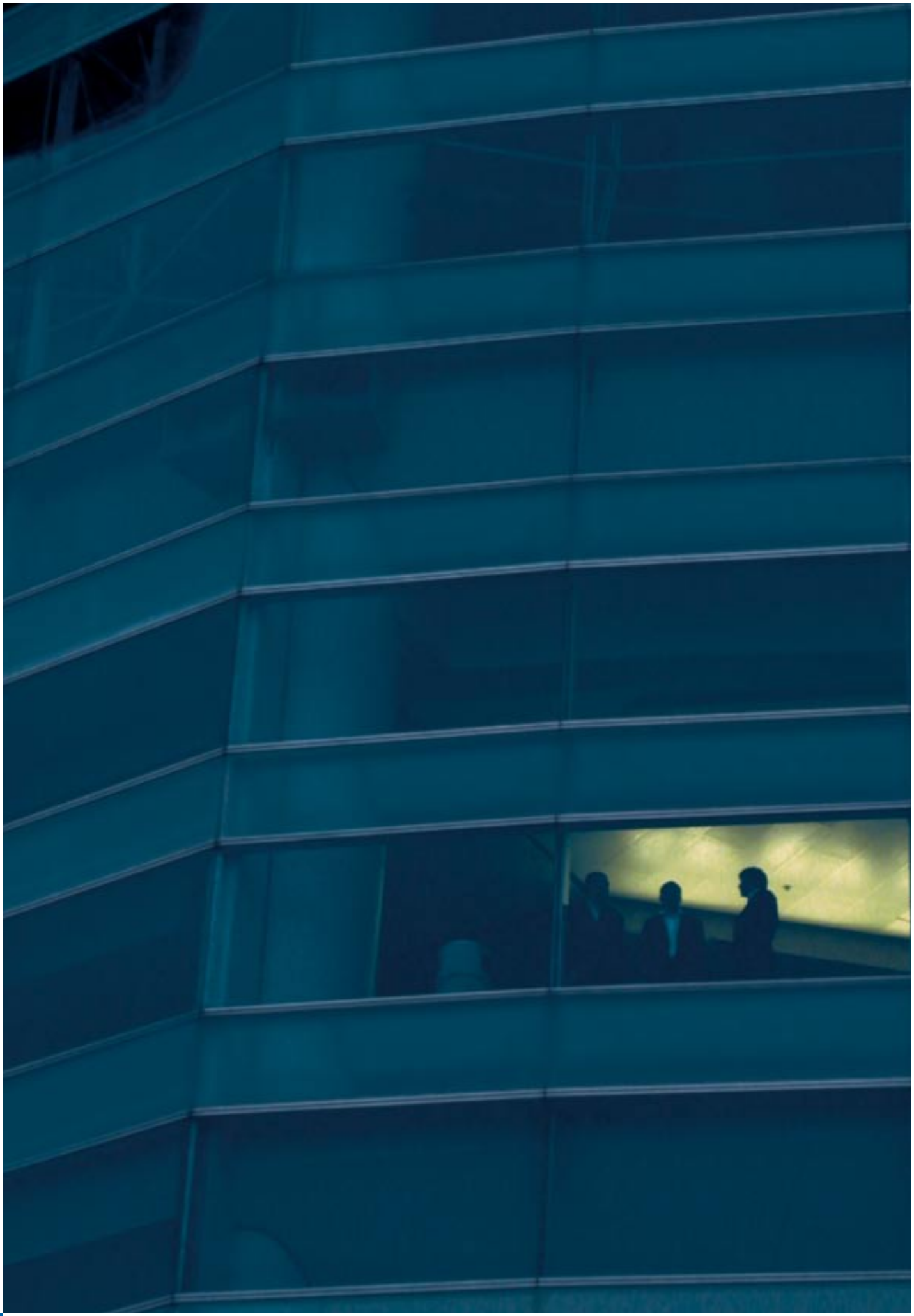
Teilnahme an der Studie:

GRAFIK 1 Quelle: Corporate Trust 2007

Abgefragt wurden sowohl Informationen zum Unternehmen, den Sicherheitsvorkehrungen, Spionagefällen und festgestellten Tätern, als auch die vermutete Entwicklung von Informationsabfluss und die zukünftigen Präventionsmaßnahmen im Unternehmen. Die Fragen wurden dabei so angelegt, dass die vorgegebenen Auswahlmöglichkeiten der einzelnen Antworten erfahrungsgemäß 80 Prozent der denkbaren Antworten abdeckten. Für die restlichen 20 Prozent gab es bei einer Vielzahl von Fragen die Möglichkeit der Freitexteingabe. Bei einzelnen Fragen war ebenso eine Mehrfachnennung bei den Antworten möglich.

Im August und September 2007 wurde der Fragebogen an 4.238 Unternehmen postalisch und an weitere 3.248 Unternehmen per Email versandt. Letztgenannte wurden in der Email aufgefordert, an der Befragung online teilzunehmen. Dazu wurden den Online-Teilnehmern die Zugangsdaten mitgeteilt, welche für alle gleich waren. Auf diese Weise war gewährleistet, dass nur ausgewählte Unternehmen an der Befragung teilnahmen und keine Zufallsbesucher von der Möglichkeit der Online-Befragung Gebrauch machen konnten.

Der Fragebogen enthielt am Ende der Befragung jeweils die Möglichkeit, das antwortende Unternehmen zu benennen. Es war jedoch allen Teilnehmern freigestellt, auch anonym zu antworten. Obwohl vermutet wurde, dass die Antworten zum überwiegenden Teil anonym abgegeben werden würden, war dies nicht der Fall. Ein Großteil der antwortenden Unternehmen gab sowohl vertrauliche Details zu Spionagevorfällen preis als auch den Unternehmensnamen. Von den 7.486 befragten Unternehmen antworteten genau 741 Unternehmen, dies sind 9,9 Prozent aller befragten Unternehmen. Die Antwortbereitschaft lag damit im normalen Durchschnitt anderer Befragungen. Allen teilnehmenden Führungskräften und Sicherheitsverantwortlichen danken wir auf diesem Wege nochmals recht herzlich.



Spionage in der deutschen Wirtschaft

Betroffene Unternehmen

Jedes fünfte Unternehmen wurde schon einmal ausspioniert, jedes dritte hatte bereits den Verdacht.

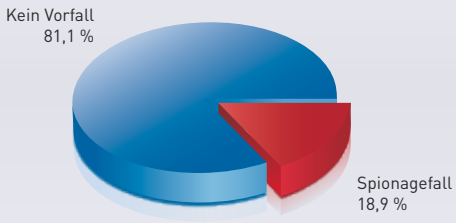
Industriespionage stellt für Deutschland ein ernst zu nehmendes Problem dar. Etwa jedes fünfte Unternehmen dürfte schon einmal davon betroffen gewesen sein, ein weiteres Drittel hatte bereits einen Verdacht auf Spionage.

18,9 Prozent der Geschäftsführer, Vorstände oder Sicherheitsverantwortlichen gaben an, dass sie bereits in mindestens einem konkreten Fall ausspioniert worden sind.

Die tatsächliche Zahl liegt vermutlich noch weitaus höher. Befragt man die Unternehmen, ob es schon einmal einen Verdacht auf Spionage gab, antwortet mehr als jedes dritte mit Ja. Genau 35,1 Prozent gaben an, dass sie einen Verdacht auf Spionage bzw. Informationsabfluss im Unternehmen hatten, der jedoch nicht ausreichend belegt werden konnte.

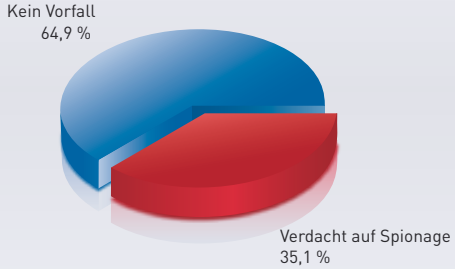
Einen Spionagefall im eigenen Haus zu haben ist für viele erschreckend, weil die Angst vor einem wirtschaftlichen Verlust oder Reputationsschaden sehr groß ist. Bei vielen Unternehmen wird das Thema jedoch verdrängt, bis ein Schaden eintritt und man gezwungen ist, aufzuklären, den Schaden zu begrenzen und weitere Maßnahmen zu ergreifen. Die vorliegende Studie zeigt jedoch, dass die deutsche Wirtschaft durchaus von Spionage betroffen ist und sich gegen ungewollten Informationsabfluss schützen sollte. Die hohe Zahl der Verdachtsfälle zeigt auch, dass es oftmals schwer ist, die nötigen Beweise zu erlangen und somit viele Vorfälle unaufgedeckt bleiben.

Gab es in ihrem Unternehmen bereits konkrete Hinweise auf Spionage bzw. einen Informationsabfluss?



GRAFIK 2 Quelle: Corporate Trust 2007

Gab es in Ihrem Unternehmen einen Verdacht auf Spionage bzw. Informationsabfluss, der nicht näher belegt werden konnte?



GRAFIK 3 Quelle: Corporate Trust 2007

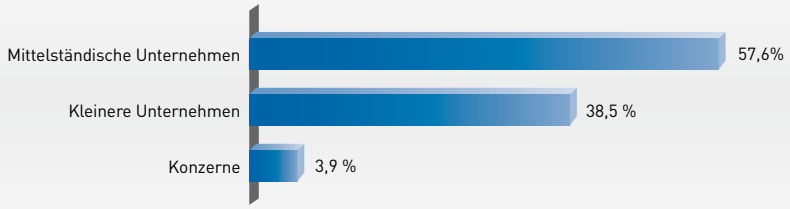
Betroffene Unternehmen

Spionage betrifft Unternehmen jeder Größenordnung.

Wirtschafts- oder Konkurrenzspionage betrifft alle Unternehmensgrößen. Sie betrifft sogar am häufigsten kleine und mittelständische Unternehmen. Viele Konzerne haben sich im Laufe der Jahre eine sehr gute Sicherheitsstruktur aufgebaut und schützen sich umfangreich gegen ungewollten Informationsabfluss. Mittelständische Unternehmen sind dagegen deutlich stärker gefährdet, Opfer eines Spionageangriffs zu werden. Sie geraten vermutlich aufgrund ihres innovativen Know-hows und weniger Sicherheitsvorkehrungen öfter in den Fokus von Spionen.

Bei den aufgedeckten Schäden und Verdachtsfällen waren mit 57,6 Prozent die mittelständischen Unternehmen (50 – 500 Millionen Umsatz oder 50 – 250 Mitarbeiter) deutlich am häufigsten betroffen, gefolgt von den kleineren Unternehmen (10 – 50 Millionen Umsatz oder 10 – 50 Mitarbeiter) mit 38,5 Prozent und den großen Konzernen (über 500 Millionen Umsatz oder mehr als 500 Mitarbeiter) mit nur 3,9 Prozent.

Schäden nach Unternehmensgröße:



GRAFIK 4 Quelle: Corporate Trust 2007

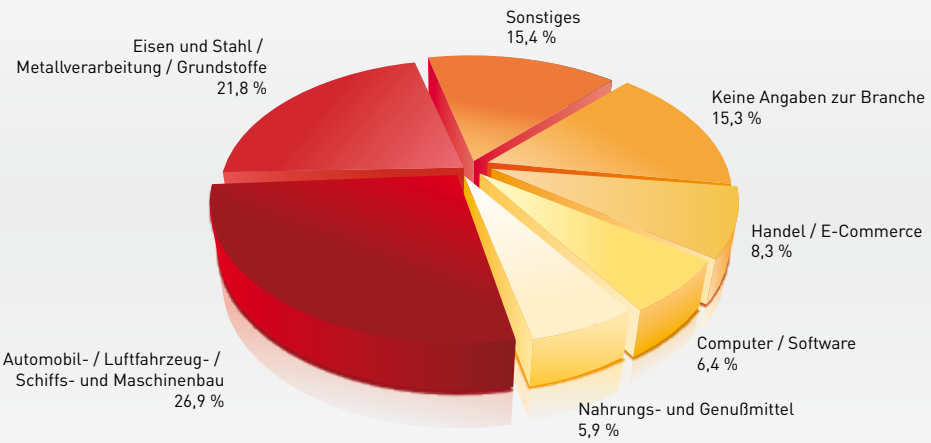
Vor allem Branchen mit technischen Innovationen sind gefährdet.

Ein Ziel der Studie war es, aufzudecken, ob es Branchen gibt, die deutlich stärker gefährdet sind als andere. Die Unternehmen wurden daher befragt, in welcher Branche sie tätig sind. Bei den aufgedeckten und vermuteten Spionagefällen stellte sich dann ein klarer Trend heraus. Das Ziel der Spionage waren meistens technische Innovationen bzw. das Know-how bei den Produktionsabläufen. Dieses Wissen stellt einen ganz entscheidenden Wettbewerbsfaktor dar und ist entscheidend für den Erfolg eines Unternehmens.

Die größte Gefahr für ein Unternehmen, durch Industriespionage geschädigt zu werden, besteht demnach in den Branchen Automobil- / Luftfahrzeug- / Schiffs- / Maschinenbau (26,9 Prozent aller geschädigten Unternehmen) sowie Eisen und Stahl / Metallverarbeitung / Grundstoffe (21,8 Prozent aller geschädigten Unternehmen). Hier gab es deutliche Häufungen von Vorfällen.

In diesem Zusammenhang fällt auf, dass die Branchen Chemie / Pharma / Biotechnologie und Banken / Finanzdienstleistungen / Versicherungen gar keine Angaben zu Schäden machten, obwohl alle anderen Sparten über Spionagevorfälle berichteten. Dies lässt sich vermutlich mit einer großen Sensibilität dieser Bereiche und der Angst vor einen Imageverlust aufgrund eines Datenklaus erklären. Gerade die Finanzbranche ist bekannt dafür, jedes Jahr hohe Beträge für die Sicherheit ihrer Systeme auszugeben. Die Chemie- / Pharma- und Biotechnologiebranche hat vermutlich einen der höchsten Forschungsetats aller Branchen. Es ist zweifelhaft, dass in diesen Bereichen tatsächlich noch keinerlei Informationsabflüsse statt gefunden haben sollen.

