CORPORATE TRUST
business risk & crisis management

Studie: Industriespionage 2012

Aktuelle Risiken für die deutsche Wirtschaft durch Cyberwar

Begleitet durch: brainloop TÜV SÜD

Inhalt

Eine Investition in Wissen bringt noch immer die besten Zinsen.

Benjamin Franklin

Vorwort

Christian Schaaf
Geschäftsführer
Corporate Trust

Die Industriespionage hat sich in den letzten Jahren dramatisch entwickelt.

Hackerangriffe auf Sony, Google, RSA, die NATO oder den IWF machen deutlich, dass der Cyberwar[1] längst zur Realität geworden ist. Der Computerwurm „Stuxnet" wurde vermutlich speziell entwickelt, um die Steuerungsanlagen Simatic S7, mit denen Frequenzumrichter von Motoren des iranischen Atomprogramms gesteuert wurden, zu sabotieren. Die genauen Ziele der Auftraggeber sind zwar nicht bekannt, die Komplexität des Angriffs zeigt jedoch, dass wir uns von einem Zeitalter der Skript-Kiddies und Cracker hin zu einer neuen Dimension der Gefährdung entwickelt haben. Die sogenannten Advanced Persistant Threats (APTs), also Angriffe durch eine fortgeschrittene und andauernde Bedrohung, veranschaulichen, dass die Cyber-Kriminellen[2] ihre Ziele und Taktiken verändert haben und heute wesentlich aggressiver vorgehen als früher. Die veränderte Bedrohungslage wird ein grundlegendes Umdenken in Bezug auf IT-Sicherheit, Informationsschutz und die Grundregeln für den Wissensaustausch erforderlich machen.

Der Abfluss von sensiblem Know-how stellt für jedes Unternehmen eine ernst zu nehmende Bedrohung dar. Der Wettbewerbsvorteil schwindet und konkurrierende Unternehmen können eigene Produkte günstiger am Markt positionieren, weil sie Entwicklungskosten einsparen. Da es in Deutschland jedoch keine konkreten Zahlen, Daten oder Fakten zur aktuellen Bedrohung durch Industriespionage gibt, war die vorliegende Studie nötig, um ein klares Bild der tatsächlichen Vorfälle zu erhalten und wieder einmal realistisch das Risiko für die Wirtschaft einschätzen zu können.

Unter Industriespionage versteht man die Zusammenfassung aller Spionagetätigkeiten zum Nachteil eines Unternehmens. Dazu gehören sowohl die Wirtschaftsspionage durch ausländische Nachrichtendienste als auch die Konkurrenzausspähung durch Mitbewerber und Spionage durch organisierte Verbrecherbanden oder illoyale Mitarbeiter. Die Informationszugriffe können dabei sehr unterschiedlich erfolgen.

1)Cyberwar: Darunter versteht man die kriegerische Auseinandersetzung im und um den virtuellen Raum, den sog. Cyberspace, mit Mitteln vorwiegend aus dem Bereich der Informationstechnik. Cyberwar bezeichnet auch die Aktivitäten staatlicher Spezialeinheiten, um Gegner oder sonstige Ziele online auszukundschaften bzw. sie im Ernstfall zu sabotieren.

2)Cyber-Kriminelle: Täter, die für ihre Straftaten überwiegend Computer bzw. das Internet als Tatwaffe einsetzen.

Staatliche Stellen mit ihren vielfältigen technischen Mitteln und häufig einer Vielzahl von menschlichen Ressourcen setzen zunehmend auf die Möglichkeiten der Spionage über das Internet. Ob dies schon ein Krieg ist, sei dahingestellt; es steht jedoch fest, dass sich auch deutsche Unternehmen gegen die neuen Bedrohungen wappnen sollten, um weiterhin ihre starke wirtschaftliche Position am Weltmarkt behalten zu können.

Obwohl nach der aktuell vom Bundeskriminalamt (BKA) herausgegebenen Polizeilichen Kriminalstatistik 2010[3] (PKS) die Zahl aller erfassten Straftaten um zwei Prozent zurückgegangen ist, stiegen im gleichen Zeitraum die Fälle von „Ausspähen, Abfangen von Daten" um 32,2 Prozent an. Nach dem ebenfalls vom BKA herausgegebenen Bundeslagebild Wirtschaftskriminalität 2010[4] ist die Anzahl der Fälle, bei denen das Internet als Tatmittel genutzt wurde, um 190 Prozent angestiegen, dies betrifft also mehr als 25 Prozent aller registrierten Fälle. Die Angreifer rüsten auf – dieser Bedrohung muss man sich stellen.

Wenn es um den Schutz des eigenen Know-how geht, ist es zwar wichtig, ein vernünftiges Bewusstsein für die Risiken zu haben, es ist jedoch ebenso wichtig, ein gesundes Vertrauen in die eigenen Sicherheitsvorkehrungen und die Zuverlässigkeit seiner Mitarbeiter zu setzen. Zu wenig Sicherheit ist fahrlässig, zu viel Sicherheit ist unwirtschaftlich. In diesem Spannungsfeld sollte man mit dem richtigen Augenmaß nur bedarfsgerechte Maßnahmen im eigenen Unternehmen implementieren, um nicht zu verschrecken. Sicherheit sollte niemals als Hemmschuh empfunden werden oder Selbstzweck sein. Sicherheit, auch die zum Schutz vor Industriespionage, sollte helfen, die wirtschaftlichen Ziele des Unternehmens zu erreichen. Sicherheit sollte ermöglichen und nicht verhindern. Daher ist es wichtig, die aktuellen Risiken zu kennen, um nur dort in Sicherheit zu investieren, wo es tatsächlich nötig ist.

In diesem Sinne hat Corporate Trust zusammen mit der Brainloop AG und der TÜV SÜD AG versucht, mit dieser Studie die aktuelle Bedrohung für die deutsche Wirtschaft realistisch zu erfassen. Durch die Dokumentation aller tatsächlichen Vorfälle, Schäden, bestehenden Sicherheitsvorkehrungen und der Erwartungen für die Zukunft können zielgerichtete Empfehlungen gegeben sowie ein Best Practice-Ansatz abgeleitet werden.

Ihr
Christian Schaaf

3)Polizeiliche Kriminalstatistik (PKS): Zusammenstellung aller der Polizei bekannt gewordenen strafrechtlichen Sachverhalte unter Beschränkung auf ihre erfassbaren wesentlichen Inhalte. Die PKS soll im Interesse einer wirksamen Kriminalitätsbekämpfung zu einem überschaubaren und möglichst verzerrungsfreien Bild der angezeigten Kriminalität führen. (http://www.bka.de/DE/Publikationen/PolizeilicheKriminalstatistik/pks__node.html)

4)Bundeslagebild Wirtschaftskriminalität 2010: http://www.bka.de/nn_193360/DE/Publikationen/JahresberichteUndLagebilder/Wirtschaftskriminalitaet/wirtschaftskriminalitaet__node.html?__nnn=true

Vorwort

Im Fokus der Spionage: deutsche Unternehmen und ihr Know-how

Eine Begleiterscheinung der Globalisierung ist die Zunahme des Wettbewerbs zwischen Unternehmen und Volkswirtschaften. „Made in Germany" steht hierbei für technologischen Fortschritt, höchste Qualität und erfolgreichen internationalen Wettbewerb.

Die Innovationskraft insbesondere mittelständischer Unternehmen ist ein Markenzeichen der deutschen Wirtschaft und ein wesentlicher Wettbewerbsfaktor.

Die Wirtschaftskraft Deutschlands ist eine der Grundlagen für Wohlstand und Stabilität.

Der internationale Wettbewerb um zukunftsfähige Produkte und Anwendungen findet aber auch mit Mitteln und Methoden der Spionage statt. Konkurrierende Unternehmen und fremde Nachrichtendienste versuchen, auf diesem Weg produktorientiertes sowie unternehmens- und marktrelevantes Know-how zu beschaffen.

Mittelständische Firmen sind sich häufig der Bedrohung durch illegalen Know-how-Transfer nicht bewusst. Sie verfügen nur selten über ein umfassendes und effektives Informationsschutzkonzept.

Die Ergebnisse der vorliegenden Studie von „Corporate Trust" belegen erneut: Spionage ist Realität!

Eine stetig zunehmende Herausforderung sind die elektronischen Angriffe auf Rechner und Computernetzwerke. Ergebnis der meist unentdeckt bleibenden Operationen sind ungewollter Informationsabfluss, eine Fremdsteuerung oder auch Sabotage einzelner Rechner und ggf. auch von IT-Netzwerken.

Seit einigen Jahren sind Angriffe dieser Art auch auf Bundesministerien und andere öffentliche Stellen mit steigender Zahl feststellbar. Für den Bereich der Wirtschaft gibt es keine Vergleichszahlen, jedoch ist hier von einem erheblichen Dunkelfeld auszugehen. Diese Entwicklung führte

im vergangenen Jahr dazu, dass im Bereich des Bundesministeriums des Innern das „Cyber-Abwehr-Zentrum" errichtet wurde, um das Erkenntnisaufkommen und die Analysefähigkeit sowie die Zusammenarbeit der zuständigen Behörden zu optimieren.

Eine nicht unbeträchtliche Bedrohung geht auch von „Innentätern" aus, die in Anbetracht ihrer legalen Zugangsmöglichkeiten und ihres Insiderwissens über innerbetriebliche Schwachstellen in der Lage sind, den Unternehmen mehr Schaden zuzufügen als externe Täter.

Die Sensibilisierung der Mitarbeiter in Sicherheitsfragen und ihre Einbindung in das Sicherheitsmanagement ist daher unabdingbare Voraussetzung für einen wirksamen Informationsschutz.

Im Rahmen eines Sicherheitsmanagements sollte vorrangig das Erfolgswissen – die sogenannten „Kronjuwelen" – ermittelt und dessen Schutz priorisiert werden.

Hierbei besteht nach Aussage der Studie noch erheblicher Nachholbedarf.

Die von „Corporate Trust" vorgelegte Studie zeigt einmal mehr die Vielfalt und die Zunahme der Risiken für die Unternehmen und die Notwendigkeit, vor allem den präventiven Wirtschaftsschutz deutlich zu intensivieren.

Die vorliegende Studie bestätigt leider auch die Erfahrung der Verfassungsschutzbehörden, dass Unternehmen sich bei Spionageverdacht noch zu selten an die Sicherheitsbehörden wenden.

Die Behörden für Verfassungsschutz sind die „Dienstleister" für Spionageabwehr in Deutschland.

Das Wirtschaftsschutzkonzept des Bundesamtes für Verfassungsschutz „Prävention durch Information" basiert auf jahrzehntelanger Erfahrung in der Aufklärung und Abwehr von Wirtschaftsspionage sowie der vertraulichen Kooperation mit den Betroffenen.

Das Angebot des BfV umfasst vielfältige „Security-Awareness"-Aktivitäten, so z.B. bilaterale Sicherheitsgespräche, Sensibilisierungsvorträge in Unternehmen und bei Verbänden, diverse Publikationen, einen elektronischen Newsletter sowie ein umfangreiches Internetangebot zum Wirtschaftsschutz.

Wirtschaftsschutz ist eine gemeinsame Aufgabe von Staat und Wirtschaft: Wirtschaftsschutz ist Teamwork!

Dr. Alexander Eisvogel
Vizepräsident,
Bundesamt für Verfassungsschutz

Ergebnisse in Kürze

- In Deutschland gab es bei den Fallzahlen von Industriespionage eine Steigerung um 2,5 Prozent. Während bei der Studie 2007 nur 18,9 Prozent angaben, durch mindestens einen konkreten Fall von Spionage geschädigt worden zu sein, waren es 2012 insgesamt 21,4 Prozent. Zusammen mit den Verdachtsfällen, die nicht konkretisiert bzw. eindeutig belegt werden konnten – 2012 bei 33,2 Prozent aller befragten Unternehmen – mussten sich damit 54,6 Prozent der deutschen Wirtschaft mit Industriespionage beschäftigen.
- Der Mittelstand ist immer noch deutlich am häufigsten von Spionage betroffen. Bei der Auswertung aller Schäden, unter Berücksichtigung des Verhältnisses zwischen Beteiligung an der Befragung und tatsächlichen Fallzahlen, verzeichnet der Mittelstand mit 23,5 Prozent im Verhältnis die meisten Vorfälle. Es folgen die Konzerne mit einer Häufigkeit von 18,8 Prozent und die Kleinunternehmen mit 15,6 Prozent.
- Der deutschen Wirtschaft entsteht durch Industriespionage jährlich ein Gesamtschaden von ca. 4,2 Milliarden Euro. Im Vergleich zur Studie 2007 (2,8 Milliarden Euro) entspricht dies einem Anstieg um exakt 50,0 Prozent und belegt eindringlich, wie hoch das neue Bedrohungspotenzial durch Cyberwar[1] tatsächlich ist.
- Die Häufigkeit der finanziellen Schäden durch Industriespionage ist ebenfalls deutlich angestiegen. Während bei der Studie 2007 nur 64,4 Prozent der geschädigten Unternehmen angaben, einen finanziellen Schaden erlitten zu haben, waren es 2012 bereits 82,8 Prozent. Dies stellt einen Anstieg um 28,7 Prozent dar.
- Bei der Unterscheidung der Schäden nach Unternehmensgröße fiel auf, dass Kleinbetriebe nur Schäden bis maximal 100.000 Euro feststellten, die finanziellen Negativauswirkungen im Mittelstand vor allem im Bereich 10.000 bis 100.000 Euro lagen (53,5 Prozent) und 23,5 Prozent der geschädigten Konzerne auch im Bereich über einer Million Euro Schäden bezifferten.
- Die Spionage fand hauptsächlich in den GUS-Staaten (27,0 Prozent der Fälle), Europa (26,6 Prozent), Deutschland (26,1 Prozent) und in Nordamerika (25,2 Prozent) statt. Industriespionage direkt vor Ort in Asien identifizierten die Unternehmen nur in 10,4 Prozent aller Vorkommnisse. Anscheinend gehen die Firmen konkreten Hinweisen sehr stark nach und können die Angriffsorte auch identifizieren. Nur 6,3 Prozent aller geschädigten Unternehmen war es völlig unklar, wo die Spionage bzw. der Informationsabfluss stattfand.
- Nach wie vor sind der Vertrieb mit 18,3 Prozent sowie Forschung & Entwicklung mit 16,0 Prozent die am häufigsten ausspionierten Bereiche. Danach kommen die Bereiche Mergers & Acquisitions mit 14,2 Prozent, die IT-Administration bzw. IT-Services mit 12,7 Prozent, Fertigung/Produktion mit 8,4 Prozent, Personal mit 7,5 Prozent, Einkauf mit 5,7 Prozent und der Bereich Management/Geschäftsleitung mit 5,1 Prozent.
- Die häufigsten Schäden entstehen durch eigene Mitarbeiter, externe Geschäftspartner und Hackerangriffe[2]. Die bewusste Informationsweitergabe bzw. der Datendiebstahl durch eigene Mitarbeiter war bei 47,8 Prozent der konkreten Spionagehandlungen für den Informationsabfluss verantwortlich. Zusammen mit den Fällen von Social Engineering[3] (22,7 Prozent), bei denen Mitarbeiter geschickt ausgefragt wurden, waren Mitarbeiter damit in 70,5 Prozent aller Fälle an Industriespionage beteiligt.
- Rechtsstreitigkeiten und Imageschäden bei Kunden oder Lieferanten sind die häufigsten Folgen von Industriespionage. 65,4 Prozent der geschädigten Unternehmen beklagen hohe Kosten für Rechtsstreitigkeiten und 59,9 Prozent einen entsprechenden Imageschaden. Immerhin noch rund ein Drittel aller Unternehmen (36,0 Prozent) verzeichnete auch Umsatzeinbußen durch den Verlust von Wettbewerbsvorteilen.
- Nur bei jedem fünften Vorfall – exakt bei 19,9 Prozent – wurden der Verfassungsschutz oder die Polizeibehörden hinzugezogen, bei 57,6 Prozent zumindest externe Sicherheitsfachleute wie Computer- oder Abhörschutzspezialisten bzw. forensische Ermittler.
- Bereits mehr als die Hälfte der Unternehmen hat den Informationsschutz zur Chefsache erklärt bzw. einen Chief Information Security Officer (CISO) etabliert. Auf die Frage, wer sich um die zentralen Belange des Informationsschutzes kümmert, gaben 31,2 Prozent an, dass dies zur Chefsache erkoren sei, und bei 20,4 Prozent der Firmen gibt es bereits einen CISO.
- Die Sicherheitsmaßnahmen hinken in der Regel der tatsächlichen Bedrohung hinterher. Fast die Hälfte aller Unternehmen (49,2 Prozent) hat immerhin eine vertragliche Vereinbarung zur Geheimhaltung bzw. Vertraulichkeit mit externen Geschäftspartnern, 46,4 Prozent

1)Cyberwar: Darunter versteht man die kriegerische Auseinandersetzung im und um den virtuellen Raum, den sog. Cyberspace, mit Mitteln vorwiegend aus dem Bereich der Informationstechnik. Cyberwar bezeichnet auch die Aktivitäten staatlicher Spezialeinheiten, um Gegner oder sonstige Ziele online auszukundschaften bzw. sie im Ernstfall zu sabotieren.

2)Hackerangriff: Unerlaubtes Eindringen in fremde Computer- oder Netzwerksysteme, meist durch das Überwinden von Sicherheitsmechanismen.

3)Social Engineering: Ausspionieren über das persönliche Umfeld, durch zwischenmenschliche Beeinflussung bzw. durch geschickte Fragestellung, meist unter Verschleierung der eigenen Identität (Verwenden einer Legende). Social Engineering hat das Ziel, unberechtigt an Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen.

4)Sicherheits-Policy: (auch Sicherheitsrichtlinie oder Sicherheitsleitlinie) Beschreibt den erstrebten Sicherheitsanspruch eines Unternehmens und konzeptionell die Maßnahmen, um dorthin zu kommen.

5)Sensibilisierung: Unterweisung bzw. Schulung der Mitarbeiter zu einer bestimmten Gefahrenlage mit Bezugnahme auf eine aktuelle Bedrohung.

haben eine Sicherheits-Policy[4] mit klaren Regeln für den Informationsschutz. Jedoch beziehen nur 7,5 Prozent externe Partner über eine technische Möglichkeit, z.B. eine sog. Document Compliance Management Lösung, in die Sicherheits-Policy mit ein.

- In den meisten Fällen ist den Führungsverantwortlichen und Mitarbeitern gar nicht deutlich bewusst, welches Know-how schützenswert ist. Eine Schutzbedarfsanalyse sollte für alle unmissverständlich regeln, welche Daten/Informationen geheim, vertraulich oder offen zugänglich sind. Nur 20,4 Prozent der befragten Unternehmen gaben an, eine solche Schutzbedarfsanalyse bereits erstellt und allen Mitarbeitern bekannt gegeben zu haben.
- Die IT-Sicherheitsvorkehrungen sind noch nicht ausreichend, um sich effektiv gegen Cyberwar[1] zu schützen. Zwar verfügen annähernd 90 Prozent der Unternehmen über einen Passwortschutz auf allen Geräten und eine entsprechende Absicherung des Firmennetzwerks gegen Angriffe von außen, jedoch nur 18,9 Prozent setzen auf verschlüsselten E-Mail-Verkehr und nur 18,6 Prozent verbieten es, USB-Sticks und portable Festplatten oder CD-Brenner an den PC anzuschließen.
- Auf die Gefahren von Social Engineering[3] ist lediglich ein Viertel aller Mitarbeiter vorbereitet. 73,9 Prozent der Unternehmen führen keine regelmäßigen Schulungen zur Sensibilisierung[5] durch.
- Unternehmen verlassen sich zumeist auf Geheimhaltungsverpflichtungen in den Arbeitsverträgen, die Integrität von neuen Bewerbern wird dagegen nur selten geprüft. Während es bei 79,1 Prozent aller befragten Firmen bereits einen entsprechenden Passus in den Arbeitsverträgen gibt, prüfen nur 5,9 Prozent vor der Einstellung die Integrität des Bewerbers.
- Obwohl bei Industriespionage die häufigsten Schäden durch Mitarbeiter entstehen, machen sich zu wenige Unternehmen Gedanken über die Loyalität ihrer Angestellten. Nur bei 34,8 Prozent der Firmen wird eine regelmäßige Mitarbeiterbefragung zur Erfassung der Loyalität durchgeführt. Dieser Loyalitäts-Index[6] kann einen klaren Aufschluss darüber geben, wie es um das Betriebsklima bestellt ist und woran es im Unternehmen mangelt.
- Während 81,4 Prozent bauliche Sicherheitsvorkehrungen gegen unberechtigte Zutritte treffen, findet nur bei etwas mehr als einem Drittel (exakt 38,5 Prozent) eine Überwachung von besonders sensiblen Bereichen durch Video- oder Zugangskontrollen statt. Abhörsichere Besprechungsräume gibt es sogar nur bei 2,2 Prozent aller Unternehmen. Einen Sweep[7], bei dem solche Bereiche nach Wanzen abgesucht werden, lassen nur 2,2 Prozent regelmäßig durchführen.
- Die meisten Unternehmen gehen bei Geschäftsreisen ins Ausland viel zu sorglos mit ihren Informationen um. 55,6 Prozent gaben an, keinerlei Sicherheitsvorkehrungen zu treffen. Nur ca. jedes sechste Unternehmen rüstet seine Angestellten mit verschlüsselter Hard- und/oder Software für eine geschützte Kommunikation (16,4 Prozent) oder speziell vorbereiteten Reise-Laptops mit Minimalkonfiguration und nur geringem Datenbestand (14,1 Prozent) aus bzw. sensibilisiert seine Mitarbeiter durch eine Schulung für das erhöhte Risiko von Industriespionage (12,1 Prozent).
- Zwar haben nur 18,8 Prozent aller Unternehmen, die Steuerungsanlagen einsetzen, einen konkreten Angriff festgestellt, jedoch gaben 63,6 Prozent dieser Unternehmen an, dass Schäden deutliche finanzielle Auswirkungen für das Unternehmen haben könnten. 36,4 Prozent gaben sogar an, dass ein Angriff zu einem Ausfall oder einer Fehlsteuerung führen könnte, welche die Umwelt wesentlich gefährden könnten. Immerhin noch 13,0 Prozent gehen sogar davon aus, dass ein Ausfall oder eine Fehlsteuerung die Versorgungslage in Teilen der Bevölkerung gefährden könnten.
- Über drei Viertel aller befragten Firmen gehen davon aus, dass die zukünftige Bedrohung durch Industriespionage zunimmt. Jedoch glaubt nur noch die Hälfte, dass dies auch für ihr eigenes Unternehmen zutrifft. Zum Vergleich: 2007 gaben noch 66,3 Prozent der Unternehmen an, dass ihr eigenes Risiko für Industriespionage gleich bleiben würde. Bei der aktuellen Studie sehen dies nur noch 47,7 Prozent so optimistisch.
- Als häufigstes Risiko betrachten die Unternehmen die zunehmende Verwendung mobiler Geräte wie Tablets und Smartphones (63,7 Prozent), gefolgt von der sinkenden Sensibilität der eigenen Mitarbeiter im Umgang mit vertraulichen Daten (54,3 Prozent). Auch das zunehmende Outsourcing[8] von Dienstleistungen (52,4 Prozent) und der zunehmende Einsatz von Cloud-Services[9] (47,7 Prozent) werden als Bedrohungen der Zukunft eingeschätzt. Die vermehrten Aktivitäten staatlich gelenkter Hackergruppen sehen 44,1 Prozent der Firmen als zunehmendes Risiko für ihr Know-how.

6)Loyalitäts-Index: Beurteilung von Unternehmen und Organisationen im Hinblick auf kriminelle und fahrlässige Handlungen von Mitarbeitern. Der Loyalitäts-Index liefert durch eine Mitarbeiterbefragung mit einer psychologisch fundierten Vorgehensweise Parameter, welche auf potenzielle Risiken hinweisen.

7)Sweep: Absuche nach Wanzen mit technischen Geräten durch Hochfrequenz-Spezialisten. Dient in der Regel der Lauschabwehr.

8)Outsourcing: Damit wird in der Ökonomie die Abgabe von Unternehmensaufgaben und -strukturen an Drittunternehmen bezeichnet. Es ist eine spezielle Form des Fremdbezugs von bisher intern erbrachter Leistung, wobei in der Regel Verträge die Dauer und den Umfang der Leistung festschreiben.

9)Cloud-Service: (auch Cloud-Computing) Umschreibt den Ansatz, abstrahierte IT-Infrastrukturen (z.B. Rechenkapazitäten, Datenspeicher, Netzwerk-Kapazitäten oder auch ← fertige Software) dynamisch an den Bedarf angepasst über ein Netzwerk zur Verfügung zu stellen. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud-Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z.B. Rechenleistung, Speicherplatz), Plattformen und Software.

Methodik der Studie

Die vorliegende Studie „Industriespionage 2012 – Aktuelle Risiken für die deutsche Wirtschaft durch Cyberwar" wurde in Zusammenarbeit mit der Brainloop AG und der TÜV SÜD AG auf der Grundlage einer Befragung von 6.924 deutschen Unternehmen erstellt. Für die Studie wurde ein repräsentativer Querschnitt aus ca. 65.000 Unternehmen nach dem Zufallsprinzip ausgewählt und befragt.

Um ein möglichst umfassendes Bild der aktuellen Bedrohung zu erhalten, wurde großer Wert darauf gelegt, die Befragung branchenübergreifend durchzuführen und sämtliche Unternehmensgrößen zu berücksichtigen, vom Kleinunternehmen bis zum Konzern, jeweils gemessen an Umsatzvolumen und Anzahl der Mitarbeiter. Es wurden allerdings nur Unternehmen mit mindestens zehn Mitarbeitern bzw. einem Umsatz über einer Million Euro berücksichtigt. Aus den vorangegangenen Studien der letzten Jahre wurde deutlich, dass sich viele Unternehmen trotz ihres hohen Umsatzes und der Vielzahl ihrer Mitarbeiter noch zum Mittelstand zählen. Daher wurde vor allem berücksichtigt, zu welcher Kategorie sich die Unternehmen selbst zugehörig fühlten.

Die Befragung wurde im Januar und Februar 2012 durchgeführt und richtete sich überwiegend an die Mitglieder des Vorstands bzw. der Geschäftsführung (48,9 Prozent aller Antworten), jedoch auch an die Leiter Unternehmenssicherheit (7,5 Prozent), Leiter IT (6,9 Prozent), Leiter Interne Revision (6,9 Prozent), Compliance Officer (6,7 Prozent), Chief Information Security Officer/CISO (6,4 Prozent), Leiter Risikomanagement (4,7 Prozent), Leiter Finanzen, Controlling oder Rechnungswesen (2,3 Prozent), Leiter Personal (0,3 Prozent) und Leiter Recht (0,2 Prozent). Darüber hinaus gaben 9,2 Prozent der Befragten an, zu einem sonstigen Bereich im Unternehmen zu gehören.

Erstaunlicherweise wurde der Fragebogen nur in 6,4 Prozent aller Fälle vom Chief Information Security Officer (CISO) eines Unternehmens ausgefüllt, also von genau der Stelle, die sich hauptverantwortlich um den Informationsschutz kümmern sollte. Die Ergebnisse zeigen, dass es bisher vermutlich in den wenigsten Unternehmen eine solche Position gibt bzw. dass der Informationsschutz heute tatsächlich in den meisten Unternehmen zur „Chefsache" erklärt wurde.

Für die Befragung wurde ein standardisierter Fragebogen postalisch an die Unternehmen versandt. Darüber hinaus wurde ihnen die Möglichkeit geboten, auf einer eigens dafür erstellten Webseite online den Fragebogen zu beantworten. Dafür wurden im Anschreiben die für alle Teilnehmer einheitlichen Benutzerdaten angegeben. So wurde gewährleistet, dass nur angeschriebene Unternehmen an der Onlinebefragung teilnehmen konnten. Zusätzlich wurden 30 Unternehmen in telefonischen Interviews direkt zu ihren Erfahrungen mit Industriespionage befragt.

