CORPORATE TRUST
business risk & crisis management

Studie: Industriespionage 2014

Cybergeddon der deutschen Wirtschaft durch NSA & Co.?

Begleitet durch: AON SECURITON ZURICH

Inhalt

Glück entsteht oft durch Aufmerksamkeit in kleinen Dingen,
Unglück oft durch Vernachlässigung kleiner Dinge.

Wilhelm Busch

Vorwort

Christian Schaaf
Geschäftsführer
Corporate Trust

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

Der Begriff „Cyber" scheint mittlerweile allgegenwärtig zu sein und kaum ein Lebensbereich bleibt davon verschont. Immer häufiger hört man vom „Internet der Dinge" – gemeint ist damit die Vernetzung von Alltagsgegenständen, um uns das Leben zu erleichtern. Die Zukunft verspricht uns Autos, die den Fahrer nicht nur bei der schnellsten Routenführung unterstützen, sondern gleich selbst fahren. Die Steuerung der Hauselektronik können wir bequem per Fernzugriff über das Internet erledigen und der Kühlschrank meldet selbstständig, wenn die Milch ausgeht. Moderne Uhren zeigen nicht mehr nur die Zeit, sondern zeichnen jede Laufstrecke auf, messen unseren Puls und informieren den Arzt, wenn etwas ungewöhnlich ist. Unser Privatleben verlagert sich damit mehr und mehr ins Internet und die Daten werden öffentlicher.

Während wir uns im privaten Bereich noch fragen können, ob wir dieser Technisierung an allen Stellen Einzug in unser Leben gewähren wollen, scheint es für den wirtschaftlichen Bereich kaum Alternativen zu geben. Die technischen Errungenschaften des Internets haben zu einer Beschleunigung bei den Prozessen und einer globalen Vernetzung der Unternehmen mit Lieferanten, Joint-Venture-Partnern, Dienstleistern und Kunden geführt. Die meisten Maschinen verfügen über Steuerungsgeräte, die bei Bedarf auch über das Internet gewartet werden können, sodass kein Techniker mehr vor Ort sein muss. Eine gut funktionierende IT-Infrastruktur wird immer wichtiger: PC, Laptop, Tablet oder Smartphone sind aus dem Business-Alltag kaum mehr wegzudenken. Für Unternehmen in Deutschland und Österreich steigt durch die fortschreitende Digitalisierung und Vernetzung der Systeme jedoch auch immer mehr ihre Anfälligkeit für Cyberattacken[1].

Die Anzahl von Hackerangriffen[2], Viren[3], Trojanern[4] oder sonstiger Malware[5] nimmt rasant zu. Auch wenn es sich in vielen Fällen um Angriffe der Organisierten Kriminalität[6], konkurrierender Unternehmen oder sogenannter Hacktivisten[7] handelt, nimmt die Spionage durch ausländische Nachrichtendienste ebenfalls ständig zu. Der Whistleblower Edward Snowden veröffentlichte am 9. Juni 2013 erstmals Informationen über die Spähprogramme PRISM[8] und TEMPORA[9] des amerikanischen Nachrichtendienstes NSA[10] sowie des englischen GCHQ[11]. Deutsche Unternehmen werden offen-

1) Cyberattacke: Der gezielte Angriff von außen auf größere, für eine spezifische Infrastruktur wichtige Computernetzwerke.
2) Hackerangriff: Unerlaubtes Eindringen in fremde Computer- oder Netzwerksysteme, meist durch das Überwinden von Sicherheitsmechanismen.
3) Virus (Computervirus): Ein sich selbst verbreitendes Computerprogramm, welches sich in andere Computerprogramme einschleust und sich damit reproduziert. Die Klassifizierung als Virus bezieht sich hierbei auf die Verbreitungs- und Infektionsfunktion. Einmal gestartet kann es vom Anwender nicht kontrollierbare Veränderungen am Status der Hardware, am Betriebssystem oder an der Software vornehmen (Schadfunktion). Viren zählen zur Malware.
4) Trojaner: Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund jedoch ohne Wissen des Anwenders eine andere Funktion ausführt.
5) Malware: Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Malware ist ein Oberbegriff, der u. a. auch den Computervirus umfasst.
6) Organisierte Kriminalität: So werden Tätergruppierungen (Banden) bezeichnet, bei denen mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig zusammenwirken, um die von Gewinn- und Machtstreben bestimmte planmäßige Begehung von Straftaten durchzuführen, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, und dabei gewerbliche oder geschäftsähnliche Strukturen verwenden, Gewalt oder andere zur Einschüchterung geeignete Mittel anwenden und Einfluss auf Politik, Massenmedien, öffentliche Verwaltungen, Justiz oder die Wirtschaft nehmen.

sichtlich auch von befreundeten Staaten ausspioniert. Es ist unbestritten, dass eine gewisse staatliche Überwachung der Kommunikationsströme nötig ist, um Verbrechen aufzuklären oder bestenfalls sogar zu verhindern. Deutschland und Österreich sind hier vermutlich in vielen Fällen auf die Unterstützung des großen Bündnispartners USA angewiesen. Aber wie viel Überwachung muss sein und wer kann zukünftig die Einhaltung der Grenzen des staatlichen Zugriffs kontrollieren?

Persönlich wird sich für uns alle in Zukunft die Frage stellen, inwieweit Überwachung in einem Rechtsstaat tatsächlich nötig ist und wo wir ihr zustimmen. Die Anschläge des 11. September 2001 haben gezeigt, wie verletzlich wir durch Terroranschläge sind. Daraufhin wurden in den USA eine ganze Reihe von Gesetzen und Sonderbefugnissen erlassen, die mehr staatliche Kontrolle und praktisch einen uneingeschränkten Zugriff auf elektronische Kommunikation erlauben. Die Möglichkeiten der Überwachung können jedoch auch für andere Zwecke genutzt und nicht alle Anschläge damit verhindert werden, wie das Attentat beim Boston-Marathon am 15. April 2013 gezeigt hat. Wollen wir also langfristig einer weltweiten Überwachung sämtlicher Kommunikation und jedes Klicks im Internet zustimmen, auch wenn wir damit vielleicht nur eine „vermeintliche" Sicherheit erlangen, oder müssen wir im privaten Umfeld künftig noch mehr Wert auf die Vertraulichkeit unserer Daten legen?