Geschädigte Branchen:



GRAFIK 5 Quelle: Corporate Trust 2007

Spionage in der deutschen Wirtschaft

Schäden durch Spionage

Die finanziellen Schäden durch Industriespionage liegen in Milliardenhöhe.

Deutschen Unternehmen entsteht durch Industriespionage jährlich ein Schaden von ca. 2,8 Milliarden Euro. Befragt nach ihren finanziellen Schäden durch die Spionage, gaben immerhin 7,2 Prozent der betroffenen Unternehmen an, einen Schaden von über einer Million Euro erlitten zu haben.

Insgesamt hatten 64,4 Prozent der geschädigten Unternehmen finanzielle Verluste zu beklagen, von einigen Tausend bis über eine Million Euro je Vorfall.

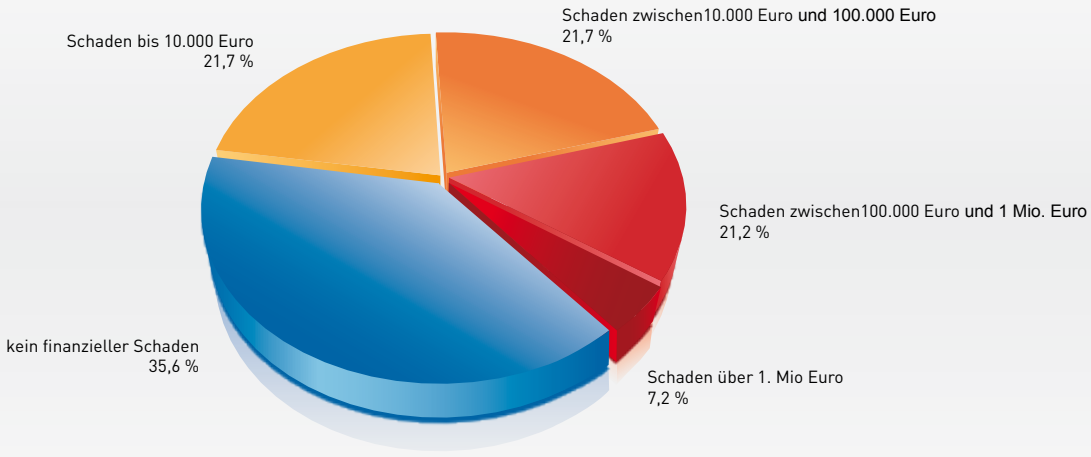
Zählt man die einzelnen Schäden bei betroffen Unternehmen zusammen und rechnet es anhand ihres prozentualen Anteils auf ca. 65.000 Unternehmen in Deutschland hoch, so ergibt sich daraus eine Schadenssumme von ca. 2,8 Milliarden Euro für die deutsche Wirtschaft.

Berücksichtigt wurde dabei nur die Kategorie von Unternehmen mit mindestens 10 Millionen Umsatz bzw. mindestens 10 Mitarbeitern, aus der repräsentativ für diese Befragung ausgewählt wurde. Bei den Schadenssummen wurde jeweils nur von einem Mittelwert ausgegangen, also z.B. 50.000,- Euro bei der Kategorie von 10.000,- bis 100.000,- Euro.

Rechnet man die Schäden auf die insgesamt ca. 3,2 Millionen Unternehmen [9] in Deutschland hoch, so dürfte der tatsächliche Schaden noch deutlich höher liegen.

Bei dem Großteil davon handelt es sich jedoch um Kleinstunternehmen [10], die in der Studie nicht untersucht wurden.

Welcher finanzielle Schaden wurde durch Spionage angerichtet?



GRAFIK 6 Quelle: Corporate Trust 2007

9)steuerpflichtige Unternehmen Quelle: Das Statistische Jahrbuch 2006

10)Kleinstunternehmen Definition der EU für KMU (Kleine und mittlere Unternehmen) – Kleinstunternehmen: weniger als 10 Mitarbeiter oder weniger als 2 Millionen Euro Umsatz

SCHÄDEN DURCH SPIONAGE

Durch Informationsabfluss von eigenen Mitarbeitern entstehen die häufigsten Schäden.

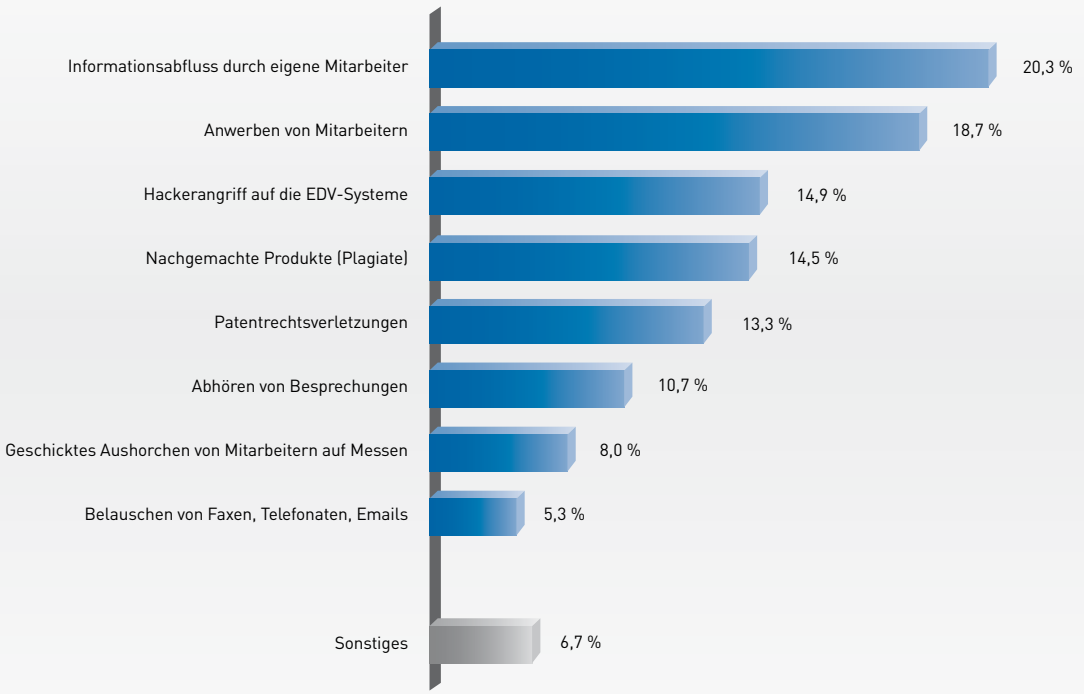
Als signifikantes Problem stellt sich der Informationsabfluss durch eigene Mitarbeiter dar. Hier lagen für die Unternehmen die häufigsten Schäden. Sowohl Mitarbeiter im Unternehmen als auch ausgeschiedene Mitarbeiter sorgten dafür, dass Informationen unberechtigt weiter gegeben wurden.

Bei den ausgeschiedenen Mitarbeitern kristallisierten sich vor allem zwei Kategorien als Täter heraus – Mitarbeiter, die sich selbstständig gemacht hatten und Mitarbeiter, die zur Konkurrenz gegangen waren. Exakt 20,3 Prozent aller Spionagefälle wurden in Form von Informationsabfluss durch eigene Mitarbeiter begangen.

In 18,7 Prozent der Fälle kam es dazu, dass Mitarbeiter von der Konkurrenz oder einem ausländischen Geheimdienst angeworben wurden. Dies zeigt deutlich, dass es sehr häufig illegale Anwerbeversuche [11] gibt. Bei dieser Form der Spionage werden erst zwischenmenschliche Beziehungen aufgebaut, bevor die Mitarbeiter gezielt nach Unternehmens-Informationen gegen Bezahlung gefragt werden.

Immerhin noch in 8 Prozent der Fälle führte das geschickte Aushorchen von Mitarbeitern auf Messen zum Verlust von sensiblen Informationen. Dies zeigt, dass Mitarbeiter nicht ausreichend für die Vorgehensweise solcher „Anwerber" [11] sensibilisiert sind und Messen ein gebräuchliches Forum für Informationsangriffe darstellen.

Welchen konkreten Handlungen fanden statt? (Mehrfachnennungen möglich)



GRAFIK 7 Quelle: Corporate Trust 2007

11)Anwerben / Anwerber Von einem Geheimdienst oder Konkurrenten ausgehender Versuch, Mitarbeiter nach Informationen aus dem Unternehmen zu befragen bzw. sie als fortwährende Quelle zu gewinnen. Häufig geht der eigentlichen Frage nach Informationen der Aufbau einer zwischenmenschlichen Beziehung voraus.

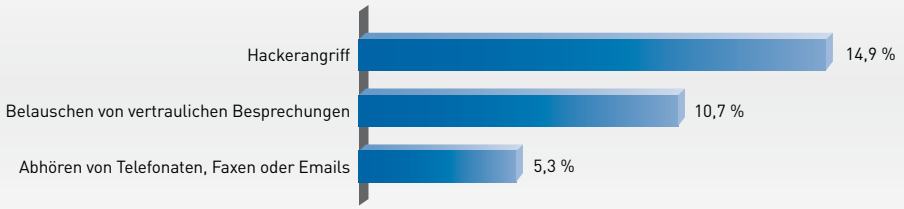
Hacker- und Lauschangriffe sind weit verbreitet.

Die Befragung der Unternehmen ergab: 14,9 Prozent der geschädigten Firmen erlitten einen Schaden aufgrund eines Hackerangriffs [12] auf die EDV-Systeme. Damit steht jeder siebte Fall von Spionage in Zusammenhang mit einem Angriff auf die Firmen-IT durch Hacker.

Darüber hinaus werden aber auch sämtliche anderen Kommunikationsmöglichkeiten einer Firma für Abhör- und Lauschzwecke [13] mißbraucht. 10,7 Prozent aller Unternehmen hatten bereits einen Abfluss von sensiblen Informationen, weil eine vertrauliche Besprechung belauscht wurde. Immerhin noch bei 5,3 Prozent kam es zu einem Schaden, weil Telefonate, Faxe oder Emails abgehört wurden.

Die Angriffsformen sind vielfältig. Sie reichen von vertraulichen Emails, die ohne Wissen des Versenders automatisch an eine dritte Person weiter geleitet werden, über Wanzen in Telefonen oder Steckdosen bis hin zu Minisendern in Faxgeräten oder Scannern, die jedes Dokument an einen Empfänger außerhalb des Unternehmens übertragen.

Schäden durch klassische Angriffsformen:



GRAFIK 8 Quelle: Corporate Trust 2007

12)Hackerangriff Unerlaubtes Eindringen in fremde Computer- oder Netzwerksysteme, meist durch Überwinden der Sicherheitsmechanismen.

13)Lauschangriff Nachrichtendienstlicher Sprachgebrauch für die akustische Überwachung bzw. das Abhören von Gesprächen.

SCHÄDEN DURCH SPIONAGE

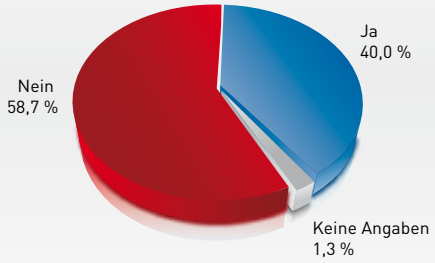
Schäden sind überwiegend in Deutschland.

Obwohl 40 Prozent aller befragten Unternehmen angaben, auch im Ausland Tochterunternehmen bzw. Niederlassungen zu haben, war der Großteil der Vorfälle doch in Deutschland. Hier fanden 76,9 Prozent aller Spionageangriffe statt und nur 15,4 Prozent in einem ausländischen Tochterunternehmen oder einer ausländischen Niederlassung.

Dies zeigt deutlich, das Hauptangriffsziel liegt in Deutschland. Eventuell werden die Angriffe in Deutschland deutlich öfter registriert, weil die Sicherheitsstrukturen besser sind als im Ausland oder weil die Vorfälle im Ausland vor dem Mutterunternehmen in Deutschland vertuscht werden.

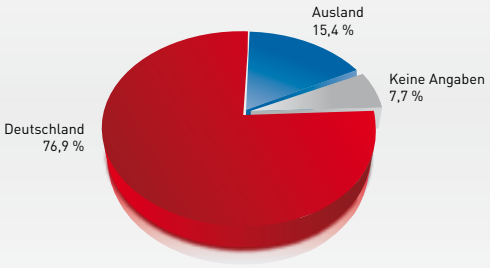
Es kann aber auch daran liegen, dass das interessante Know-how in Deutschland liegt und die Informationen bei den ausländischen Gesellschaften nicht in dem Umfang zur Verfügung stehen, dass sich Angriffe lohnen würden.

Haben Sie Auslandsniederlassungen?



GRAFIK 9 Quelle: Corporate Trust 2007

War der Fall oder Verdacht auf Spionage in Deutschland oder bei einer ausländischen Tochter bzw. Niederlassung?



GRAFIK 10 Quelle: Corporate Trust 2007

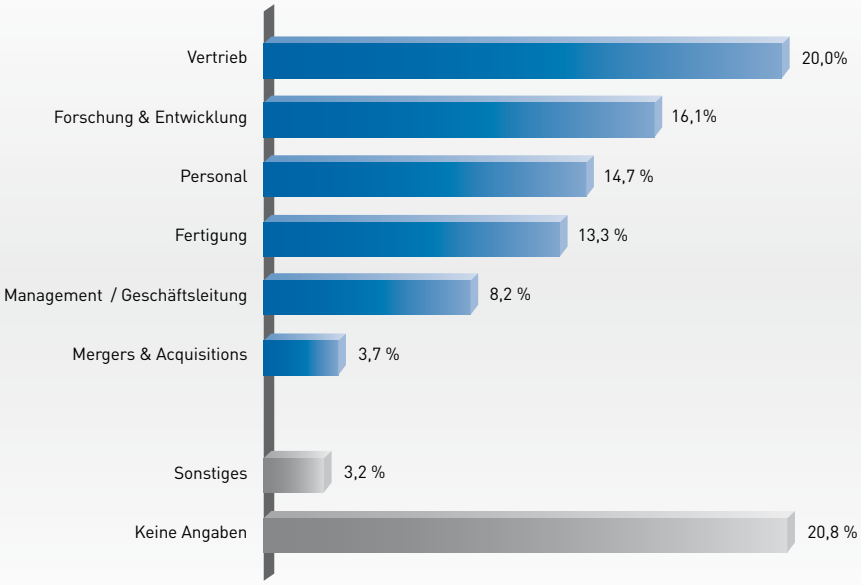
Der Vertrieb wurde noch häufiger als Forschung und Entwicklung ausspioniert.