Die Beteiligung fiel, ähnlich der Vorgängerstudie aus dem Jahr 2007, in den verschiedenen Branchen sehr unterschiedlich aus. Dies kann zum einen darauf zurückzuführen sein, dass in einzelnen Bereichen eine differenzierte Wahrnehmung der Risiken vorherrscht oder zum anderen, dass in manchen Branchen immer noch eine geringere Bereitschaft besteht, über die Probleme zu sprechen.

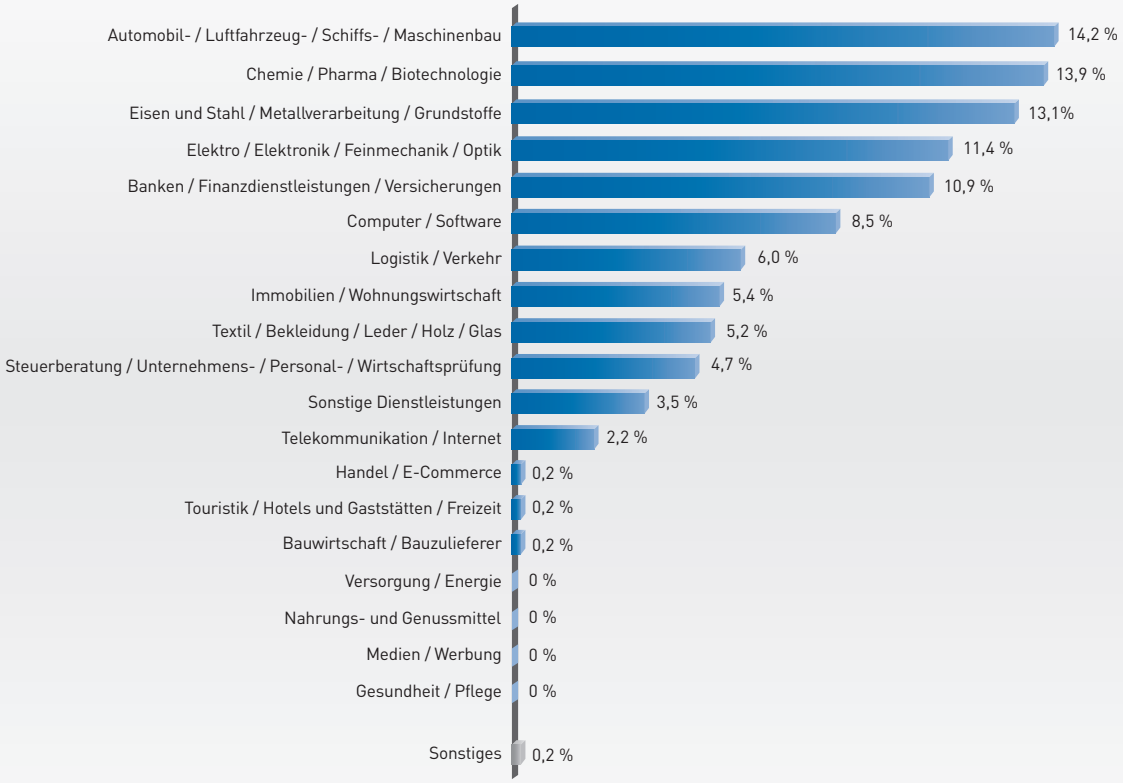
Im ersten Bereich der Befragung wurden Informationen zum Unternehmen selbst erhoben, danach zu den Vorfällen und Risiken, den aktuellen Sicherheitsvorkehrungen im Unternehmen (speziell zur Sicherheit in Steuerungsanlagen), zur Einschätzung der künftigen Risiken und zur weiteren Prävention. Die Befragung war dabei so angelegt, dass die vorgegebenen Antwortoptionen erfahrungsgemäß 80 Prozent der denkbaren Antworten abdeckten. Für die restlichen 20 Prozent gab es überwiegend die Möglichkeit, zusätzliche Antworten in Form eines Freitextes zu geben. Bei den meisten Fragen waren Mehrfachantworten zugelassen.

Am Ende der Befragung wurde den Teilnehmern die Gelegenheit geboten, ihre Kontaktdaten anzugeben. Als kleines Dankeschön erhielten sie für ihre Beteiligung eine kostenlose Erstberatung. Es war jedoch allen Teilnehmern freigestellt, auch anonym zu antworten. Die meisten Unternehmen wollten keine Angaben zur Firma machen. Dies war insbesondere in solchen Fällen festzustellen, wo gravierende Spionagevorfälle erwähnt wurden und auch entsprechende Schäden aufgetreten waren.

Von den 6.924 angeschriebenen Firmen antworteten genau 597 Teilnehmer, dies entspricht 8,6 Prozent aller befragten Unternehmen. Die Antwortbereitschaft lag damit im normalen Durchschnitt vergleichbarer Studien, jedoch unter dem Durchschnitt der Studie Industriespionage aus dem Jahr 2007 (9,9 Prozent).

Corporate Trust möchte sich auf diesem Wege ganz herzlich bei der Brainloop AG und der TÜV SÜD AG für ihre partnerschaftliche Begleitung der Studie sowie bei allen Teilnehmern für ihren wesentlichen Beitrag zum Gelingen der Studie bedanken.

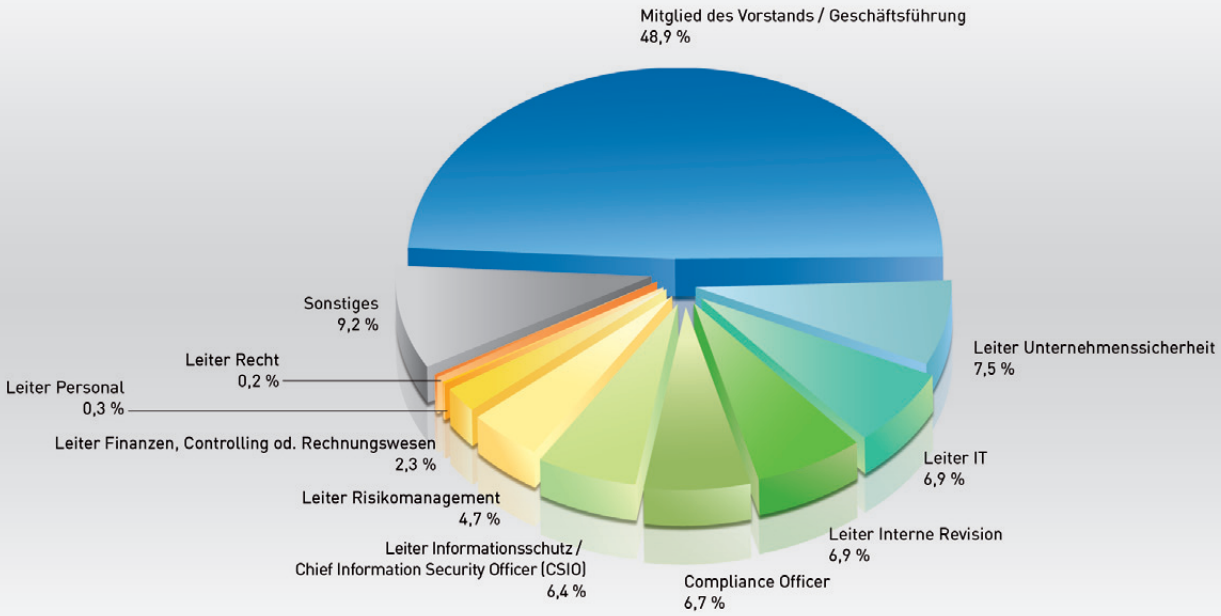
Teilnahme an der Studie



GRAFIK 1

Quelle: Corporate Trust 2012

Welche Position nehmen Sie im Unternehmen ein?



GRAFIK 2

Quelle: Corporate Trust 2012

Betroffene Unternehmen

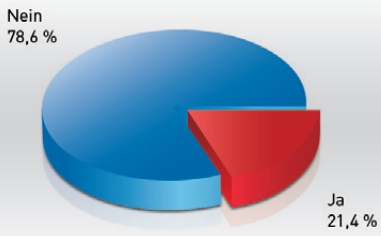
Über 20 Prozent aller Unternehmen hatten in den letzten drei Jahren einen konkreten Spionagevorfall.

Das Risiko durch Industriespionage stellt in Deutschland eine ernst zu nehmende Bedrohung dar. Während bei der Studie im Jahr 2007 18,9 Prozent der Teilnehmer angaben, in mindestens einem konkreten Fall ausspioniert worden zu sein, hatten bei der aktuellen Befragung bereits 21,4 Prozent aller befragten Unternehmen in den letzten drei Jahren konkrete Spionagevorfälle bzw. einen Informationsabfluss zu verzeichnen. Dies entspricht einer Steigerung von 2,5 Prozent und bedeutet, dass in den letzten drei Jahren immerhin jedes fünfte Unternehmen von Spionage betroffen war.

Bei den Verdachtsfällen verhielt es sich ähnlich. Im Jahr 2007 gaben 35,1 Prozent der Vorstände, Geschäftsführer oder Sicherheitsverantwortlichen an, einen Verdacht auf Spionage bzw. Informationsabfluss verzeichnet zu haben, der nicht näher belegt werden konnte. Im Jahr 2012 reduzierten sich die Verdachtsfälle geringfügig auf 33,2 Prozent aller befragten Unternehmen.

Dies zeigt, dass sich in der Gesamtheit (konkrete Spionagefälle und Verdachtsfälle) 54,6 Prozent der deutschen Wirtschaft mit Industriespionage auseinandersetzen mussten. Gerade die hohe Zahl der Verdachtsfälle, die nicht eindeutig belegt werden konnten – immerhin jedes dritte Unternehmen war hiervon betroffen – dürfte ein Beweis dafür sein, dass es für deutsche Firmen immer noch schwierig ist, Spionage umfassend aufzuklären. Hier fehlen oftmals nicht nur die entsprechenden internen Ressourcen oder das Know-how für Forensik und die sehr speziellen Ermittlungen, sondern auch die Bereitschaft, sich bei einem solchen Vorfall an die Behörden zu wenden oder an die Öffentlichkeit zu gehen. Zu stark ist immer noch die Angst, dass durch ein bekannt gewordenes „Leck" ein Reputationsschaden entstehen könnte.

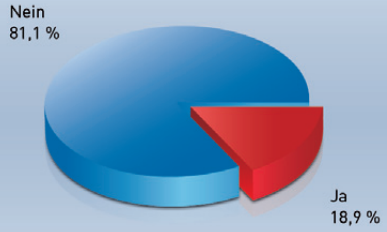
Gab es in Ihrem Unternehmen in den letzten drei Jahren konkrete Spionage-Vorfälle bzw. einen Informationsabfluss?



GRAFIK 3

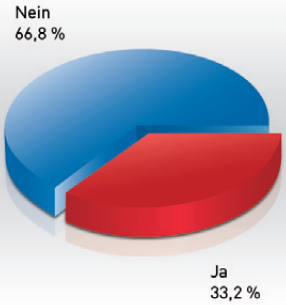
Quelle: Corporate Trust 2012

Stand: 2007



Quelle: Studie Industriespionage 2007

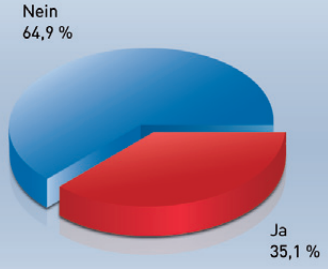
Gab es in Ihrem Unternehmen einen Verdacht auf Spionage bzw. Informationsabfluss, der nicht konkretisiert bzw. eindeutig belegt werden konnte?



GRAFIK 4

Quelle: Corporate Trust 2012

Stand: 2007



Quelle: Studie Industriespionage 2007

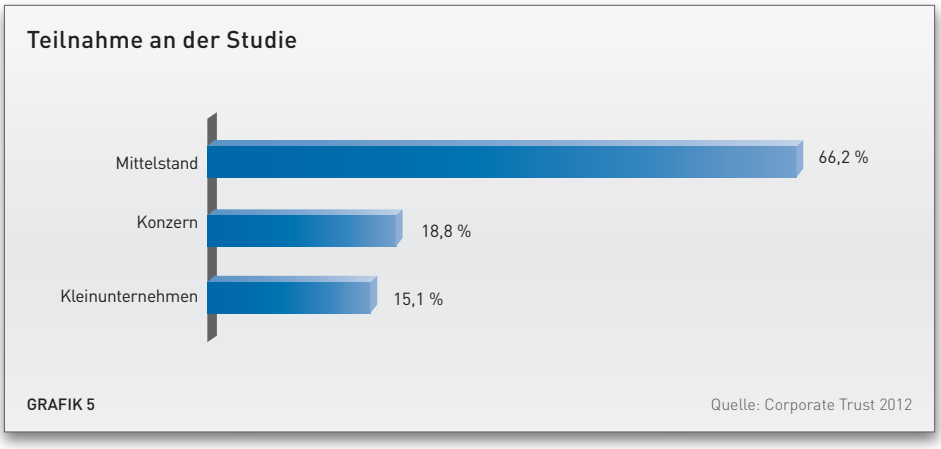
Betroffene Unternehmen

Der Mittelstand ist noch immer am stärksten gefährdet.

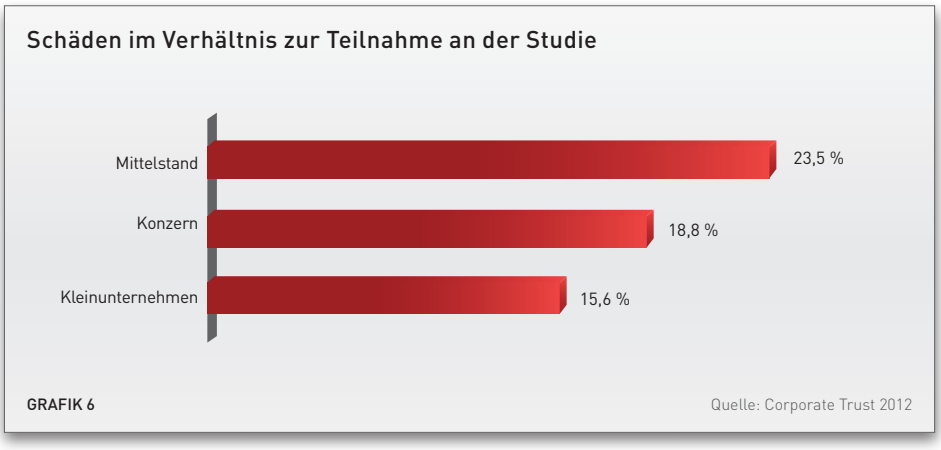
Von den befragten Unternehmen waren 66,2 Prozent dem Mittelstand zuzurechnen (dies entspricht laut einer Richtlinie der EU-Kommission einem Unternehmen mit 50 bis 250 Mitarbeitern oder 50 bis 500 Millionen Euro Umsatz oder alternativ denjenigen, die sich in der Befragung selbst als Mittelstand bezeichneten), 18,8 Prozent waren Konzerne (mehr als 250 Mitarbeiter oder mehr als 500 Millionen Euro Umsatz) und 15,1 Prozent Kleinunternehmen (10 bis 50 Mitarbeiter oder 10 bis 50 Millionen Euro Umsatz). Jedes Unternehmen ist heute gefährdet, Opfer eines Hackerangriffs[1] oder Informationsabflusses zu werden. In den letzten drei Jahren waren jedoch die mittelständischen Unternehmen am häufigsten von Spionage betroffen und unterliegen daher anscheinend dem höchsten Risiko.

Von den insgesamt durch einen Informationsangriff geschädigten Unternehmen (21,4 Prozent der Teilnehmer) waren 10,9 Prozent Kleinunternehmen, 16,4 Prozent Konzerne und 72,7 Prozent mittelständische Firmen. Gemessen am Verhältnis zu ihrer Beteiligung an der Befragung waren damit 15,6 Prozent der Kleinunternehmen, 18,8 Prozent der Konzerne und 23,5 Prozent der Mittelständler betroffen.

Dies zeigt, dass gerade der Mittelstand mit seiner hohen Innovationsfähigkeit und Produktqualität stark im Fokus von Industriespionage steht. Mittelständische Firmen sind zwar das Rückgrat der deutschen Wirtschaft, haben jedoch vermutlich immer noch nicht genügend Sicherheitsvorkehrungen getroffen, um dem Abfluss von Know-how wirkungsvoll entgegenzutreten. Deutsche Konzerne sind hier mit ihren Corporate Security-Abteilungen offenbar besser gerüstet.



GRAFIK 5 Quelle: Corporate Trust 2012



GRAFIK 6 Quelle: Corporate Trust 2012

1)Hackerangriff: Unerlaubtes Eindringen in fremde Computer- oder Netzwerksysteme, meist durch das Überwinden von Sicherheitsmechanismen.

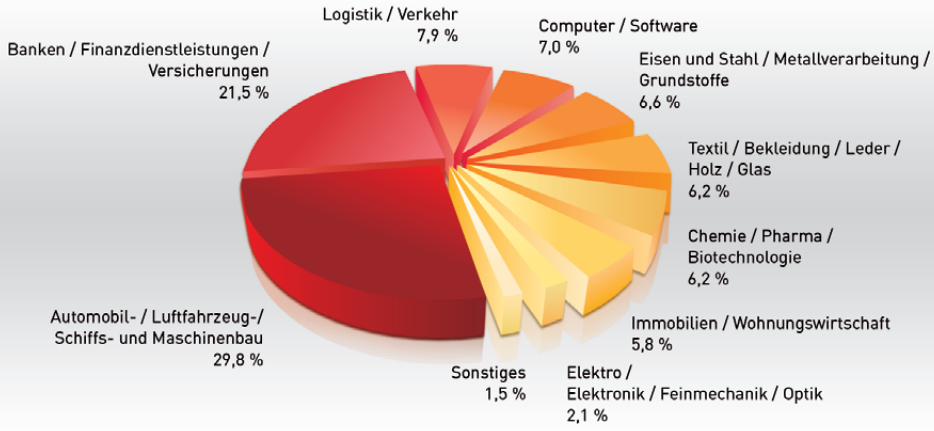
Am häufigsten sind die Finanzwirtschaft und der Maschinenbau betroffen.

Die Bewertung, welches individuelle Risiko für ein Unternehmen besteht, kann sich auch an der Häufigkeit orientieren, wie oft Angriffe auf Unternehmen der gleichen Branche, mit vergleichbarem Know-how oder ähnlichen Produkten stattfinden. Daher war es in der Befragung wichtig, zu erfahren, welche Branchen besonders vielen Fällen von Industriespionage ausgesetzt sind. Viele der teilnehmenden Unternehmen gaben bei der Frage nach konkreten Spionagehandlungen mehrere Vorfälle an, sodass dies auch in die Gefährdung je Branche mit einfloss.

Die Unternehmen wurden daher neben ihrer Umsatzgröße und Mitarbeiterzahl auch nach ihrer Branchenzugehörigkeit gefragt. Bei den tatsächlichen Spionagefällen ergaben sich dabei vor allem für zwei Branchen deutlich erhöhte Risiken: So kam es bei der wesentlich zum Rückgrat der deutschen Wirtschaft gehörenden Automobil- / Luftfahrzeug- / Schiffs- und Maschinenbaubranche mit 29,8 Prozent am häufigsten zu Schäden. Dies stellt noch einmal eine Steigerung um 2,9 Prozent im Vergleich zur Studie von 2007 dar; damals war der Maschinenbau mit 26,9 Prozent ebenfalls am stärksten betroffen. In der aktuellen Erhebung folgt allerdings mit 21,5 Prozent die Finanzdienstleistungsbranche. Interessanterweise beteiligte sich das Segment „Banken / Finanzdienstleistungen / Versicherungen" im Jahr 2007 nicht an der Studie; somit konnte auch keine Erfassung der Schadenszahlen erfolgen.

Die Ergebnisse aus diesen Antworten sollten allerdings nicht dazu verleiten, weniger geschädigte Branchen automatisch als geringer gefährdet einzustufen – niedrigere Schadenszahlen können sich ebenso aus einer geringeren Studienbeteiligung in einem bestimmten Segment ergeben. Außerdem herrscht in einzelnen Branchen erfahrungsgemäß eine geringere Sensibilität für die Wahrnehmung von Spionage bzw. es existieren weniger Sicherheitsvorkehrungen, sodass es oftmals schwerer fällt, Informationsabfluss überhaupt zu bemerken.

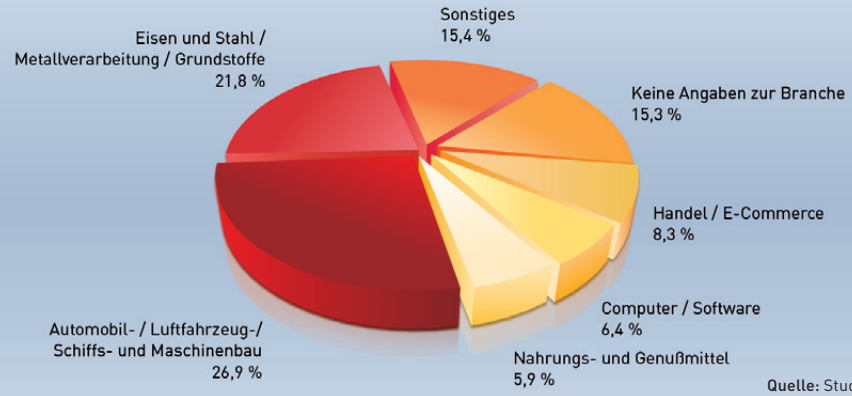
Geschädigte Branchen



GRAFIK 7

Quelle: Corporate Trust 2012

Stand: 2007



Quelle: Studie Industriespionage 2007

Betroffene Unternehmen

Die Geschäftstätigkeit im Ausland erhöht das Risiko deutlich.

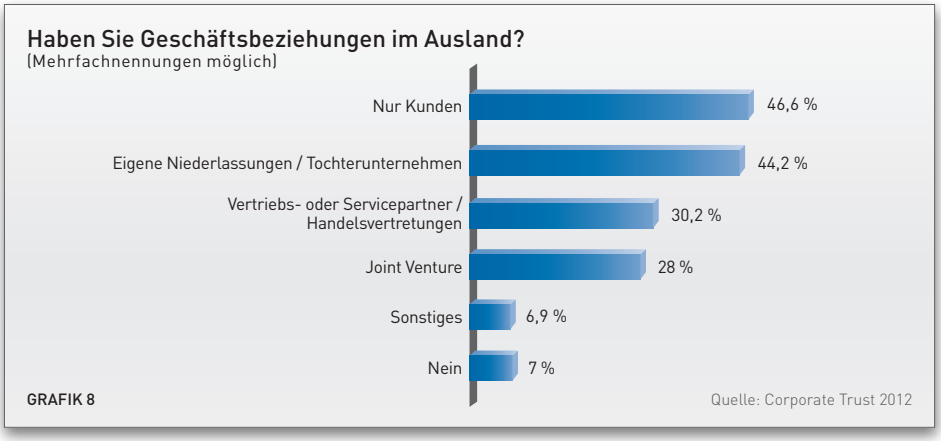
Von allen befragten Firmen gaben lediglich 7,0 Prozent an, keine Geschäftsbeziehungen ins Ausland zu unterhalten. Die meisten Unternehmen (46,6 Prozent) verfügen zumindest über Kunden im Ausland, 44,2 Prozent betreiben eigene Niederlassungen bzw. Tochterunternehmen, 30,2 Prozent haben Handelsvertretungen, Vertriebs- oder Servicepartner und 28,0 Prozent sogar ein Joint Venture.

Bei den Regionen, in die Geschäftsbeziehungen unterhalten werden, war Europa mit 86,1 Prozent am häufigsten vertreten, gefolgt von Asien (55,8 Prozent), Nordamerika (53,4 Prozent) und den GUS-Staaten (45,2 Prozent).

Ein Großteil der deutschen Wirtschaft ist damit global unterwegs und deshalb auch unterschiedlichsten Risiken ausgesetzt.

Bei der Betrachtung, welche Unternehmen Schäden durch Industriespionage angeben und gleichzeitig Geschäftsbeziehungen im Ausland unterhalten, wird das Risiko deutlich: Bei exakt 96,0 Prozent aller Firmen gibt es ein Auslandsengagement, nur 4,0 Prozent der Unternehmen mit einem Spionagevorfall haben keine geschäftlichen Beziehungen ins Ausland.

Aufgrund der geringen Zahl von 7,0 Prozent der Unternehmen, die keinerlei Auslandsbeziehungen unterhalten, ist die hohe Zahl an geschädigten Unternehmen mit Auslandsengagement (96,0 Prozent) allerdings nicht verwunderlich. Dies zeigt vermutlich auch, dass sich überwiegend Firmen an der Studie beteiligten, die im Ausland präsent sind und daher offenbar stärker für die Risiken von Industriespionage sensibilisiert sind.



GRAFIK 8

Quelle: Corporate Trust 2012

GRAFIK 9

Quelle: Corporate Trust 2012

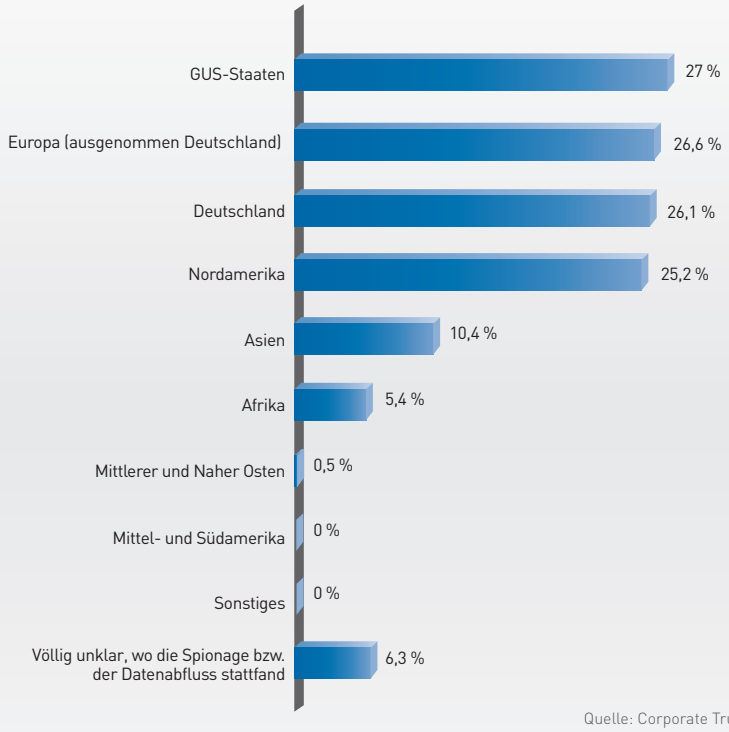
Spionage findet (neben Deutschland) vor allem in den GUS-Staaten, Europa und Nordamerika statt.

Während bei der Studie 2007 noch 76,9 Prozent der geschädigten Unternehmen angaben, dass die Spionage oder zumindest der Verdacht auf einen solchen Vorfall in Deutschland stattfand, sind es aktuell nur noch 26,1 Prozent. Das Bewusstsein der Unternehmen für kriminelle Angriffe im Ausland dürfte damit deutlich gestiegen sein. Nur noch 6,3 Prozent der Firmen sind sich völlig im Unklaren darüber, wo die Spionage bzw. der Datenabfluss stattfand. Die meisten Vorfälle ereigneten sich in den GUS-Staaten (27,0 Prozent), gefolgt von Europa (26,6 Prozent), Deutschland (26,1 Prozent), Nordamerika (25,2 Prozent) und Asien (10,4 Prozent).