Für die Unternehmen wird es langfristig sogar eine Überlebensfrage sein, wie wichtig sie den Schutz ihrer sensiblen Daten nehmen und wie sie mit ihrer Kommunikation umgehen. Die Innovationsfähigkeit unserer Wirtschaft bei der Entwicklung hochwertiger Produkte garantiert ein wachsendes Bruttoinlandsprodukt; selbstverständlich kann dies Begehrlichkeiten wecken. Viele der großen Industrienationen haben mittlerweile ganze Heerscharen von eigenen Hacker-Teams, die für staatliche Zwecke Daten beschaffen. Es stellt sich die Frage, ob damit der wirtschaftliche Wettbewerb von Unternehmen in einigen Ländern zunehmend mit staatlicher Unterstützung geführt wird und wir uns bereits im „Cybergeddon"[12] befinden?

Die Bedrohung für die deutsche Wirtschaft ist sehr real und richtet jährlich einen Milliardenschaden an. Corporate Trust hat zusammen mit AON Risk Solutions, der Securiton GmbH und der Zurich Gruppe Deutschland eine Befragung in Deutschland und Österreich durchgeführt, um die aktuelle Bedrohung und den tatsächlichen Schaden für die Wirtschaft zu erheben. Dies soll zu einer Sensibilisierung aller Wirtschaftsbeteiligten führen und den Unternehmen ermöglichen, das eigene Gefährdungspotenzial realistisch einzuschätzen. Nur wer den Feind und die Angriffswege kennt, kann entsprechend reagieren!

In diesem Sinne wünsche ich Ihnen viel Vergnügen bei der Lektüre der vorliegenden Studie. Selbstverständlich freuen wir uns immer über Anregungen oder Hinweise zu aktuellen Fällen.

Ihr

Christian Schaaf

7) Hacktivisten:	Eine meist lose organisierte Gruppe von Hackern, die versucht, ihre politischen oder ideologischen Ziele durch Angriffe im Internet durchzusetzen.
8) PRISM:	Ein seit 2005 existierendes und als Top Secret eingestuftes Programm zur Überwachung und Auswertung elektronischer Medien und elektronisch gespeicherter Daten. Es wird von der NSA betrieben und ermöglicht die umfassende Überwachung von Personen, die digital kommunizieren, innerhalb und außerhalb der USA.
9) TEMPORA:	Codename für eine britische Geheimdienstoperation des GCHQ zur Überwachung des weltweiten Telekommunikations- und Internet-Datenverkehrs.
10) NSA (National Security Agency):	Größter Auslandsgeheimdienst der Vereinigten Staaten von Amerika. Die NSA ist für die weltweite Überwachung, Entschlüsselung und Auswertung elektronischer Kommunikation zuständig und in dieser Funktion ein Teil der Intelligence Community, in der sämtliche Nachrichtendienste der USA zusammengefasst sind.
11) GCHQ (Government Communications Headquarters):	Eine britische Regierungsbehörde (Nachrichtenbehörde und Sicherheitsdienst), die sich mit Kryptografie, Verfahren zur Datenübertragung und mit der Fernmeldeaufklärung befasst.
12) Cybergeddon:	An „Armageddon" oder „Harmagedon" angelehnter Begriff, der eine finale oder endzeitliche Entscheidungsschlacht im Cyberraum (virtueller Raum aller auf Datenebene vernetzten IT-Systeme im globalen Internet) bezeichnen soll.

Vorwort

Dr. Hans-Georg Maaßen
Präsident
Bundesamt für Verfassungsschutz

Wirtschafts- und Industriespionage - die reale Bedrohung.

„Made in Germany“ ist begehrt!

Das Know-how deutscher Unternehmen – „Made in Germany“ – ist weltweit begehrt, auch bei fremden Nachrichtendiensten und ausländischen Wettbewerbern.

In einem sich zunehmend verschärfenden wirtschaftlichen Wettbewerb um Produkte und Absatzmärkte richten sich Wirtschaftsspionage und Konkurrenzausspähung verstärkt gegen technologieorientierte und innovative mittelständische Unternehmen - das Rückgrat der deutschen Industrie. Aus Erfahrung wissen wir, dass sich diese Unternehmen der Risiken ungewollten Know-how-Verlustes oft nur wenig bewusst sind und selten über ein wirksames Informationsschutzkonzept verfügen.

Die Ergebnisse der Studie „Industriespionage 2014“ von „Corporate Trust“ zeigen erneut: Die Bedrohung ist real. Jedes zweite der befragten Unternehmen hat in den vergangenen zwei Jahren einen vermuteten oder konkreten Spionagevorfall festgestellt. Im besonderen Maße waren hiervon mittelständische Unternehmen des Maschinenbaus betroffen. Die Ergebnisse sind nicht überraschend. Sie bestätigen sowohl die bisherigen Studienergebnisse von „Corporate Trust“ als auch das Lagebild der Spionageabwehr des BfV.

Das Bedrohungsszenario ist umfassend. Neben klassischen Methoden der Spionage hat das digitale Zeitalter neue, bislang ungeahnte Möglichkeiten der Spionage und Sabotage eröffnet. Doch auch

unter den geänderten Vorzeichen bleibt der Faktor Mensch entscheidend für die Sicherheit eines Unternehmens. Sichere IT ist ohne den sensibilisierten und sicherheitsbewusst handelnden Mitarbeiter kaum realisierbar.