Entgegen den Erwartungen war nicht Forschung & Entwicklung sondern der Vertrieb der am stärksten durch Spionage betroffene Unternehmensbereich. 20 Prozent der Spionageangriffe hatten zum Ziel, an vertriebliche Informationen wie Kundenlisten oder Vertreternetze zu gelangen. Forschung & Entwicklung war dahinter auf Platz 2 mit 16,1 Prozent der Angriffe. Ein Großteil der Unternehmen gab zwar an, einen Spionagevorfall im eigenen Unternehmen erlitten zu haben, wollten aber nicht den betroffenen Bereich nennen.

Der Bereich Personal ist eine weitere verwundbare Stelle im Unternehmen. Qualifizierte Mitarbeiter und das Top-Management sind auch bei der Konkurrenz gefragt. Sie haben Zugang zu sensiblen Informationen und sind oftmals die Leistungsträger. So lässt es sich erklären, dass 14,7 Prozent der Spionagefälle im Bereich Personal und weitere 8,2 Prozent im Bereich Management/Geschäftsleitung stattfanden. Für viele Unternehmen ist es daher ein wichtiger Grundsatz, „Headhunter-Anrufe“ [14)] abzuwehren. Diese haben das Ziel, Mitarbeiter abzuwerben und damit wertvolles Know-how abzuziehen, meistens zur Konkurrenz. Rechnet man die beiden Bereiche Personal und Management / Geschäftsleitung als die Mitarbeiter eines Unternehmens zusammen, so wäre dies mit insgesamt 22,9 Prozent sogar der am häufigsten ausspionierte Bereich.

In der Fertigung treffen die Patente neuer Entwicklungen und das Wissen über die Arbeitsprozesse für eine wirtschaftliche Herstellung zusammen. Hier liegt deshalb viel Unternehmens-Know-how. Der Bereich Fertigung war mit 13,3 Prozent der Fälle ebenfalls ein stark betroffener Bereich für kriminelle Angriffe auf das Firmenwissen.

In welchem Bereich wurde spioniert bzw. bestand der Verdacht auf Spionage?



GRAFIK 11 Quelle: Corporate Trust 2007

14)Headhunter Englischer Begriff für einen Personalvermittler. Häufig wird mit aggressiven Methoden versucht, Mitarbeiter bei einem Konkurrenten des suchenden Unternehmens abzuwerben.

SCHÄDEN DURCH SPIONAGE

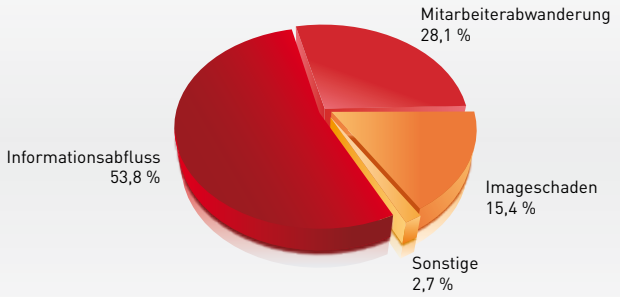
Unternehmen kämpfen nicht nur mit finanziellen Folgen.

Doch für viele Unternehmen geht es nicht nur um die finanziellen Folgen. Der Reputationsverlust bei Kunden und das schwindende Ansehen in der Belegschaft wiegen oft weitaus schwerer. Wenn Kunden das Vertrauen in die Produkte verloren haben und Mitarbeiter abwandern, ist der wirtschaftliche Erfolg gefährdet, weil er oftmals vom guten Image und der Verfügbarkeit qualifizierter Mitarbeiter abhängig ist. Diese negativen Veränderungen können sich für ein Unternehmen als weitaus schwerwiegender erweisen.

Nach den immateriellen Schäden befragt, wurde am häufigsten der eigentliche Informationsabfluss (53,8 Prozent aller Nennungen) als Problem genannt. Das entsprechende Know-how war teilweise im Unternehmen ganz abhanden gekommen bzw. musste es mit der Konkurrenz geteilt werden. Weitere 28,1 Prozent nannten die Mitarbeiterabwanderung und 15,4 Prozent den entstandenen Imageschaden als negative Folge nach einem Spionagevorfall.

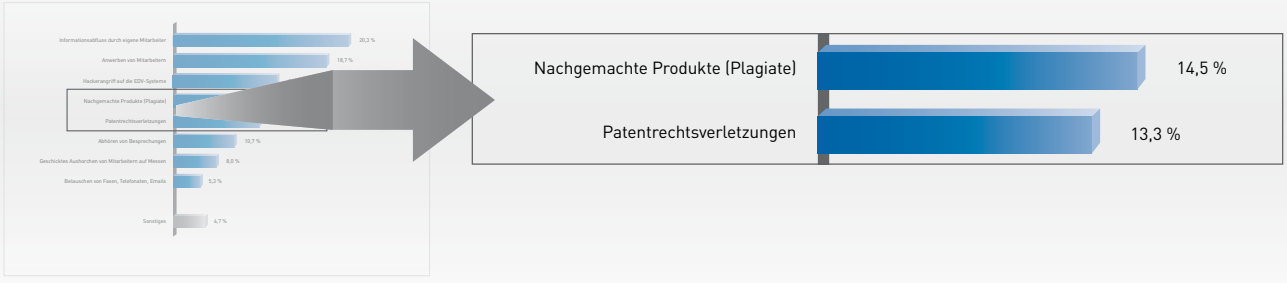
Eine weitere negative Folge von Informationsabfluss sind die daraus entstehenden Nachahmerprodukte. Plagiate sind ein großer Schaden für die deutsche Wirtschaft und es ist anscheinend immer noch sehr einfach, geschütztes Know-how zu kopieren. Nachgemachte Produkte mit 14,5 Prozent (Auszug Grafik 7) und Patentrechtsverletzungen mit 13,3 Prozent (Auszug Grafik 7) stellen einen erwartungsgemäß hohen Anteil an der Schadensstatistik dar. Zusammen machen sie fast ein Drittel aller Folgen im Zusammenhang mit Spionage aus.

Schäden im Unternehmen:



GRAFIK 12 Quelle: Corporate Trust 2007

Auswirkungen von Informationsabfluss:



AUSZUG GRAFIK 7 Quelle: Corporate Trust 2007

„Ein falscher Freund kann mehr Schaden verursachen als ein wahrer Feind.“

Werner Braun,
(1951 - 2006), deutscher Aphoristiker.

Spionage in der deutschen Wirtschaft

Die Täter

In einem Viertel der Spionagefälle waren eigene Mitarbeiter die Täter.

In Zeiten steigender Angst vor einem Arbeitsplatzverlust, permanent wachsender Arbeitsbelastung und oftmals mangelnder Wertschätzung der Arbeitsleistung, sind viele Mitarbeiter immer öfter bereit, sich am eigenen Unternehmen zu bereichern. Loyalität gegenüber dem Arbeitgeber ist heute längst nicht mehr selbstverständlich. Da werden Einbußen beim Lohn schon mal durch einen kleinen Nebenverdienst ausgeglichen.

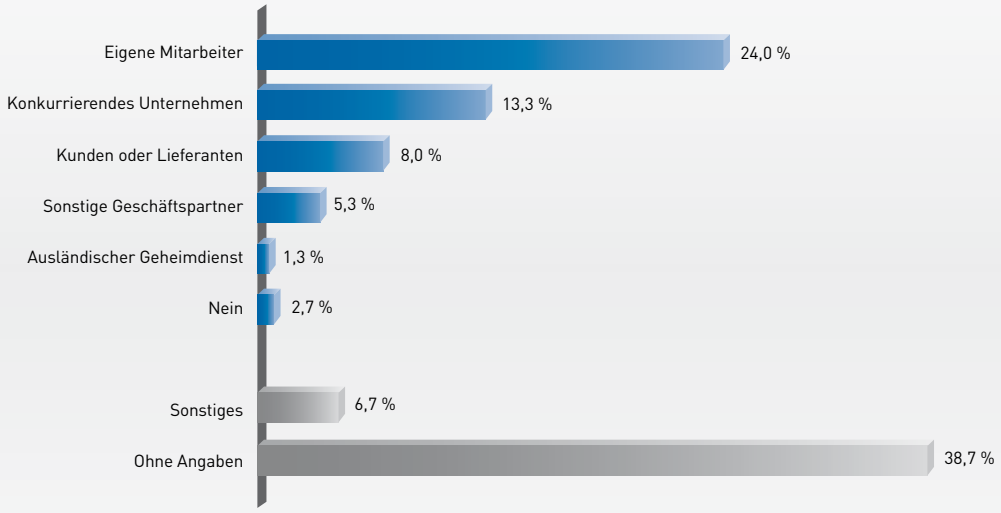
Aufgrund der modernen Kommunikationsmittel ist es meist einfach, unbemerkt sensible Daten aus dem Unternehmen an einen gut zahlenden Empfänger zu transferieren. Viele Mitarbeiter können hier nicht widerstehen und gehen auf unseriöse Angebote der Konkurrenz ein oder sorgen schon mal für die Zukunft vor. Sie decken sich mit zugänglichen Informationen aus dem eigenen Unternehmen ein.

Mit diesem Firmen-Know-how hat man bei einem Arbeitsplatzverlust oftmals die Eintrittskarte für den Wiedereinstieg bei der Konkurrenz in der Tasche.

Die eigenen Mitarbeiter waren in 24 Prozent aller Fälle verantwortlich für den Informationsabfluss im Unternehmen. Sie stellen damit die größte Tätergruppe bei der Spionage dar. Auch von der Konkurrenz geht eine nicht zu unterschätzende Gefahr aus. Sie wurde in 13,3 Prozent der Fälle als Verursacher des Spionageangriffs identifiziert. In der Häufigkeit nur noch auf Rang 3 waren Kunden oder Lieferanten mit 8 Prozent Anteil bei den Tätern.

Bei 6,7 Prozent der Fälle konnten die geschädigten Unternehmen keine Hinweise auf die Täter geben und bei 38,7 Prozent machten die Unternehmen gar keine Angaben zu den Tätern.

Gab es Hinweise auf die Täter?



GRAFIK 13 Quelle: Corporate Trust 2007

DIE TÄTER

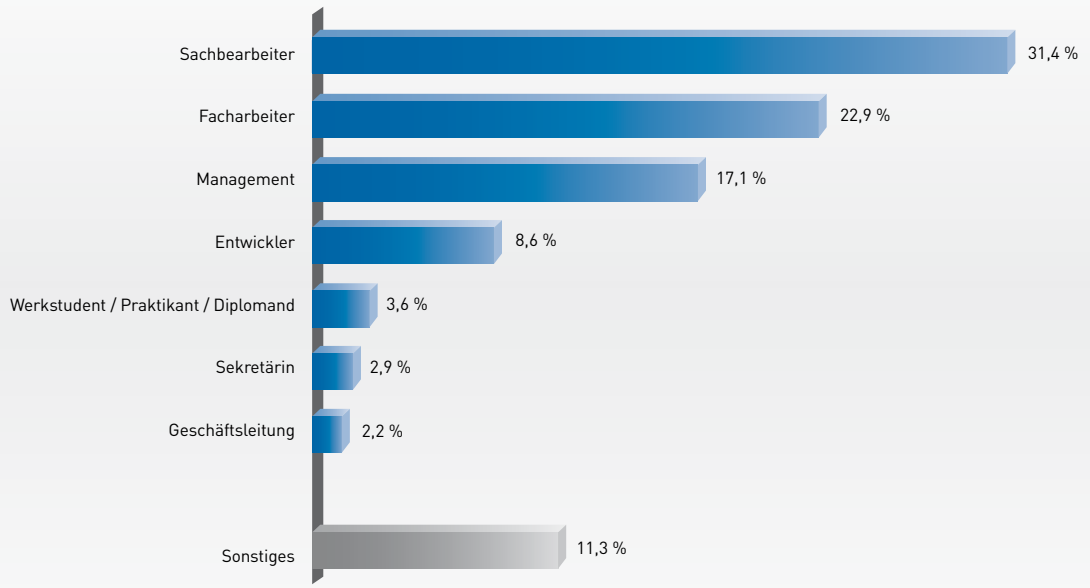
Sachbearbeiter sind am anfälligsten für Spionage, gefolgt von den Facharbeitern und dem Managment.

Die Unternehmen wurden im Zuge der Studie befragt, welche Mitarbeiter konkret für die Spionage verantwortlich waren. Die häufigsten Täter waren Sachbearbeiter mit 31,4 Prozent, gefolgt von den Facharbeitern mit 22,9 Prozent und dem Management mit 17,1 Prozent. Diese drei Bereiche verursachen damit zusammen über zwei Drittel aller Schäden für die Unternehmen.

Die Sachbearbeiter scheinen am häufigsten gegenüber ihrem Unternehmen illoyal zu werden. Sie haben in der Regel viele Zugriffsberechtigungen [15] und kommen damit auch an sensibelste Unterlagen und Informationen.

Verwunderlich ist, dass das Management als zweite Führungsebene ebenfalls sehr anfällig für Spionage ist. Im Gegensatz zur ersten Führungsebene, der Geschäftsleitung, die mit 2,2 Prozent nur sehr selten an den kriminellen Handlungen beteiligt war, kommt das Management damit deutlich häufiger in Versuchung, sich auf Kosten ihres Arbeitgebers zu bereichern, indem sie Informationen verkaufen.