Die geringen Schadenszahlen für Asien könnten zum einen darauf zurückzuführen sein, dass sich mittlerweile die Mehrzahl der Unternehmen des Risikos bewusst sind, bei Geschäften in China einen Informationsabfluss zu erleiden. Folglich wurden sicherlich oftmals verstärkte Schutzmaßnahmen implementiert und die Mitarbeiter entsprechend auf ihre Reisen nach Asien vorbereitet. Zum anderen ist es jedoch auch möglich, dass gerade die gehäuften Hackerangriffe aus dem Reich der Mitte zwar als solche erkannt, jedoch aufgrund des Angriffs auf ein Unternehmenssystem in Deutschland als Angriffe „in Deutschland" gewertet wurden. Erstaunlich scheinen außerdem die Zahlen von Spionagevorfällen in Europa (26,6 Prozent) und Nordamerika (25,2 Prozent). Offenbar werden die Bedingungen im internationalen Geschäftsfeld härter und es wird von Konkurrenten zunehmend mit verbotenen Mitteln gearbeitet.

Das Ergebnis zeigt, dass nach wie vor von einer hohen Spionagetätigkeit durch die Nachrichtendienste Chinas und der GUS-Staaten auszugehen ist – also der klassischen Wirtschaftsspionage[1] – , Unternehmen jedoch ebenso bei ihrer Geschäftstätigkeit in Europa oder Nordamerika von Industriespionage betroffen sein können. Dies erfordert vermutlich ein Umdenken bei der Sensibilisierung von Mitarbeitern und der Planung von Geschäftsprozessen.

Können Sie konkretisieren, wo die Spionage zum Nachteil Ihres Unternehmens stattfand? (Mehrfachnennungen möglich)



GRAFIK 10

Quelle: Corporate Trust 2012

1)Wirtschaftsspionage: Staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben.

Schäden durch Spionage

Die finanziellen Schäden durch Industriespionage sind deutlich angestiegen.

Der deutschen Wirtschaft entsteht durch Industriespionage jährlich ein Gesamtschaden von ca. 4,2 Milliarden Euro. Im Vergleich zur Studie 2007 (2,8 Milliarden Euro) entspricht dies einem Anstieg um 50,0 Prozent und belegt eindringlich, wie hoch das neue Bedrohungspotenzial durch Cyberwar tatsächlich ist.

In Deutschland gibt es ca. 3,1 Millionen umsatzsteuerpflichtige Unternehmen. Etwa zwei Drittel davon sind Einzelunternehmen. Für die Befragung wurden lediglich Unternehmen mit mindestens 10 Mitarbeitern bzw. einem Umsatz über einer Million Euro ausgewählt. Somit wurde (analog zur Studie 2007) von einer Referenzgröße von ca. 65.000 zu berücksichtigenden deutschen Unternehmen ausgegangen. Bei den Schadenssummen wurde jeweils nur ein Mittelwert angenommen, also z.B. 55.000 Euro bei der Kategorie von 10.000 bis 100.000 Euro.

Für die Hochrechnung des Gesamtschadens auf die zu referenzierenden 65.000 Unternehmen wurde der Gesamtschaden von ca. 8,4 Milliarden Euro noch einmal um 50 Prozent bereinigt, weil davon auszugehen ist, dass sich vor allem Unternehmen mit einer erhöhten Sensibilität für Industriespionage an der Studie beteiligten. Unter Bezugnahme auf die erhobenen Schadensfälle und die prozentuale Verteilung der finanziellen Schäden je Unternehmensgröße ist daher – sehr konservativ gerechnet – der deutschen Wirtschaft ein Gesamtschaden von mindestens 4,2 Milliarden Euro entstanden.

Insgesamt hatten 82,9 Prozent der geschädigten Unternehmen einen finanziellen Schaden zu verzeichnen. Dies stellt einen Anstieg um 28,7 Prozent dar (Studie 2007: 64,4 Prozent).

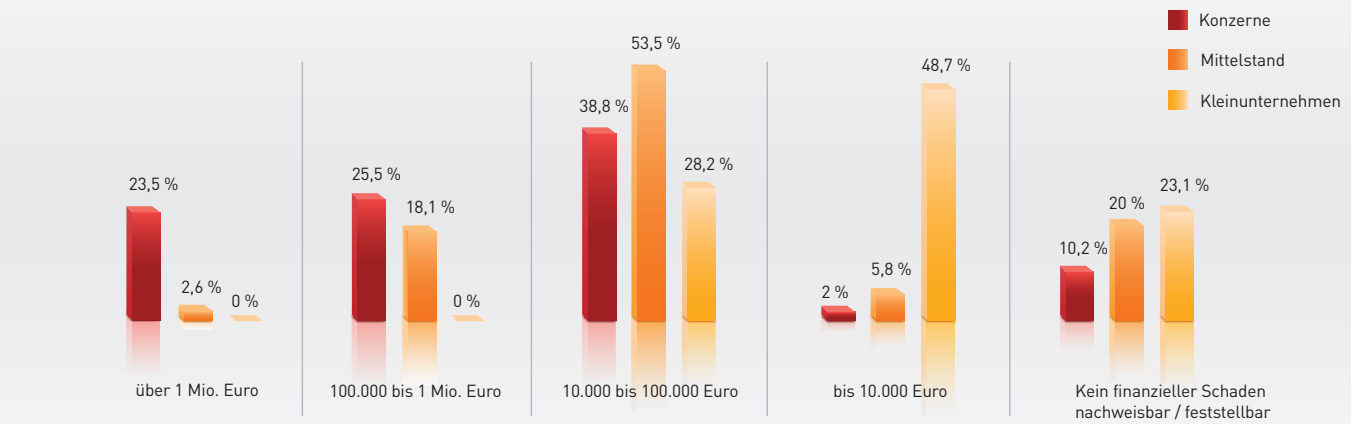
Am deutlichsten fällt der Anstieg bei der Schadenshöhe im Bereich zwischen 10.000 und 100.000 Euro aus: Hier verdreifachten sich die Schäden von 14,3 Prozent (2007) auf 45,3 Prozent (2012). Auch die Schäden über einer Million Euro stiegen von 7,2 Prozent (Studie 2007) auf 9,1 Prozent (Studie 2012) an. Lediglich die Schäden bis 10.000 Euro sanken von 21,7 Prozent (2007) auf 10,4 Prozent (2012).

Interessant war auch, dass bei der Differenzierung der Schäden nach Unternehmensgröße die Kleinbetriebe nur Schäden bis maximal 100.000 Euro feststellten, die finanziellen Negativauswirkungen im Mittelstand vor allem im Bereich von 10.000 bis 100.000 Euro lagen (53,5 Prozent) und 23,5 Prozent der geschädigten Konzerne auch im Bereich über einer Million Euro Schäden bezifferten.

Die starke Veränderung bei den finanziellen Schäden der Unternehmen ist zum Teil auf das veränderte Bedrohungsspektrum – Stichwort „Cyberwar" – zurückzuführen, vermutlich jedoch auch auf eine veränderte Wahrnehmung von Industriespionage. Ein gesteigertes Bewusstsein für Risiken und die Notwendigkeit von Informationsschutz führt zwangsläufig zu einer stärkeren Sensibilisierung für die Auswirkungen.

Heute existieren in vielen Unternehmen mehr Sicherheitsvorkehrungen in der IT sowie bei der Qualitätssicherung mit Kunden und Lieferanten. Hackerattacken, unberechtigte Datenzugriffe oder neue Konkurrenten mit identischen Produkten werden daher schneller als Spionage identifiziert und die Schäden erkannt.

Schäden nach Unternehmensgröße

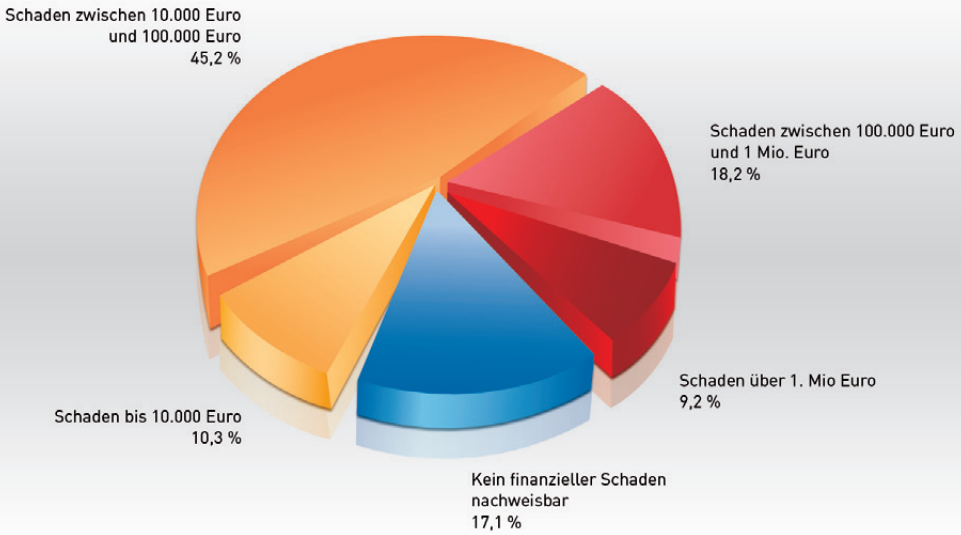


GRAFIK 11

Quelle: Corporate Trust 2012

Schäden durch Spionage

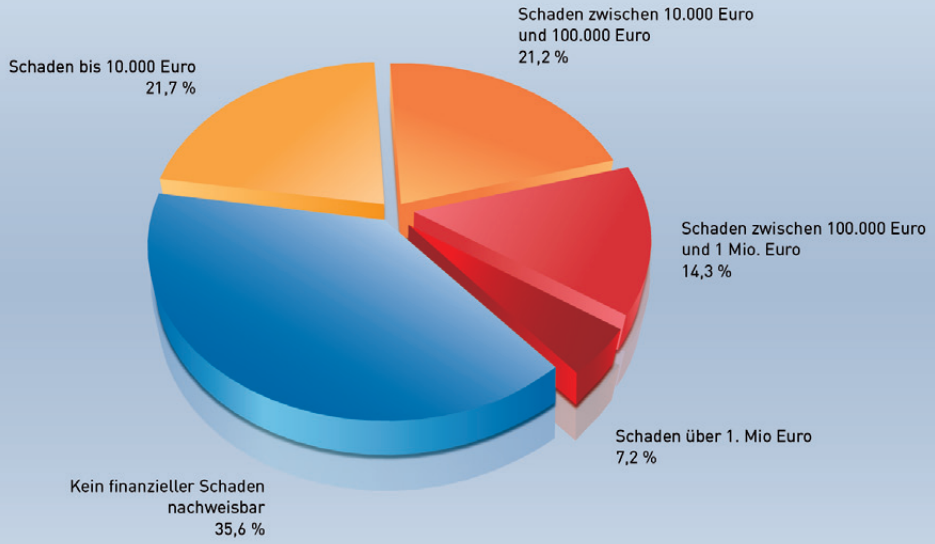
Kann der Schaden durch Spionage finanziell beziffert werden?



GRAFIK 12

Quelle: Corporate Trust 2012

Stand: 2007



Quelle: Studie Industriespionage 2007

Industriespionage geschieht am häufigsten im Vertrieb, gefolgt von Forschung & Entwicklung sowie Mergers & Acquisitions

Bei der aktuellen Befragung wurde der Vertrieb mit 18,3 Prozent von den betroffenen Unternehmen abermals am häufigsten als Angriffsziel für Industriespionage genannt; bereits 2007 war dies der am stärksten betroffene Bereich. Wie nicht anders erwartet, ist Forschung & Entwicklung mit 16,0 Prozent der zweitgefährdetste Bereich, gefolgt von Mergers & Acquisitions mit 14,2 Prozent aller Angriffe sowie IT-Administration und IT-Service mit 12,7 Prozent.

Forschung & Entwicklung war 2007 mit 16,1 Prozent ebenfalls der am zweithäufigsten betroffene Bereich, jedoch war damals Mergers & Acquisitions mit 3,7 Prozent der Bereich, in dem am wenigsten spioniert wurde. Dies hat sich offenbar stark verändert und belegt, dass die strategischen Pläne eines Unternehmens (vor allem im Hinblick auf Expansionsziele und potenzielle Übernahmekandidaten) zu den interessantesten Informationen für Spionage gehören.

Alle Angaben im Freitext zu „Sonstiges" (3,3 Prozent) bezogen sich fast ausschließlich auf Kunden- oder Lieferantendaten. Hier scheint es so, dass diese Informationen von den Unternehmen nicht eindeutig dem Bereich Vertrieb oder Einkauf zugeordnet werden konnten. Wahrscheinlich handelt es sich hier bei den Schadensfällen überwiegend um Vorkommnisse, bei denen Mitarbeiter das Unternehmen verließen und Kunden- oder Lieferantendaten mitnahmen.

Interessant ist auch, dass nur noch 8,6 Prozent der geschädigten Unternehmen keine Angaben darüber machen konnten oder wollten, in welchem Bereich spioniert wurde; bei der Befragung 2007 waren es immerhin noch 20,8 Prozent. Dies ist vermutlich ein Beleg dafür, dass Unternehmen bereits mehr und bessere Sicherheitsvorkehrungen implementiert haben, die es ihnen ermöglichen, einen Informationsabfluss zu erkennen.

In welchem Bereich wurde spioniert bzw. fand der Informationsabfluss statt?
(Mehrfachnennungen möglich)

GRAFIK 13

Quelle: Corporate Trust 2012

Schäden durch Spionage

Schäden entstehen vor allem durch eigene Mitarbeiter sowie externe Geschäftspartner und Hackerangriffe.

Weiterhin stellen die eigenen Mitarbeiter eines der größten Risiken für Unternehmen dar. Bei der Befragung zu den konkreten Handlungen wurde unterschieden zwischen bewusster Informationsweitergabe bzw. dem Datendiebstahl für eigene Zwecke und dem fahrlässigen Informationsabfluss, z.B. bei der Handhabung von Daten, im Umgang mit Geräten oder durch Social Engineering[1].

Dabei stellte sich heraus, dass 47,8 Prozent der konkret festgestellten Spionagefälle auf die bewusste Informations- oder Datenweitergabe bzw. den Datendiebstahl durch eigene Mitarbeiter zurückzuführen sind. Nicht wesentlich geringer war die Häufigkeit beim Abfluss von Daten durch externe Dritte wie Zulieferer, Dienstleister oder Berater: 46,8 Prozent der geschädigten Unternehmen gaben an, hierdurch ausspioniert worden zu sein. Hackerangriffe erreichen mit 42,4 Prozent ebenfalls noch eine sehr hohe Schadensquote.

Bei der Frage nach den konkreten Handlungen waren Mehrfachnennungen erlaubt. Dadurch war es für die Unternehmen möglich, sowohl die Handlungen mehrerer einzelner Industriespionage-Vorfälle zu benennen als auch verschiedene Handlungen bei nur einem Angriff anzugeben. Von dieser Option machten viele der geschädigten Unternehmen Gebrauch.

Die Angriffsqualität bei Industriespionage verändert sich; sogenannte APT (Advanced Persistant Threats), also Angriffe durch eine fortgeschrittene und andauernde Bedrohung, nehmen deutlich zu. Dadurch stellen die Unternehmen heute oftmals kombinierte Schadenshandlungen fest. Bei einem Hackerangriff ist es umso leichter, in die Systeme einzudringen, je mehr internes Wissen über das Unternehmen bekannt ist. Daher gibt es in Verbindung mit einem solchen Hackerangriff[2] häufig auch erkannte Social Engineering-Anrufe bzw. detektierte Versuche, auf die E-Mail-Kommunikation zuzugreifen oder Telefone zu manipulieren.

Welche konkreten Handlungen fanden statt?
(Mehrfachnennungen möglich)

GRAFIK 14

Quelle: Corporate Trust 2012

1)Social Engineering: Ausspionieren über das persönliche Umfeld, durch zwischenmenschliche Beeinflussung bzw. durch geschickte Fragestellung, meist unter Verschleierung der eigenen Identität (Verwenden einer Legende). Social Engineering hat das Ziel, unberechtigt an Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen.

2)Hackerangriff: Unerlaubtes Eindringen in fremde Computer- oder Netzwerksysteme, meist durch das Überwinden von Sicherheitsmechanismen.

Technische Angriffe sind noch immer ein gebräuchliches Mittel, um an sensible Informationen zu gelangen.

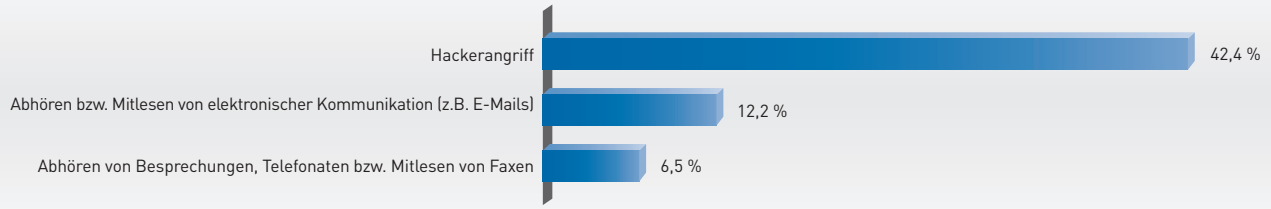
Bei der Durchführung der aktuellen Befragung wurde Wert darauf gelegt, vergleichbare Aussagen zur Studie 2007 zu erhalten, um hierdurch die Entwicklung von Industriespionage zu erkennen.

Während 2007 nur bei 14,9 Prozent aller Fälle ein Hackerangriff[2] als konkrete Spionagehandlung zugrunde lag, waren es 2012 bereits 42,4 Prozent. Die Schäden durch Hackerangriffe haben sich damit annähernd verdreifacht.

In Bezug auf das Abhören von Telefonaten, bzw. das Mitlesen von Faxen oder E-Mails ist die Entwicklung nicht ganz so drastisch. Für die Auswertung wurden die konkreten Handlungen „Abhören und Mitlesen von elektronischer Kommunikation, z.B. E-Mails" (12,2 Prozent) und „Abhören von Besprechungen, Telefonaten bzw. das Mitlesen von Faxen" (6,5 Prozent) zusammengefasst. Diese Vorkommnisse wurden damit in insgesamt 18,7 Prozent aller Fälle festgestellt, spielen also in fast jedem fünften Fall von Industriespionage eine Rolle.

Vergleicht man die Ergebnisse mit der Studie 2007, so muss man auch dort die beiden Formen „Belauschen von vertraulichen Besprechungen" (10,7 Prozent) und „Abhören von Telefonaten bzw. Mitlesen von Faxen oder E-Mails" (5,3 Prozent) zusammenfassen. Hieraus ergibt sich eine Gesamthäufigkeit von 16,0 Prozent. Im Vergleich zur aktuellen Studie beläuft sich damit der Anstieg bei dieser technischen Form von Spionage auf 2,7 Prozent.

Schäden durch klassische Angriffsformen



GRAFIK 15

Quelle: Corporate Trust 2012

Stand: 2007

Quelle: Studie Industriespionage 2007

Schäden durch Spionage

Rechtsstreitigkeiten und Imageschäden bei Kunden oder Lieferanten sind die häufigsten Folge von Industriespionage.

Die Folgen von Spionage können unterschiedliche Auswirkungen haben. Oftmals ist ein Informationsabfluss feststellbar, ohne dass unmittelbar ein Zusammenhang mit einem konkreten Schaden erkannt wird. Dieser kann sich zum einen erst wesentlich später einstellen (z.B. wenn ein Mitbewerber mit dem gestohlenen Know-how plötzlich billigere Plagiate anbietet), zum anderen können aber auch die sofort eingeleiteten rechtlichen Schritte verhindern, dass bei einem Konkurrenten überhaupt ein Vorteil entsteht. Für ein Unternehmen ist trotzdem ein Schaden entstanden, weil auch die Auseinandersetzung mit dem Fall Kapazitäten bindet.

Befragt nach der konkreten Schädigung bei den Fällen von Spionage bzw. dem Verdacht, gaben 65,4 Prozent der Unternehmen an, dass sie hohe Kosten für Rechtsstreitigkeiten hatten. An zweiter Stelle (59,9 Prozent) wurden Imageschäden bei Kunden oder Lieferanten genannt, gefolgt von Patentrechtsverletzungen (44,2 Prozent) und Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen (36,0 Prozent).

Auffallend ist dabei, dass zwar nur etwa ein Drittel aller Unternehmen durch die Industriespionage Umsatzeinbußen registrierte, jedoch fast 60 Prozent Imageschäden bei Kunden oder Lieferanten verzeichneten. Die Angst der Firmen vor einem Reputationsschaden ist also berechtigt. Kunden oder Lieferanten reagieren negativ, wenn der Verdacht besteht, dass vertrauliche Daten abgeflossen sind.

Interessant war bei dieser Frage, dass nur annähernd jedes fünfte Unternehmen einen Ausfall bzw. eine Schädigung von IT-Geräten verzeichnete. Dies ist vermutlich darauf zurückzuführen, dass die Angriffe bei Industriespionage in der Regel gegen die „Vertraulichkeit" der Daten gerichtet sind und weniger gegen die „Verfügbarkeit" von Informationen oder EDV-Systemen.

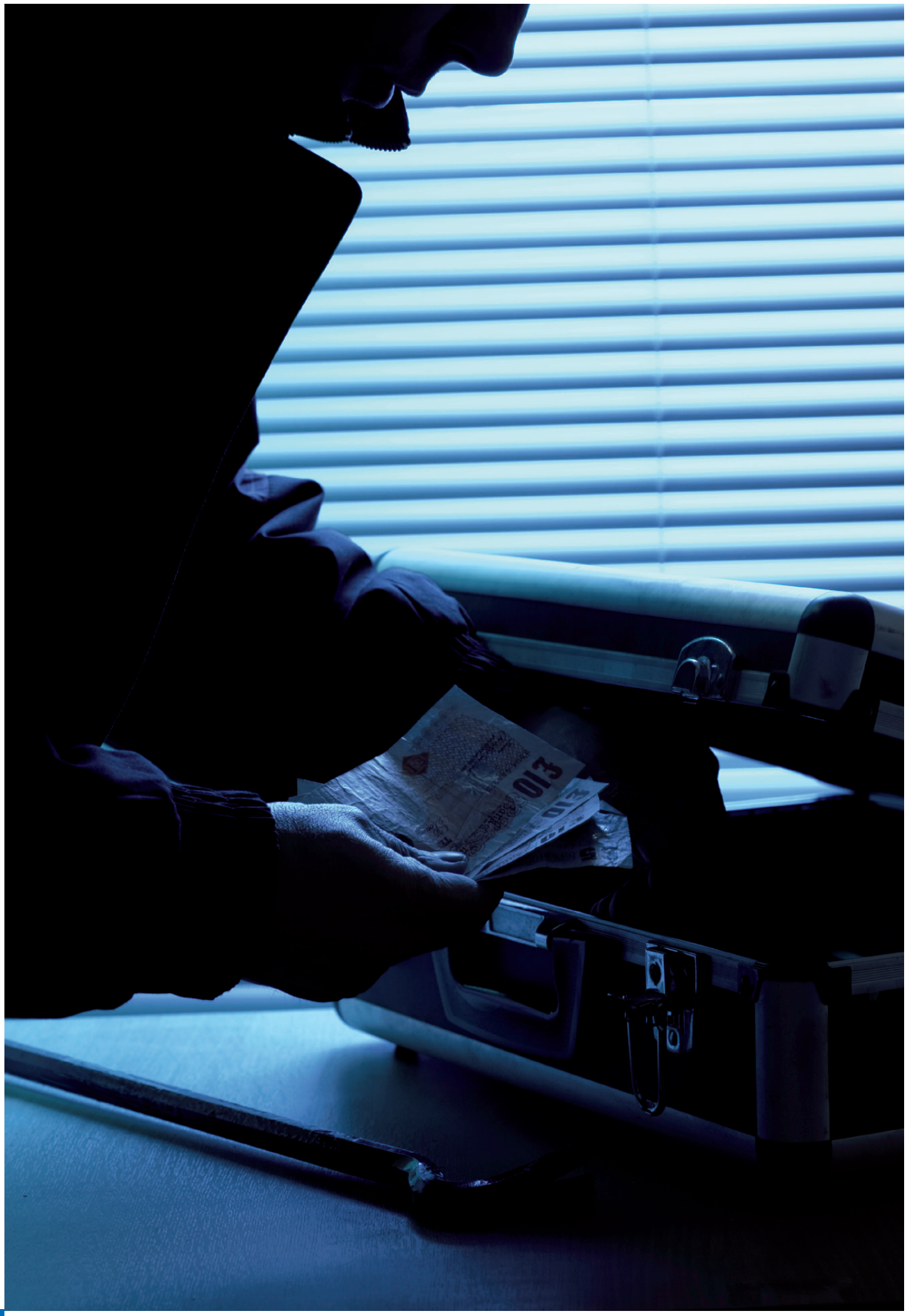
Gab es Hinweise auf eine konkrete Schädigung (materiell / immateriell) für das Unternehmen?
(Mehrfachnennungen möglich)

GRAFIK 16

Quelle: Corporate Trust 2012

Ohne Sicherheit vermag der Mensch weder seine Kräfte auszubilden noch die Frucht derselben zu genießen; denn ohne Sicherheit ist keine Freiheit

Wilhelm von Humboldt



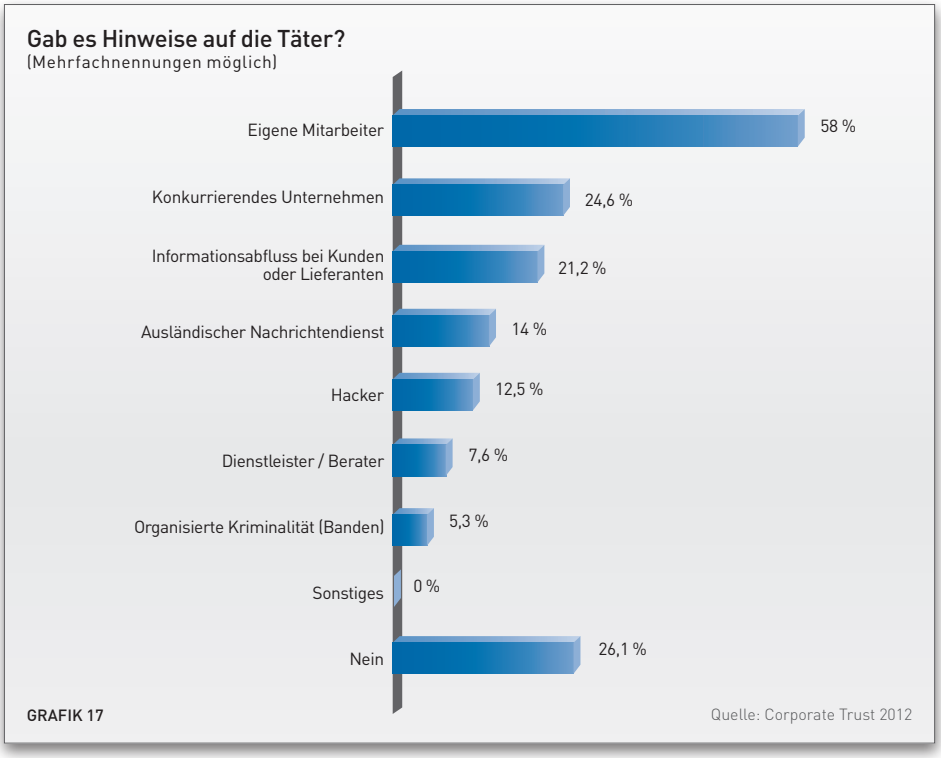
Die Täter

In den meisten Fällen sind eigene Mitarbeiter an der Spionage beteiligt.