Das BfV als Dienstleister für Spionageabwehr und Wirtschaftsschutz!

Noch viel zu selten wenden sich betroffene Unternehmen an die Verfassungsschutzbehörden. Der beste Schutz, einen Schadensfall zu verhindern bzw. seine Auswirkungen zu begrenzen, ist die Prävention. Das Leitmotiv der umfassenden Security-Awareness der Verfassungsschutzbehörden ist daher „Prävention durch Information". Die Verfassungsschutzbehörden sehen sich als Partner der Unternehmen und bieten ihnen kompetente und vertrauenswürdige Sensibilisierung sowie Unterstützung in Schadensfällen an. Mittelständische Unternehmen sind hierbei eine der Kernzielgruppen des Wirtschaftsschutzkonzeptes der Verfassungsschutzbehörden

Wirtschaftsschutz ist Teamwork!

Die vorliegende Studie von „Corporate Trust" belegt erneut, dass die vielfältigen Herausforderungen im Wirtschaftsschutz ein Zusammenwirken von Staat und Wirtschaft erfordern. Nur mit gegenseitigem Verständnis und gemeinsamen Handeln lässt sich ein effektiver Wirtschaftsschutz realisieren. Eine sichere Wirtschaft leistet auch einen Beitrag zu sozialer Sicherheit und gesellschaftlicher Stabilität unseres Landes. Wirtschaftsschutz ist daher nicht nur ein Wettbewerbsvorteil, sondern auch ein Stück Zukunftssicherung.

Ihr
Dr. Hans-Georg Maaßen

Ergebnisse in Kürze

- Jedes zweite Unternehmen hatte in den vergangenen beiden Jahren einen Spionageangriff oder Verdachtsfall zu beklagen. Konkret waren 26,9 Prozent in Deutschland und 27,1 Prozent in Österreich von einem konkreten Vorfall betroffen. Weitere 27,4 Prozent (Deutschland) bzw. 19,5 Prozent (Österreich) hatten zumindest einen Verdachtsfall.
  In Deutschland stellt dies einen Anstieg um 5,5 Prozent im Vergleich zu den Ergebnissen aus der Studie 2012 dar. Für Österreich wurden die Zahlen erstmalig erhoben.

- Der jährliche finanzielle Schaden durch Industriespionage beläuft sich in Deutschland auf 11,8 Milliarden Euro und in Österreich auf 1,6 Milliarden Euro. Für die Berechnung des Schadens wurden 300.000 Unternehmen in Deutschland und 42.000 Unternehmen in Österreich berücksichtigt. Bei der Studie wurden nur Unternehmen mit mehr als 10 Mitarbeitern sowie einem Umsatz bzw. einer Bilanzsumme von mehr als 1 Million Euro befragt.

- 77,5 Prozent (Deutschland) bzw. 75,0 Prozent (Österreich) der betroffenen Unternehmen hatten durch die Spionageangriffe einen finanziellen Schaden zu verzeichnen. Bei einem Großteil der Firmen lag der Schaden zwischen 10.000 und 100.000 Euro. Immerhin 4,5 Prozent (Deutschland) bzw. 3,1 Prozent (Österreich) hatten sogar einen Schaden über 1 Million Euro zu beklagen.

- Mehr als ein Drittel aller Unternehmen (Deutschland: 40,8 Prozent; Österreich: 36,4 Prozent) hatte einen materiellen Schaden zu verzeichnen. Am meisten hatten die Unternehmen mit dem Ausfall bzw. Diebstahl oder der Schädigung von IT- oder Telekommunikationsgeräten zu kämpfen (Deutschland: 53,0 Prozent; Österreich: 58,1 Prozent). An zweiter Stelle bei den Auswirkungen lagen in Deutschland mit 26,8 Prozent und in Österreich mit 23,3 Prozent die Umsatzeinbußen durch den Verlust von Wettbewerbsvorteilen.

- Unternehmen erleiden durch Industriespionage aber auch immaterielle Schäden; 37,1 Prozent in Deutschland und 30,5 Prozent in Österreich waren insgesamt davon betroffen. Am häufigsten waren Patentrechtsverletzungen (Deutschland: 54,3 Prozent; Österreich: 58,3 Prozent) sowie Imageschäden bei Kunden oder Lieferanten (Deutschland: 26,8 Prozent; Österreich: 22,2 Prozent).

- Nach wie vor steht der Mittelstand verstärkt im Fokus der Angreifer. Die Beteiligung mittelständischer Unternehmen an der Studie war zwar am stärksten (Deutschland: 67,7 Prozent; Österreich: 62,7 Prozent), im Verhältnis zur Beteiligung waren hier die Schäden jedoch auch am höchsten. In Deutschland wurden 30,8 Prozent der mittelständischen Unternehmen, 23,5 Prozent der Konzerne und 17,2 Prozent der Kleinunternehmen geschädigt. In Österreich lagen die Schadensraten näher zusammen: Hier waren 29,7 Prozent der mittelständischen Unternehmen, 28,6 Prozent der Konzerne und 23,3 Prozent der Kleinunternehmen betroffen.

- Der Maschinenbau ist wieder die am stärksten in Mitleidenschaft gezogene Branche. 50 Prozent aller Schäden ereigneten sich in nur drei (Deutschland) bzw. vier (Österreich) Branchen. Der Automobil-, Luftfahrzeug-, Schiffs- und Maschinenbau war mit 22,5 Prozent in Deutschland und 18,2 Prozent in Österreich jeweils die am stärksten betroffene Gruppe.