Bitte konkretisieren Sie die beteiligten eigenen Mitarbeiter:

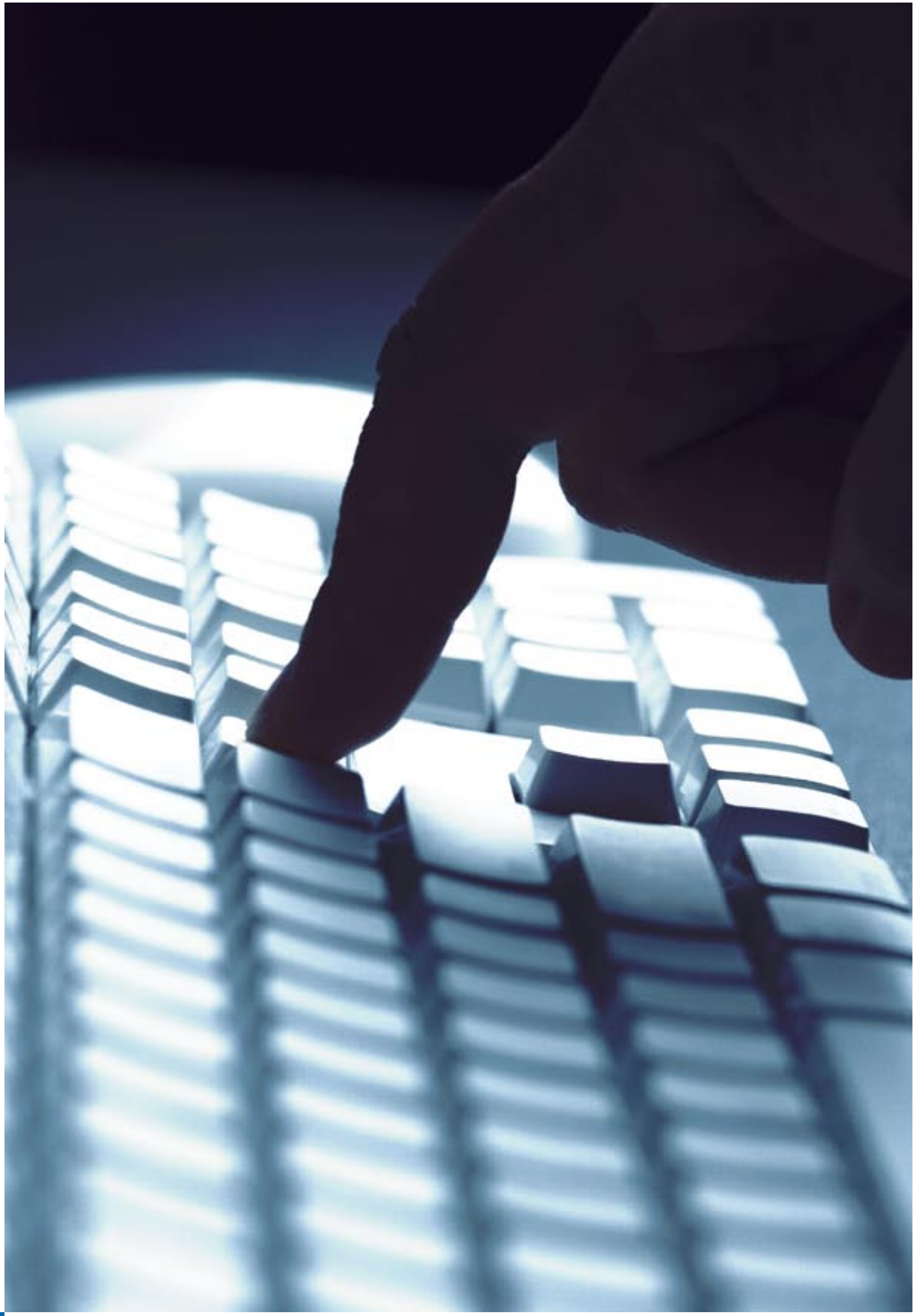


GRAFIK 14 Quelle: Corporate Trust 2007

15)Zugriffsberechtigung Festgelegter Bereich innerhalb der EDV-Systeme, auf die einzelne Personen zugreifen können.

„Ein Spion am rechten Ort ersetzt 20.000 Mann an der Front. “

Napoleon I. Bonaparte,
(1769 - 1821), französischer Feldherr und Politiker,
Kaiser der Franzosen von 1804 - 1814/15



Spionage in der deutschen Wirtschaft

Aufklärung der Vorfälle

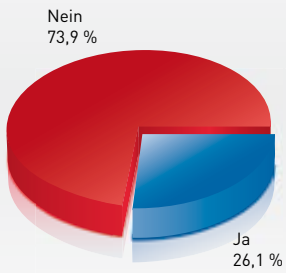
Nur in den wenigsten Fällen wurden die Behörden oder externe Spezialisten zur Aufklärung hinzugezogen.

Spionage ist für die meisten Firmen ein schwieriges Thema. Zum einen hat man nur selten damit zu tun, zum anderen gibt es vermutlich keine Spezialisten dafür im eigenen Unternehmen. Für die Betroffenen stellen sich deshalb einige wesentliche Fragen. Wie soll man agieren, wenn ein Vorfall bekannt wird? Hat man die nötigen Sicherheitsstrukturen, um den Vorfall professionell aufzuklären? Welcher Schaden wurde bereits angerichtet und welchen größeren Schaden kann man vielleicht noch verhindern? Wer soll informiert bzw. in die Aufklärung mit involviert werden?

Keine leichte Aufgabe, wenn man bedenkt, dass im Fall von Informationsabfluss sofortiges Handeln erforderlich ist, um möglichst schnell alle Beweise zu sichern.

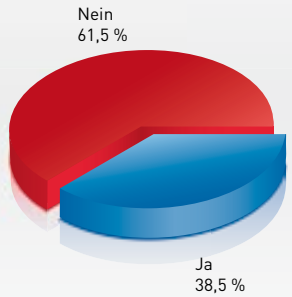
Trotzdem holen sich nur wenige Unternehmen Hilfe von Experten. So wurden nur in 26,1 Prozent der Fälle die Behörden hinzugezogen und nur in 38,5 Prozent externe Spezialisten. Den externen Spezialisten wurde damit Vorrang gegeben. Dies zeigt, dass die Unternehmen erst einmal versuchen, mit nichtstaatlichen Spezialisten unter eigener Regie Aufklärung zu betreiben. Sie befürchten, dass ihr Fall in der Öffentlichkeit bekannt werden könnte, sobald die Behörden eingeschaltet werden. Dies kann zu einem Reputationsschaden führen.

Wurden die Ermittlungsbehörden eingeschaltet?



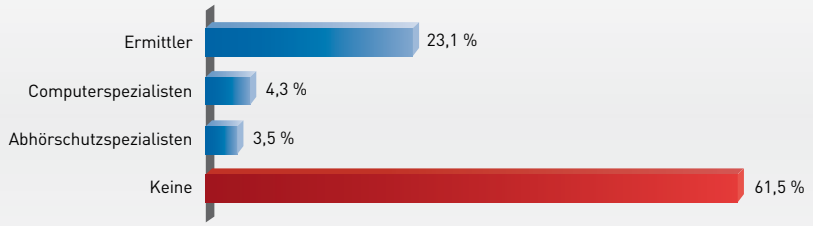
GRAFIK 15 Quelle: Corporate Trust 2007

Wurden externe Sicherheitsspezialisten eingeschaltet?



GRAFIK 16 Quelle: Corporate Trust 2007

Welche externen Sicherheitsspezialisten wurden eingeschaltet?



GRAFIK 17 Quelle: Corporate Trust 2007

Bei den Unternehmen, die externe Hilfe zu Rate zogen, wurden vor allem externe Ermittler beauftragt. Sie sollten in 23,1 Prozent der Fälle die Spionagevorfälle aufklären. Obwohl auch bei der technischen Wanzenabsuche [16] oder der Sicherung von IT-Datenprotokollen die Unternehmen häufig auf die Mithilfe von Spezialisten angewiesen wären, wurden diese nur in 4,3 Prozent (Computerspezialisten) bzw. 3,5 Prozent (Abhörschutzspezialisten für die Wanzenabsuche) eingeschaltet.

16)Wanzen Technische, meist miniaturisierte, Bauteile bzw. Funksender zum Abhören von Gesprächen oder Aufzeichnen von Informationen.


LCP 2.2
SERVER 2.1
LCP 2.1

Spionage in der deutschen Wirtschaft

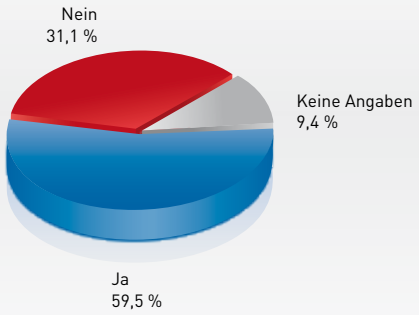
Vorkehrungen gegen Informationsabfluss

Die meisten Unternehmen gehen mit dem Thema Schutz gegen Spionage zu leichtfertig um.

Ohne ein gewisses Maß an Sicherheitsvorkehrungen kann heute kein Unternehmen auskommen. Zumindest ein ordentliches Verschlußsystem für Türen und Fenster, eine Alarmanlage oder eine Firewall für die IT-Systeme gehören zum Standard. Doch wie sieht es mit dem Schutz gegen Spionage aus? Hier werden nicht nur gewitzte Konkurrenten tätig und machen sich neue technische Möglichkeiten zur illegalen Informationsbeschaffung zunutze, sondern auch ausländische Geheimdienste setzen ihr gesamtes technisches Know-how ein, um an die gewünschten Informationen zu kommen.

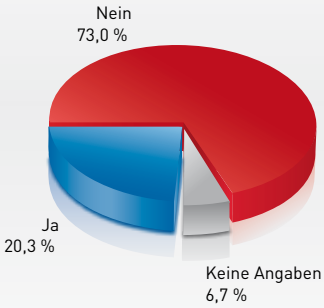
Auf die Frage, ob die präventiven Vorkehrungen in ihrem eigenen Unternehmen ausreichend seien, um sich dagegen zu schützen, antworteten 59,5 Prozent der Unternehmen mit Ja. Verwunderlich ist aber, dass nur 20,3 Prozent der Unternehmen angaben, auch über eine dementsprechende Sicherheitsorganisation zu verfügen, die diesen Schutz bewerkstelligen sollte. Zumindest gaben 41,3 Prozent an, dass es einen Sicherheitsverantwortlichen im Unternehmen gäbe.

Sind aus Ihrer Sicht die präventiven Vorkehrungen im Unternehmen ausreichend, um sich wirkungsvoll gegen Spionage zu schützen?



GRAFIK 18 Quelle: Corporate Trust 2007

Gibt es in Ihrem Unternehmen eine Sicherheitsorganisation, die sie professionell gegen Industriespionage schützen kann?



GRAFIK 19 Quelle: Corporate Trust 2007

VORKEHRUNGEN GEGEN INFORMATIONSABFLUSS

Der Abhörschutz wird in der Regel vernachlässigt.

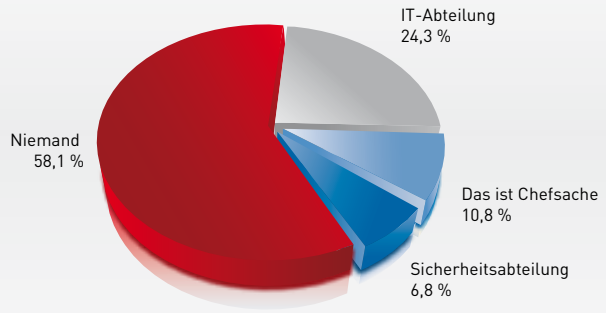
Gerade der Abhörschutz nimmt eine zentrale Bedeutung beim Schutz gegen Spionage ein. Dazu gehört nicht nur die Frage, ob es abhörsichere Besprechungsräume oder Telefonleitungen geben soll, sondern auch die Prozessdefinition, wann und an wen Emails offen bzw. verschlüsselt übersandt werden dürfen.

Ein wichtiger Punkt ist in dem Zusammenhang auch, dass Mitarbeiter unterwiesen werden sollten, welche Gefahren ihnen im Ausland drohen. Es sollte klare Anweisungen dazu geben, auf welche Weise im Ausland sicher mit dem Unternehmen kommuniziert werden kann, ohne dass Dritte diese Informationen mithören können.

Leider wird dieses Thema allzu oft verdrängt. Bei 58,1 Prozent aller Unternehmen gibt es niemanden, der sich mit dem Abhörschutz auseinandersetzt, bei 24,3 Prozent ist es immerhin noch die IT-Abteilung und nur in 6,8 Prozent ist die Sicherheitsabteilung dafür verantwortlich. Bei den befragten Unternehmen gab nur jedes zehnte Unternehmen an, dass sich der Chef persönlich um die zentralen Belange des Abhörschutzes kümmert.

Die Unternehmen wurden im Anschluß nach den Sicherheitsvorkehrungen in den einzelnen Segmenten befragt, um genauere Informationen über die getroffenen Maßnahmen und die tatsächliche Sicherheit zu erlangen. Dabei wurden neben dem bereits erwähnten Segment Sicherheitsorganisation auch die Segmente Objektsicherheit, IT, Personal und Organisation / Prozesse erfragt.

Wer kümmert sich im Unternehmen um die zentralen Belange des Abhörschutzes?



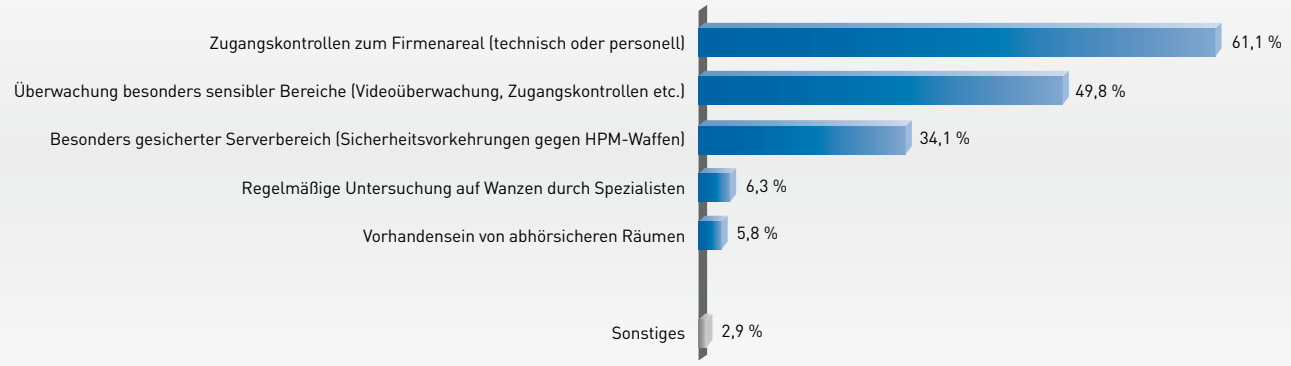
GRAFIK 20 Quelle: Corporate Trust 2007

Objektsicherheit wird häufig durch Zugangskontrollen abgebildet – abhörsichere Räume dagegen fehlen.