Bei Industriespionage fällt es den Unternehmen oft schwer, sofort und eindeutig einen Täter zu identifizieren. Häufig sind intensive forensische EDV-Auswertungen und weitere Ermittlungen nötig, um Hinweise auf die Verdächtigen zu erhalten. Die Erfahrung hat gezeigt, dass in vielen Fällen externe Täter mit internen Mitarbeitern zusammenarbeiten oder durch Social Engineering[1] versuchen, über achtlose Mitarbeiter an interne Informationen zu gelangen. Teilweise genügt es ihnen schon, dabei sogenannte Soft Skills[2] herauszufinden, die es dann ermöglichen, Passwörter zu generieren oder gezielt einen Angriff auf ein bestimmtes System vorzubereiten. Mitarbeiter können aber auch dadurch zu Tätern werden, dass sie Datengeräte wie Laptops, Smartphones oder Tablets verlieren bzw. allzu arglos bei der Weitergabe von Daten verfahren.

Sie können also sowohl mittelbare Täter sein, indem sie von externen Angreifern „abgeschöpft"[3] werden oder leichtfertig mit Daten umgehen, als auch böswillige Täter. Bei letzterem werden in der Regel gezielt Informationen beim eigenen Arbeitgeber kopiert, um damit zu einem Konkurrenten zu wechseln, sich selbstständig zu machen oder sie für hohe Beträge an Konkurrenten oder ausländische Nachrichtendienste zu verkaufen.

Bei dieser Studie konnten die Unternehmen daher mehrfach ankreuzen, wen sie als Täter identifizierten. Erschreckend ist, dass eigene Mitarbeiter das größte Bedrohungspotenzial für Unternehmen darstellen: Sie waren in 58,0 Prozent aller Fälle an der Industriespionage beteiligt – mittelbar als arglose Gehilfen oder unmittelbar als böswillige Täter. Konkurrierende Unternehmen stellen mit 24,6 Prozent die zweithäufigste Tätergruppe dar; Kunden oder Lieferanten, bei denen der Informationsabfluss passierte, waren mit 21,2 Prozent ebenfalls ein sehr häufiger Täterkreis. Die ausländischen Nachrichtendienste und Hacker hingegen scheinen nach Aussage der Unternehmen bei Industriespionage nicht so sehr ins Gewicht zu fallen.



1)Social Engineering: Ausspionieren über das persönliche Umfeld, durch zwischenmenschliche Beeinflussung bzw. durch geschickte Fragestellung, meist unter Verschleierung der eigenen Identität (Verwenden einer Legende). Social Engineering hat das Ziel, unberechtigt an Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen.

2)Soft Skills: Soziale Kompetenz; die Gesamtheit der persönlichen Fähigkeiten und Einstellungen, die dazu beitragen, individuelle Handlungsziele mit den Einstellungen und Werten einer Gruppe zu verknüpfen und in diesem Sinne auch das Verhalten und die Einstellungen von Mitmenschen zu beeinflussen.

3)Abschöpfen: Gezieltes Gewinnen von Informationen, oftmals ohne dass der Mensch gegenüber weiß, dass er als Datenquelle benutzt wird oder unter Verwendung einer Legende.

Aufklärung der Vorfälle

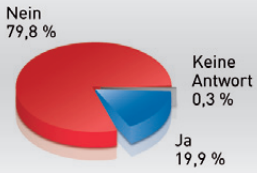
Bei Industriespionage werden vor allem externe Computerspezialisten mit der Aufklärung beauftragt.

Die Aufklärungsbemühungen der deutschen Wirtschaft sind in den letzten Jahren deutlich angestiegen. Schalteten 2007 nur 38,5 Prozent der Unternehmen externe Sicherheitsspezialisten mit ein, so sind es 2012 bereits 57,6 Prozent. Diese Steigerung um 49,6 Prozent gegenüber der letzten Studie ist zwar erfreulich, spiegelt sich aber leider nicht bei der Meldebereitschaft an öffentliche Stellen wieder. Danach befragt, ob bei einem Vorfall oder Verdacht auf Industriespionage der Verfassungsschutz oder die Ermittlungsbehörden eingeschaltet wurden, gaben nur 19,9 Prozent der Unternehmen an, dies getan zu haben. Dies entspricht im Vergleich zur Studie 2007 (26,1 Prozent) sogar einem leichten Rückgang.

Anscheinend ist die Angst der Unternehmen immer noch zu hoch, dass durch das Einschalten der Behörden der Vorfall automatisch an die Öffentlichkeit gelangen und damit ein Reputationsschaden entstehen könnte. Leider haben viele Unternehmen noch nicht erkannt, dass gerade der Verfassungsschutz großes Know-how bei der Bekämpfung von Wirtschaftsspionage hat, nicht dem Legalitätsprinzip unterliegt, damit Straftaten nicht automatisch verfolgen muss und daher sehr stark im Sinne des Unternehmens handeln kann. Die neuen Bedrohungen durch Cyberwar werden mittel- bis langfristig nur in den Griff zu bekommen sein, wenn Wirtschaft und Behörden zusammenarbeiten. Dies bedeutet auch, dass es einen vermehrten Informationsaustausch geben muss und Vorfälle den Behörden gemeldet werden sollten.

Auf die Frage, welche externen Sicherheitsspezialisten eingeschaltet wurden, gaben 47,6 Prozent an, dass nach einem Vorfall oder Verdacht Computerspezialisten die Systeme geprüft hätten. Dies zeigt, dass sich die deutsche Wirtschaft bereits auf die zunehmenden Angriffe einstellt und heute viel öfter versucht, die Vorfälle umfassend aufzuklären. Auch forensische Ermittler, die den Vorfall intern und extern aufklären sollten, wurden fast bei einem Drittel aller Fälle hinzugezogen. Selbst Spezialisten zum Abhörschutz, die einen Sweep[1] zur Absuche nach Wanzen durchführten, kamen bei jedem zehnten Fall von Industriespionage zum Einsatz.

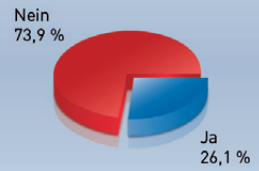
Wurden der Verfassungsschutz oder die Ermittlungsbehörden eingeschaltet?



GRAFIK 18

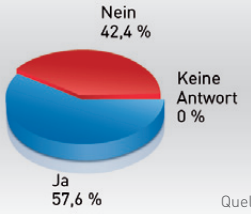
Quelle: Corporate Trust 2012

Stand: 2007



Quelle: Studie Industriespionage 2007

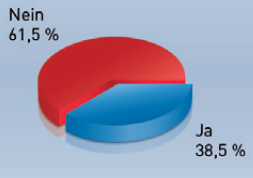
Wurden externe Sicherheitsspezialisten eingeschaltet?



GRAFIK 19

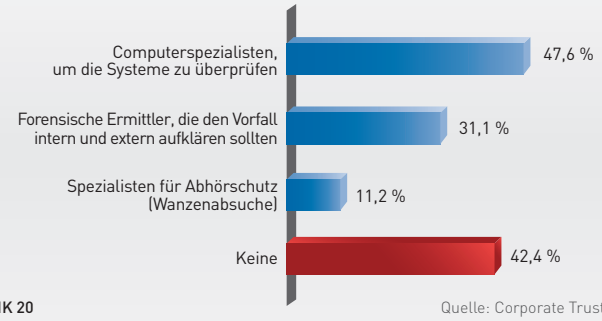
Quelle: Corporate Trust 2012

Stand: 2007



Quelle: Studie Industriespionage 2007

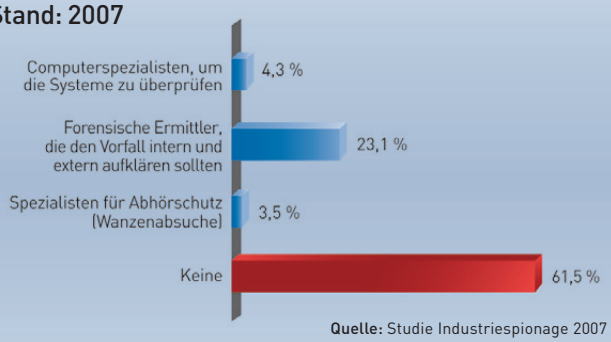
Welche externen Sicherheitsspezialisten wurden eingeschaltet?
(Mehrfachnennungen möglich)



GRAFIK 20

Quelle: Corporate Trust 2012

Stand: 2007



Quelle: Studie Industriespionage 2007

1)Sweep: Absuche nach Wanzen mit technischen Geräten durch Hochfrequenz-Spezialisten. Dient in der Regel der Lauschabwehr.

Sicherheitsvorkehrungen im Unternehmen

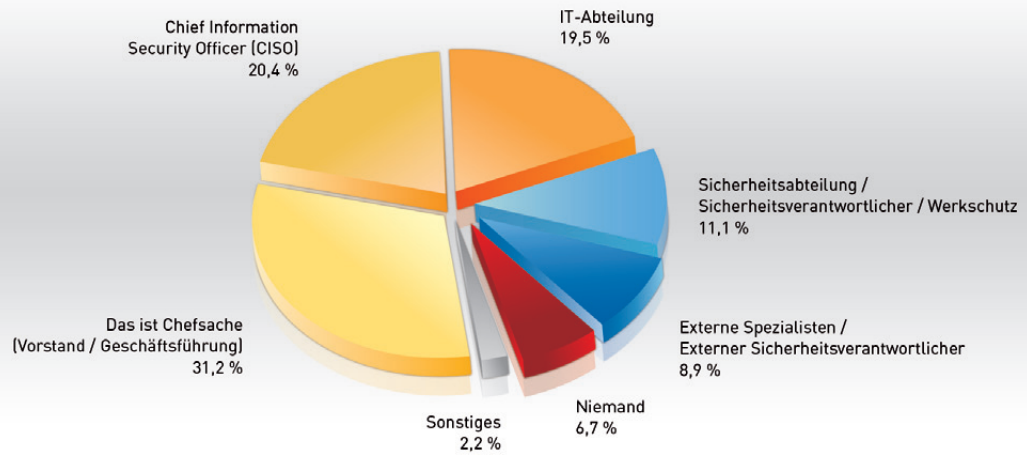
Allgemein

Bereits die Hälfte aller Unternehmen haben den Informationsschutz zur Chefsache erklärt bzw. einen Chief Information Security Officer (CISO) etabliert.

Sicherheit und speziell der Informationsschutz sollten Chefsache sein. Die Aufgaben sind übergreifend und umfassend, sodass ein Entscheider möglichst Zugriff auf alle Bereiche haben sollte. In vielen Unternehmen ist dies daher Aufgabe der Geschäftsleitung oder es wird eine Stabsstelle Chief Information Security Officer (CISO) geschaffen. Dieser soll sich ausschließlich um den Informationsschutz im Unternehmen kümmern. Allerdings sollte die Position nicht der IT unterstellt sein, weil gerade hier eine Unabhängigkeit bestehen müsste, um auch IT-Prozesse hinterfragen und bei Bedarf Änderungen durchsetzen zu können. Neben IT-Themen können bei einem umfassenden Informationsschutz aber auch die Ablauforganisation, der Bereich Personal, das Facility Management oder der Vertrieb tangiert sein.

In deutschen Unternehmen wird dies als entsprechend wichtiges Thema wahrgenommen. Bei 31,2 Prozent aller Firmen ist der Informationsschutz bereits zur Chefsache erkoren. Dies erklärt auch die ungewöhnlich hohe Beteiligung von Vorständen und Geschäftsführern (48,9 Prozent) an der Befragung (siehe Methodik). Zusammen mit den Chief Information Security Officers – bei der Befragung gaben immerhin 20,4 Prozent an, eine solche Stelle eingerichtet zu haben – gehen damit mehr als die Hälfte aller deutschen Unternehmen den richtigen Weg zum Schutz ihrer vertraulichen Daten. Nicht verwunderlich ist, dass auch die IT-Abteilungen bei annähernd jedem fünften Unternehmen für den Schutz des kritischen Know-how verantwortlich sind. Daten und Informationen werden allzu oft mit IT oder EDV-Systemen gleichgesetzt. Interessant ist in diesem Zusammenhang, dass nur 11,1 Prozent der Firmen den Sicherheitsabteilungen bzw. dem Sicherheitsverantwortlichen oder dem Werkschutz den Informationsschutz anvertrauen.

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



GRAFIK 21

Quelle: Corporate Trust 2012

Sicherheitsvorkehrungen im Unternehmen

Allgemein

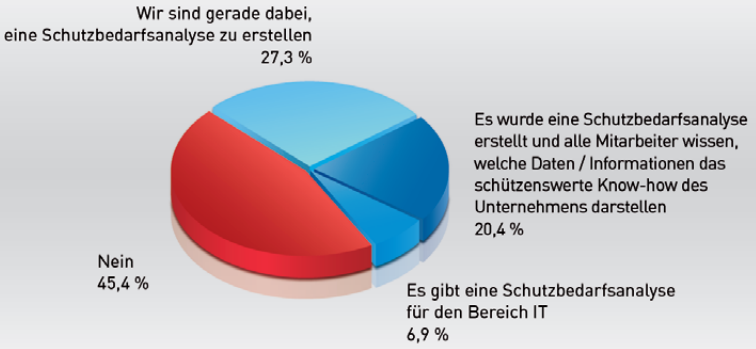
Nur jedes fünfte Unternehmen in Deutschland hat klar definiert, welches Know-how schützenswert ist.

Zu wenig Sicherheit ist gefährlich und erhöht das Risiko wirtschaftlicher Schäden, während zu viel Sicherheit teuer und unwirtschaftlich ist. Für alle Sicherheitsmaßnahmen müssen also unternehmerisches Risiko und Gesamtkosten gegeneinander abgewogen werden. Ein professioneller Informationsschutz unterscheidet verschiedene Sicherheitsstufen, die bedarfsgerecht durch Sicherheitsmaßnahmen geschützt werden. Anstatt generell alles zu schützen, werden die Schutzmaßnahmen an die Vertraulichkeit der Informationen angepasst. Dazu benötigt ein Unternehmen eine klare Regelung, welche Informationen geheim, vertraulich oder offen zugänglich sind. Idealerweise eignet sich hierfür eine Schutzbedarfsanalyse, um für unterschiedlichste Informationen den individuellen Bedarf herauszuarbeiten.

Leider hat nur etwa jedes fünfte Unternehmen in Deutschland (20,4 Prozent) eine umfassende Schutzbedarfsanalyse erstellt. Ein weiteres Viertel (27,3 Prozent) hat die Wichtigkeit des Themas erkannt und ist dabei, eine Schutzbedarfsanalyse zu erstellen. In 6,9 Prozent wurde eine Schutzbedarfsanalyse speziell für den Bereich IT erstellt – meist ist in diesem Bereich der Leidensdruck, Sicherheitsinvestitionen sinnvoll steuern zu können, besonders hoch.

Generell ist aber der Status Quo dieses Themas sehr unbefriedigend. Wie sollen Mitarbeiter wissen, wie in Zeiten von sozialen Netzwerken und Social Engineering mit wettbewerbsentscheidendem Know-how umzugehen ist, wenn gar nicht klar ist, welche Informationen überhaupt wettbewerbsentscheidend sind? Wie kann ein Unternehmen festlegen, an welchen Stellen sich der hohe Aufwand für eine Verteidigung gegen Industriespionage lohnt, wenn gar nicht klar ist, was die wichtigen „Kronjuwelen" sind?

Gibt es in Ihrem Unternehmen eine Schutzbedarfsanalyse, die klar und für alle Mitarbeiter unmissverständlich regelt, welche Daten / Informationen geheim, vertraulich oder offen zugänglich sind?



GRAFIK 22

Quelle: Corporate Trust 2012

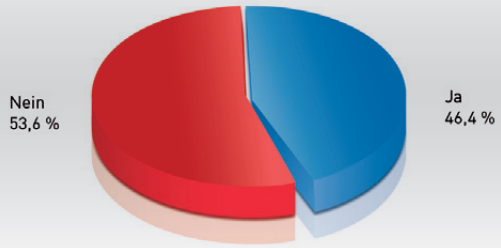
Über die Hälfte aller Unternehmen besitzt keine Sicherheits-Policy mit klaren Regeln für den Informationsschutz.

Weil zu wenig Sicherheit fahrlässig ist, sollten Sicherheitsmaßnahmen immer nur wirklich bedarfsgerecht eingesetzt werden. Die Sicherheits-Policy eines Unternehmens, oftmals auch Sicherheitsleitlinie genannt, soll den angestrebten Sicherheitsanspruch beschreiben. Darin wird geregelt, welche Maßnahmen getroffen werden und wie das sensible Unternehmens-Know-how zu schützen ist. Eine solche Sicherheits-Policy ist damit ein maßgebliches Steuerungsinstrument hin zu einer bedarfsgerechten Sicherheit.

Wichtig ist, dass eine solche Sicherheits-Policy allen Mitarbeitern bekannt ist und Verstöße entsprechend geahndet werden. Bislang haben lediglich 46,4 Prozent aller Unternehmen eine solche Sicherheits-Policy, über die Hälfte (53,6 Prozent) verzichtet darauf, diese Leitlinie in ihrem Betrieb einzuführen.

Basierend auf der Auswertung der Frage nach einer Schutzbedarfsanalyse verwundert dieses Ergebnis kaum. Die Aufstellung einer Sicherheits-Policy ohne eine Schutzbedarfsanalyse gleicht einem Blindflug. Interessant ist allerdings der Querbezug zur Frage nach der Verantwortlichkeit im Informationsschutz, da die Sicherheits-Policy in gewisser Weise den Auftrag dieser Position definiert. In vielen Unternehmen wird also die Sicherheitsverantwortung eher aus dem Bauch heraus wahrgenommen. Da solche Entscheidungen von den Mitarbeitern oft nicht nachvollzogen werden können, wird Sicherheit meist als Gängelung wahrgenommen. Eine fehlende bzw. ungenügend kommunizierte Sicherheits-Policy führt dazu, dass Mitarbeiter die Sicherheitsanstrengungen als unnötige Erschwerung ihrer Arbeit empfinden, weshalb sie die einzelnen Maßnahmen umgehen.

Haben Sie für Ihr Unternehmen eine Sicherheits-Policy mit klaren Regelungen für den Informationsschutz, die allen Mitarbeitern bekannt ist?



GRAFIK 23

Quelle: Corporate Trust 2012

Sicherheitsvorkehrungen im Unternehmen

IT

Die IT-Sicherheitsvorkehrungen sind noch nicht ausreichend, um sich im Cyberwar[1] effektiv zu schützen.

9,4 Prozent der Befragten gaben an, dass ihnen die IT-Sicherheitsvorkehrungen des Unternehmens nicht bekannt sind. Klammert man diese Personengruppe aus, haben alle deutschen Unternehmen einen Passwortschutz (90,6 Prozent) und nahezu alle Unternehmen (86,1 Prozent) eine Firewall im Einsatz. Für immerhin die Hälfte der Unternehmen gehören die Verschlüsselung von Netzwerkverbindungen zu Partnern (48,9 Prozent), die Absicherung von Heimarbeitsplätzen und die Verschlüsselung von Daten auf Laptops (jeweils 46,6 Prozent) zum guten Ton. Die breit am Markt verfügbaren Basistechnologien zur Absicherung der IT werden also von den Unternehmen durchaus angenommen.

Diese traditionellen Maßnahmen reichen zur Abwehr von Skriptkiddies[2] auch sicherlich aus. Im Kampf gegen Industriespionage oder gar staatlich gelenkte Hackergruppen[3] ist jedoch mehr erforderlich. Bereits einfachste halborganisatorische Maßnahmen, wie die Beschränkung von Zugriffen aus ausländischen Niederlassungen (21,6 Prozent) oder die regelmäßige Überprüfung zugeteilter Rechte (28,3 Prozent), werden nur selten umgesetzt. Das größte Problem zeigt sich aber in der Überwachung der Log-Daten: Nur 20,9 Prozent der Firmen geben an, ihre IT kontinuierlich – und damit ohne konkreten Anlass – auf Sicherheitsvorfälle zu überprüfen. Die Entdeckung von Informationsabfluss ist damit in den meisten Fällen ein Zufallsfund.

Dass der Einsatz von Biometrie oder Tokens (28,0 Prozent) sowie das Verbot von USB-Sticks und Ähnlichem (18,6 Prozent) oft an der Benutzerakzeptanz scheitert, ist ein altbekanntes Problem. Ähnlich verhält es sich mit der Einführung einer Data Leakage Prevention (18,1 Prozent) oder verschlüsselter E-Mails (18,9 Prozent); hier scheuen die Firmen meist den nicht unerheblichen technischen Aufwand. In diesen Fällen ist die IT-Sicherheitsindustrie gefragt, einfachere und benutzerfreundlichere Lösungen zu präsentieren. Obwohl diese Technologie vergleichsweise jung ist, geben 23,5 Prozent der Befragten an, ein Mobile-Device-Management-System einzusetzen, um die Sicherheitsrisiken durch mobile Geräte wie Smartphones und Tablets im Griff zu behalten.

Erstaunlich niedrig bleibt die Zahl der Zertifizierungen. Gaben 2007 noch 10,7 Prozent der Unternehmen an, nach BSI-Standards zertifiziert zu sein, stieg die Zahl innerhalb von fünf Jahren lediglich auf 13,9 Prozent.

1)Cyberwar: Darunter versteht man die kriegerische Auseinandersetzung im und um den virtuellen Raum, den sog. Cyberspace, mit Mitteln vorwiegend aus dem Bereich der Informationstechnik. Cyberwar bezeichnet auch die Aktivitäten staatlicher Spezialeinheiten, um Gegner oder sonstige Ziele online auszukundschaften bzw. sie im Ernstfall zu sabotieren.

2)Skriptkiddie: Sinnbild für einen stereotypischen Jugendlichen, das sich alltagssprachlich auf den Bereich der Computersicherheit bezieht. Trotz mangelnder Grundlagenkenntnisse nutzt ein Skriptkiddie vorgefertigte Automatismen, um (meist unter schriftlicher Anleitung) in fremde Computersysteme einzudringen oder sonstigen Schaden anzurichten. Die Bezeichnung hat Anklänge von unreifem Verhalten und Vandalismus. Daneben besteht eine weitere Verwendung im Bereich der Computerprogrammierung. Dort nimmt der Begriff Bezug auf eine Person, die fremden Quellcode für eigene Projekte zusammenkopiert, um deren Effekte zu nutzen, ohne jedoch den Code zu verstehen.

3)Hacktivisten: Eine meist lose organisierte Gruppe von Hackern, die versucht, ihre politischen oder ideologischen Ziele durch Angriffe im Internet durchzusetzen.

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

(Mehrfachnennungen möglich)

GRAFIK 24

Quelle: Corporate Trust 2012

Sicherheitsvorkehrungen im Unternehmen

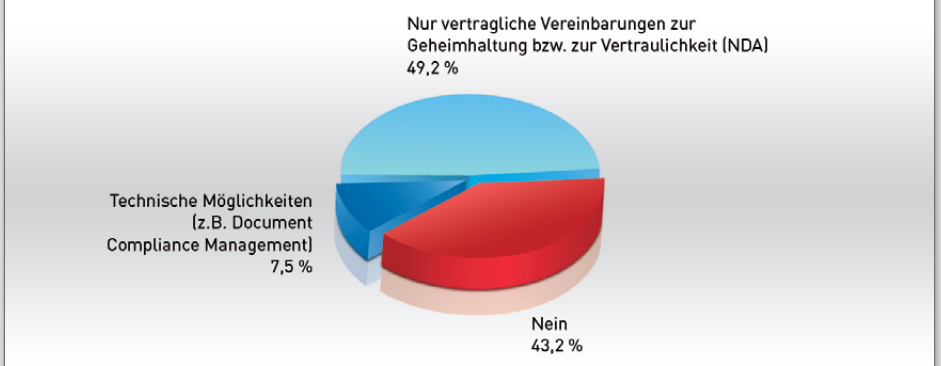
IT

Die wenigsten Unternehmen haben geeignete Sicherheitsvorkehrungen, um den sicheren Datenaustausch mit Externen zu gewährleisten.

43,2 Prozent der deutschen Unternehmen haben keinerlei klare Vereinbarungen mit ihren externen Partnern getroffen, um den sicheren Informationsaustausch zu regeln. Nur etwa die Hälfte aller Unternehmen (49,2 Prozent) gab an, mit externen Geschäftspartnern eine vertragliche Vereinbarung zur Geheimhaltung bzw. Vertraulichkeit[1] getroffen zu haben. Dies ist viel zu wenig, da solche schriftlichen Vereinbarungen das absolute Mindestmaß an Schutz des eigenen Know-how darstellen sollten. Technische Möglichkeiten, z.B. ein Document Compliance Management, setzen sogar nur 7,5 Prozent der deutschen Betriebe ein, um einen sicheren Datenaustausch zu gewährleisten.

Heutzutage werden die meisten vertraulichen Dokumente, wie z.B. Verträge und Finanzdokumente, in digitaler Form bearbeitet und auch ausgetauscht. Insbesondere vertrauliche Dokumente werden aufgrund ihrer Relevanz für das Unternehmen häufig digital mit externen Partnern (wie beispielsweise Steuerberatern, Wirtschaftsprüfern, Rechts- und Patentanwälten oder Kooperationspartnern) ausgetauscht. Ohne technologische Möglichkeiten, wie sie etwa eine Document Compliance Management Lösung bietet, können Unternehmen diese Dokumente weder ausreichend schützen noch deren unkontrollierte Weitergabe verhindern. Hinzu kommt das Risiko, dass beim Einsatz von Standard-E-Mail-Tools vertrauliche Dokumente versehentlich an falsche Empfänger geschickt werden. Generell wird das Thema Compliance und Schutz vertraulicher Dokumente für Unternehmen immer wichtiger. Diesen Trend spiegeln auch neue gesetzliche Regelungen wider, zu denen EHUG[2], GDPdU[3] oder SOX[4] gehören. Technologische Lösungen für Document Compliance Management unterstützen die Umsetzung dieser Auflagen in idealer Weise.

Sind Sicherheits-Policies vorhanden, die Externe mit einbeziehen?



GRAFIK 25 Quelle: Corporate Trust 2012

1)Geheimhaltungsverpflichtung: (auch Vertraulichkeitsvereinbarung) Schriftliche Vereinbarung über den Umgang mit vertraulichen Informationen.
2)EHUG: Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister.
3)GDPdU: Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen.
4)SOX (Sarbanes-Oxley-Act): US-amerikanisches Bundesgesetz, das die Verlässlichkeit der Berichterstattung von Unternehmen, die den öffentlichen Kapitalmarkt der USA in Anspruch nehmen, verbessern soll.

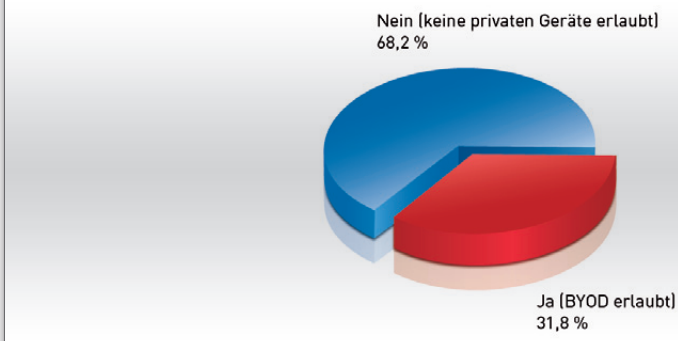
Immer mehr Mitarbeiter setzen ihr privates Mobilgerät auch für Firmenzwecke ein.