- Unternehmen werden vor allem in Asien, Osteuropa und den GUS-Staaten durch Spionage geschädigt. Bei den meisten Angriffen fällt es vermutlich schwer, genau zu identifizieren, wo der Informationsabfluss bzw. die Spionage stattfand. Trotzdem konnten Unternehmen die Angriffe in vielen Fällen eingrenzen. Demnach fanden bei deutschen Unternehmen die meisten Angriffe in Asien (38,8 Prozent), den GUS-Staaten (32,6 Prozent) und Osteuropa (31,7 Prozent) statt. Österreichische Unternehmen wurden am häufigsten in Osteuropa (36,4 Prozent) und den GUS-Staaten (30,9 Prozent) geschädigt.

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

2) 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.

- Am häufigsten wurden von den Unternehmen Hackerangriffe[1] auf EDV-Systeme und Geräte (Deutschland: 49,6 Prozent; Österreich: 41,8 Prozent) festgestellt. Die zweithäufigste Angriffsform war ebenfalls technischer Natur: Das Abhören bzw. Abfangen von elektronischer Kommunikation wurde in Deutschland in 41,1 Prozent und in Österreich in 40,0 Prozent der Fälle festgestellt. In Deutschland war Social Engineering[2] mit 38,4 Prozent die dritthäufigste Angriffsform, in Österreich die bewusste Informations- oder Datenweitergabe bzw. der Datendiebstahl durch eigene Mitarbeiter (38,2 Prozent).

- Forschung und Entwicklung (Deutschland: 26,3 Prozent; Österreich: 18,2 Prozent) sowie die Bereiche IT-Administration/IT-Service (Deutschland: 21,4 Prozent; Österreich 21,8 Prozent) waren in beiden Ländern die begehrtesten Spionageziele. An dritter Stelle lag in Deutschland der Vertrieb mit 18,3 Prozent (Österreich: 14,6 Prozent) und in Österreich der Bereich Mergers & Acquisitions mit 16,4 Prozent (Deutschland: 14,7 Prozent).

- Hacker stellen mittlerweile die größte Tätergruppe dar. In Deutschland gaben 41,5 Prozent und in Österreich 32,7 Prozent aller Unternehmen an, Hacker als Täter identifiziert zu haben. Während in Deutschland Kunden oder Lieferanten mit 26,8 Prozent die zweitgrößte Tätergruppe darstellten, waren es in Österreich mit 30,9 Prozent die eigenen Mitarbeiter (vor den Kunden oder Lieferanten mit 23,6 Prozent).

- Unternehmen versuchen Angriffe in der Regel selbst zu lösen, ohne fremde Unterstützung. Nur bei einem Viertel der Fälle in Deutschland (25,9 Prozent) und nur etwa bei jedem siebten Fall in Österreich (14,6 Prozent) wurden staatliche Stellen oder externe Spezialisten von den Unternehmen hinzugezogen. Zu groß ist anscheinend immer noch die Angst, dass etwas an die Öffentlichkeit durchsickern könnte.

- In Deutschland kümmert sich meistens der Chef um den Informationsschutz (34,4 Prozent), in Österreich ist dies überwiegend Aufgabe der IT-Abteilung (33,1 Prozent). Erstaunlich ist, dass in Deutschland 14,8 Prozent der Unternehmen angaben, dass sich niemand um den Informationsschutz kümmert. Dies ist eine Steigerung von 8,1 Prozent im Vergleich zur Studie von 2012 (6,7 Prozent). In Österreich waren es gar 32,2 Prozent der Firmen, die keinen Verantwortlichen für die Belange des Informationsschutzes hatten.

- Nicht einmal jedes zwanzigste Unternehmen hat die finanziellen Risiken eines Datenverlustes vernünftig abgesichert: Nur 3,6 Prozent der deutschen und 3,4 Prozent der österreichischen Firmen verfügen über eine entsprechende Cyber-Versicherung. 24,2 Prozent (Deutschland) bzw. 22,0 Prozent (Österreich) wollen sich dies zumindest für die Zukunft überlegen. Allerdings gaben auch nur 28,9 Prozent der deutschen und 36,4 Prozent der österreichischen Firmen an, ausreichend über die am Markt verfügbaren Versicherungslösungen informiert zu sein.

- Den Unternehmen in beiden Ländern ist bewusst, dass Industriespionage noch deutlich zunehmen wird. Lediglich 26,5 Prozent in Deutschland und 21,1 Prozent in Österreich glauben, dass die Bedrohung durch Spionage gleich bleiben wird; die überwiegende Mehrheit (Deutschland: 52,6 Prozent; Österreich: 41,7 Prozent) geht davon aus, dass sie zunehmen wird, 28,6 Prozent (Deutschland) bzw. 26,3 Prozent (Österreich) erwarten sogar einen starken Anstieg.

- Unternehmen unterschätzen den Wert von Cyber-Versicherungen für den Risikotransfer. Auf die Frage, wie wichtig Cyber-Versicherungen zukünftig für sie seien, gaben zumindest 74,3 Prozent (Deutschland) bzw. 72,0 Prozent (Österreich) der Unternehmen an, dass sie dies für optional hielten. Etwa jedes zehnte Unternehmen (Deutschland: 10,1 Prozent; Österreich: 8,5 Prozent) hält sie leider für unnötig.

Methodik der Studie

Die Studie „Industriespionage 2014 – Cybergeddon der Wirtschaft durch NSA & Co.?" wurde in Zusammenarbeit mit AON Risk Solutions, der Securiton GmbH und der Zurich Gruppe Deutschland erstellt. Erstmalig wurden sowohl in Deutschland als auch in Österreich das Risiko und die aktuellen Vorfälle erfasst. Für die Erstellung der Studie wurde nach dem Zufallsprinzip ein repräsentativer Querschnitt aller Firmen ausgewählt und dann 6.767 Unternehmen in Deutschland sowie 1.396 Unternehmen in Österreich befragt.