Nur jedes zwanzigste Unternehmen verfügt über die Möglichkeit, vertrauliche Besprechungen in einem abhörgeschützen Raum [17] durchzuführen. Wichtige Informationen können so jederzeit an die Konkurrenz oder einen fremden Geheimdienst gelangen. Das technische Equipment zum Abhören von Besprechungen befindet sich heute in vielerlei Händen. Die meisten Unternehmen in Deutschland verwenden zum Schutz ihres sensiblen Know-hows Standard-Sicherheitssysteme wie Zugangskontrollen zum Firmenareal (61,1 Prozent der Befragten) oder die Überwachung von besonders sensiblen Bereichen durch Videoüberwachungsanlagen oder separate Zugangskontrollsysteme (49,8 Prozent).

Gerade der Serverbereich stellt ein Herzstück der Lagerung von Firmen-Know-how dar. Hier sollte ein besonderes Maß an Sicherheit herrschen. Immerhin 34,1 Prozent der Unternehmen gaben an, besondere Vorkehrungen gegen Angriffe mit sogenannten HPM-Waffen getroffen zu haben. HPM steht für High-Power-Microwaves. Die Angriffe mit solchen Waffen sollen durch die Aussendung eines hochfrequenten Impulses die elektronischen Bauteile von Geräten in einem Unternehmen beschädigen. Organische Lebewesen werden dadurch in der Regel nicht in Mitleidenschaft gezogen. Deshalb wird ein solcher Angriff durch anwesende Personen nicht sofort bemerkt. Je nach Impulsstärke kann ein HPM-Angriff bis hin zum Totalausfall der Systeme führen.

Welche Sicherheitsvorkehrungen haben Sie im Bereich Objektsicherheit getroffen? (Mehrfachnennungen möglich)



GRAFIK 21 Quelle: Corporate Trust 2007

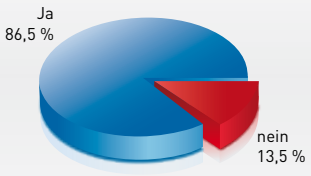
17)Abhörgeschützter Raum Architektonische Abschirmung eines Raumes durch technische Maßnahmen, um ungewollte Funkübertragungen zu verhindern.

VORKEHRUNGEN GEGEN INFORMATIONSABFLUSS

Die IT-Sicherheit als wesentlicher Baustein zum Schutz gegen Spionage.

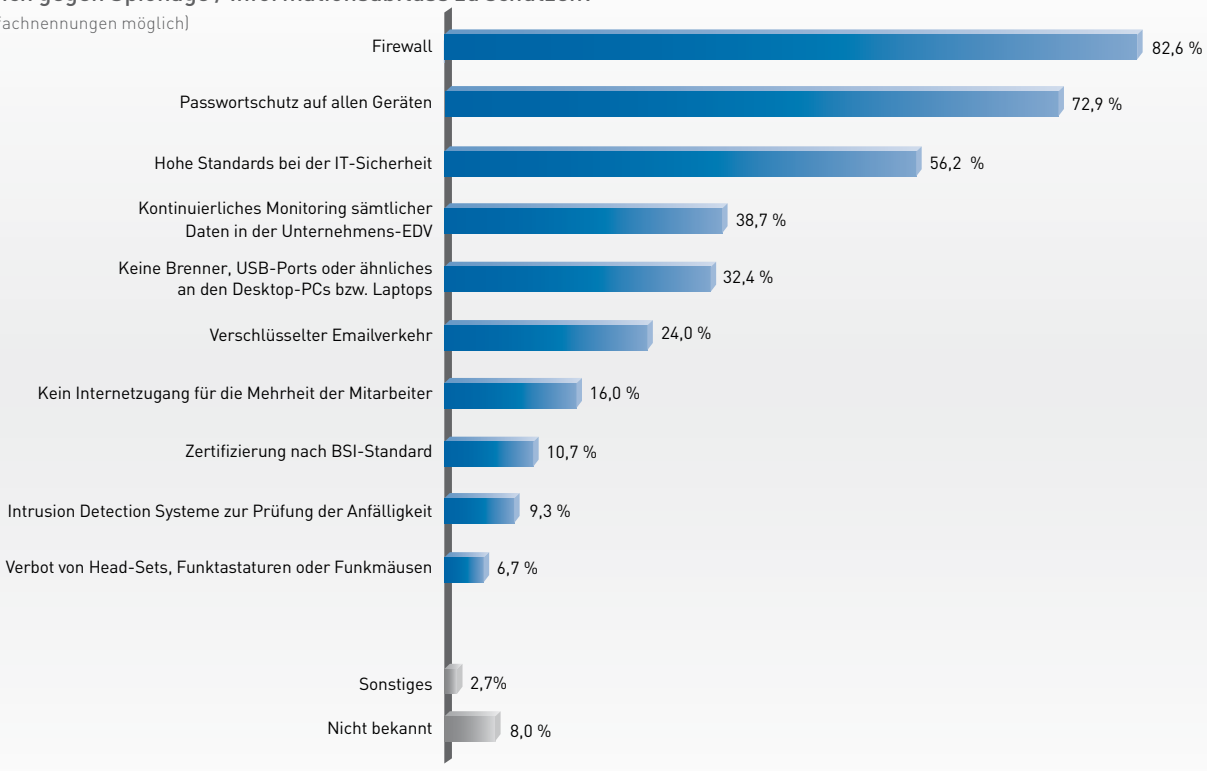
Die IT-Systeme bieten vielfältige Angriffsmöglichkeiten für Datendiebe. Dies ist den meisten Unternehmen bewusst. Daher haben sie auch vielfältige Vorkehrungen gegen fremde Zugriffe getroffen. In fast allen Unternehmen, genau 86,5 Prozent, gibt es einen IT-Verantwortlichen. Bei den einzelnen Sicherheitsvorkehrungen nimmt das Thema Firewall mit 82,6 Prozent eine herausragende Position ein. Das Thema Passwortschutz gehört immerhin für fast drei Viertel aller Unternehmen zum Standard. Dies bedeutet aber auch, dass 27,1 Prozent keinen Passwortschutz auf allen IT-Peripheriegeräten haben. Auch der verschlüsselte Emailverkehr gehört nur bei etwa einem Viertel aller Unternehmen zum Standard. Dies bedeutet, dass sensible Informationen bei drei Viertel aller Unternehmen ungeschützt übermittelt werden.

Gibt es in Ihrem Unternehmen einen IT-Verantwortlichen als zentralen Ansprechpartner?



GRAFIK 22 Quelle: Corporate Trust 2007

Welche Sicherheitsvorkehrungen haben Sie im IT-Bereich getroffen, um sich gegen Spionage / Informationsabfluss zu schützen?
(Mehrfachnennungen möglich)



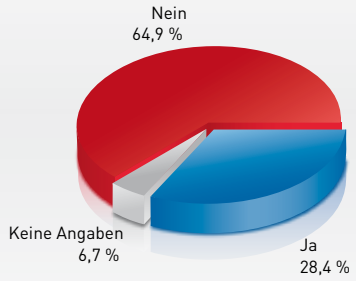
GRAFIK 23 Quelle: Corporate Trust 2007

Mitarbeiter sind ungenügend auf „Social Engineering“ vorbereitet.

64,9 Prozent aller Unternehmen bereiten Ihre Mitarbeiter nicht auf die Gefahren durch sogenanntes Social Enginering [18] vor. Die Methode des Social Engineering ist es, gezielt mit Mitarbeitern auf Messen, am Abend in den Messehotels oder bei sonstigen Veranstaltungen ins Gespräch zu kommen. Immerhin bei 8 Prozent aller geschädigten Unternehmen kam es durch Social Engineering auf einer Messe zu einem Informationsabfluss (siehe Grafik 7).

Durch unauffällige Anbahnungsgespräche und geschickte Fragestellungen wird versucht, aus den Mitarbeitern geheime Informationen oder sensible Details heraus zu locken. Viele Mitarbeiter, gerade wenn sie auf Messen nur bestimmten Kunden ihre Fachkenntnisse präsentieren sollen, werden arglose Opfer eines solchen Angriffs. Sie rechnen nicht damit, dass ihr Gegenüber sie bewußt ausgewählt hat und das nette Gespräch nur einen einzigen Zweck verfolgt – Erkenntnisse über vertrauliches Firmen-Know-how.

Werden Ihre Mitarbeiter vor dem Besuch von Messen oder sonstigen Veranstaltungen auf die Gefahr durch sogenanntes Social Engineering[18] vorbereitet?



GRAFIK 24 Quelle: Corporate Trust 2007

18)Social Engineering Ausspionieren über das persönliche Umfeld, durch zwischenmenschliche Beeinflussungen und meist durch geschickte Fragestellungen. Social Engeneering hat das Ziel, unberechtigt an Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen.

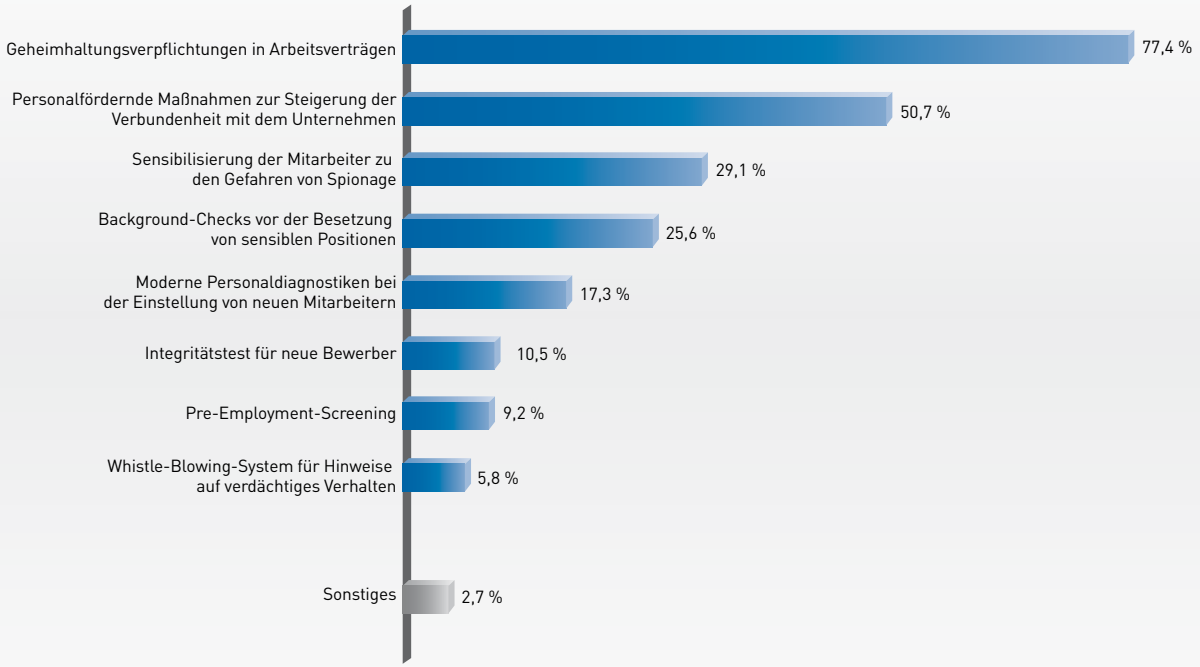
VORKEHRUNGEN GEGEN INFORMATIONSABFLUSS

Gerade im Bereich Personal werden die präventiven Möglichkeiten nur unzureichend ausgeschöpft.

Die Geheimhaltungsverpflichtungen in den Arbeitsverträgen gehören bei 77,4 Prozent aller Unternehmen zum Sicherheitsstandard. Leider überprüfen aber nur gut ein Viertel aller Unternehmen ihre Mitarbeiter mit einem Background-Check [19] auf verdächtige Hinweise, bevor sie diese an sensiblen Positionen einsetzen. Integritätstests für neue Bewerber lässt gar nur jedes zehnte Unternehmen durchführen.

Mitarbeiter sind das wertvollste Kapital eines Unternehmens. Sie stellen aber auch eine große Gefahr dar, wenn es um den Abfluss von Firmen-Know-how geht. Gerade deshalb sollte jedes Unternehmen bemüht sein, eine möglichst hohe Verbundenheit der Mitarbeiter mit dem Unternehmen zu erreichen. Dies kann zum Beispiel durch personalfördernde Maßnahmen geschehen. Bei der Befragung gab nur die Hälfte aller Unternehmen an, davon Gebrauch zu machen.

Welche Sicherheitsvorkehrungen haben Sie im Bereich Personal getroffen?
(Mehrfachnennungen möglich)



GRAFIK 25 Quelle: Corporate Trust 2007

19) **Background-Check** Überprüfung von Mitarbeitern bezüglich ihren früheren Arbeitgeber, finanziellen Verhältnisse, Firmenbeteiligungen bzw. verdächtigen Lebensumstände.