Durch die immer stärkere Verbreitung von mobilen Geräten im privaten Bereich müssen sich Unternehmen immer häufiger mit der Frage beschäftigen, wie sie mit dem Einsatz dieser Geräte im Unternehmen umgehen. Während ein Drittel der befragten Unternehmen (31,8 Prozent) den Einsatz erlaubt, verweigern immerhin zwei Drittel (68,2 Prozent) den Einsatz komplett. Dies liegt möglicherweise daran, dass es in den Unternehmen keine klare Vorstellung darüber gibt, wie man private mobile Geräte sinnvoll und gleichzeitig sicher integrieren kann.

Die Innovationswelle, welche durch iPhones und iPads in der IT losgetreten wurde, macht auch vor der Sicherheit nicht Halt. Junge sogenannte High Potentials[5] sind immer weniger bereit, ein restriktiv konfiguriertes Zweitgerät neben dem eigenen iPhone mitzuschleppen und erwarten den Einsatz moderner Tablet-Technologien auch von ihrem Arbeitgeber. Dies erfordert zwar ein Umdenken in der Administration, ist technisch aber kein Problem; ein privates iPhone kann genauso abgesichert werden wie ein firmeneigenes. Im Gegenteil sind geringere Anschaffungskosten, geringerer Supportaufwand und am Ende sogar eine erhöhte Sorgfalt des Mitarbeiters im Umgang mit dem Gerät auch sicherheitstechnisch von Vorteil. Die Probleme, die in diesem Bereich gelöst werden müssen, sind überwiegend rechtlicher Natur. Um ein Beispiel zu geben: Darf der Arbeitgeber das private iPhone eines Mitarbeiters bei dessen Ausscheiden aus der Firma fernlöschen?

Eine komfortable und zugleich sichere Lösung bietet Document Compliance Management. Diese Anwendung ermöglicht es, durch den Einsatz einer „Device Policy" und einer speziellen App für das iPad serverseitig genau festzulegen, welche Geräte auf unternehmenskritische Dokumente zugreifen dürfen. Alle Zugriffe werden genau protokolliert und schränken den Wildwuchs der verwendeten Geräte ein.

Lassen Sie eine BYOD-Strategie (Bring your own device) im Unternehmen zu und ist damit der Einsatz von privaten Mobilgeräten wie iPad, anderen Tablets oder Smartphones erlaubt?



GRAFIK 26 Quelle: Corporate Trust 2012

5)High Potential: Ein Hochschulabsolvent oder junger Berufstätiger (auch „Young Professional" genannt), dem man prinzipiell aufgrund seiner bisherigen Laufbahn zutraut, im Unternehmen schnell Verantwortung zu übernehmen und die Karriereleiter in rasantem Tempo zu erklimmen.

Personal

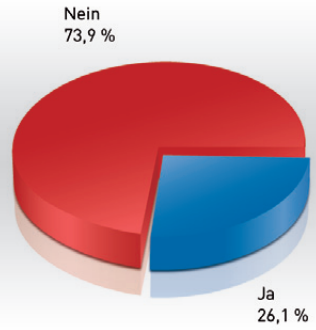
Drei Viertel aller Unternehmen versäumen es, ihre Mitarbeiter auf die Gefahren von Social Engineering vorzubereiten.

Unter Social Engineering versteht man das Ausspionieren oder Ausforschen eines Menschen über das persönliche Umfeld, meist durch zwischenmenschliche Beeinflussung bzw. durch geschickte Fragestellungen. In der Regel verschleiert der Angreifer dabei seine Identität und verwendet stattdessen eine Legende. Social Engineering hat das Ziel, unberechtigt an vertrauliche Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen. Oftmals genügen aber auch schon sog. Soft Skills[1] eines Mitarbeiters, um damit den weiteren Angriff vorbereiten zu können.

Nur 26,1 Prozent der deutschen Unternehmen führen regelmäßig Schulungen für ihre Mitarbeiter durch, um sie für diese Gefahren zu sensibilisieren. Dies bedeutet, fast drei Viertel aller Unternehmen haben ihre Mitarbeiter noch niemals darauf hingewiesen. Dies ist insbesondere deshalb fahrlässig, weil gerade im Zeitalter des zunehmenden Cyberwar[2] von den professionellen Tätern immer öfter „menschliche Quellen" genutzt werden, um ihre Hackerangriffe[3] vorzubereiten. Die Kenntnis über interne Bezeichnungen, Verfahrensabläufe, verwendete IT-Systeme oder Ansprechpartner erleichtert erheblich die Erstellung eines gezielten Trojaners[4] für den Zugang zum Firmennetzwerk.

Mitarbeiter, die wissen welche Gefahren ihnen durch Social Engineering drohen können, sind in der Regel besser darauf vorbereitet und reagieren entsprechend, wenn sie am Telefon, bei einem persönlichen Gespräch mit einem Dienstleister oder auf einer Messe ausgeforscht werden sollen.

Gibt es regelmäßige Schulungen für Mitarbeiter, um sie für die Gefahren von Social Engineering (geschicktes Aushorchen) zu sensibilisieren?



GRAFIK 27

Quelle: Corporate Trust 2012

1)Soft Skills: Soziale Kompetenz; die Gesamtheit der persönlichen Fähigkeiten und Einstellungen, die dazu beitragen, individuelle Handlungsziele mit den Einstellungen und Werten einer Gruppe zu verknüpfen und in diesem Sinne auch das Verhalten und die Einstellungen von Mitmenschen zu beeinflussen.

2)Cyberwar: Darunter versteht man die kriegerische Auseinandersetzung im und um den virtuellen Raum, den sog. Cyberspace, mit Mitteln vorwiegend aus dem Bereich der Informationstechnik. Cyberwar bezeichnet auch die Aktivitäten staatlicher Spezialeinheiten, um Gegner oder sonstige Ziele online auszukundschaften bzw. sie im Ernstfall zu sabotieren.

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

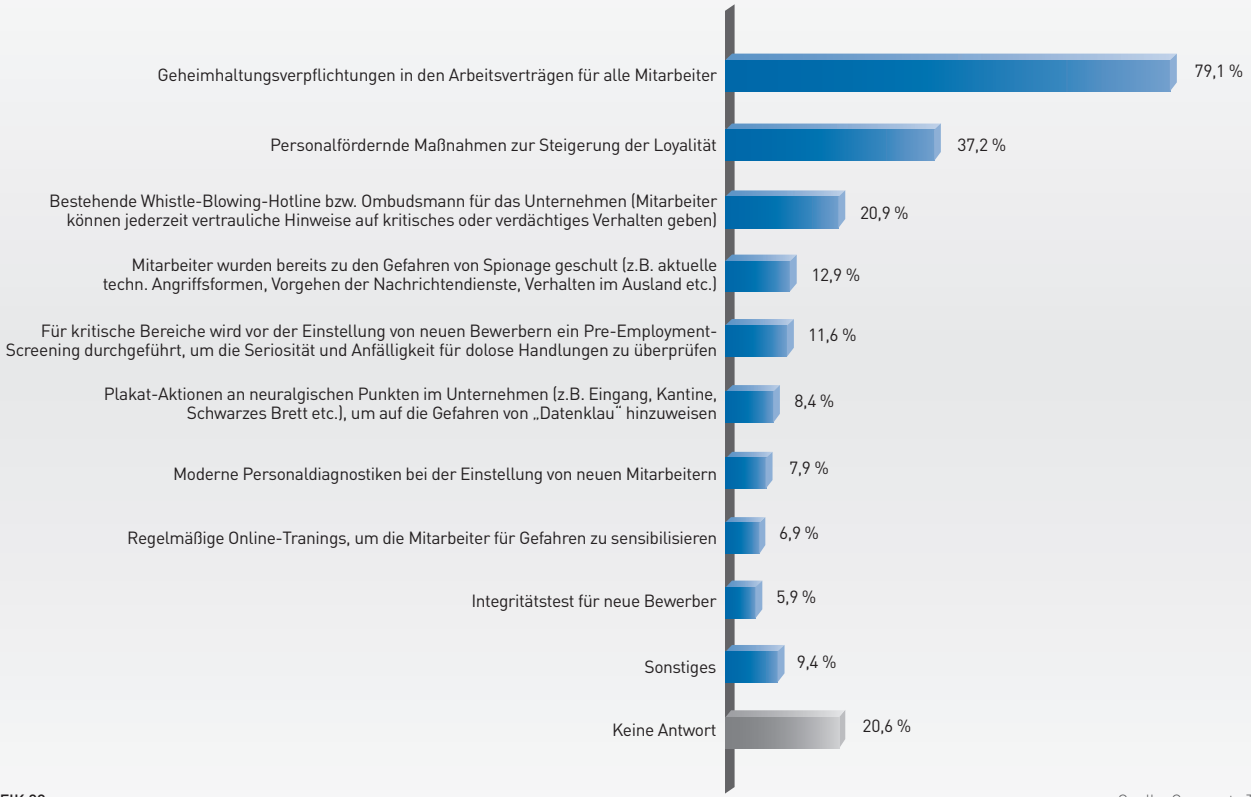
4)Trojaner: Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund jedoch ohne Wissen des Anwenders eine andere Funktion ausführt.

Unternehmen verlassen sich zumeist auf Geheimhaltungsverpflichtungen in den Arbeitsverträgen, die Integrität von neuen Bewerbern wird dagegen nur selten überprüft.

Immerhin haben 79,1 Prozent der befragten Unternehmen Geheimhaltungsverpflichtungen[5] in den Arbeitsverträgen vereinbart, doch einen Integritätstest für neue Bewerber führen leider nur 5,9 Prozent durch; ein Pre-Employment-Screening für Bewerber in kritische Bereichen (von 11,6 Prozent der Unternehmen genannt) gibt es auch viel zu selten. Genau damit würden jedoch „schwarze Schafe" frühzeitig erkannt. Wer in einem sensiblen Bereich arbeitet, wie z.B. Forschung & Entwicklung, Mergers & Acquisitions oder der IT-Abteilung, hat in der Regel Zugriff auf höchst sensible Unternehmensdaten. Hier sollte sichergestellt sein, dass ein neuer Bewerber alle Anforderungen an Seriosität und Zuverlässigkeit erfüllt, bevor er Zugriff auf solches Know-how bekommt.

Personalfördernde Maßnahmen zur Steigerung der Loyalität gaben immerhin noch 37,2 Prozent an. Dies war die am zweithäufigsten genannte Sicherheitsvorkehrung, um einen Datenabfluss (böswillig oder leichtfertig) durch eigene Mitarbeiter zu verhindern. Gerade die Loyalität spielt eine wesentliche Rolle beim Kampf gegen Informationsabfluss. Zum einen sind loyale Mitarbeiter viel weniger bereit, kritisches Unternehmenswissen an Konkurrenten zu verkaufen, zum anderen sind sie viel aufmerksamer, wenn es darum geht, Social Engineering[6] frühzeitig zu erkennen oder vertraulich mit Datengeräten (Laptop, Smartphone, Tablet, Handy etc.) umzugehen.

Welche Sicherheitsvorkehrungen gibt es im Bereich Personal, um sich gegen Spionage oder ungewollten Informationsabfluss zu schützen?
(Mehrfachnennungen möglich)



GRAFIK 28

Quelle: Corporate Trust 2012

5)Geheimhaltungsverpflichtung: (auch Vertraulichkeitsvereinbarung) Schriftliche Vereinbarung über den Umgang mit vertraulichen Informationen.

6)Social Engineering: Ausspionieren über das persönliche Umfeld, durch zwischenmenschliche Beeinflussung bzw. durch geschickte Fragestellung, meist unter Verschleierung der eigenen Identität (Verwenden einer Legende). Social Engineering hat das Ziel, unberechtigt an Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen.

Sicherheitsvorkehrungen im Unternehmen

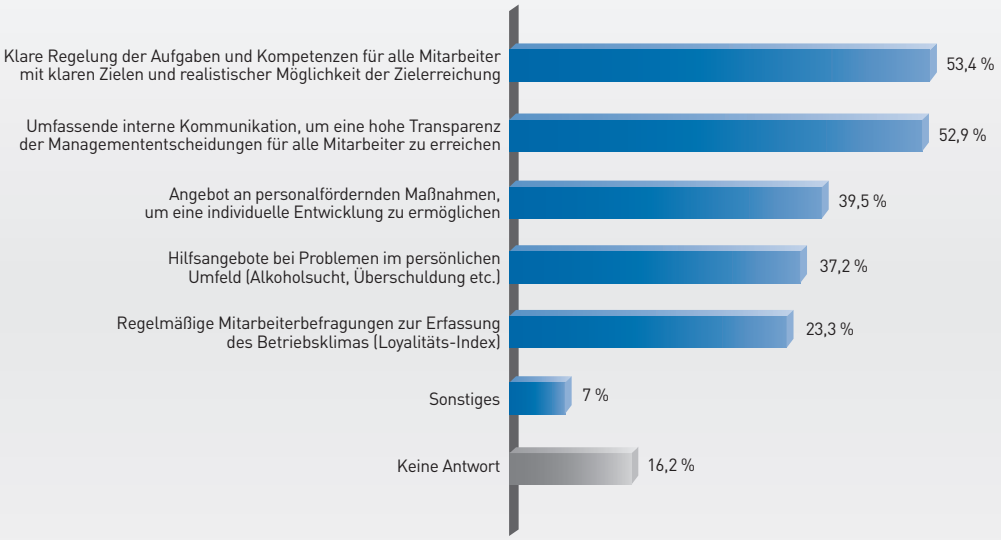
Personal

Nur jedes dritte Unternehmen führt eine regelmäßige Analyse des Betriebsklimas (Loyalitäts-Index) durch.

Zur Loyalität von Mitarbeitern tragen neben der Zufriedenheit mit dem Arbeitsplatz und der Bezahlung auch Faktoren wie Vertrauen in das Unternehmen, Kommunikation untereinander, Konfliktbewältigung, Feedback von Vorgesetzten, Aufstiegsmöglichkeiten oder Zusammenarbeit mit anderen Bereichen bei. Kurz gesagt, das Betriebsklima spielt eine wesentliche Rolle. Diese Unternehmenskultur etabliert sich in einem Unternehmen jedoch nur langfristig. Häufig werden von Führungsverantwortlichen Richtlinien vorgegeben, um die gewünschte Kultur zu erreichen. Dabei ist es wichtig, dass sie entsprechend mit Vorbildfunktion vorangehen und sich selbst an die Regeln halten.

Um zu überprüfen, ob sich dies auch in den Köpfen der Mitarbeiter durchsetzt, ist es ebenso wichtig, regelmäßig abzufragen, wo es Schwachpunkte gibt. Ähnlich einem Arzt, der einen Gesundheits-Check durchführt, muss das Unternehmen analysieren, welche Prozesse die Loyalität der Mitarbeiter fördern oder beeinträchtigen. Leider führt nur etwa ein Drittel aller Unternehmen (34,8 Prozent) einen solchen Loyalitäts-Index[1] durch. Bei der Hälfte aller befragten Firmen existieren zumindest klare Regelungen für die Aufgaben und Kompetenzen der Mitarbeiter (53,4 Prozent) sowie eine umfassende interne Kommunikation (52,9 Prozent). Einen Feedbackbogen zur Bewertung der Vorgesetzten durch die Mitarbeiter gibt es leider nur bei etwa jedem vierten Unternehmen.

Welche Maßnahmen haben Sie getroffen, um die Loyalität der Mitarbeiter zu fördern?
(Mehrfachnennungen möglich)



GRAFIK 29

Quelle: Corporate Trust 2012

1)Loyalitäts-Index: Beurteilung von Unternehmen und Organisationen im Hinblick auf kriminelle und fahrlässige Handlungen von Mitarbeitern. Der Loyalitäts-Index liefert durch eine Mitarbeiterbefragung mit einer psychologisch fundierten Vorgehensweise Parameter, welche auf potenzielle Risiken hinweisen.

Objektsicherheit

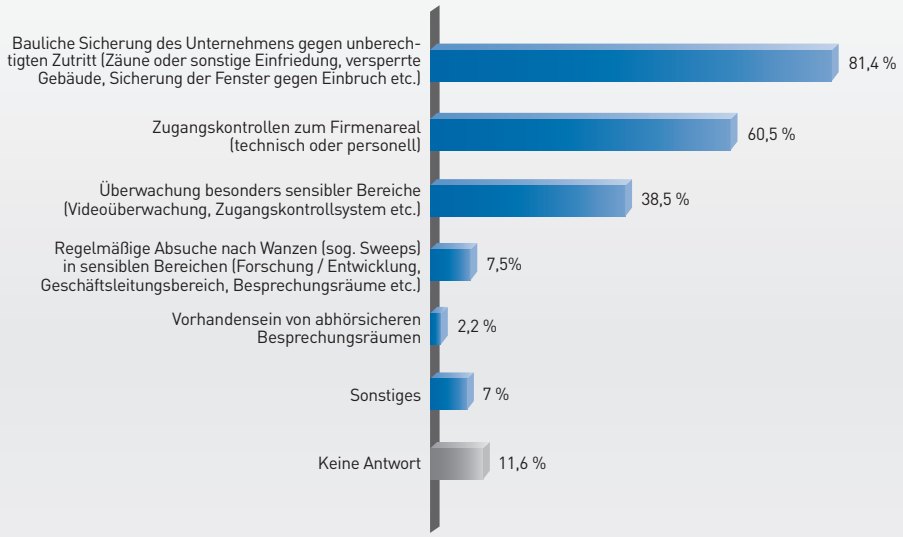
In der Regel gibt es zwar eine bauliche Sicherung gegen fremde Zutritte, jedoch keine abhörgeschützten Räume bzw. Sweeps in gefährdeten Bereichen.

81,4 Prozent aller deutschen Unternehmen haben bauliche Sicherheitsvorkehrungen wie Zäune, versperrte Türen oder Fenstersicherungen gegen Einbruch getroffen. Immerhin noch 60,5 Prozent führen eine Zugangskontrolle (technisch oder personell) zum Firmenareal durch oder überwachen die besonders sensiblen Bereiche durch Videoüberwachung, Zugangskontrollen oder Ähnliches (38,5 Prozent).

Das Risiko „Abhören" wird leider allzu oft nachlässig betrachtet, obwohl es technisch immer einfacher wird. Bei 6,5 Prozent aller Fälle von Industriespionage wurde es als konkrete Spionagehandlung identifiziert.

Eine regelmäßige Absuche nach Wanzen[2] mit technischen Geräten durch Hochfrequenz-Spezialisten, ein sogenannter Sweep[3], wird jedoch nur von 7,5 Prozent der Unternehmen durchgeführt. Und leider gibt es nur bei 2,2 Prozent aller Firmen einen abhörsicheren Besprechungsraum[4], obwohl dies deutlich zum Informationsschutz beitragen würde. Solche Maßnahmen dienen besonders der Lauschabwehr[5]. Sie sollten überall dort zum Standard gehören, wo besonders kritische Unternehmensinformationen kommuniziert werden bzw. wo es sich um einen hoch sensiblen Bereich handelt.

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



GRAFIK 30

Quelle: Corporate Trust 2012

2)Wanzen: Technische, meist miniaturisierte Bauteile bzw. Funksender zum Abhören von Gesprächen oder Aufzeichnen von Informationen.
3)Sweep: Absuche nach Wanzen mit technischen Geräten durch Hochfrequenz-Spezialisten. Dient in der Regel der Lauschabwehr.
4)Abhörgeschützter Raum: Architektonische Abschirmung eines Raumes durch technische Maßnahmen, um ungewollte Funkübertragungen zu verhindern.
5)Lauschangriff: Nachrichtendienstlicher Sprachgebrauch für die akustische Überwachung bzw. das Abhören von Gesprächen.

Sicherheitsvorkehrungen im Unternehmen

Sichere Prozesse

Geheimhaltungsverpflichtungen gehören häufig zum Standard, eine abhörsichere Kommunikation dagegen nur bei jedem zehnten Unternehmen.

Nach den prozesstechnischen Vorkehrungen befragt, gaben 55,8 Prozent der Unternehmen an, zumindest Geheimhaltungsverpflichtungen[1] mit allen Geschäftspartnern abzuschließen. Klare Regelungen über den Umgang mit schützenswerten Informationen gibt es bei 34,8 Prozent und eine Clean-Desk-Policy, die vorschreibt, dass nach Arbeitsende keine offen zugänglichen Unterlagen auf Schreibtischen oder Ablagen verbleiben, noch bei jedem vierten Unternehmen (25,6 Prozent).

Obwohl es aufgrund der wachsenden Bedrohungen durch Cyberwar[2] zunehmend wichtiger wird, dass sich jemand mit hohem Sicherheitsverständnis intensiv und umfassend um die Belange des Informationsschutzes kümmert, haben nur 20,3 Prozent aller Unternehmen einen Sicherheitsverantwortlichen oder Chief Information Security Officer (CISO). Außerdem ist es verwunderlich, dass nur 11,6 Prozent der Unternehmen die Möglichkeit zur abhörsicheren Kommunikation per E-Mail oder Telefon nutzen.

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

GRAFIK 31

Quelle: Corporate Trust 2012

1)Geheimhaltungsverpflichtung: (auch Vertraulichkeitsvereinbarung) Schriftliche Vereinbarung über den Umgang mit vertraulichen Informationen.

2)Cyberwar: Darunter versteht man die kriegerische Auseinandersetzung im und um den virtuellen Raum, den sog. Cyberspace, mit Mitteln vorwiegend aus dem Bereich der Informationstechnik. Cyberwar bezeichnet auch die Aktivitäten staatlicher Spezialeinheiten, um Gegner oder sonstige Ziele online auszukundschaften bzw. sie im Ernstfall zu sabotieren.

Sicherheit bei Auslandsreisen

Die meisten Unternehmen gehen bei Geschäftsreisen ins Ausland viel zu sorglos mit ihren Informationen um.

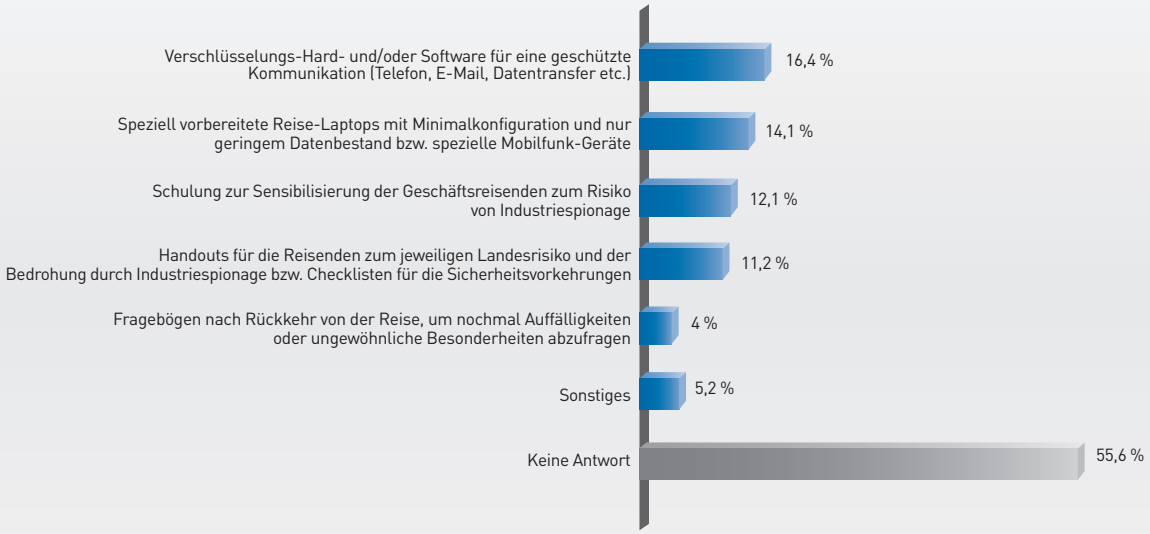
Gerade bei Geschäftsreisen ins Ausland besteht eine erhöhte Bedrohung für den Abfluss von sensiblem Unternehmens-Know-how. Die normalen Schutzvorkehrungen der Firma, wie z.B. eine bauliche Zugriffsbeschränkung auf IT-Equipment oder die Unternehmens-Firewall[3], sind fern der Heimat nicht vorhanden. Daher sollten die Unternehmen entsprechende Vorkehrungen treffen, damit Daten auch im Ausland sicher aufbewahrt werden, Kommunikation über einen geschützten Kanal erfolgt und die Mitarbeiter durch Sensibilisierungsmaßnahmen[4] auf die Risiken vorbereitet sind.

Dies geschieht aber nur in den wenigsten Fällen. 55,6 Prozent aller Unternehmen haben anscheinend keinerlei Sicherheitsvorkehrungen für Geschäftsreisen ins Ausland getroffen. Nur 16,4 Prozent geben ihren Mitarbeitern eine verschlüsselte Hard- und/oder Software an die Hand, damit sie sicher kommunizieren können.

Lediglich 14,1 Prozent haben spezielle Reise-Laptops vorbereitet, damit der Verlust, Diebstahl oder Hackerangriff[5] im Ausland nicht allzu gravierende Folgen hat. Spezielle Handouts[6], welche die Reisenden auf das jeweilige Landesrisiko und die Bedrohung durch Industriespionage vorbereiten, existieren sogar nur in jedem zehnten Unternehmen.

Wie bei den meisten Sicherheitsvorkehrungen spielt der Faktor Mensch auch bei der Reisesicherheit eine ganz wesentliche Rolle. Mitarbeiter, die das Risiko kennen, sind viel eher in der Lage, kritische Situationen richtig einzuschätzen und sich entsprechend zu verhalten. Daher sollte gerade vor Geschäftsreisen in Länder mit einem erhöhten Bedrohungspotenzial Wert auf die Sensibilisierung der Mitarbeiter gelegt werden. Leider nutzen nur 12,1 Prozent der Unternehmen diese Möglichkeit.

Welche Sicherheitsvorkehrungen haben Sie getroffen, um Informationsabfluss bei Mitarbeitern auf Auslandsreisen zu verhindern?
(Mehrfachnennungen möglich)



GRAFIK 32

Quelle: Corporate Trust 2012

3)Firewall: Ein System (meist Hard- und Software), welches dazu dient, den Netzwerkzugriff zu beschränken, basierend auf Absender- oder Zieladresse und genutzten Diensten. Sie überwacht in der Regel den durch sie hindurch laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht. Auf diese Weise sollen unerlaubte Netzwerkzugriffe verhindert werden.

4)Sensibilisierung: Unterweisung bzw. Schulung der Mitarbeiter zu einer bestimmten Gefahrenlage mit Bezugnahme auf eine aktuelle Bedrohung.

5)Hackerangriff: Unerlaubtes Eindringen in fremde Computer- oder Netzwerksysteme, meist durch das Überwinden von Sicherheitsmechanismen.

6)Handout: Ausgedruckte Zusammenfassung der wichtigsten Informationen zu einem Sachverhalt, z.B. einer Präsentation, einer Länderanalyse oder den Sicherheitsrisiken und Verhaltensregeln zu einem Reiseland.

Sicherheitsvorkehrungen im Unternehmen

Sicherheit von Steuerungsanlagen

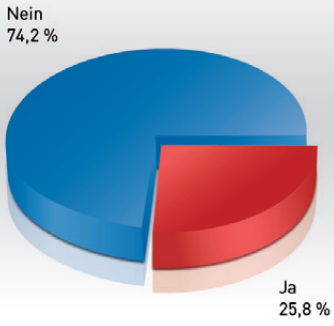
Ein Viertel der befragten Unternehmen betreibt und wartet Steuerungsanlagen[1] für Produktions- oder Leitsysteme.

Ein Viertel der Unternehmen, die sich an dieser Studie beteiligt haben, betreibt industrielle Automations- und Leittechnik. Unter diesem Begriff werden alle Hardware- und Software-Komponenten sowie alle Prozesse zusammengefasst, die auf einen sicheren und zuverlässigen Betrieb eines Industrieprozesses einwirken oder diesen beeinflussen können. Die folgenden Fragen rund um die Sicherheit von Automations- und Leittechnik wurden also von 154 Firmen quer durch alle Branchen beantwortet.