Industriespionage findet nicht nur bei den Großunternehmen statt, sondern schädigt sämtliche Wirtschaftsbereiche, vom Konzern über den Mittelstand bis hin zu den Kleinunternehmen. Für die Studie war es wichtig, eine möglichst umfassende Lageeinschätzung für Deutschland und Österreich abgeben zu können. Daher wurde die Befragung branchenübergreifend und quer über alle Unternehmensgrößen durchgeführt. Berücksichtigt wurden jedoch in beiden Ländern nur Unternehmen mit mindestens zehn Mitarbeitern und einem Umsatz bzw. einer Bilanzsumme über einer Million Euro.

Da es keine verbindlichen Definitionen für die Einordnung in eine Unternehmensgröße gibt, wurden für Deutschland die Kriterien des Instituts für Mittelstandsforschung Bonn und für Österreich die KMU-Definition der Wirtschaftskammer Österreich angelegt. Die Bewertung richtete sich daher nach der Anzahl der Mitarbeiter und dem Umsatzvolumen. Darüber hinaus wurde es jedoch den Unternehmen selbst überlassen, sich in eine Kategorie (Konzern, Mittelstand, Kleinunternehmen) einzuordnen. Dies sollte vor allem inhabergeführten Unternehmen die Möglichkeit bieten, sich aufgrund ihrer mittelständisch geprägten Ausrichtung und Führungskultur dem Mittelstand zuzurechnen, obwohl sie häufig über mehr Mitarbeiter und ein größeres Umsatzvolumen verfügen.

Für die Befragung wurden im April 2014 insgesamt 8.163 Vorstände, Geschäftsführer bzw. Leiter für die Bereiche Risikomanagement, Unternehmenssicherheit, Informationsschutz, Recht, Finanzen, Controlling, IT, Interne Revision, Compliance oder Personal postalisch und per E-Mail mit einem standardisierten Fragebogen angeschrieben. Den Unternehmen wurde es freigestellt, die Befragung anonym durchzuführen oder das Unternehmen zu nennen. Als kleines Dankeschön für ihre Beteiligung erhalten sie eine kostenlose Erstberatung.

Die Befragung konnte auch online durchgeführt werden. Dazu wurden sowohl in der E-Mail als auch im postalischen Anschreiben für alle Teilnehmer gleiche Benutzerdaten (Benutzername und Passwort) mitgeteilt. Dies sollte gewährleisten, dass keine „Zufallsbesucher" der Studien-Webseite die Befragung ausfüllen konnten, sondern nur teilnahmeberechtigte Firmen. Zusätzlich wurden 30 Unternehmen in telefonischen Interviews direkt zu ihren Erfahrungen mit Industriespionage befragt.

Von allen angeschriebenen Unternehmen antworteten genau 530 Teilnehmer (6,5 Prozent aller befragten Firmen). Von den Teilnehmern stammten 412 Antworten aus Deutschland und 118 Antworten aus Österreich. Dies entspricht einer Beteiligung von 6,1 Prozent in Deutschland und von 8,5 Prozent in Österreich. Die Gesamtbeteiligung lag damit etwas niedriger als in den Vorjahren (2007: 9,9 Prozent; 2012: 8,6 Prozent). Dies ist vermutlich auf eine verstärkte Zahl von Umfragen zu den Themen Spionage und Cybercrime in den letzten Monaten zurückzuführen und hat damit evtl. zu einer gewissen „Teilnahmemüdigkeit" geführt. Die relativ hohe Beteiligung in Deutschland und Österreich (6,1 Prozent bzw. 8,5 Prozent) zeigt auch, dass dieses Thema in beiden Ländern eine wichtige Rolle für die Wirtschaft spielt.

Wie bei den Studien zuvor wurden im ersten Bereich der Befragung Informationen zum Unternehmen erhoben. Anschließend wurden Vorfälle, erkannte Schäden und erwartete Risiken für die Zukunft, aktuelle Sicherheitsvorkehrungen sowie mögliche Schwachstellen erfasst. Die Befragung wurde 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 anzugeben. Bei den meisten Fragen waren Mehrfachantworten zugelassen.

Corporate Trust möchte sich auf diesem Wege ganz herzlich bei AON Risk Solutions, der Securiton GmbH und der Zurich Gruppe Deutschland für ihre partnerschaftliche Begleitung sowie bei allen Teilnehmern für ihren wesentlichen Beitrag zum Gelingen der Studie bedanken.

Teilnahme an der Studie

GRAFIK 1

Quelle: Corporate Trust 2014

Betroffene Unternehmen

Jedes zweite Unternehmen hatte in den vergangenen beiden Jahren einen konkreten Spionageangriff oder Verdachtsfall.

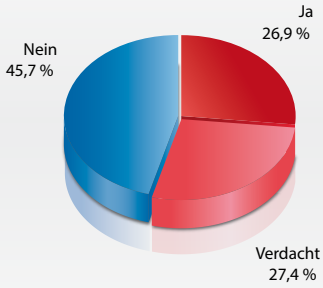
Die Schäden durch Industriespionage nehmen deutlich zu. Während bei der letzten Befragung im Jahr 2012 in Deutschland nur 21,4 Prozent aller befragten Unternehmen einen konkreten Spionagevorfall zu beklagen hatten, waren es bei der aktuellen Studie bereits 26,9 Prozent, die in den vergangenen beiden Jahren durch Spionage geschädigt wurden. Dies stellt einen Anstieg um 5,5 Prozent dar. In Österreich wurde die Befragung zum ersten Mal durchgeführt, daher gibt es keine Vergleichszahlen aus den Vorjahren. Trotzdem stellt Spionage auch hier eine ernst zu nehmende Bedrohung dar. Über ein Viertel aller Unternehmen hatte einen konkreten Spionagevorfall, genau 27,1 Prozent.

Zählt man die Verdachtsfälle mit hinzu – in Deutschland immerhin weitere 27,4 Prozent und in Österreich 19,5 Prozent –, so musste sich in den beiden Ländern rund jede zweite Firma (in Deutschland exakt 54,3 Prozent und in Österreich 46,6 Prozent) mit einem Spionagevorfall im eigenen Unternehmen befassen.