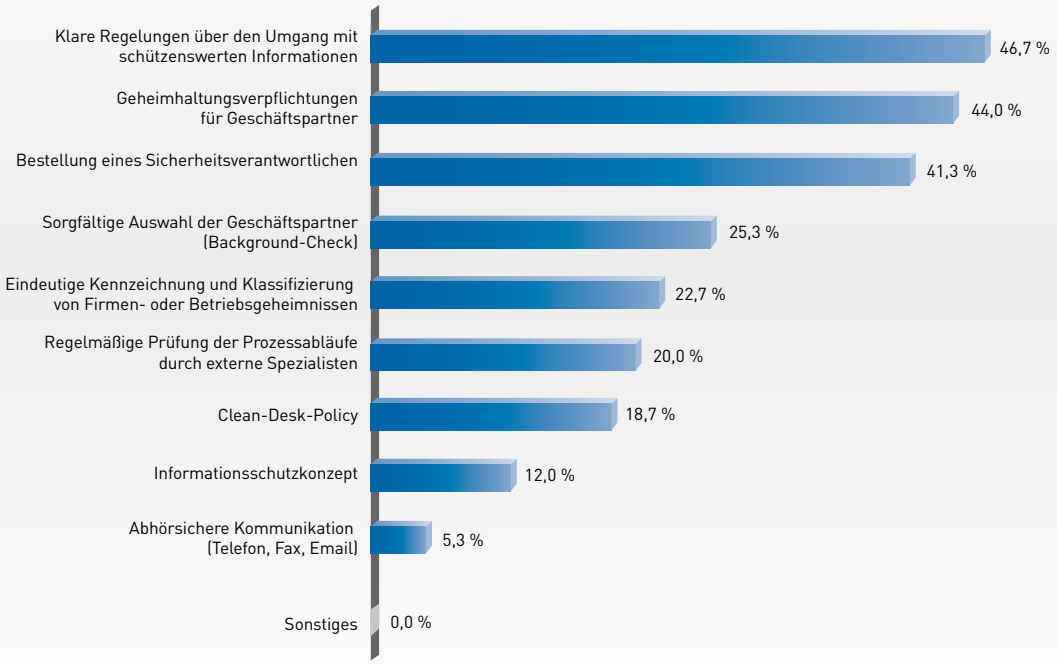
Sichere Prozesse sind ein wichtiger Baustein für den Schutz des Firmen-Know-hows.

IT-Systeme können noch so sicher sein, wenn die Prozesse, die dahinter stehen, nicht nach Sicherheitsgesichtspunkten strukturiert sind, nützen sie nichts. Wenn eine Tür das beste Sicherheitsschloss hat, nützt es doch nichts, wenn jemand diese Tür offen stehen lässt. Daher ist es wichtig, dass es sicherheitsrelevante Prozesse zum Schutz von Informationen im Unternehmen gibt.

Nicht einmal die Hälfte aller befragten Unternehmen hatte klare Regelungen für den Umgang mit schützenswerten Informationen getroffen. Trotzdem stellt dies die am häufigsten durchgeführte Maßnahme für den Schutz gegen Spionage dar. Wenigstens 44,0 Prozent vereinbaren Geheihaltungsverpflichtungen [20] mit Geschäftspartnern und 41,3 Prozent hatten einen Sicherheitsverantwortlichen im Unternehmen.

In diesem Zusammenhang fiel auf, dass nur etwa jedes fünfte Unternehmen ihre Mitarbeiter durch eine Clean-Desk-Policy [21] verpflichtet, keine offen zugänglichen Unterlagen auf den Schreibtischen oder Ablagen liegen zu lassen, wenn sie bei Arbeitsende ihren Arbeitsplatz verlassen. Ein Informationsschutzkonzept, zur Analyse der tatsächlichen Gefahren für das Unternehmen und strikter Vorgaben für den Umgang mit sensiblen Informationen, hatten gar nur 12,0 Prozent erstellt.

Welche prozesstechnischen Vorkehrungen haben Sie getroffen, um sich gegen Industriespionage zu schützen? (Mehrfachnennungen möglich)



GRAFIK 26 Quelle: Corporate Trust 2007

20)Geheimhaltungsverpflichtung Schriftliche Vereinbarung über den Umgang mit vertraulichen Informationen.

21)Clean-Desk-Policy Schriftliche Vereinbarung mit den Mitarbeitern, dass nach Arbeitsende keine schriftlichen Unterlagen offen zugänglich auf den Schreibtischen liegen gelassen werden dürfen.

SPIONAGE IN DER DEUTSCHEN WIRTSCHAFT

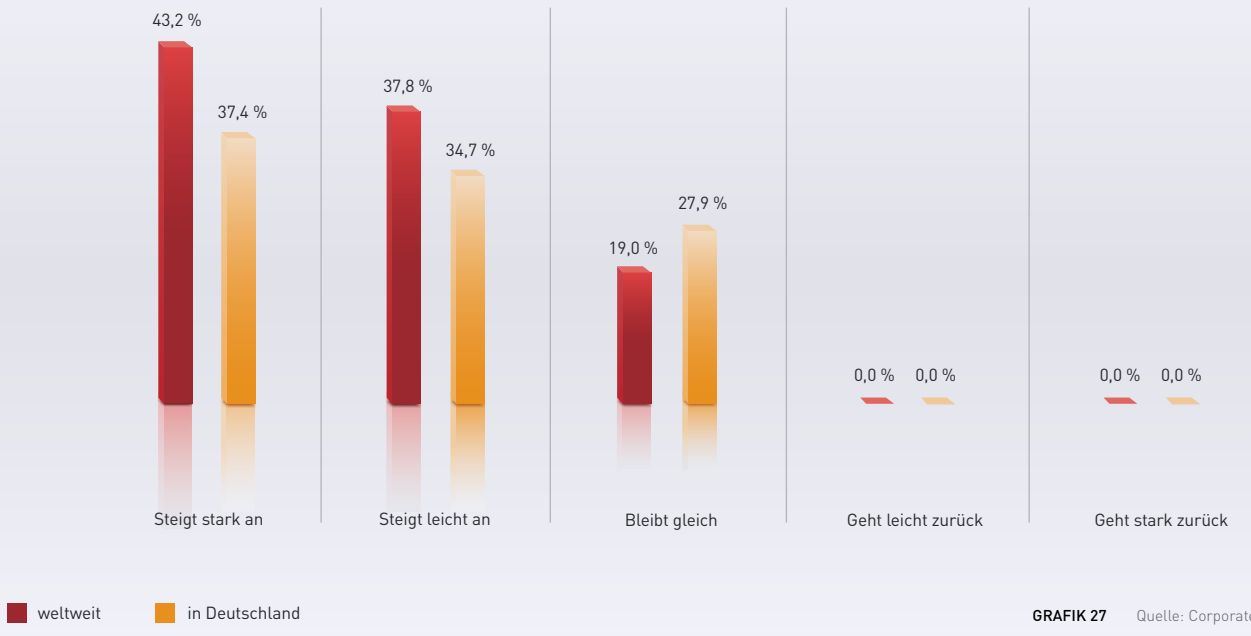
EINSCHÄTZUNG DER RISIKEN

Das Risiko von Industriespionage wird unterschätzt.

Kein einziges befragtes Unternehmen glaubte, dass die Bedrohung durch Industriespionage sinken würde. Obwohl über 80 Prozent aller befragten Unternehmen davon ausgingen, dass Industriespionage in den nächsten Jahren sowohl in Deutschland als auch weltweit ansteigen wird, glauben nur 33,7 Prozent, dass die Bedrohung auch für ihr eigenes Unternehmen steigt. Dies zeigt, dass die Risikoeinschätzung für das eigene Unternehmen deutlich positiver eingestuft wird als die allgemeine Gefahreneinschätzung.

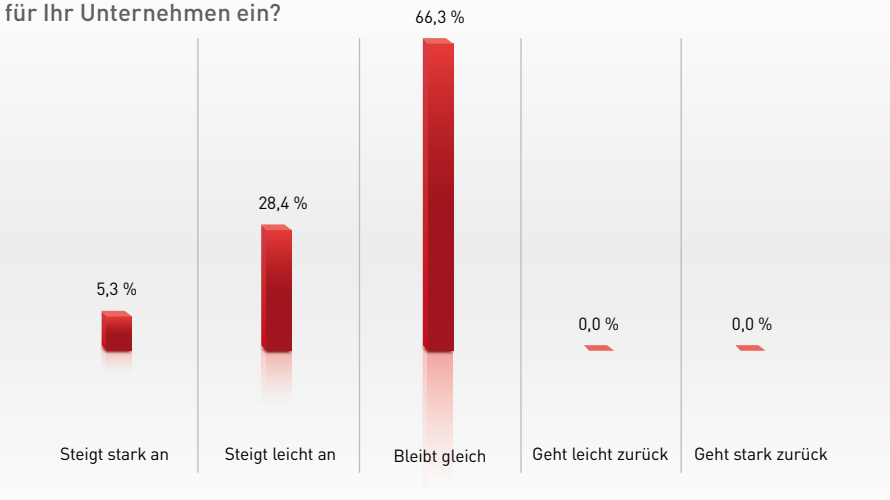
Es zeigt jedoch auch, dass es vermutlich ein trügerischer Schluß ist und das Risiko von Industriespionage unterschätzt wird.

Wie ist Ihre Einschätzung für die künftige weltweite und deutschlandweite Entwicklung von Industriespionage?



GRAFIK 27 Quelle: Corporate Trust 2007

Wie schätzen Sie die zukünftige Bedrohung durch Industriespionage für Ihr Unternehmen ein?



GRAFIK 28 Quelle: Corporate Trust 2007

Das Risiko für das eigene Unternehmen wird unterschätzt. Zwei Drittel aller Unternehmen glauben, dass sie in Zukunft nicht mehr gefährdet sein werden als bisher.

SCHLUSSFOLGERUNGEN / AUSBLICK

BEWERTUNG DER ERGEBNISSE

Die deutsche Wirtschaft ist durch Indutriespionage gefährdet.

Fast ein Fünftel aller Unternehmen (genau 18,9 Prozent) hatte in den letzten Jahren bereits einen Spionagefall in der eigenen Firma zu beklagen. Der Informationsabfluss durch eigene Mitarbeiter ist dabei die größte Gefahr. Exakt bei 20,3 Prozent aller Fälle handelt es sich um einen Verrat von Interna durch eigene Mitarbeiter. Rechnet man alle Spionagehandlungen zusammen, sind die Mitarbeiter mit 24,0 Prozent sogar die größte Tätergruppe.

Die Schäden für die deutsche Wirtschaft liegen nach den hier gewonnenen Erkenntnissen in Höhe von mindestens 2,8 Milliarden Euro. Dabei ist bei dieser Zahl nur das Hellfeld - wie die Experten Delikte nennen, die den Behörden bekannt geworden sind - berücksichtigt. Die meisten Fälle werden in den Unternehmen vermutlich gar nicht erkannt.

Obwohl nur selten Vorfälle in der Öffentlichkeit bekannt werden, ist Know-How-Abfluss durch Spionage ein aktuelles Problem für die deutsche Wirtschaft, mit einem Schaden in Milliardenhöhe.

SCHLUSSFOLGERUNGEN / AUSBLICK

AUSBLICK

Vor allem die Prävention gegen Innentäter sollte verbessert werden.

Berücksichtigt man die Einschätzung der Unternehmen für die zukünftige Entwicklung des Risikos für Spionage, so stellt man fest, dass es für das eigene Unternehmen meist unterschätzt wird. Es werden daher vermutlich weiterhin zu wenige Präventionsmaßnahmen ergriffen.

Viele Unternehmen sehen den Schutz vor Industriespionage / Informationsabfluss nur als Schutz gegen Angriffe von außen. Die Täter sitzen jedoch sehr häufig im eigenen Unternehmen. Versucht man das Handeln zu erklären, warum eigene Mitarbeiter kriminell werden und Informationen verkaufen, so gibt es zwei Theorien aus der amerikanischen Kriminologie:

1. Rational Choice
(Cornish & Clarke, 1985, USA)

Die Entscheidung eines Täters für oder gegen Kriminalität beruht auf einer Kosten-Nutzen-Analyse. Die Einflussgrößen sind damit der Nutzen, also erlangte Beute oder Anerkennung, sowie die Kosten, also das Entdeckungsrisiko, Gewissen oder z.B. Strafmaß.

Der potenzielle Täter ist eher zu einer Tat bereit, wenn der Nutzen aufgrund einer günstigen Gelegenheit höher eingeschätzt wird, als das Entdeckungsrisiko. Dieser Ansatz eignet sich z.B. zur Erklärung bei Delikten der Wirtschaftskriminalität oder bei Versicherungsbetrug.

Wenn sich einem Mitarbeiter eine günstige Gelegenheit bietet, sich am Arbeitgeber zu bereichern, wird er eher zum Täter, wenn die Wahrscheinlichkeit entdeckt zu werden, gering ist. Ungenügende präventive Vorkehrungen und Kontrollen begünstigen daher das kriminelle Verhalten von Mitarbeitern.

2. Routine Activity Approach
(Cohen & Felson, 1979, USA)

Das Risiko, Opfer einer Straftat zu werden, wird maßgeblich durch drei Faktoren bestimmt.

- Es gibt einen motivierten Täter, der zur Begehung einer Straftat bereit ist.
- Es handelt sich um ein Rechtsgut (eine Beute), welches für den Täter interessant ist bzw. bietet sich dem Täter eine günstige Gelegenheit.
- Für dieses Rechtsgut (Beute) gibt es keinen ausreichenden Schutz.