Es liegt der Schluss nahe, dass der Schutz gegen Angriffe (Security) für diese Unternehmen – gerade auch im Hinblick auf die Steuerungsanlagen[1] – mittlerweile neben der Betriebssicherheit (Safety) ein wichtiges Thema ist. Hier zeigt sich ein gewachsenes Bewusstsein für IT-Sicherheit im Bereich der Automatisierungstechnik. Dies korrespondiert mit der steigenden Zahl bekannt gewordener Angriffe[2] auf diese Automatisierungstechnik. Zudem wird von verschiedenen Seiten die Einschätzung geäußert, dass in der Zukunft von Angriffen[3] auf automatisierte Prozesse ausgegangen werden muss. Außerdem muss in diesem Zusammenhang bedacht werden, dass Anlagen für die industrielle Automations-und Leittechnik heute mehr und mehr aus standardisierten Hardware- und Software-Komponenten zusammengesetzt werden. Dadurch werden diese Anlagen deutlich angreifbarer, was den Verantwortlichen in den Unternehmen zunehmend Sorgen bereitet.

Leider hat kein Unternehmen aus der Energiewirtschaft diese Fragen beantwortet, obwohl diese herausgehobenen Versorgungsstrukturen im Rahmen der aktuellen Veränderungen in der Netzstruktur besonders gefährdet erscheinen. Es gibt in diesem Bereich also noch ein Dunkelfeld, welches durch die vorliegende Studie nicht aufgeklärt werden konnte.

Werden in Ihrem Unternehmen Produktions- oder Leitungssysteme bzw. sonstige technische Anlagen durch Computersysteme (sog. Steuerungsanlagen) gesteuert oder betreuen, betreiben oder warten Sie solche Anlagen?



GRAFIK 33

Quelle: Corporate Trust 2012

1)Steuerungsanlagen: (industrielle Automations- und Leittechnik) Alle Hard- und Software-Komponenten, die für einen sicheren und zuverlässigen Betrieb eines Industrieprozesses notwendig sind sowie alle Prozesse, die darauf einwirken oder diesen beeinflussen können.

2) http://www.heise.de/security/meldung/Industrieleittechnik-Sicherheitsluecken-in-Huelle-und-Fuelle-1212186.html

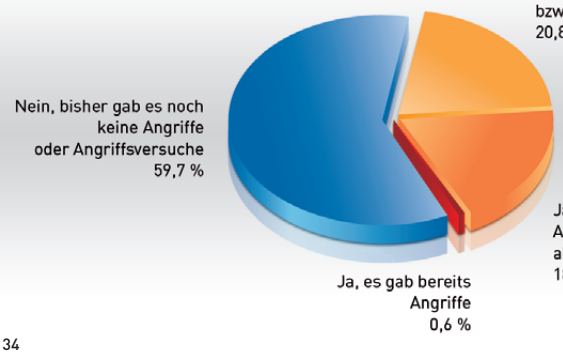
3) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf?__blob=publicationFile

Bereits bei 40 Prozent der Unternehmen wurden Steuerungsanlagen angegriffen oder Angriffe vermutet.

Bereits 40 Prozent der Unternehmen haben Angriffe auf ihre Anlagen festgestellt oder vermuten, dass diese angegriffen wurden. Zwar können nur 0,6 Prozent mit Gewissheit sagen, dass sie angegriffen wurden, jedoch hegten weitere 20,8 Prozent einen Verdacht auf Angriffe, den sie nicht konkretisieren bzw. eindeutig belegen konnten, und 18,8 Prozent gehen davon aus, dass sie zwar angegriffen wurden, bisher jedoch kein nachweisbarer Schaden entstanden ist. Auch hier bestätigen die Zahlen, dass Unternehmen heute nicht mehr automatisch davon ausgehen sollten, dass ihre Steuer- und Prozesstechnik als sicher betrachtet werden kann und keinen Angriffen ausgesetzt ist.

Militärstrategen haben den Cyberspace[4] als neues Schlachtfeld auserkoren. Dementsprechend beginnen große Nationen wie die USA oder China, adäquate Einheiten auszubilden. Während der Ausbildung müssen diese Einheiten üben. Die Zahlen zeigen, dass die Cyberangriffe, die wir bislang sehen, eher den Manövern auf einem Truppenübungsplatz mit kleinen, klar festgelegten Manöverzielen gleichen, als einem echten Krieg. Ähnliche Umfrageergebnisse zeigten sich zu Beginn der Virenproblematik oder der Applikationssicherheitsthemen: Verdachtsfälle und Angriffe ohne Schaden. Das Thema Sicherheit in der industriellen Automations- und Leittechnik steht ganz am Anfang.

Gab es in Ihrem Unternehmen bereits konkrete Angriffe auf Steuerungsanlagen?



GRAFIK 34

Quelle: Corporate Trust 2012

4)Cyberspace: Dient umgangssprachlich als Synonym für das Internet bzw. den virtuellen Raum.

Sicherheitsvorkehrungen im Unternehmen

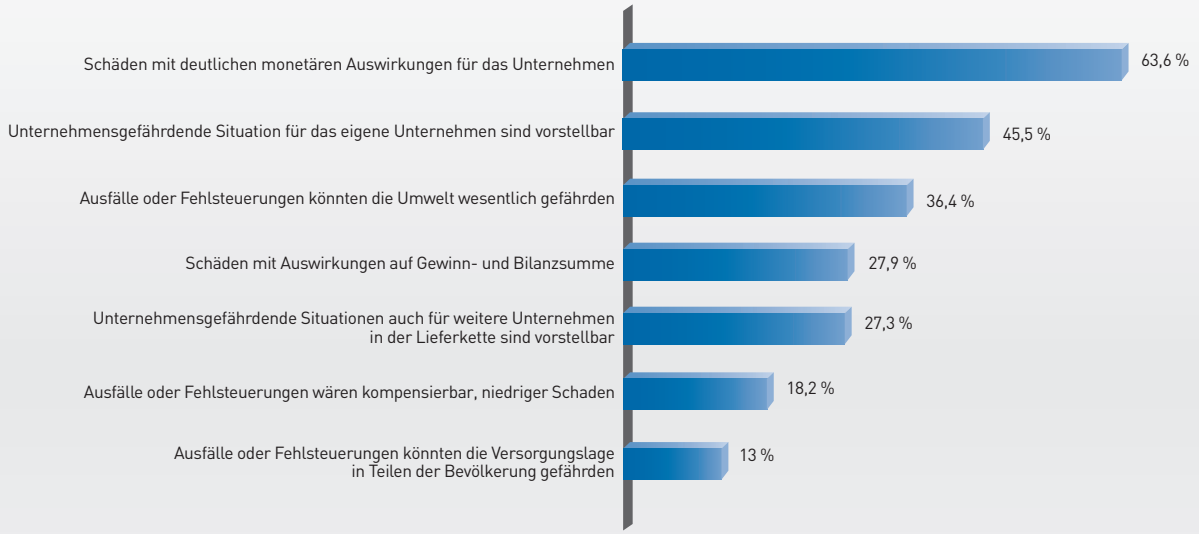
Sicherheit von Steuerungsanlagen

Die meisten Unternehmen halten Schäden mit deutlichen Auswirkungen auf das eigene Unternehmen sowie Partner und Umwelt für möglich.

Die meisten Unternehmen halten erhebliche Schäden bei Angriffen auf ihre Steuerungsanlagen für möglich. Nur 18,2 Prozent der Unternehmen schätzen die möglichen Schäden als gering ein. Dies zeigt, dass das Gefahrenpotenzial den Verantwortlichen sehr bewusst ist und auch die möglichen Auswirkungen auf Umwelt und Partnerfirmen gesehen werden. 45,5 Prozent halten sogar unternehmensgefährdende Situationen für möglich. Diese Ergebnisse veranschaulichen, dass hinter der Prozessleittechnik häufig Prozesse stehen, die einen deutlich höheren Schutzbedarf aufweisen als zum Beispiel Systeme für die „Büro-IT".

Viele der Firmen beschäftigen sich im Kontext der Steuerungsanlagen mit der Arbeitssicherheit (Safety), also den Gefahren für Leib und Leben. Daher haben die Unternehmen einen sehr klaren Blick auf die möglichen Risiken. Aus dieser Interpretation ergibt sich, dass Sicherheitsmaßnahmen in diesen Unternehmen umgesetzt werden müssen, um dem erhöhten Schutzbedarf gerecht zu werden. Gleichzeitig dürfen diese Maßnahmen den Anforderungen der Safety nicht zuwiderlaufen.

Welcher Schaden kann durch einen Angriff auf die von Ihnen benutzten Steuerungsanlagen schlimmstenfalls entstehen?
(Mehrfachnennungen möglich)



GRAFIK 35

Quelle: Corporate Trust 2012

In der Regel entspricht das Sicherheitsniveau der Firmen nicht dem tatsächlichen Schutzbedarf.

Es wird deutlich, dass ein hoher Schutzbedarf für Steuerungsanlagen besteht. Viele der Sicherheitsmaßnahmen, die diesem Schutzbedarf angemessen wären, werden aber in weniger als der Hälfte der Unternehmen umgesetzt. Regelmäßige Audits und Penetrationstests werden etwa nur in jedem fünften Unternehmen durchgeführt. Der Schutz vor Malware (19,5 Prozent der Unternehmen setzen Virenscanner auf den Steuerungskomponenten ein, bei 40,3 Prozent der Unternehmen sind Virenscanner auf den weiteren Komponenten der Leitstelle im Einsatz) und das Patchmanagement (regelmäßige Software-Updates gibt es nur bei 37,7 Prozent der Unternehmen) sind im Bereich der Prozesstechnik anscheinend nicht etabliert.

Der Schutz vor Malware und Angriffen ist damit schwach ausgestattet. Besorgniserregend ist auch, dass ein Sicherheitskonzept für Steuerungsanlagen und Leitstellen nur in 50,0 Prozent der Fälle in die Sicherheitsstrategie des Unternehmens integriert ist. Zusammenfassend muss festgestellt werden, dass die Unternehmen hinsichtlich der IT-Sicherheit sowohl technisch als auch organisatorisch wesentliche Aufgaben vor sich haben.

Der Vorteil ist, dass für diese Aufgaben Lösungswege existieren, die bereits in der Büro-IT funktionieren. Unternehmen sollten nun diese etablierten Ansätze (unter Berücksichtigung der Besonderheiten) auf die Automations- und Leittechnik übertragen.

Welche Maßnahmen haben Sie zum Schutz Ihrer Steuerungsanlagen ergriffen?
(Mehrfachnennungen möglich)

GRAFIK 36

Quelle: Corporate Trust 2012

Einschätzung der künftigen Risiken

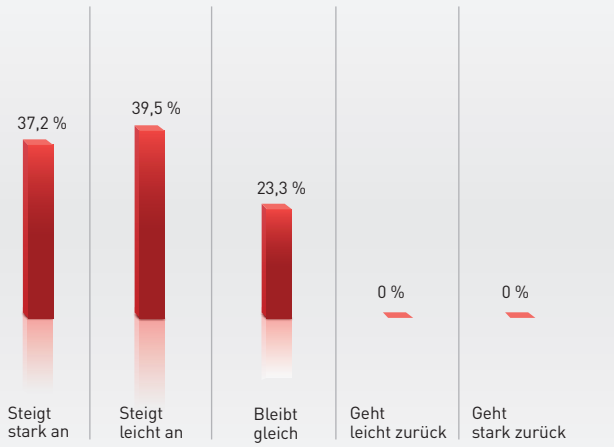
Deutsche Unternehmen erkennen zwar das steigende Risiko, sehen sich selbst jedoch noch immer zu wenig gefährdet.

Seit 2007 hat sich das Bewusstsein der deutschen Unternehmen bei der Einschätzung des eigenen Risikos nur geringfügig geändert. Immer noch denken die meisten Firmen, dass ihr individuelles Risiko geringer sei als das der übrigen Wirtschaft.

Bereits vor fünf Jahren nahmen insgesamt 72,1 Prozent der Unternehmen an, dass das allgemeine Risiko für Industriespionage ansteigen werde, jedoch nur 33,7 Prozent glaubten dies auch für ihren persönlichen Betrieb. Bei der aktuellen Studie sehen zwar insgesamt 76,7 Prozent der Unternehmen eine künftige Steigerung bei der Bedrohung durch Industriespionage (37,2 Prozent vermuten einen starken und 39,5 Prozent einen leichten Anstieg), jedoch nur 52,3 Prozent bewerten dies auch so für ihre eigene Firma.

Dies zeigt, dass die Unternehmen zunehmend erkennen, dass ihr Risiko durch Industriespionage ansteigen wird. Leider schätzen jedoch immer noch zu viele Unternehmen (47,7 Prozent) ihr eigenes Risiko zu gering ein.

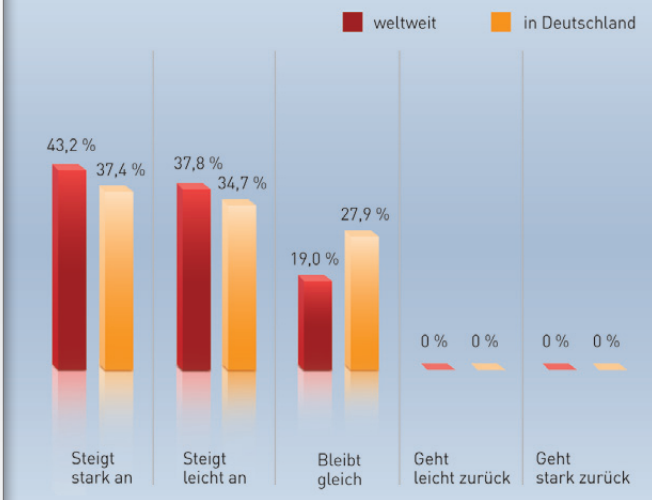
Wie ist Ihre Einschätzung für die zukünftige Entwicklung von Industriespionage allgemein?



GRAFIK 37

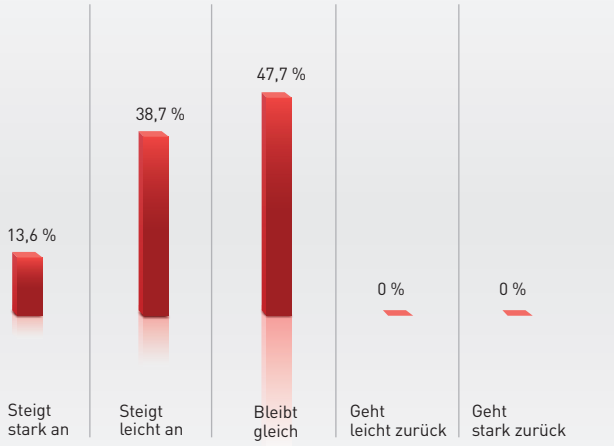
Quelle: Corporate Trust 2012

Stand:2007



Quelle: Studie Industriespionage 2007

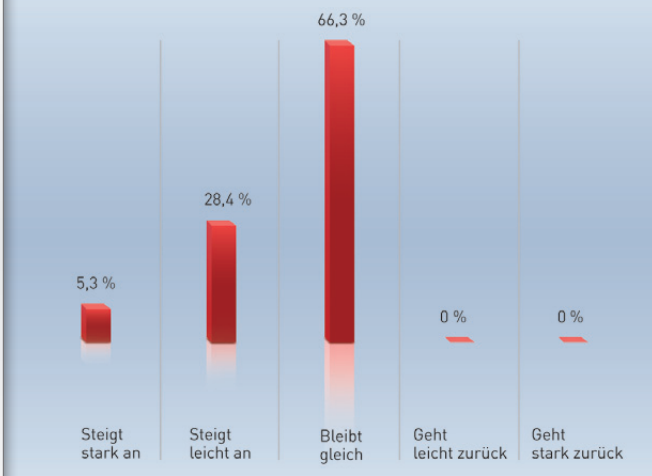
Wie schätzen Sie die zukünftige Bedrohung durch Industriespionage speziell für Ihr Unternehmen ein?



GRAFIK 38

Quelle: Corporate Trust 2012

Stand:2007



Quelle: Studie Industriespionage 2007

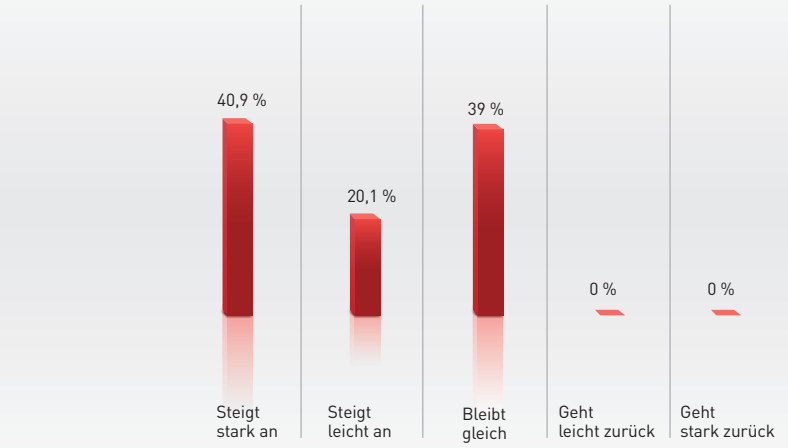
Einschätzung der künftigen Risiken

Die Systeme der Automations- und Leittechnik rücken zunehmend in den Fokus der Angreifer.

40,9 Prozent der Unternehmen, die Automations- und Leittechnik einsetzen, rechnen für die Zukunft mit einer stark steigenden Gefährdung ihrer Systeme, weitere 20,1 Prozent gehen von einer leichten Erhöhung aus. Angesichts der immensen Auswirkungen von Angriffen auf Steuerungsanlagen[1] (siehe Seite 46), die von unternehmensgefährdenden Situationen bis hin zu Umweltschäden oder Engpässen in der Versorgung der Bevölkerung reichen, gewinnt diese Einschätzung an Brisanz.

Der interessanteste Punkt bei diesen Ergebnissen offenbart sich bei der Frage nach dem „Warum": Welche Angreifer suchen sich als Ziel die Steuerungsanlagen eines Unternehmens? Neben Hacktivisten[2], die eine Firma aus politischen Motiven lahmlegen wollen, und Konkurrenten, die von einem Lieferausfall profitieren könnten, sind hier vor allem die staatlich gelenkten Cyberwar[3]-Einheiten zu nennen.

Wie ist Ihre Einschätzung bzgl. der künftigen Gefährdung von Steuerungsanlagen?



GRAFIK 39

Quelle: Corporate Trust 2012

1)Steuerungsanlagen: (industrielle Automations- und Leittechnik) Alle Hard- und Software-Komponenten, die für einen sicheren und zuverlässigen Betrieb eines Industrieprozesses notwendig sind sowie alle Prozesse, die darauf einwirken oder diesen beeinflussen können.

2)Hacktivisten: Eine meist lose organisierte Gruppe von Hackern, die versucht, ihre politischen oder ideologischen Ziele durch Angriffe im Internet durchzusetzen.

3)Cyberwar: Darunter versteht man die kriegerische Auseinandersetzung im und um den virtuellen Raum, den Cyberspace, mit Mitteln vorwiegend aus dem Bereich der Informationstechnik. Cyberwar bezeichnet auch die Aktivitäten staatlicher Spezialeinheiten, um Gegner oder sonstige Ziele online auszukundschaften bzw. sie im Ernstfall zu sabotieren.

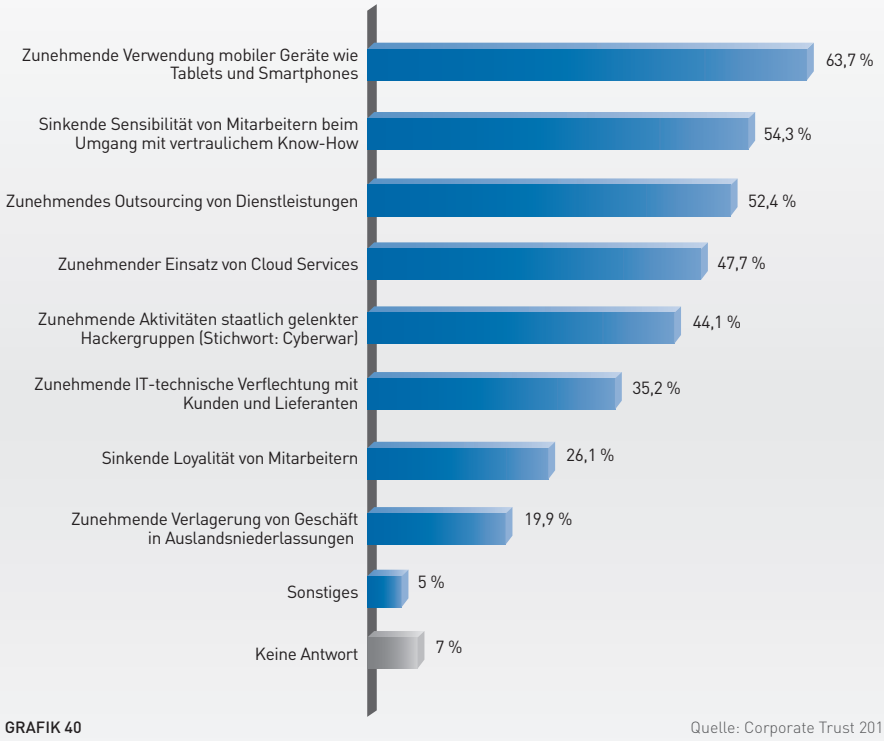
Die zunehmende Verwendung von Mobilgeräten stellt die Wirtschaft zukünftig vor neue Herausforderungen.

Gemessen an der hohen Beteiligung eigener Mitarbeiter beim Informationsabfluss – immerhin 58,0 Prozent der konkreten Fälle (siehe Seite 27) – verwundert die Einschätzung zum künftigen Risiko durch sinkende Mitarbeiter-Loyalität (26,1 Prozent). Dass Mitarbeiter böswillig Daten kopieren, um sie für eigene Zwecke zu verwenden, wird nur allzu gerne unterschätzt. Lediglich den leichtfertigen Umgang mit kritischen Unternehmensinformationen, bedingt durch sinkende Sensibilität, trauen 54,3 Prozent der Firmen ihren Mitarbeitern zu.

Als bedrohlich wird mit 63,7 Prozent vor allem die zunehmende Verwendung von mobilen Geräten wie Tablets und Smartphones bewertet. Auch die Informationsverarbeitung durch Dienstleister wird kritisch beurteilt. 52,4 Prozent nennen das zunehmende Outsourcing[4] von Dienstleistungen und 47,7 Prozent die Verwendung von Cloud-Services[5] als zunehmendes Risiko. Fast die Hälfte der Unternehmen sehen die zunehmenden Aktivitäten staatlich gelenkter Hackergruppen[6] (also die Bedrohung, die gemeinhin unter dem Begriff „Cyberwar" zusammengefasst wird) als künftiges Problem für ihr Know-how.

Die große Anzahl an Antworten zu dieser Frage überrascht. Um eine Entwicklung als Risiko zu sehen, muss ein Unternehmen diese im eigenen Haus für die Zukunft erwarten und sie gleichzeitig als Problem für den Know-how-Schutz identifizieren. An dieser Frage zeigt sich damit deutlich der Zielkonflikt zwischen Innovationsbereitschaft und Sicherheit, in dem viele Unternehmen stecken. Obwohl die meisten Firmen die Zunahme von Outsourcing, Cloud-Services oder mobilen Geräten als Bedrohung wahrnehmen, sehen sie diese Entwicklung für das eigene Unternehmen jedoch als notwendig, wenn nicht gar unvermeidbar an.

Welche Entwicklung sehen Sie als zunehmendes Risiko für Ihr Know-How?
(Mehrfachnennungen möglich)



GRAFIK 40

Quelle: Corporate Trust 2012

4)Outsourcing: Damit wird in der Ökonomie die Abgabe von Unternehmensaufgaben und -strukturen an Drittunternehmen bezeichnet. Es ist eine spezielle Form des Fremdbezugs von bisher intern erbrachter Leistung, wobei in der Regel Verträge die Dauer und den Umfang der Leistung festschreiben.

5)Cloud-Service (auch Cloud-Computing) Umschreibt den Ansatz, abstrahierte IT-Infrastrukturen (z.B. Rechenkapazitäten, Datenspeicher, Netzwerk-Kapazitäten oder auch ← fertige Software) dynamisch an den Bedarf angepasst über ein Netzwerk zur Verfügung zu stellen. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud-Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z.B. Rechenleistung, Speicherplatz), Plattformen und Software.

6)Hackerangriff: Unerlaubtes Eindringen in fremde Computer- oder Netzwerksysteme, meist durch das Überwinden von Sicherheitsmechanismen.

Einschätzung der künftigen Risiken

Auf die Risiken durch eigene Mitarbeiter sind die Unternehmen am wenigsten vorbereitet.

Sicherheitsvorkehrungen sind wichtig, um unkontrollierten Datenabfluss zu vermeiden. Allerdings haben die Unternehmen erkannt, dass an vielen Stellen die Vorkehrungen noch nicht ausreichend sind. So gaben 58,1 Prozent an, noch nicht entsprechend gegen Social Engineering[1], also das geschickte Ausfragen von Mitarbeitern, geschützt zu sein. Dies stellt zwar einen leichtfertigen Informationsabfluss dar, doch auch auf den böswilligen Datendiebstahl scheinen die Unternehmen noch nicht richtig vorbereitet zu sein. So geben 46,6 Prozent der befragten Firmen an, keine ausreichenden Vorkehrungen gegen die bewusste Informations-/Datenweitergabe bzw. den Datendiebstahl durch eigene Mitarbeiter getroffen zu haben.

Dagegen glauben zwei Drittel aller Unternehmen, für die klassischen Hackerangriffe[2] bereits entsprechend gerüstet zu sein. Nur ein Drittel gibt an, dass dies eine Bedrohung darstellt, gegen die sie noch zu wenig geschützt sind.

Die Antworten auf diese Frage geben Anlass zu großer Sorge. Kaum eines der befragten Unternehmen hält sich in allen Punkten für ausreichend geschützt, mehr als 92 Prozent der Firmen haben mehrfache Angaben gemacht. Die Daten zeigen die weiterhin hohe Gefährdung der Wirtschaft sehr anschaulich – in jedem der hier genannten Sicherheitsthemen hält sich mindestens ein Viertel der Unternehmen für angreifbar.

Für welche Bedrohungen halten Sie die Schutzvorkehrungen Ihres Unternehmens für nicht ausreichend?
(Mehrfachnennungen möglich)

GRAFIK 41

Quelle: Corporate Trust 2012

1)Social Engineering: Ausspionieren über das persönliche Umfeld, durch zwischenmenschliche Beeinflussung bzw. durch geschickte Fragestellung, meist unter Verschleierung der eigenen Identität (Verwenden einer Legende). Social Engineering hat das Ziel, unberechtigt an Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen.

2)Hackerangriff: Unerlaubtes Eindringen in fremde Computer- oder Netzwerksysteme, meist durch das Überwinden von Sicherheitsmechanismen.

Die Welt gehört denen, die zu ihrer Eroberung ausziehen, bewaffnet mit Sicherheit und guter Laune.

Charles Dickens

Schlussfolgerungen

Bewertung der Ergebnisse

Cyberwar ist mittlerweile eine reale Bedrohung für die deutsche Wirtschaft.

Der finanzielle Gesamtschaden durch Industriespionage ist für die deutsche Wirtschaft in den letzten fünf Jahren um ca. 50 Prozent gestiegen und liegt, konservativ gerechnet, bei mindestens 4,2 Milliarden Euro. Während im Jahr 2007 nur 64,4 Prozent der geschädigten Unternehmen auch einen finanziellen Schaden zu beklagen hatten, sind es 2012 bereits 82,9 Prozent.