Die hohe Zahl der Verdachtsfälle belegt abermals eindeutig, dass Spionage meistens schwer nachzuweisen bzw. überhaupt erst festzustellen ist. In vielen Fällen gibt es zwar den Verdacht auf Plagiate, Konkurrenzprodukte, die den eigenen Entwicklungen ähnlich sehen, oder Wettbewerbsvorteile durch ausspioniertes Know-how, jedoch keinerlei Hinweise auf die Täter. Daher ist für die meisten Unternehmen schwer zu benennen, ob es sich um Spionage durch einen ausländischen Nachrichtendienst, die Konkurrenz, Organisierte Kriminalität[1], einen versierten Hacker[2] oder einfach durch eigene Mitarbeiter handelt.

Gab es in Ihrem Unternehmen konkrete Spionagefälle?

Deutschland

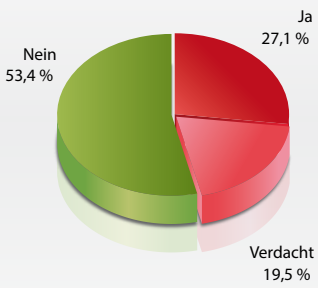


GRAFIK 2

Quelle: Corporate Trust 2014

Gab es in Ihrem Unternehmen konkrete Spionagefälle?

Österreich



GRAFIK 3

Quelle: Corporate Trust 2014

1) Organisierte Kriminalität: So werden Tätergruppierungen (Banden) bezeichnet, bei denen mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig zusammenwirken, um die von Gewinn- und Machtstreben bestimmte planmäßige Begehung von Straftaten durchzuführen, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, und dabei gewerbliche oder geschäftsähnliche Strukturen verwenden, Gewalt oder andere zur Einschüchterung geeignete Mittel anwenden und Einfluss auf Politik, Massenmedien, öffentliche Verwaltungen, Justiz oder die Wirtschaft nehmen.

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

Betroffene Unternehmen

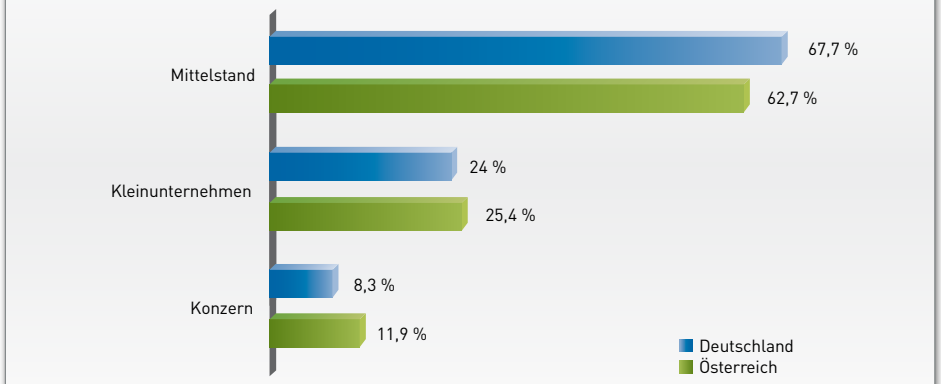
Nach wie vor ist der Mittelstand verstärkt im Fokus der Angreifer.

Um die Unternehmen nach ihrer Größe kategorisieren zu können, wurden die Kennziffern „Umsatz" und „Mitarbeiterzahl" abgefragt. Darüber hinaus wurde den Unternehmen die Möglichkeit gegeben, sich selbst einer Kategorie zuzuordnen, da bei den Befragungen der Vorjahre festgestellt wurde, dass sich viele Unternehmen trotz höheren Mitarbeiter- und Umsatzzahlen noch dem Mittelstand zuordnen. Demnach lag die Teilnahmequote an der Befragung in Deutschland bei 24,0 Prozent Kleinunternehmen, 67,7 Prozent mittelständische Unternehmen und 8,3 Prozent Konzerne. In Österreich wurde ein ähnliches Ergebnis erreicht: Hier wirkten 25,4 Prozent Kleinunternehmen, 62,7 Prozent mittelständische Unternehmen und 11,9 Prozent Konzerne an der Befragung mit.

Bei den geschädigten Unternehmen zeigte sich in beiden Ländern ein klares Bild. Der Mittelstand ist im Verhältnis am stärksten durch Spionage betroffen; in Deutschland hatten 30,8 Prozent der teilnehmenden mittelständischen Unternehmen einen konkreten Angriff zu verzeichnen, in Österreich 29,7 Prozent. Während in Deutschland der Abstand zu den am zweithäufigsten betroffenen Konzernen (23,5 Prozent) relativ deutlich ausfällt, waren in Österreich die Konzerne mit 28,6 Prozent annähernd gleich häufig geschädigt wie der Mittelstand.

Gerade der Mittelstand ist daher gut beraten, das Thema Industriespionage nicht auf die leichte Schulter zu nehmen. Er repräsentiert in der Regel einen Großteil der Unternehmen in beiden Ländern, stellt die meisten Arbeitsplätze und garantiert durch permanente Innovationen und hohe Qualität eine wachsende Wirtschaftsleistung. Während Kleinunternehmen in der Regel international nicht so präsent sind und damit weniger wahrgenommen werden, steht der Mittelstand heute ähnlich wie die großen Konzerne voll im Blickpunkt und weckt Begehrlichkeiten.