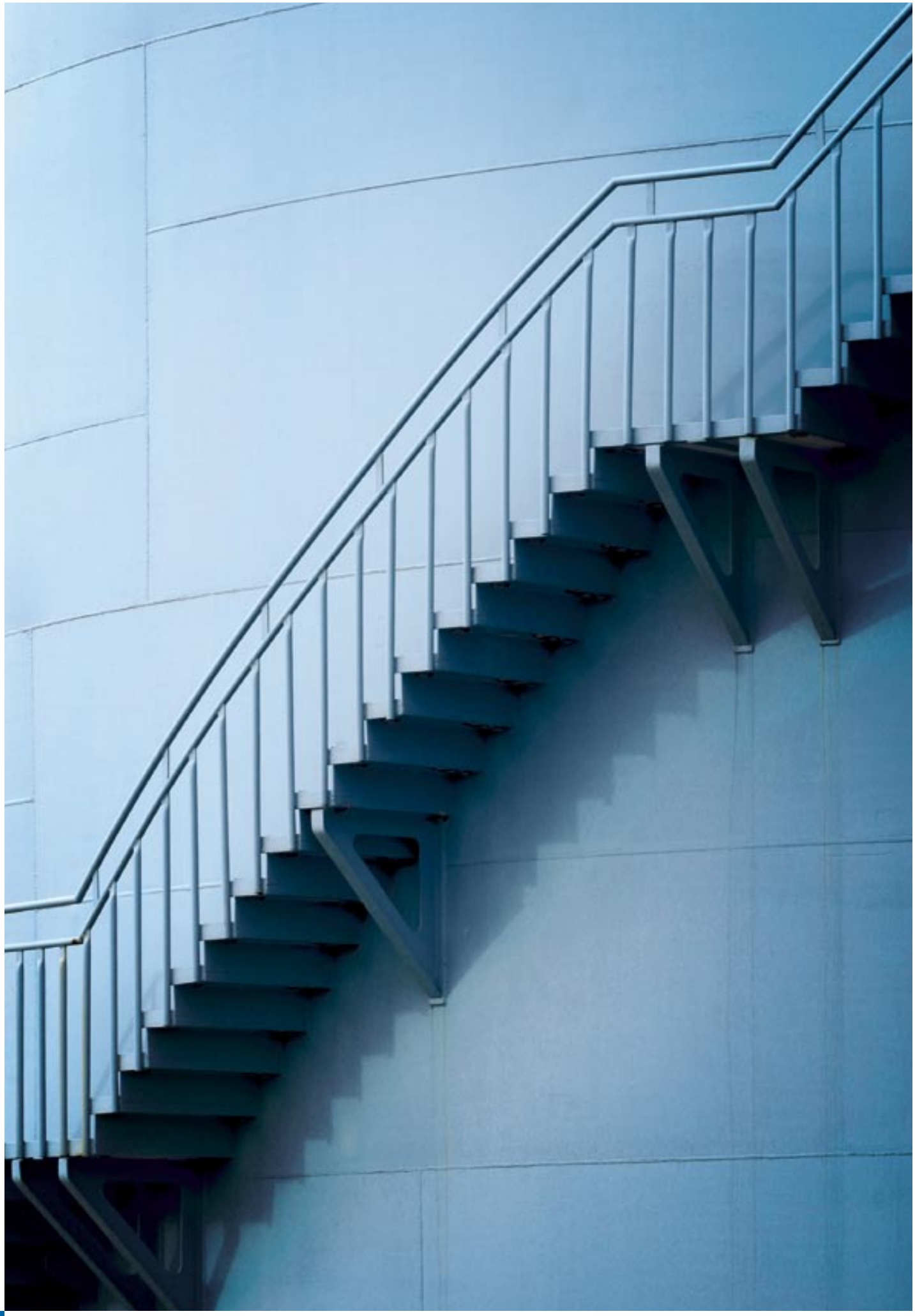
Der zu einem Diebstahl motivierte Täter ist eher in der Lage, die für ihn interessante Beute zu stehlen, wenn es keine Kontrollen gibt und Behältnisse nicht verschlossen sind.

Ein Mitarbeiter ist verärgert über sein Unternehmen oder erhält von der Konkurrenz ein finanzielles Angebot für Datenbeschaffung. Wenn das Angebot hoch genug ist und er unkontrollierten Vollzugriff auf alle IT-Systeme hat, kann er jederzeit Daten davon kopieren und weiter verkaufen, wenn niemand regelmäßig die Zugriffe kontrolliert.

Sieht man sich die Entwicklungen der Polizeilichen Kriminalstatistik (PKS) für die Bereiche Ausspähen von Daten und Wettbewerbsdelikte an, so stellt man fest, dass es hier deutliche Anstiege gab. Im Schnitt seit 2001 jährlich um 11,2 Prozent bei den Wettbewerbsdelikten und um 27,5 Prozent bei der Ausspähung von Daten. Dies lässt den Schluss zu, dass es auch weiterhin bei diesen Deliktsfeldern [22] einen Anstieg geben wird.

Wenn Unternehmen nicht ausreichend präventive Vorkehrungen gegen Industriespionage treffen, wird zunehmend Know-how abfließen. Bei ungenügender Kontrolle und unsicheren Prozessen werden zukünftig noch mehr Mitarbeiter für Schäden verantwortlich sein.

22)Deliktsfelder Kriminalistischer Ausdruck für verschiedene strafbare Handlungen innerhalb eines zusammengehörenden Bereiches.



Präventionsmassnahmen

Nicole Weyerstall
Leiterin Industriekunden
Financial Lines
AIG EUROPE S.A.

„Wir vermitteln und bezahlen nicht nur die notwendigen Berater um einen Spionagefall aufzudecken, sondern gewähren auf Wunsch auch Schadensersatz wenn die vertraulichen Informationen von Dritten verwendet werden."

Wirtschafts- oder Industriespionage stellt die Deutsche Wirtschaft vor neue Herausforderungen. Die Schäden durch den Abfluss von wichtigem Firmen Know-how können ein Unternehmen massiv bedrohen oder sogar in seiner Existenz gefährden. Die Forderungen nach Schutzmöglichkeiten richten sich daher seit langem auch an die Versicherungswirtschaft.

Bisher war der finanzielle Schaden aufgrund von Spionage nicht versicherbar. In der Vertrauensschadenversicherung, welche die klassischen Risiken von Wirtschaftskriminalität abdeckt, sind die typischen Spionageziele „Betriebs- und Geschäftsgeheimnisse" weitgehend ausgeschlossen.

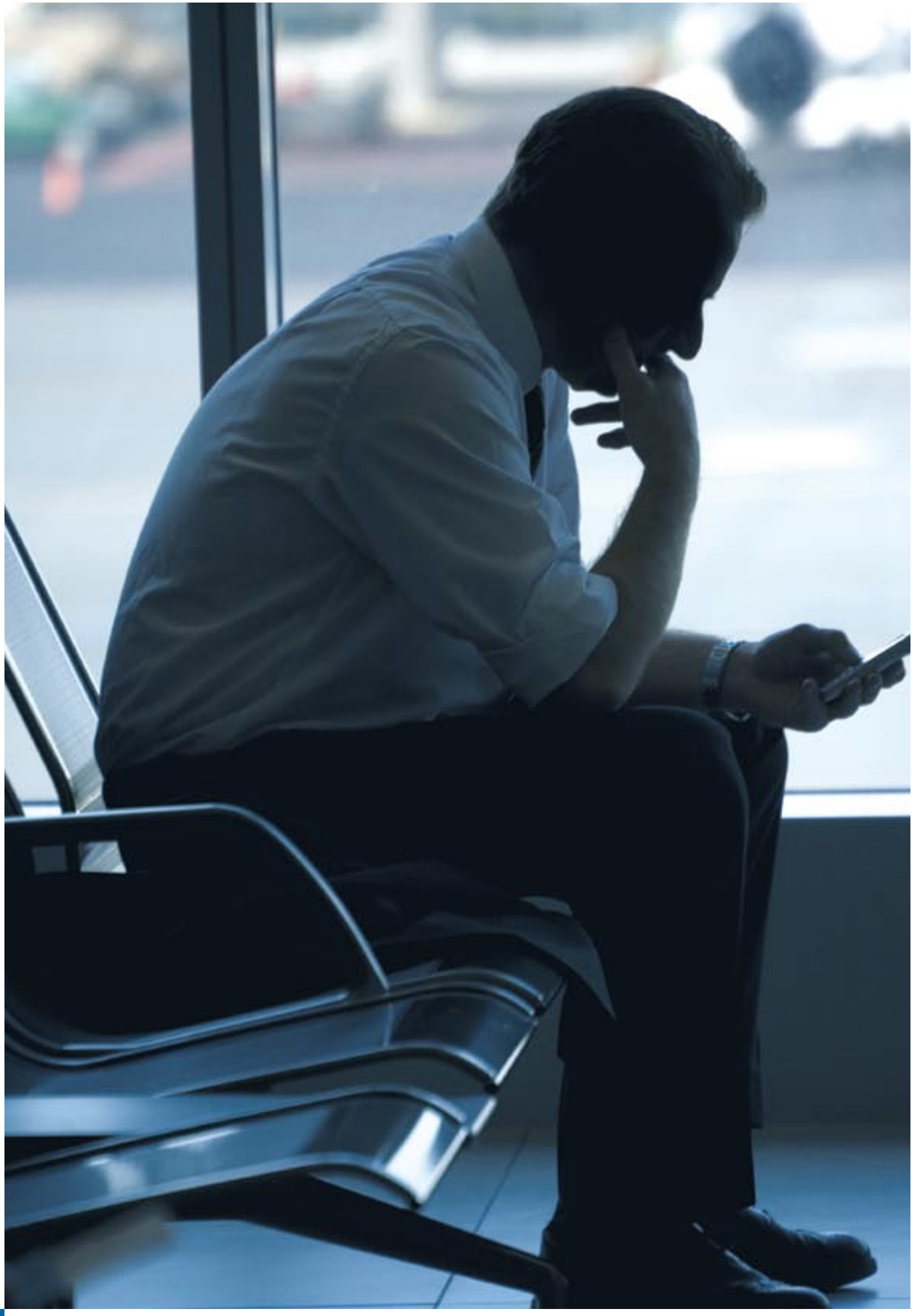
Um dem stetig steigenden Risiko für Unternehmen und deren Nachfrage nach adäquatem Versicherungsschutz zu entsprechen, hat die AIG Europe erstmalig ein Versicherungsprodukt entwickelt, das die Betriebs- und Geschäftsgeheimnisse unserer Versicherungsnehmer schützt. Wir vermitteln und bezahlen nicht nur die notwendigen Berater um einen Spionagefall aufzudecken, sondern gewähren auf Wunsch auch Schadensersatz wenn die vertraulichen Informationen von Dritten verwendet werden.

Die Leistungen aus der neuen Spionageversicherung beinhalten im Rahmen der Bedingungen z.B.

- Einen Tag Präventionsberatung durch Sicherheitsspezialisten
- Die Übernahmen der Kosten für die vollständige Ermittlung des Spionagefalles bereits bei einem begründeten Verdacht
- Ein umfängliches Rechtsgutachten mit einer Empfehlung für die Unternehmen
- Die Kosten eines PR Beraters zum Schutz der Reputation
- Den Ersatz einer fiktiven Lizenzgebühr
- Den Ersatz von Vermögensschäden aufgrund einer Betriebsunterbrechung
- Rechtskosten zur Abwehr von Spionagevorwürfen gegen das eigene Unternehmen

Mit den präventiven Leistungen in diesem Versicherungsprodukt möchten wir es den Unternehmen ermöglichen, ihre Betriebs- und Geschäftsgeheimnisse besser zu schützen. Sollten sie dennoch das Opfer von Industriespionage werden, bieten wir die notwendige Unterstützung für eine professionelle Ermittlung der Täter, die Rechtsberatung sowie den Schutz der Reputation und den Ersatz finanzieller Schäden.

Ihre
Nicole Weyerstall



PRÄVENTIONSMASSNAHMEN

GEPLANTE VORKEHRUNGEN DER UNTERNEHMEN

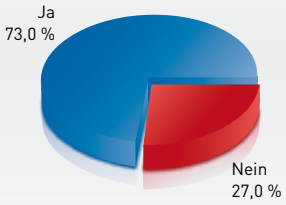
Verbindliche Richtlinien für sensible Mitarbeiter.

Jedes vierte Unternehmen gab an, dass es ausreichend Sicherheitsvorkehrungen gegen Spionage getroffen habe und daher keine weitere Prävention betreiben wolle. Dies stimmt zwar nachdenklich, bedeutet aber auch, dass 73 Prozent aller Unternehmen in Zukunft mehr in punkto Schutz gegen Informationsabfluss tun wollen.

Es gibt keine Musterlösungen bei der Prävention gegen Spionage bzw. Informationsabfluss. Die einzelnen Maßnahmen sollten auf das jeweilige Unternehmen, die individuelle Bedrohung sowie die unterschiedlichen wirtschaftlichen Anforderungen und Gegebenheiten angepasst werden. Es gibt jedoch einige Standard-Sicherheitsvorkehrungen, die von jedem Unternehmen eingehalten werden sollten um sich effektiv gegen den Zugriff auf das Firmen-Know-how zu schützen.

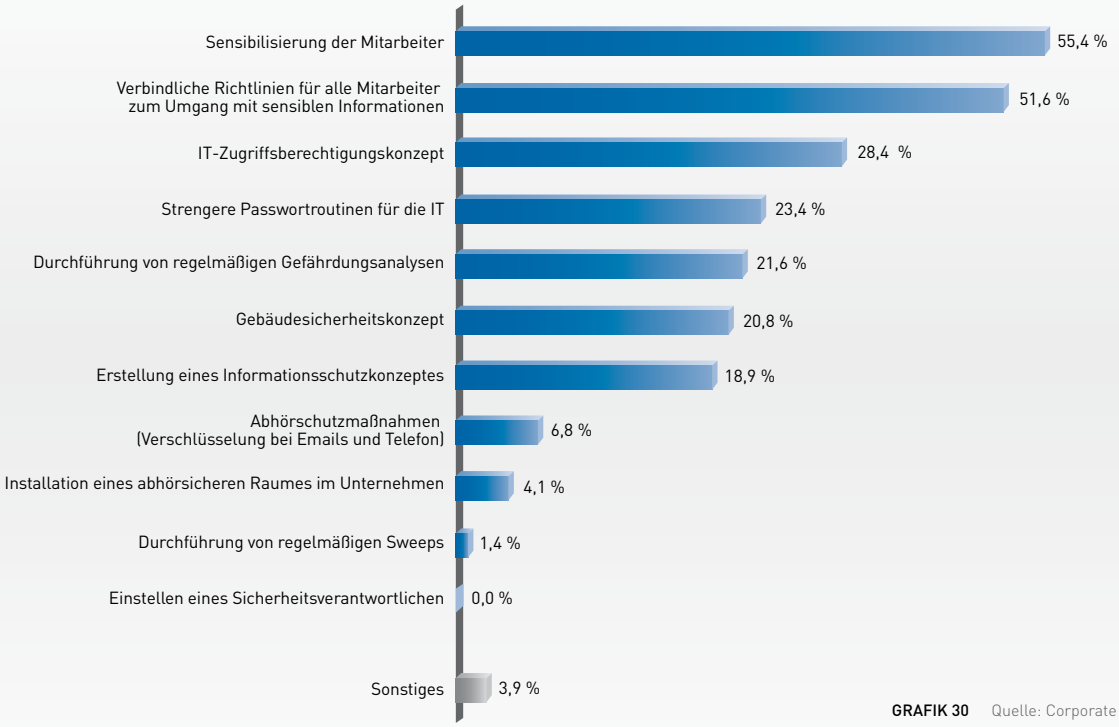
Die Unternehmen wurden nach Standard-Maßnahmen befragt. Sie gaben an, ihre Mitarbeiter in Zukunft mehr für dieses Thema sensibilisieren zu wollen. Darüber hinaus sollen ganz verbindliche Richtlinien für den Umgang mit sensiblen Informationen im Unternehmen erlassen werden. Nur jedes vierte Unternehmen will zukünftig auch auf die Einhaltung von strengeren Passwortroutinen achten.