Nach wie vor stellt der Faktor Mensch das größte Risiko dar. Unternehmen gaben in über 70 Prozent der Fälle an, dass Mitarbeiter unmittelbar (durch Datenweitergabe oder Datendiebstahl) bzw. mittelbar (indem sie durch Social Engineering[1] geschickt ausgehorcht wurden) an dem Informationsabfluss beteiligt waren. Bisher hatte zwar nur jedes vierte Unternehmen entsprechende Awareness-Kampagnen[2] und jedes dritte Unternehmen eine Mitarbeiterbefragung zur Erfassung der Loyalität (Loyalitäts-Index[3]) durchgeführt, in Zukunft wollen aber mindestens 68,3 Prozent ihre Mitarbeiter für die Risiken durch Industriespionage sensibilisieren.

Betrachtet man die hohe Zahl der Angriffe auf Steuerungsanlagen[4] (immerhin rund 40 Prozent aller Unternehmen, die solche Technik einsetzen, gaben dies an), ist es vermutlich nur dem Zufall zu verdanken, dass noch keine gravierenderen Schäden in Deutschland bzw. zum Nachteil für deutsche Unternehmen bekannt geworden sind. 36,4 Prozent der Unternehmen gaben an, dass Ausfälle oder Fehlsteuerungen die Umwelt wesentlich gefährden könnten. Weitere 13,0 Prozent gaben an, dass Ausfälle oder Fehlsteuerungen die Versorgungslage in Teilen der Bevölkerung gefährden könnte.

Die Schäden durch Industriespionage steigen an und wirken sich nicht nur finanziell auf das Betriebsergebnis aus, sondern auch auf die Reputation des Unternehmens. Viele Fälle der letzten Jahre sind zunehmend von einer Professionalisierung der Täter gekennzeichnet. Social Engineering-Angriffe[1] gehen mit Hacker-Attacken[5] einher, bis die Spione ihr Ziel erreichen. In vielen Fällen werden dabei die Möglichkeiten des Internets bzw. einer weltweiten Vernetzung der Unternehmen genutzt. Der Cyberwar[6] ist damit längst zur Realität für die deutsche Wirtschaft geworden.

1)Social Engineering:	Ausspionieren über das persönliche Umfeld, durch zwischenmenschliche Beeinflussung bzw. durch geschickte Fragestellung, meist unter Verschleierung der eigenen Identität (Verwenden einer Legende). Social Engineering hat das Ziel, unberechtigt an Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen.
2)Awareness:	Bewusstsein oder Gewahrsein über die eigene Handlung oder zur Betonung der aktiven Haltung bzw. Aufmerksamkeit gegenüber einem bestimmten Sachverhalt.
3)Loyalitäts-Index:	Beurteilung von Unternehmen und Organisationen im Hinblick auf kriminelle und fahrlässige Handlungen von Mitarbeitern. Der Loyalitäts-Index liefert durch eine Mitarbeiterbefragung mit einer psychologisch fundierten Vorgehensweise Parameter, welche auf potenzielle Risiken hinweisen.
4)Steuerungsanlagen:	(industrielle Automations- und Leittechnik) Alle Hard- und Software-Komponenten, die für einen sicheren und zuverlässigen Betrieb eines Industrieprozesses notwendig sind sowie alle Prozesse, die darauf einwirken oder diesen beeinflussen können.
5)Hackerangriff:	Unerlaubtes Eindringen in fremde Computer- oder Netzwerksysteme, meist durch das Überwinden von Sicherheitsmechanismen.
6)Cyberwar:	Darunter versteht man die kriegerische Auseinandersetzung im und um den virtuellen Raum, den Cyberspace, mit Mitteln vorwiegend aus dem Bereich der Informationstechnik. Cyberwar bezeichnet auch die Aktivitäten staatlicher Spezialeinheiten, um Gegner oder sonstige Ziele online auszukundschaften bzw. sie im Ernstfall zu sabotieren.

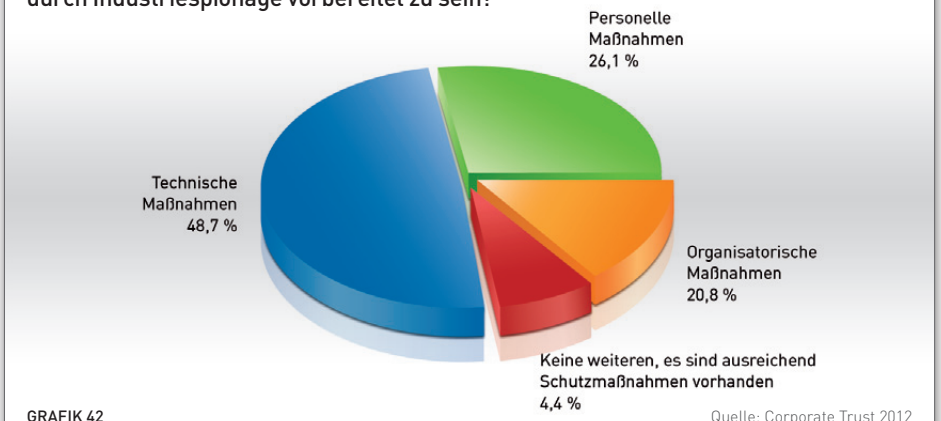
PRÄVENTION

Unternehmen wollen in Zukunft überwiegend technische Maßnahmen zur Sicherung des eigenen Know-how treffen.

Die überwiegende Mehrheit der Unternehmen befürchtet, dass Industriespionage in den nächsten Jahren ansteigen wird. Daher sollen auch entsprechende Sicherheitsvorkehrungen getroffen werden, um die Risiken zu minimieren. Nur 4,4 Prozent der befragten Unternehmen gaben an, keine weiteren Sicherheitsvorkehrungen implementieren zu wollen, 20,1 Prozent wollen organisatorische Maßnahmen verbessern, 26,1 Prozent an den personellen Maßnahmen arbeiten und 48,7 Prozent der antwortenden Unternehmen zusätzliche technische Maßnahmen einführen.

Dies zeigt deutlich, dass der Informationsschutz überwiegend als technische Anforderung gesehen wird. Daher ist er vielfach ausschließlich in der IT-Abteilung verankert. Die Bedrohung durch das Verhalten eigener Mitarbeiter oder ungenügender Prozesse wird bewusst verdrängt. IT-Sicherheit ist jedoch nur ein Baustein eines umfangreichen Sicherheitskonzepts zur Bekämpfung von Industriespionage.

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



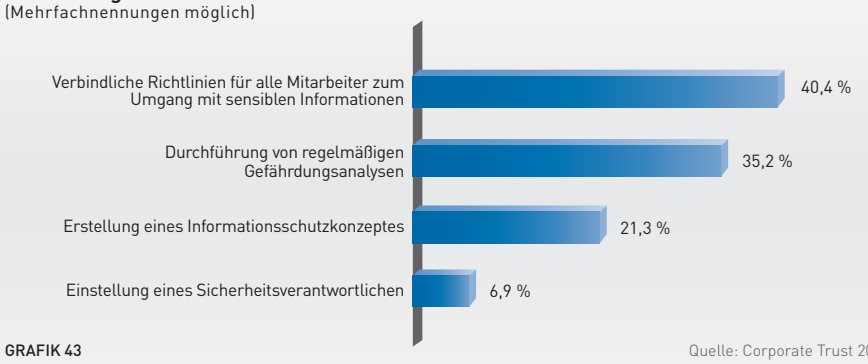
GRAFIK 42

Quelle: Corporate Trust 2012

Bei den organisatorischen Maßnahmen wollen 40,4 Prozent zumindest für alle Mitarbeiter verbindliche Richtlinien zum Umgang mit sensiblen Informationen erstellen und 35,2 Prozent regelmäßige Gefährdungsanalysen durchführen. Die meisten Unternehmen haben aber noch nicht akzeptiert, dass ein Sicherheitsverantwortlicher, der sich neben anderen Anforderungen auch umfassend um den Schutz der vertraulichen Daten kümmern kann, wesentliche Vorteile bringen würde. Daher planen nur 6,9 Prozent, in Zukunft einen Sicherheitsverantwortlichen einzustellen.

Immer mehr Unternehmen erkennen die Risiken eines Verlusts unternehmenskritischer Dokumente. Dieser Verlust kann durch zunehmende Industriespionage oder auch durch einen zu sorglosen Umgang mit vertraulichen Unterlagen erfolgen. In beiden Fällen kann der Informationsabfluss geschäftsschädigend oder sogar existenzgefährdend sein.

Welche organisatorischen Maßnahmen werden Sie treffen?
(Mehrfachnennungen möglich)



GRAFIK 43

Quelle: Corporate Trust 2012

GRAFIK 44 Quelle: Corporate Trust 2012

GRAFIK 45 Quelle: Corporate Trust 2012

Technische Maßnahmen zur Absicherung des sensiblen Know-how stehen daher bei den Unternehmen ganz oben auf der Liste. So wollen 35,0 Prozent der Firmen in der nächsten Zeit eine Lösung zum Document Compliance Management einführen, um die Mitarbeiter beim vertraulichen Datenaustausch zu unterstützen. 33,0 Prozent wollen die Gebäudesicherheit verbessern und 32,7 Prozent mehr in Verschlüsselungstechnologie für E-Mails, Telefonie und die Anbindung ihrer Außenstellen investieren. Nur knapp 16 Prozent wollen dagegen auf den Einsatz von biometrischen oder Token-basierten Verfahren zur Benutzeranmeldung setzen.

Bei den personellen Maßnahmen gibt es einen starken Trend, die Mitarbeiter zukünftig besser zu sensibilisieren, um sie so auf die neuen Bedrohungen durch Cyberwar[1] vorzubereiten. Mit 68,3 Prozent planen mehr als zwei Drittel aller Unternehmen, dies zu tun. Dies ist sehr vernünftig, weil damit bereits ein Großteil der „versehentlichen" Datenabflüsse verhindert werden kann. Die Geschäftsreisenden werden dagegen auch weiterhin nur bei jedem sechsten Unternehmen entsprechende Handouts[2] bekommen, um sich intensiv auf die Auslandsreise und die erhöhten Risiken von Datenabfluss vorzubereiten. Dies fällt ähnlich gering aus wie die geplanten Maßnahmen zur Erfassung der Mitarbeiter-Loyalität. Nur 16,1 Prozent wollen hier regelmäßige Mitarbeiterbefragungen durchführen.

Obwohl 46,6 Prozent der Unternehmen angaben, dass sie die bewusste Informationsweitergabe bzw. den Datendiebstahl durch eigene Mitarbeiter als hohe Bedrohung einschätzen (siehe Auswertung Seite 52), wollen nur die wenigsten eine regelmäßige Mitarbeiterbefragung zum Loyalitäts-Index[3] durchführen. Dieser würde ihnen jedoch sehr deutlich aufzeigen, worin die Gründe für eine sinkende Mitarbeiter-Loyalität liegen.

1)Cyberwar: Darunter versteht man die kriegerische Auseinandersetzung im und um den virtuellen Raum, den Cyberspace, mit Mitteln vorwiegend aus dem Bereich der Informationstechnik. Cyberwar bezeichnet auch die Aktivitäten staatlicher Spezialeinheiten, um Gegner oder sonstige Ziele online auszukundschaften bzw. sie im Ernstfall zu sabotieren.

2)Handout: Ausgedruckte Zusammenfassung der wichtigsten Informationen zu einem Sachverhalt, z.B. einer Präsentation, einer Länderanalyse oder den Sicherheitsrisiken und Verhaltensregeln zu einem Reiseland.

3)Loyalitäts-Index: Beurteilung von Unternehmen und Organisationen im Hinblick auf kriminelle und fahrlässige Handlungen von Mitarbeitern. Der Loyalitäts-Index liefert durch eine Mitarbeiterbefragung mit einer psychologisch fundierten Vorgehensweise Parameter, welche auf potenzielle Risiken hinweisen.

Florian Oelmaier
Leiter IT Sicherheit und
Computerkriminalität
Corporate Trust GmbH

Technologische Innovationen, neue Angreifer, kombinierte Bedrohungen aus IT und Non-IT: Wer heute seine Sicherheit nicht weiterentwickelt, ist der Verlierer von morgen.

CORPORATE TRUST
business risk & crisis management

„The Times They Are a-Changin" war der Titel eines der Lieblingslieder von Steve Jobs, es stammt aus der Feder von Bob Dylan. Und in kaum einem Fachgebiet passt dieses Motto besser als im Bereich der Sicherheit. Die vorliegende Studie von Corporate Trust greift das Thema Industriespionage wieder auf, welches bereits in einer Studie vor fünf Jahren behandelt wurde. Und während wir in den Ergebnissen eine konstante, aber eher gemächliche Weiterentwicklung der Sicherheitsmaßnahmen in den Unternehmen erkennen, sieht die Welt außen herum heute sehr verändert aus.

Die neuen Möglichkeiten von Cloud-Computing und mobilen Geräten wie Smartphones oder Tablet-PCs bieten Unternehmen Produktivitätsvorteile und gleichzeitig den Mitarbeitern mehr Lebensqualität. Mitarbeiter bringen ihre privaten Geräte mit zur Arbeit und greifen damit auf Unternehmens-Know-how zu. Eine Firma wie Apple, die vor fünf Jahren noch niemand im Sicherheitsbereich auf der Agenda hatte, führte vor vier Jahren mit den Apps und dem App-Store eine Reihe völlig neuer Sicherheitstechnologien ein. Auf der anderen Seite sind auch neue Bedrohungen aufgetaucht: Vor fünf Jahren sprach noch niemand von staatlich gelenkten IT-Angriffen oder Cyberwar. Hacktivisten[1] Gruppen wie z.B. Anonymous oder Lulzsec waren gänzlich unbekannt.

Fazit: Getrieben durch die neuen Entwicklungen muss sich die Sicherheit weiterentwickeln. Neue Technologien müssen für das eigene Unternehmen nutzbar gemacht, neue Angreifer abgewehrt werden. Ein „Weiter so!" ist ein Rückschritt.

Der wichtigste Punkt in dieser Weiterentwicklung ist aus unserer Sicht die Verzahnung von klassischer Sicherheit und IT-Sicherheit. In vielen Unternehmen existieren zwei Sicherheitsorganisationen parallel: die Themen der „klassischen" Sicherheit wie z.B. Werkschutz, bauliche Sicherheit sowie personelle Sicherheit auf der einen Seite und die IT-Themen auf der anderen Seite. Oft endet diese Situation in einer Art „Burgfrieden": Die klassische Sicherheit ist froh, die komplexen und unverständlichen IT-Sicherheitsthemen losgeworden zu sein. Auf der anderen Seite ist die IT-Sicherheitsabteilung damit zufrieden, sich rein auf die technische Seite der IT konzentrieren zu können. Diese Trennung ist – angesichts der Veränderungen – nicht mehr zeitgemäß. Eine interdisziplinär verzahnte Abwehr von Angriffen kann nur durch Experten für klassische Sicherheit und IT-Sicherheit gemeinsam aufgebaut werden.

1)Hacktivisten: Eine meist lose organisierte Gruppe von Hackern, die versucht, ihre politischen oder ideologischen Ziele durch Angriffe im Internet durchzusetzen.

Wenn es ernst wird mit der Sicherheit: Corporate Trust

Corporate Trust ist einer der wenigen Marktteilnehmer, der diese Zeichen der Zeit erkannt hat. Ehemalige Polizisten und Sicherheitsverantwortliche aus Konzernen arbeiten Hand in Hand mit IT-Sicherheitsexperten und Profis für alle Themen rund um den baulichen Schutz oder die Krisenkommunikation. Auf diese Weise kann Corporate Trust den Brückenschlag zwischen den Disziplinen verwirklichen und in ein Unternehmen hineinbringen; entsprechend sind wir ein gefragter Partner, wenn es um die Aufklärung von Spionagefällen geht. Diese Verbindung ermöglicht es aber auch, eine neue Dimension von präventiven Dienstleistungsprodukten anzubieten.

Eine interdisziplinäre Schutzbedarfsanalyse hilft, die wirklich wertvollen Assets des Unternehmens zu identifizieren. Ein zielgerichtetes Audit unterstützt die Bemühungen der Firmen, systematisch alle noch fehlenden Maßnahmen zu erkennen. Hat ein Unternehmen einen umfassenden Informationsschutz implementiert, kann ein Spionage-Penetrationstest prüfen, wo noch Schwachstellen existieren. Sekundär kann im Rahmen von Spionage-Penetrationstests festgestellt werden, wie gut Vorfälle im Unternehmen detektiert und aufgeklärt werden können.

Um die Einstiegshürde möglichst niedrig zu gestalten, bieten wir einen IT-Security-Check an, der es einem Unternehmen ermöglicht, in sehr kurzer Zeit eine Experteneinschätzung über die Lage der IT-Sicherheit zu erhalten. Dabei werden in fünf Schritten die aktuelle Bedrohungslage und möglichen Risiken für einen Informationsabfluss erfasst. Das Leistungspaket richtet sich insbesondere an mittelständische Firmen, die aufgrund ihrer Größe noch keine eigene IT-Sicherheitsabteilung unterhalten.

Neben der Verteidigung gegen Angriffe hat die Sicherheit aber auch eine gestaltende Rolle zu übernehmen. So erfordert z.B. der Aufbau eines überall verfügbaren Informationszugriffs für ein Unternehmen viel Fingerspitzengefühl. Sicherheit ist beim Unternehmenseinsatz von iPads, iPhones und den neuen Windows 8-Geräten eine unabdingbare Notwendigkeit. Und auch die Frage, welche Unternehmensdaten in Cloud-Infrastrukturen verarbeitet werden können und welche unter eigener Kontrolle verbleiben sollten, erfordert entsprechende Erfahrung. Da wir sämtliche Angriffsmöglichkeiten und Sicherheitsprobleme der neuen Technologien kennen, können wir Sie hier umfassend beraten.

Über all diesen Angeboten steht unsere Unternehmensmission: Wir wollen eine Umgebung schaffen, in der Sie sich absolut sicher und ungestört auf Ihre Ziele und die Ziele Ihres Unternehmens konzentrieren können. Dies gilt vor allem auch in der IT. Wir sehen es als unsere Aufgabe, Sicherheit zu schaffen, ohne Ideen und Innovationen zu verhindern.

Auf diese Weise können wir dazu beitragen, den Innovationsstau in der Sicherheit abzubauen und die deutschen Unternehmen im Bereich Informationsschutz wieder auf einen akzeptablen Stand zu bringen.

Die Welt hat sich weitergedreht. Bleiben Sie nicht zurück!

Ihr
Florian Oelmaier

Peter Weger
Chief Executive Officer
Brainloop AG

Vertrauen ist die Basis jeder Zusammenarbeit. Wie die Studie zeigt, wird jedoch das Informationskapital eines Unternehmens durch Wirtschaftskriminalität oder illoyales Verhalten von Mitarbeitern bedroht. Um die Wettbewerbsposition zu stärken, muss daher der Zugriff auf unternehmenskritische Inhalte abgesichert und im Detail protokolliert werden.

brainloop

Deutschland ist eine technologie- und exportorientierte Nation, deren Stärke auf Wissensvorsprung und Innovationen basiert. Dieses Wissen weckt weltweit immer wieder großes Interesse. Im Zeitalter des digitalen Informationsaustauschs sind Unternehmen daher ständig der Gefahr ausgesetzt, dass sich Begehrlichkeiten Bahn brechen und vertraulich Dokumentiertes das Unternehmen verlässt. Da auch die Medien regelmäßig von Pannen wie Spionageangriffen oder unbefugter Weiterleitung von Interna berichten, haben inzwischen auch die Unternehmenslenker ein Bewusstsein für Sicherheitslücken entwickelt. Die Bedrohung des Informationskapitals, das Unternehmen auf Dauer wettbewerbsfähig macht, wird dementsprechend ernst genommen. Alles, was im Rahmen von innovativen Forschungsprojekten, Kooperationen, neuen Beteiligungen oder anderen Geschäftsvorhaben zu Papier gebracht wurde, stellt einen unternehmerischen Wert dar, der geschützt werden muss. Nun kann man im Sinne eines professionellen Informationsschutzes die Dokumente einzeln betrachtet als „streng vertraulich", „vertraulich" und „öffentlich zugänglich" klassifizieren. Das darf aber nicht darüber hinweg täuschen, dass ein Unternehmen grundsätzlich auf die Loyalität und Diskretion seiner Mitarbeiter angewiesen ist, egal, welche Dokumente sie gerade bearbeiten. Was intern ist, sollte intern bleiben. Soweit die Theorie.

Austausch von Dokumenten im Alltag: Effizient, aber sicher?

In der Praxis findet die Kooperation im Unternehmen und mit externen Geschäftspartnern schnell und möglichst barrierefrei statt. Die Grenzen zwischen „innen" und „außen" verschwimmen. Dabei geht der ungeschützte Austausch oft vertraulicher Dokumente per E-Mail, dem häufig Zeitdruck und auch ein Mangel an technologischen Alternativen zugrunde liegen, selbstverständlich zu Lasten der Datensicherheit. Wer die Effizienz der betrieblichen Abläufe auf Dauer erhöhen will, sollte an der Sicherheit nicht sparen. Informationen gehören zum wichtigsten Kapital eines Unternehmens und sollten daher durchgängig vor Missbrauch und Verlust geschützt werden. Wer möchte verantworten, dass wettbewerbsrelevantes Wissen unverschlüsselt und ohne jegliche Schutzfunktionalitäten im Netz zirkuliert? Die Folgen sind ein unerwünschter Kontrollverlust sowie die Gefahr von Diebstahl oder Spionage. Häufig kommt es auch zu unbeabsichtigten Fehlhantierungen, sodass E-Mails aus Versehen dem falschen Adressaten zugesandt werden und dieser in den Besitz unternehmenskritischer Informationen gelangt. Eine weitere Herausforderung stellt der Schutz des Dokuments während des Verbleibs auf dem Server dar. Wie kann es dort vor dem Einblick durch interne, unberechtigte Anwender geschützt werden und gleichzeitig einem ausgewählten Kreis von Mitarbeitern zur Verfügung stehen? Idealerweise setzen Unternehmen hier auf eine web-basierte Lösung für Document Compliance Management, die das Dokument verschlüsselt, von der Entstehung bis zur Ablage oder zum finalen Löschen begleitet und im Sinne guter Compliance aufzeichnet, was zwischenzeitlich mit ihm geschehen ist.

Der offenbar vorherrschende Spagat zwischen der Dokumentenbereitstellung und dem bestmöglichen Schutz derselben

wird durch den Wunsch vieler Mitarbeiter, unterwegs auf vertrauliche Unterlagen zugreifen zu können, weiter verschärft. Flexibles Arbeiten und die jederzeitige Verfügbarkeit der Informationen sind praktisch. Der Umstand, dass jeder Anwender schlussendlich mit seinem eigenen Mobile Device aktiv wird (BOYD = Bring Your Own Device), ist es nicht. Auch hier unterstützt das Document Compliance Management die Prozesse und erlaubt die zentrale Verwaltung der mobilen Endgeräte auf Serverseite. Damit sind die Devices keine Unbekannten mehr und können je nach Unternehmensentscheid für den Empfang und die Bearbeitung vertraulicher Dokumente autorisiert werden.

Wie die Ausführungen zeigen, kommt dem Mitarbeiter in der gesamten Sicherheitsthematik eine tragende Rolle zu. Entscheidend ist die Sensibilisierung jedes Einzelnen im Umgang mit Sicherheitsstandards im Unternehmen. Was die Handhabung vertraulicher Dokumente angeht, gibt es inzwischen jedoch gute technologische Möglichkeiten, wie das Document Compliance Management der Brainloop AG, um die Mitarbeiter im sicheren Umgang mit vertraulichen Unterlagen anzuleiten und zu entlasten.

Barrierefrei und sicher:
Document Compliance Management

Dem Missbrauch und Verlust vertraulicher Dokumente lässt sich mit dem Einsatz für Document Compliance Management wirksam begegnen. Wie auch die Studienergebnisse zeigen, sind Informationen besonders gefährdet, wenn sie den schützenden Rahmen der unternehmenseigenen Infrastruktur verlassen. Hier setzt die Lösung für Document Compliance Management an und bietet eine barrierefreie Zusammenarbeit im Unternehmen und mit externen Partnern, die zugleich sicher und regelkonform ist. Das grenzüberschreitende Netz ist leicht zu bedienen. Die Einführung erfolgt schnell und unkompliziert ohne Installationen auf dem Client – weder intern noch bei externen Geschäftspartnern. Dadurch werden die Hürden für den Einstieg in das Arbeiten mit der Lösung auf ein Minimum gesenkt. Viele Unternehmen setzen die webbasierte Plattform in allen Abteilungen ein (Konzernlösung) und stellen sie über ein internes Einkaufsportal zur Verfügung, was die Handhabung vereinfacht und die Schnelligkeit der Einführung abermals erhöht. Ebenfalls lässt sich auf dieser Basis eine einheitliche Compliance-Richtlinie zum Umgang mit sensiblen Dokumenten für das ganze Unternehmen etablieren. Sowohl die Sicherheitskategorien für die Dokumente als auch die Berechtigungskonzepte für die Abteilungen und Projektteams müssen in diesem Fall nur ein Mal von zentraler Stelle eingerichtet werden.

Alle Dokumente werden auf einem Hochsicherheitsserver mit einer 256-Bit-Verschlüsselung gespeichert und zwischen Client und Server mit 128-Bit-Verschlüsselung übertragen, was ein Mitlesen oder Ausspionieren der Inhalte unmöglich macht. Für den maximalen Schutz beim Zugriff auf die Plattform sorgt die 2-Faktor-Authentifizierung mit Passwort und TAN. Alle Bearbeitungsschritte werden protokolliert, damit Zugriffe und Änderungen am Dokument jederzeit detailliert nachvollzogen und zugeordnet werden können (Compliance). Die Zusammenarbeit wird dadurch vollkommen transparent. Je nach Wunsch können die Dokumente zusätzlich mit weitreichenden Sicherheitsfunktionalitäten ausgestattet werden, die beispielsweise den exklusiven Download mit Wasserzeichen erlauben oder aber ein Dokument nur zum Lesen auf dem Bildschirm anzeigen. Falls mobile Endgeräte (iPad) zum Einsatz kommen, werden diese einer „Device Policy" folgend in die Sicherheitszone der Brainloop-Lösung integriert und zentral auf dem Server freigeschaltet, was dem Wildwuchs der verwendeten Endgeräte Einhalt gebietet und die Sicherheit adäquat erhöht.

Das Brainloop Document Compliance Management ist damit eine Investition, die den Dokumentenaustausch eines Unternehmens langfristig auf ein sicheres Fundament stellt und die Effizienz der Zusammenarbeit erhöht. Während die Sicherheit der Dokumente auf der Plattform automatisch garantiert wird, ermöglicht Brainloop den Mitarbeitern ein sorgloseres Vorgehen im Umgang mit ihren Unterlagen. Jeder sieht nur so viel, wie er für seine tägliche Arbeit braucht, und hat damit den Kopf frei für sein Kerngeschäft. Gleichzeitig werden die Mitarbeiter bei der Einhaltung verbindlicher Richtlinien im Umgang mit sensiblen Informationen bestmöglich unterstützt.

Sicher ist: Der ganzheitliche Schutz Ihrer vertraulichen Dokumente trägt in entscheidendem Maße zur Wettbewerbsfähigkeit Ihres Unternehmens bei!

Ihr
Peter Weger

Dr. Thomas Störtkuhl
Product Manager Industrial IT Security
Embedded Systems
TÜV SÜD AG

Sicherheit und Zuverlässigkeit in einer automatisierten Welt basieren auf Security for Safety.