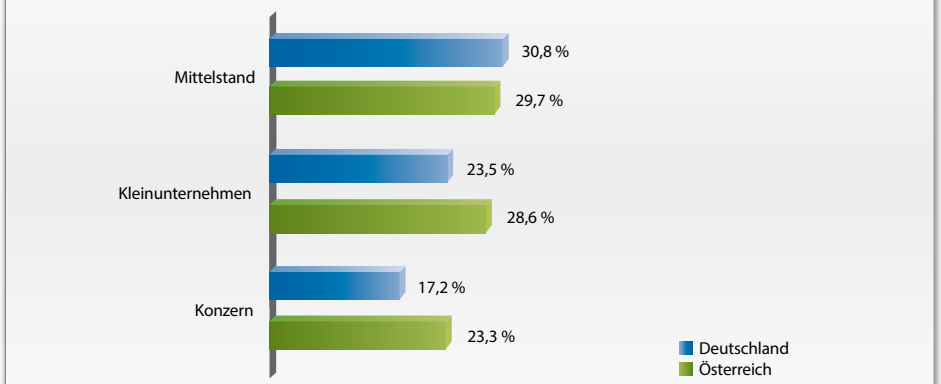
Teilnahme an der Studie



GRAFIK 4

Quelle: Corporate Trust 2014

Schäden im Verhältnis zur Teilnahme an der Studie



GRAFIK 5

Quelle: Corporate Trust 2014

Nie zuvor in der Geschichte der Menschheit war
der Zugang zu Informationen so schnell und einfach.

Vinton Cerf

Betroffene Unternehmen

Der Maschinenbau ist wieder die am stärksten betroffene Branche.

Bei der aktuellen Studie war auffallend, dass über 50 Prozent aller Schäden in nur drei (Deutschland) bzw. vier Branchen (Österreich) entstanden. Die Spionage richtete sich vermutlich in den meisten Fällen gegen Unternehmen, deren Produkte und Dienstleistungen aufgrund ständiger Innovationen und hoher Qualitätsstandards weltweit geschätzt werden. Gütesiegel wie „Made in Germany" oder „Made in Austria" sind Ausdruck dieser Qualität und machen es anscheinend interessant, sie zu kopieren.

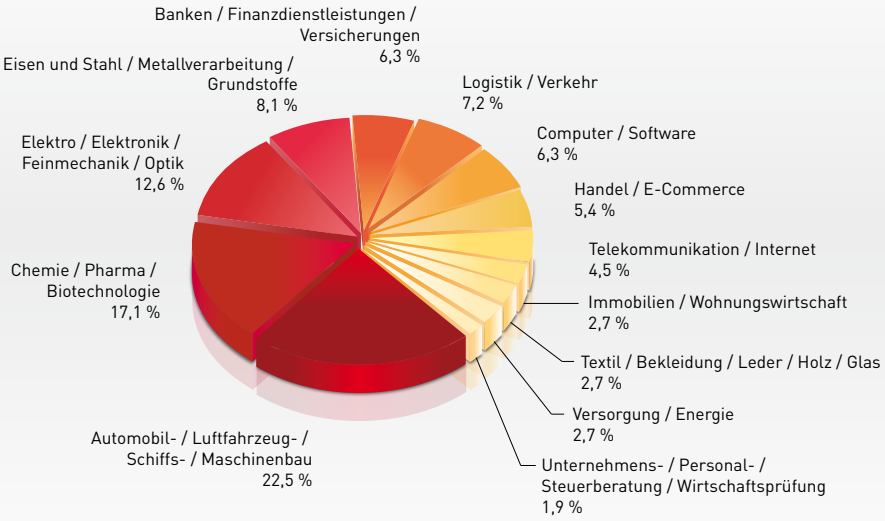
Grundsätzlich sollte kein Unternehmen davon ausgehen, aufgrund der Zugehörigkeit zu einer bisher weniger betroffenen Branche, nicht durch Industriespionage gefährdet zu sein. Die Häufigkeitszahlen in den einzelnen Unternehmensgruppen können sowohl etwas mit der Teilnahmebereitschaft einzelner Branchen zu tun haben als auch mit der Awareness[1] in den Unternehmen, um solche Vorfälle überhaupt festzustellen. In beiden Ländern war der Automobil-, Luftfahrzeug-, Schiffs- und Maschinenbau am stärksten von Spionage betroffen; so ereigneten sich in Deutschland 22,5 Prozent aller Fälle in diesem Segment, in Österreich immerhin 18,2 Prozent. An zweiter Stelle lag in Deutschland mit 17,1 Prozent der Bereich Chemie/Pharma/Biotechnologie und an dritter Stelle mit 12,6 Prozent die Branche Elektro/Elektronik/Feinmechanik/Optik. Hier gab es länderübergreifend leichte Unterschiede: Zwar lag in Österreich ebenfalls der Bereich Elektro/Elektronik/Feinmechanik/Optik mit 12,7 Prozent an dritter Stelle, die zweithäufigsten Schäden ereigneten sich jedoch mit 14,6 Prozent in der Branche Eisen und Stahl/Metallverarbeitung/Grundstoffe.

Einige Branchen machten keinerlei Angaben über Schäden. Dies muss jedoch nicht zwangsläufig heißen, dass es in diesen Branchen keine Spionage gab. Zum einen wäre es ungewöhnlich, wenn einzelne Bereiche tatsächlich von jeglichen Angriffen verschont geblieben wären; zum anderen gibt es nach wie vor eine hohe Scheu, Schadensfälle publik zu machen. Die Angst vor einem Reputationsschaden lässt viele Unternehmen immer noch vor jeglicher Kommunikation nach außen zurückschrecken, selbst zu staatlichen Stellen wie den Verfassungsschutzämtern oder dem Bundesamt für Sicherheit in der Informationstechnik.

1) Awareness: Bewusstsein oder Gewahrsein über die eigene Handlung oder Betonung der aktiven Haltung bzw. Aufmerksamkeit gegenüber einem bestimmten Sachverhalt.