Wird Ihr Unternehmen in Zukunft weitere Vorkehrungen gegen Industriespionage treffen?



GRAFIK 29 Quelle: Corporate Trust 2007

Welche Vorkehrungen wird Ihr Unternehmen in Zukunft treffen, um auf die Risiken durch Industriespionage vorbereitet zu sein? (Mehrfachnennungen möglich)



GRAFIK 30 Quelle: Corporate Trust 2007

Präventionsmassnahmen

Informationsschutzkonzept

Ganzheitlicher Ansatz für alle Unternemensbereiche.

Der alles entscheidende Schlüssel im Kampf gegen Industriespionage ist die Prävention. Hier gibt es effektive Maßnahmen, um Industriespionage zu vermeiden. Um eine existenzielle Gefährdung für die Wettbewerbsfähigkeit eines Unternehmens zu vermeiden, empfehlen wir einen ganzheitlichen Ansatz für alle Bereiche.

Bei einem Informationsschutzkonzept von Corporate Trust werden zuerst alle Unternehmensbereiche auf Schwachstellen analysiert. Dies erfolgt in den Bereichen

- Organisation
- Personal
- Prozesse
- Objektsicherheit
- Sicherheitskoordination
- IT

Die Identifikation der Risiken (Schwachstellenanalyse) erfolgt im Rahmen eines Audits durch die Feststellung der einzelnen Schwachstellen, Bewertung des jeweiligen Risikos für einen Informationsabfluss und einer Empfehlung für sichernde Maßnahmen.

Aus der Schwachstellenanalyse ergibt sich ein ganzheitliches Konzept für den Soll-Zustand „Schutz des Unternehmens Know-how". Die einzelnen Maßnahmen werden dann sukzessive im Unternehmen implementiert und so ein Informationsabfluss verhindert.

Technische Massnahmen

Lauschabwehr erfordert den Einsatz von Technik.

Die Angriffe auf Unternehmen mit nachrichtendienstlichen Mitteln werden heutzutage nicht mehr nur durch die Geheimdienste, sondern in zunehmendem Maße auch durch konkurrierende Unternehmen und Kriminelle betrieben. Die technischen Mittel um Telefonate abzuhören, Faxe oder Emails abzufangen, kleine Funksender zum Belauschen von Gesprächen anzubringen oder sämtliche Tastenaschläge eines PC mit zu protokollieren sind teilweise im freien Verkauf zu erhalten. Dank Ebay, Spy Shops oder eines gut bestückten Graumarktes kann damit eine Vielzahl von Unberechtigten auf fremdes Wissen zugreifen. Um sich dagegen zu schützen ist man auf die Hilfe von technischen Spezialisten angewiesen.

- Sweeps (Absuche nach Wanzen mit technischen Geräten)
- Verschlüsselung der Kommunikation (Telefon, Fax, Email, VoIP)
- Einbau abhörsicherer Räume (optisch fast nicht erkennbar)

PRÄVENTIONSMASSNAHMEN

SCHUTZ GEGEN HACKERANGRIFFE

IT-Sicherheit ist kein starrer Zustand – sondern ein ständiger Prozess.

Um sich gegen Cyber-Kriminalität schützen zu können, ist es erforderlich erst einmal den individuellen Bedarf eines Unternehmens zu analysieren. Corporate Trust begreift IT-Sicherheit zum Schutz gegen Hackerangriffe als permanenten Prozess. Dabei berücksichtigen wir nicht nur technische, sonder auch infrastrukturelle, organisatorische und personelle Aspekte.

Unsere IT-Experten erarbeiten zusammen mit Ihrem Team eine individuelle Strategie zum Schutz gegen Angriffe aus dem Netz.

STRIKTE VORGABEN FÜR SICHERE PROZESSE

Klare Regelungen erleichtern den Umgang mit sensiblen Informationen.

Für den Umgang mit sensiblen Informationen müssen im Unternehmen klare Regelungen getroffen werden. Das gesamte Personal eines Unternehmens sollte zuerst für die Gefahren durch Industriespionage sensibilisiert werden, damit ein Verständnis für die erforderlichen Maßnahmen herrscht. Danach sollten klare Anweisungen für die Durchführung der Prozesse erstellt werden. Dabei darf es keine hierarchischen Unterschiede bei der Einhaltung geben. Alle Bereiche, Geschäftsleitung, Management, Entwickler, Sachbearbeiter, Vertrieb oder Sekretärin, haben sich gleichermaßen an die Vorgaben zu halten.

Zum Schutz der Prozesse haben sich u.a. folgende Maßnahmen bewährt:

- Clean-Desk-Policy
- Eindeutige Klassifizierung und Kennzeichnung von Firmen- oder Betriebsgeheimnissen
- Klare Regelungen für den Umgang damit (Kopieren, Weitergabe, Vernichtung etc.)
- Geheimhaltungsverpflichtungen in den Arbeitsverträgen
- Sorgfältige Auswahl der Geschäftspartner (Background-Check)
- Erstellen eines Zugriffsberechtigungskonzeptes für die IT
- Restriktive Zutrittsberechtigungen für sensible Bereiche (z.B. Forschung & Entwicklung)
- Klare Anweisungen für den Emailverkehr

UMGANG MIT PERSONAL

Loyale Mitarbeiter schaffen ein sicheres Unternehmen.

Loyale Mitarbeiter bereichern sich nicht illegal am Unternehmen. Sie sind ein Kontrollorgan gegenüber anderen Mitarbeitern. Deshalb ist es wichtig, die Loyalität der Mitarbeiter zu fördern. Für sie ist es wichtig zu erkennen, dass es dem Unternehmen ernst ist mit den getroffenen Maßnahmen. Dies geschieht am besten durch eine Vorbildfunktion des Managements. Schutz vor Industriespionage muß „Chefsache" sein. Dies an nachgeordnete Stellen zu delegieren, wäre ein verkehrtes Signal. Alle Mitarbeiter sollten in den Informationsschutz mit einbezogen werden. Sie erfüllen eine hohe Schutzfunktion. Außerdem können sie Opfer eines Angriffs bzw. Zeuge eines kriminellen Kollegen werden.

Steigerung des Informationsschutzes durch personalbedingte Maßnahmen:

- Sensibilisierung der Mitarbeiter zum Thema Industriespionage
- Vorbildliches Verhalten des Managements bei Maßnahmen für Informationsschutz
- Einführung eines Whistle-Blowing-Systems [24] für Hinweise auf kriminelle Kollegen
- Beteiligung der Mitarbeiter bei der Erarbeitung von Richtlinien
- Anerkennung von vorbildlichem Verhalten in punkto Sicherheit

MONITORING

Sicherheit kann nur entstehen, wenn Menschen die Maßnahmen auch leben.

Jede Sicherheitsmaßnahme lebt von der Qualität der Umsetzung durch die Menschen. Daher ist es erforderlich, dass es permanente Kontrollen gibt, ob die Vorgaben zum Schutz vor Informationsabfluss eingehalten werden. Bei erkannten Verstößen sollte es Restriktionen geben, bei besonders qualifiziertem Verhalten auch Anerkennung.

Durch permanentes Monitoring kann man Missstände frühzeitig erkennen und die Maßnahmen anpassen. Es sollte dafür eine zentrale Stelle im Unternehmen verantwortlich sein, die fachlich qualifiziert ist und von den Mitarbeitern akzeptiert wird. Dafür sind Sicherheitsverantwortliche bzw. eine Sicherheitsorganisation am besten geeignet.

24)Whistle-Blowing Ein Informant bringt Missstände, illegales Handeln oder allgemeine Gefahren, von denen er an seinem Arbeitsplatz erfährt, an die Öffentlichkeit.

Glossar

- **Verfassungsschutzbericht**
  Der jährliche Verfassungsschutzbericht dient der Unterrichtung und Aufklärung der Öffentlichkeit über verfassungsfeindliche Bestrebungen in der Bundesrepublik Deutschland. Er beruht auf den Erkenntnissen, die das Bundesamt für Verfassungsschutz (BfV) im Rahmen seines gesetzlichen Auftrags, zusammen mit des Landesbehörden für Verfassungsschutz, gewonnen hat.

- **Polizeiliche Kriminalstatistik / PKS**
  Zusammenstellung aller der Polizei bekannt gewordenen strafrechtlichen Sachverhalte unter Beschränkung auf ihre erfassbaren wesentlichen Inhalte. Sie soll im Interesse einer wirksamen Kriminalitätsbekämpfung zu einem überschaubaren und möglichst verzerrungsfreien Bild der angezeigten Kriminalität führen.

- **Wirtschaftsspionage**
  Staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben.

- **Konkurrenzausspähung**
  Ausforschung, die ein konkurrierendes Unternehmen, Kriminelle oder die Medien gegen ein anderes Unternehmen betreiben.

- **Industriespionage**
  Umgangssprachlich für Konkurrenzausspähung oder teilweise auch für Wirtschaftsspionage.

- **Hackerangriff**
  Unerlaubtes Eindringen in fremde Computer- oder Netzwerksysteme, meist durch Überwinden der Sicherheitsmechanismen.

- **Lauschangriff**
  Nachrichtendienstlicher Sprachgebrauch für die akustische Überwachung bzw. das Abhören von Gesprächen.

- **Social Engineering**
  Ausspionieren über das persönliche Umfeld, durch zwischenmenschliche Beeinflussungen und meist durch geschickte Fragestellungen. Social Engineering hat das Ziel, unberechtigt an Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen.

- **Background-Check**
  Überprüfung von Mitarbeitern bezüglich der früheren Arbeitgeber, finanzielle Verhältnisse, Firmenbeteiligungen bzw. verdächtigen Lebensumstände.

- **Integritätstest**
  Psychologisches Testverfahren zur Überprüfung der Integrität am Arbeitsplatz. Der Test prüft vor allem die Bereiche „Persönlicher Arbeitsstil" und „Allgemeine Wertvorstellungen" ab.

- **Sensibilisierung**
  Unterweisung der Mitarbeiter zu einer bestimmten Gefahrenlage mit Bezugnahme auf eine aktuelle Bedrohung.

- **Anwerben / Anwerber**
  Von einem Geheimdienst oder Konkurrenten ausgehender Versuch, Mitarbeiter nach Informationen aus dem Unternehmen zu befragen bzw. sie als fortwährende Quelle zu gewinnen. Häufig geht der eigentlichen Frage nach Informationen der Aufbau einer zwischenmenschlichen Beziehung voraus.

- **Headhunter**
  Englischer Begriff für einen Personalvermittler. Häufig wird mit aggressiven Methoden versucht, Mitarbeiter bei einem Konkurrenten des suchenden Unternehmens abzuwerben.

- **Wanzen**
  Technische, meist miniaturisierte, Bauteile bzw. Funksender zum Abhören von Gesprächen oder Aufzeichnen von Informationen.

- **Abhörgeschützter Raum**
  Architektonische Abschirmung eines Raumes durch technische Maßnahmen, um ungewollte Funkübertragungen zu verhindern.

- **HPM-Waffen / HPM-Angriff (High Power Microwaves)**
  Durch die Aussendung eines kurzzeitigen hochfrequenten Impulses werden die elektronischen Bauteile von technischen Geräten beschädigt.

- **Geheimhaltungsverpflichtung**
  Schriftliche Vereinbarung über den Umgang mit vertraulichen Informationen.

- **Clean-Desk-Policy**
  Schriftliche Vereinbarung mit den Mitarbeitern, dass nach Arbeitsende keine schriftlichen Unterlagen offen zugänglich auf den Schreibtischen liegen gelassen werden dürfen.

- **Hellfeld**
  Kriminalistischer Ausdruck zur Bezeichnung der angezeigten bzw. den Behörden bekannt gewordenen Delikte.

- **Deliktsfelder**
  Kriminalistischer Ausdruck für verschiedene strafbare Handlungen innerhalb eines zusammengehörenden Bereiches.

- **Sweep**
  Absuche nach Wanzen mit technischen Geräten durch Hochfrequenz-Spezialisten.

- **Whistle-Blowing**
  Ein Informant bringt Missstände, illegales Handeln oder allgemeine Gefahren, von denen er an seinem Arbeitsplatz erfährt, an die Öffentlichkeit.

Ansprechpartner

Christian Schaaf
Geschäftsführer
Corporate Trust,
Business Risk &
Crisis Management GmbH

www.corporate-trust.de
schaaf@corporate-trust.de

Claudia Tödtmann
Redakteurin
Verlagsgruppe
Handelsblatt GmbH

www.vhb.de
c.toedtmann@vhb.de

Bärbel Bongartz
Diplom-Kriminologin
Büro für Angewandte
Kriminologie Hamburg

www.baerbel-bongartz.de
post@baerbel-bongartz.de

Die Studie wurde durch Corporate Trust, in Zusammenarbeit mit Frau Claudia Tödtmann, Verlagsgruppe Handelsblatt GmbH, sowie Frau Bärbel Bongartz, Büro für Angewandte Kriminologie Hamburg, erstellt. Frau Bärbel Bongartz war für die kriminologische Beratung verantwortlich.

Selbstverständlich stehen Ihnen alle Ansprechpartner jederzeit für Fragen zur Verfügung. Wir würden uns über Anregungen oder eine Nachricht zu Ihren Erfahrungen mit Industriespionage freuen.

CORPORATE TRUST
Business Risk & Crisis Management GmbH

Bavariaring 44
D-80336 München

T +49 89 599 88 75 80
F +49 89 599 88 75 820

info@corporate-trust.de
www.corporate-trust.de