Embedded Systems werden in der Produktion für das Messen, Regeln und Steuern aller Arten von Geräten und Anlagen eingesetzt. Mit ihnen wird die sogenannte industrielle Automations- und Leittechnik realisiert, die sich mehr und mehr aus standardisierten Hardware- und Softwarekomponenten zusammensetzt. Diese offenen Systeme erleichtern die Integration der einzelnen Komponenten und vermindern die Abhängigkeit von bestimmten Zulieferern. Sie ermöglichen durch standardbasierte Komponenten insbesondere auch die Vernetzung von Leittechnik und Büro-IT. Die durchgängige Kommunikation beschleunigt die Produktion, ermöglicht eine bessere Übersicht und senkt die Entwicklungs- und Produktionskosten. Neue Geschäftsmodelle und eine gesteigerte Effizienz werden hierdurch angestrebt.

Diesen Vorteilen stehen jedoch Risiken gegenüber. Die offenen Systeme sind auch „offen" für Attacken, Manipulationen und Industriespionage. Wie verwundbar Anlagen der industriellen Automations- und Leittechnik sind, hat spätestens die Attacke von Stuxnet[1] bewiesen. Hier muss zudem bedacht werden, dass Leittechnik insbesondere auch zur Steuerung kritischer Infrastrukturen wie Energienetze, Wasserversorgung etc. eingesetzt wird.

Die Herausforderungen wachsen

Weiter gelten für die industrielle Automations- und Leittechnik besondere Anforderungen an die funktionale Sicherheit (Safety) und Echtzeitfähigkeit, um Gefährdungen für Leib und Leben abzuwenden. Folgende Charakteristiken lassen sich für die heutige Situation der IT-Sicherheit im Bereich der industriellen IT-Umgebungen gemäß unserer Erfahrungen identifizieren:

- Zunehmender Regulierungsdruck bezüglich IT-Sicherheit (durch Gesetze, Verordnungen oder industrielle Standards, siehe die aktuelle Diskussion im Smart Metering-Bereich[2]), gerade auch im Bereich der kritischen Infrastrukturen
- Industrielle Automations-und Leittechnik gerät mehr und mehr in den Fokus von Hackern, Aktivisten und Staaten
- Zunehmende netzwerktechnische Kopplung von Büro-IT und industriellen IT-Umgebungen

Aus all diesen Aspekten ergeben sich hohe Anforderungen an die IT-Sicherheit, die über die Betrachtung der einzelnen Komponenten weit hinausgehen. Es kann nicht mehr einfach davon ausgegangen werden, dass in Software gegossene Safety-Funktionen nicht durch Angriffe über TCP/IP-Verbindungen kompromittiert werden können.

Die Studie zeigt: Die Sicherheit in der Automations- und Leittechnik muss verbessert werden

Die vorliegende Studie unterstützt unsere Wahrnehmung, dass folgende Schwachstellen in der Automations- und Leittechnik häufig zu finden sind:

- Ein Sicherheitsmanagement ist zum Teil nur rudimentär aufgebaut.
- Die wertvollen Assets, Daten und Informationen sind nicht definiert.
- Prozesse wie Patchmanagement oder Security Incident Handling sind oft nicht etabliert.

1) Siehe http://www.heise.de/security/meldung/Neues-Spionageprogramm-der-Stuxnet-Entwickler-1362995.html
2) Siehe http://www.all-about-security.de/security-artikel/organisation/security-management/artikel/12563-sicherheit-im-smart-metering-das-schutzprofil-fuer-kuenftige

- Der Schutz gegen Malware ist nicht ausreichend.
- Die Fernwartungszugänge sind oft ungenügend abgesichert (z.B. erfolgt bei 42,2 Prozent der Unternehmen keine starke Authentifizierung).
- Regelmäßige Audits werden in den meisten Unternehmen nicht durchgeführt.
- Das Thema IT-Sicherheit wird gegenüber Partnern nicht ausreichend kommuniziert (nur 40,3 Prozent der Unternehmen nehmen Sicherheitsaspekte in Verträge auf; ein regelmäßiges Gespräch über IT-Sicherheit mit Herstellern und Nutzern findet nur in 29,9 Prozent der Fälle statt).

Nachhaltige IT-Sicherheit kann nur durch definierte Managementprozesse realisiert werden. Hier helfen Standards.

Um Industrieunternehmen vor den genannten Risiken und Bedrohungen zu schützen, ist ein strukturiertes Vorgehen erforderlich, wie es in international anerkannten Standards wie IEC 62443 oder ISO/IEC 27001 vorgeschlagen wird. Ziel des IEC 62443 ist es, ein Cyber Security Management System (CSMS, siehe IEC 62443-2-1, analog zum Information Security Management System (ISMS) des ISO/IEC 27001) mit den Elementen Security Policy und Sicherheitsprozess gemäß des PDCA-Zyklus (Plan-Do-Check-Act) aufzubauen. Alle wesentlichen Elemente eines Managementsystems für IT-Sicherheit sind zu implementieren: Aufbau einer IT-Sicherheitsorganisation, Erstellung und Durchsetzung von Sicherheitsrichtlinien, Business Continuity Management, Risikoanalyse und -management, Benutzer- und Rechtemanagement mit geeigneten Mechanismen für Authentifizierung und Autorisierung, physische Sicherheit, Aufbau von Netzwerksegmenten mit unterschiedlichem Sicherheitsniveau, Prozess für Sicherheitsvorfälle mit Krisen- und Notfallmanagement.

Ein solches CSMS kann nicht in einem Projekt umgesetzt werden, sondern muss als Prozess verstanden werden. Es empfiehlt sich, schrittweise vorzugehen. So beginnen viele Unternehmen mit einer Sicherheitsanalyse als erste IST-Analyse bezüglich IT-Sicherheit, durch die kritische Sicherheitslücken festgestellt werden können. Mit den Ergebnissen der Sicherheitsanalyse kann häufig erst das Bewusstsein für IT-Sicherheit beim Management geweckt werden. Sie sind Grundlage für die Definition und Umsetzung erster Sicherheitsmaßnahmen und die Erstellung von Sicherheitsrichtlinien, mit denen ein Grundschutz hinsichtlich der IT-Sicherheit (Baseline Protection) für das Unternehmen festgelegt wird. Erste Sicherheitsmaßnahmen beinhalten auch die Etablierung wesentlicher Prozesse wie Security Incident Handling, Entwicklungs- bzw. Systembereitstellungsprozess, Durchführung von Audits und Management Reviews. In einem weiteren Schritt kann das Risikomanagement aufgebaut werden. Hier kann man von den Erfahrungen aus dem Bereich Safety profitieren, da dort bereits Risikoanalysen durchgeführt werden (z.B. durch den Standard IEC 61508). Angepasste Methoden können unter Umständen übernommen werden. Ziel ist es, nicht akzeptable Risiken zu erkennen, Maßnahmen zur Reduktion der Risiken abzuleiten und umzusetzen. Grundlage für Sicherheits- und Risikoanalysen ist eine Schutzbedarfsanalyse, die den Schutzbedarf der Daten und Informationen klar identifiziert. Allerdings haben viele Unternehmen nicht definiert, welche Daten und Informationen schützenswert sind, wie dies auch in der vorliegenden Studie deutlich wird (45,4% der Unternehmen haben keine Schutzbedarfsanalyse durchgeführt).

Zur Nachverfolgung der Sicherheitsmaßnahmen sind regelmäßige Audits und Penetrationstests unerlässlich. Jedoch dürfen Penetrationstests in produktiven industriellen Umgebungen nicht durchgeführt werden. Man muss alternative Wege beschreiten, indem z.B. kritische Komponenten der Automations- und Leittechnik in einem Testlabor Penetrationstests unterzogen werden.

Bei der Definition und Umsetzung von Sicherheitsmaßnahmen muss auf jeden Fall beachtet werden, dass die Anforderungen an die Safety nicht verletzt werden dürfen: Es gilt das Prinzip „Safety First". Umgekehrt muss IT-Sicherheit so implementiert werden, dass die Kompromittierung von Safety-Funktionen möglichst verhindert wird: Es gilt das Prinzip „Security for Safety". Somit ist die bekannte Defense-in-Depth-Strategie ein bewährtes Mittel, um den Zugriff auf Safety-relevante Systeme zu unterbinden.

Ganz wesentlich ist auch der Aufbau eines Security Incident and Event Managements (SIEM), um überhaupt in der Lage zu sein, Angriffe erkennen und analysieren zu können. Ein Logging-Konzept muss hierzu alle kritischen Systeme einbeziehen. Die Logdaten sollten zentral gesammelt und sicher archiviert werden. Eine der wichtigsten Maßnahmen, die es konsequent umzusetzen gilt, ist die Schulung der Mitarbeiter zum Thema IT-Sicherheit. Leider wird dies in Unternehmen oft vernachlässigt, wie auch diese Studie aufzeigt: Nur 26,1 Prozent der Unternehmen geben an, dass sie regelmäßig Schulungen für ihre Mitarbeiter durchführen, um sie für die Gefahren von sogenanntem Social Engineering zu sensibilisieren.

Ihr
Dr. Thomas Störtkuhl
Product Manager Industrial IT Security
Embedded Systems
TÜV SÜD AG

Ausblick

Bedrohung durch Cyberwar

Das Risiko durch Cyberwar[1] steigt zwar an, es gibt jedoch viele Möglichkeiten, sich dagegen zu schützen. Umfassender Informationsschutz wird künftig zum Wettbewerbsfaktor.

CORPORATE TRUST
business risk & crisis management

Die überwiegende Mehrheit der Unternehmen ist sich bewusst, dass Industriespionage in den nächsten Jahren ansteigen wird und sie sich gegen die neuen Bedrohungen des Cyberwar[1] rüsten müssen. Der Informationsschutz wird mehr denn je zu einer wettbewerbsentscheidenden Frage. Es stehen jedoch genügend Sicherheitsvorkehrungen zur Verfügung, um sich auf diese Gefahren vorzubereiten.

Der Cyberwar wird in Zukunft vor allem durch das professionalisierte Vorgehen der Täter an Bedrohungspotenzial gewinnen. Die Angreifer werden dabei zunehmend auf umfassende Ressourcen zurückgreifen, um an ihr Ziel zu gelangen. Daher ist es wichtig, sich bei der Sicherheitsstrategie für das Unternehmen darauf einzustellen. Allerdings sollte man bei aller Hysterie nicht den Blick für das Wesentliche verlieren: Sicherheit sollte niemals Selbstzweck sein, sondern vor allem eine Service-Dienstleistung, damit die wirtschaftlichen Prozesse störungsfrei ablaufen können.

Ähnlich verhält es sich mit der IT eines Unternehmens. Diese sollte Mitarbeiter unterstützen, damit sie ihre Ideen und Aufgaben möglichst schnell umsetzen können. Sie sollte helfen und nicht blockieren. Hier müssen sich in Zukunft sowohl die IT- als auch die Sicherheitsabteilung als „Ermöglicher" und nicht als „Verhinderer" verstehen.

Es existiert zwar eine reale Bedrohung durch Cyberwar für die deutsche Wirtschaft; es gibt jedoch auch jetzt bereits eine ausreichende Anzahl von IT-Sicherheitsfunktionen, Werkzeugen zur Sensibilisierung von Mitarbeitern, Tools zur Sicherung von Gebäuden und Maßnahmen zum Schutz der kritischen Prozesse. Unternehmen sollten verstehen, dass ihre Mitarbeiter der wertvollste Schutz im Kampf gegen Industriespionage sind. Gut ausgebildete, motivierte und dem Unternehmen loyal gegenüberstehende Arbeitnehmer können jeden Tag mehr helfen und besser schützen als jedes kostspielige technische System.

Unternehmen müssen daher zuerst verstehen, dass Sicherheit bei der Organisation beginnt und nur eine positive Firmenkultur, die Fairness, Vertrauen, Zuverlässigkeit und Ehrlichkeit groß schreibt, langfristig zum Erfolg führen wird. Die Firmenkultur wird vom Management und den Führungskräften vorgelebt. Daher ist es wichtig, sowohl die Führungsverantwortlichen als auch die Mitarbeiter frühzeitig in Prozesse mit einzubinden – auch in puncto Sicherheit. Sicherheitsmaßnahmen machen nur dann Sinn, wenn sie von allen verstanden, akzeptiert und gelebt werden.

1]Cyberwar: Darunter versteht man die kriegerische Auseinandersetzung im und um den virtuellen Raum, den Cyberspace, mit Mitteln vorwiegend aus dem Bereich der Informationstechnik. Cyberwar bezeichnet auch die Aktivitäten staatlicher Spezialeinheiten, um Gegner oder sonstige Ziele online auszukundschaften bzw. sie im Ernstfall zu sabotieren.

Ausblick

Bedrohung durch Cyberwar

Informationen sind besonders gefährdet, wenn sie den schützenden Rahmen der unternehmenseigenen Infrastruktur verlassen.

brainloop

In der Praxis findet die Kooperation im Unternehmen und mit externen Geschäftspartnern schnell und möglichst barrierefrei statt. Die Grenzen zwischen „innen" und „außen" verschwimmen. Dabei geht der ungeschützte Austausch oft vertraulicher Dokumente per E-Mail, dem häufig Zeitdruck und auch ein Mangel an technologischen Alternativen zugrunde liegen, zwangsläufig zu Lasten der Datensicherheit. Informationen gehören jedoch zum wichtigsten Kapital eines Unternehmens und sollten daher durchgängig vor Missbrauch und Verlust geschützt werden.

Zunächst ist unumstritten, dass dem Mitarbeiter in der gesamten Sicherheitsthematik eine tragende Rolle zukommt. Entscheidend ist die Sensibilisierung jedes Einzelnen im Umgang mit Sicherheitsstandards im Unternehmen. Was allerdings die Handhabung vertraulicher Dokumente angeht, so gibt es inzwischen gute technologische Möglichkeiten, wie das Document Compliance Management der Brainloop AG, um die Mitarbeiter im sicheren Umgang mit vertraulichen Unterlagen anzuleiten und zu entlasten.

Wie auch die Studienergebnisse zeigen, sind Informationen besonders gefährdet, wenn sie den schützenden Rahmen der unternehmenseigenen Infrastruktur verlassen. Hier setzt die Lösung für Document Compliance Management an und bietet eine barrierefreie Zusammenarbeit im Unternehmen und mit externen Partnern, die zugleich sicher und regelkonform ist. Mit der Investition in das grenzüberschreitende Netz mit doppeltem Boden stellt das Unternehmen den webbasierten Dokumentenaustausch langfristig auf ein sicheres Fundament und erhöht die Effizienz der Zusammenarbeit.

Ebenfalls bewältigt es den vorherrschenden Spagat zwischen der Dokumentenbereitstellung und dem bestmöglichen Schutz derselben, wenn Mitarbeiter unterwegs auf vertrauliche Unterlagen zugreifen möchten. Flexibles Arbeiten und die Allzeitverfügbarkeit der Informationen prägen zunehmend das alltägliche Selbstverständnis der Mitarbeiter. Dies hat zur Folge, dass viele Anwender mit ihrem eigenen Mobile Device arbeiten – ein Umstand, dem unter Sicherheitsaspekten Rechnung getragen werden muss. Mit der Möglichkeit, mobile Endgeräte auf Serverseite zu managen, gibt Document Compliance Management auch hier die passende Antwort. Die Anonymität der Devices wird aufgehoben und sie können je nach Unternehmensentscheid für den Empfang und die Bearbeitung vertraulicher Dokumente autorisiert werden.

Da die Sicherheit der Dokumente auf der Plattform automatisch garantiert ist, wird den Mitarbeitern ein sorgloseres Vorgehen im Umgang mit ihren Unterlagen ermöglicht. Jeder sieht nur so viel, wie er für seine tägliche Arbeit braucht, und hat damit den Kopf frei für sein Kerngeschäft. Gleichzeitig werden die Mitarbeiter bei der Einhaltung verbindlicher Richtlinien im Umgang mit sensiblen Informationen bestmöglich unterstützt.

Unternehmen werden in Zukunft stärker auf standardisierte Produkte, Vorgehensweisen und Prüfungen für die IT-Sicherheit im Bereich der Automations- und Leittechnik setzen.

Die Unternehmen, die Automations- und Leittechnik einsetzen, müssen für die Zukunft von einem erhöhten Risiko ausgehen. Angriffe ähnlich der Malware Stuxnet[1], wie z.B. Duqu[2], sind zu erwarten und werden deutlich zunehmen. Das Bewusstsein für IT-Sicherheit wird für den Bereich der Automations- und Leittechnik damit deutlich wachsen (müssen). Dabei werden die Zusammenhänge zwischen der funktionalen Sicherheit (zur Abwehr von Gefährdungen von Leib und Leben) und der IT-Sicherheit zu berücksichtigen sein.

Aus all dem ergibt sich, dass der Ruf nach standardisierten Produkten, Vorgehensweisen und Prüfungen für die IT-Sicherheit im Bereich der Automations- und Leittechnik stärker werden wird, um Kosten senken und einen Investitionsschutz realisieren zu können. Nicht nur die Normen IEC 62443 oder IEC 62351 für den Energiebereich spiegeln bereits die Bemühungen für eine Standardisierung der IT-Sicherheit wider; auch die Hersteller streben bereits Zertifizierungen an, die die Qualität und Effektivität der umgesetzten Funktionen für IT-Sicherheit bestätigen.

Um jedoch die eingesetzten Produkte effektiv und effizient einsetzen zu können, ist der Aufbau eines Managements für IT-Sicherheit, ein Cyber Security Management System, unabdingbar. Ansonsten bleibt das Schließen bestimmter Sicherheitslücken nur Stückwerk. Nachhaltigkeit bezüglich IT-Sicherheit – gerade auch im Umfeld der Automations- und Leittechnik – ist nur durch definierte Prozesse möglich, die eine Kontrolle, Nachverfolgung und Verbesserung der umgesetzten Sicherheitsmaßnahmen erlauben. Speziell hier unterstützen Standardisierungen die Umsetzung und Kontrolle, da Erfahrungen zur Best Practice aus vielen Unternehmen in die Standards einfließen.

Fazit: Prävention im Bereich der industriellen Automations- und Leittechnik ist möglich und gefordert. Die Prinzipien „Safety First" und „Security for Safety" sind dabei unbedingt zu beachten. Zum Erfolg führt nur ein strukturierter Ansatz, wie er auch im Standard IEC 62443-2-1 aufgezeigt wird.

1)Stuxnet Siehe http://www.heise.de/security/meldung/Neues-Spionageprogramm-der-Stuxnet-Entwickler-1362995.html
2)Duqu Siehe http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet

Glossar

- **Abhörgeschützter Raum:** Architektonische Abschirmung eines Raumes durch technische Maßnahmen, um ungewollte Funkübertragungen zu verhindern.
- **Abschöpfen:** Gezieltes Gewinnen von Informationen, oftmals ohne dass der Mensch gegenüber weiß, dass er als Datenquelle benutzt wird oder unter Verwendung einer Legende.
- **Awareness:** Bewusstsein oder Gewahrsein über die eigene Handlung oder zur Betonung der aktiven Haltung bzw. Aufmerksamkeit gegenüber einem bestimmten Sachverhalt.
- **Background-Check:** (auch Pre-Employment-Screening) Überprüfung von Mitarbeitern bezüglich früherer Arbeitgeber, finanzieller Verhältnisse, Firmenbeteiligungen sowie verdächtiger Lebensumstände.
- **Clean-Desk-Policy:** Schriftliche Vereinbarung mit den Mitarbeitern, dass nach Arbeitsende keine schriftlichen Unterlagen offen zugänglich auf den Schreibtischen liegen gelassen werden dürfen.
- **Cloud-Service:** (auch Cloud-Computing) Umschreibt den Ansatz, abstrahierte IT-Infrastrukturen (z.B. Rechenkapazitäten, Datenspeicher, Netzwerkkapazitäten oder auch fertige Software) dynamisch an den Bedarf angepasst über ein Netzwerk zur Verfügung zu stellen. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud-Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z.B. Rechenleistung, Speicherplatz), Plattformen und Software.
- **Cyber-Kriminelle:** Täter, die für ihre Straftaten überwiegend Computer bzw. das Internet als Tatwaffe einsetzen.
- **Cyberspace:** Dient umgangssprachlich als Synonym für das Internet bzw. den virtuellen Raum.
- **Cyberwar:** Darunter versteht man die kriegerische Auseinandersetzung im und um den virtuellen Raum, den sog. Cyberspace, mit Mitteln vorwiegend aus dem Bereich der Informationstechnik. Cyberwar bezeichnet auch die Aktivitäten staatlicher Spezialeinheiten, um Gegner oder sonstige Ziele online auszukundschaften bzw. sie im Ernstfall zu sabotieren.
- **Firewall:** Ein System (meist Hard- und Software), welches dazu dient, den Netzwerkzugriff zu beschränken, basierend auf Absender- oder Zieladresse und genutzten Diensten. Sie überwacht in der Regel den durch sie hindurchlaufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht. Auf diese Weise sollen unerlaubte Netzwerkzugriffe verhindert werden.
- **Geheimhaltungsverpflichtung:** (auch Vertraulichkeitsvereinbarung) Schriftliche Vereinbarung über den Umgang mit vertraulichen Informationen.
- **Hackerangriff:** Unerlaubtes Eindringen in fremde Computer- oder Netzwerksysteme, meist durch das Überwinden von Sicherheitsmechanismen.
- **Hacktivisten:** Eine meist lose organisierte Gruppe von Hackern, die versucht, ihre politischen oder ideologischen Ziele durch Angriffe im Internet durchzusetzen.
- **Handout:** Ausgedruckte Zusammenfassung der wichtigsten Informationen zu einem Sachverhalt, z.B. einer Präsentation, einer Länderanalyse oder den Sicherheitsrisiken und Verhaltensregeln zu einem Reiseland.
- **High Potential:** Ein Hochschulabsolvent oder junger Berufstätiger (auch „Young Professional" genannt), dem man prinzipiell aufgrund seiner bisherigen Laufbahn zutraut, im Unternehmen schnell Verantwortung zu übernehmen und die Karriereleiter in rasantem Tempo zu erklimmen.
- **Industriespionage:** Umgangssprachlich für Konkurrenzausspähung oder teilweise auch Wirtschaftsspionage.
- **Integritätstest:** Psychologisches Testverfahren zur Überprüfung der Integrität am Arbeitsplatz. Der Test prüft vor allem die Bereiche „Persönlicher Arbeitsstil" und „Allgemeine Wertvorstellungen".

- **Konkurrenzausspähung:** Ausforschung, die ein konkurrierendes Unternehmen, Kriminelle oder die Medien gegen ein anderes Unternehmen betreiben.
- **Lauschangriff:** Nachrichtendienstlicher Sprachgebrauch für die akustische Überwachung bzw. das Abhören von Gesprächen.
- **Loyalitäts-Index:** Beurteilung von Unternehmen und Organisationen im Hinblick auf kriminelle und fahrlässige Handlungen von Mitarbeitern. Der Loyalitäts-Index liefert durch eine Mitarbeiterbefragung mit einer psychologisch fundierten Vorgehensweise Parameter, welche auf potenzielle Risiken hinweisen.
- **Outsourcing:** Damit wird in der Ökonomie die Abgabe von Unternehmensaufgaben und -strukturen an Drittunternehmen bezeichnet. Es ist eine spezielle Form des Fremdbezugs von bisher intern erbrachter Leistung, wobei in der Regel Verträge die Dauer und den Umfang der Leistung festschreiben.
- **Polizeiliche Kriminalstatistik** (PKS): Zusammenstellung aller der Polizei bekannt gewordenen strafrechtlichen Sachverhalte unter Beschränkung auf ihre erfassbaren wesentlichen Inhalte. Die PKS soll im Interesse einer wirksamen Kriminalitätsbekämpfung zu einem überschaubaren und möglichst verzerrungsfreien Bild der angezeigten Kriminalität führen.
- **Sensibilisierung:** Unterweisung bzw. Schulung der Mitarbeiter zu einer bestimmten Gefahrenlage mit Bezugnahme auf eine aktuelle Bedrohung.
- **Sicherheits-Policy:** (auch Sicherheitsrichtlinie oder Sicherheitsleitlinie) Beschreibt den erstrebten Sicherheitsanspruch eines Unternehmens und konzeptionell die Maßnahmen, um dorthin zu kommen.
- **Skriptkiddie:** Sinnbild für einen stereotypischen Jugendlichen, das sich alltagssprachlich auf den Bereich der Computersicherheit bezieht. Trotz mangelnder Grundlagenkenntnisse nutzt ein Skriptkiddie vorgefertigte Automatismen, um (meist unter schriftlicher Anleitung) in fremde Computersysteme einzudringen oder sonstigen Schaden anzurichten. Die Bezeichnung hat Anklänge von unreifem Verhalten und Vandalismus. Daneben besteht eine weitere Verwendung im Bereich der Computerprogrammierung. Dort nimmt der Begriff Bezug auf eine Person, die fremden Quellcode für eigene Projekte zusammenkopiert, um deren Effekte zu nutzen, ohne jedoch den Code zu verstehen.
- **Social Engineering:** Ausspionieren über das persönliche Umfeld, durch zwischenmenschliche Beeinflussung bzw. durch geschickte Fragestellung, meist unter Verschleierung der eigenen Identität (Verwenden einer Legende). Social Engineering hat das Ziel, unberechtigt an Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen.
- **Soft Skills:** (Soziale Kompetenz) Die Gesamtheit der persönlichen Fähigkeiten und Einstellungen, die dazu beitragen, individuelle Handlungsziele mit den Einstellungen und Werten einer Gruppe zu verknüpfen und in diesem Sinne auch das Verhalten und die Einstellungen von Mitmenschen zu beeinflussen.
- **Steuerungsanlagen:** (Industrielle Automations- und Leittechnik) Alle Hard- und Softwarekomponenten, die für einen sicheren und zuverlässigen Betrieb eines Industrieprozesses notwendig sind sowie alle Prozesse, die darauf einwirken oder diesen beeinflussen können.
- **Sweep:** Absuche nach Wanzen mit technischen Geräten durch Hochfrequenz-Spezialisten. Dient in der Regel der Lauschabwehr.
- **Trojaner:** Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund jedoch ohne Wissen des Anwenders eine andere Funktion ausführt.
- **Vertraulichkeitsvereinbarung:** (auch Geheimhaltungsverpflichtung) Schriftliche Vereinbarung über den Umgang mit vertraulichen Informationen.
- **Wanzen:** Technische, meist miniaturisierte Bauteile bzw. Funksender zum Abhören von Gesprächen oder Aufzeichnen von Informationen.
- **Whistle-Blowing:** Ein Informant bringt Missstände, illegales Handeln oder allgemeine Gefahren, von denen er an seinem Arbeitsplatz erfährt, an die Öffentlichkeit.
- **Wirtschaftsspionage:** Staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben.

Ansprechpartner

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

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

Florian Oelmaier
Leiter IT-Sicherheit & Computerkriminalität
Corporate Trust,
Business Risk & Crisis Management GmbH

www.corporate-trust.de
oelmaier@corporate-trust.de

Die Studie **„Industriespionage 2012 - Aktuelle Risiken für die deutsche Wirtschaft durch Cyberwar"** wurde durch die Corporate Trust - Business Risk & Crisis Management GmbH erstellt. Begleitet wurde die Studie durch die Brainloop AG und die TÜV SÜD AG.

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

Peter Weger
Chief Executive Officer
Brainloop AG

www.brainloop.com
peter.weger@brainloop.de

Dr. Thomas Störtkuhl
Product Manager Industrial IT Security
Embedded Systems
TÜV SÜD AG

www.tuev-sued.com/embedded
thomas.stoertkuhl@tuev-sued.de

CORPORATE TRUST
Business Risk & Crisis Management GmbH

Graf-zu-Castell-Straße 1
D-81829 München

Tel.: +49 89 599 88 75 80
Fax: +49 89 599 88 75 820

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

Regelmäßig aktuelle Informationen
von Sicherheitsexperten

Follow us: twitter
www.twitter.com/corporatetrust