Geschädigte Branchen

Deutschland



Gesundheit / Pflege
0 %

Medien / Werbung
0 %

Nahrungs- und Genussmittel
0 %

Touristik / Hotel- und Gaststätten / Freizeit
0 %

Bauwirtschaft / Bauzulieferer
0 %

Sonstige Dienstleistungen
0 %

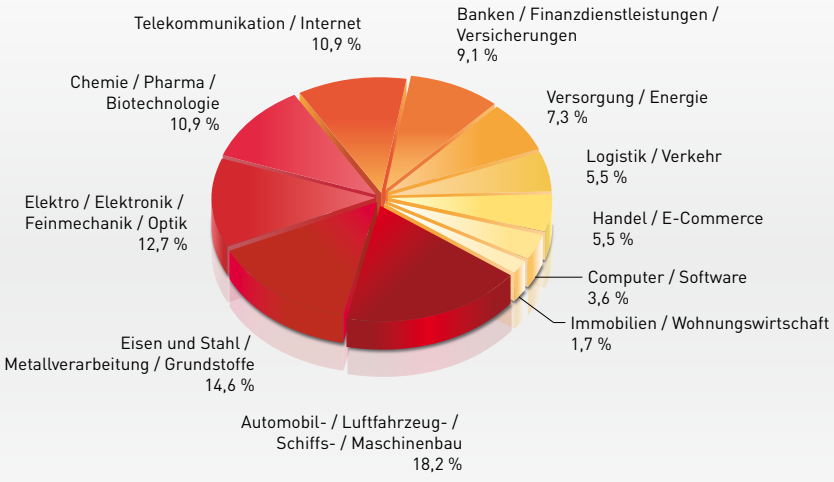
Sonstige
0 %

GRAFIK 6

Quelle: Corporate Trust 2014

Geschädigte Branchen

Österreich



Unternehmens- / Personal- / Steuerberatung / Wirtschaftsprüfung
0 %

Textil / Bekleidung / Leder / Holz / Glas
0 %

Gesundheit / Pflege
0 %

Medien / Werbung
0 %

Nahrungs- und Genussmittel
0 %

Touristik / Hotel- und Gaststätten / Freizeit
0 %

Bauwirtschaft / Bauzulieferer
0 %

Sonstige Dienstleistungen
0 %

Sonstige
0 %

GRAFIK 7

Quelle: Corporate Trust 2014

Betroffene Unternehmen

Die Geschäftsbeziehungen in kritische Länder nehmen deutlich zu.

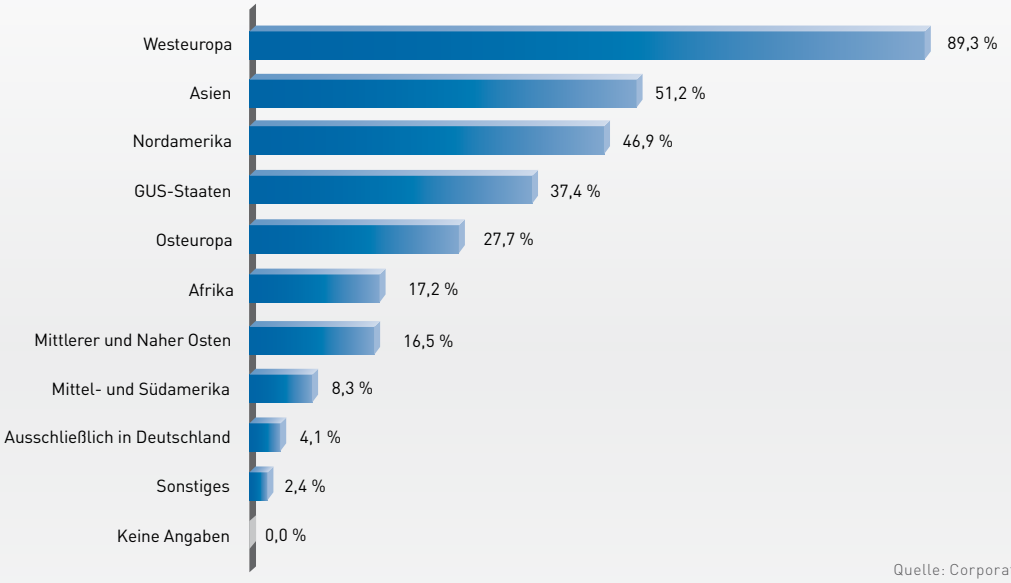
Das internationale Geschäft scheint für alle Unternehmen zunehmend wichtiger zu werden. Lediglich 4,1 Prozent der Unternehmen in Deutschland und 5,1 Prozent der Unternehmen in Österreich gaben an, keine Geschäftsbeziehungen ins Ausland zu unterhalten. Bei der Befragung 2012 waren in Deutschland noch 7,0 Prozent ohne internationale geschäftliche Kontakte.

Insgesamt kann festgestellt werden, dass die meisten wirtschaftlichen Beziehungen immer noch in Westeuropa stattfinden. Für österreichische Unternehmen sind danach jedoch vor allem die Geschäftsbeziehungen nach Osteuropa interessant. Während in Deutschland lediglich 27,7 Prozent aller Firmen angaben, geschäftliche Kontakte dorthin zu unterhalten, waren es in Österreich mit 42,4 Prozent die zweithäufigsten Geschäftsbeziehungen.

Die Unternehmen in beiden Ländern haben relativ viele Kontakte nach Asien, Nordamerika und die GUS-Staaten. Von der prozentualen Anzahl liegen diese Staaten vor allem in Österreich fast gleichauf. Da in allen drei Ländern von den staatlichen Stellen ein hoher Aufwand für das Ausforschen von Daten betrieben wird, muss davon ausgegangen werden, dass die Geschäftsbeziehungen in solche Länder das Risiko für Spionage deutlich erhöhen.

In welchen Regionen haben Sie Geschäftsbeziehungen?
(Mehrfachnennungen möglich)

Deutschland

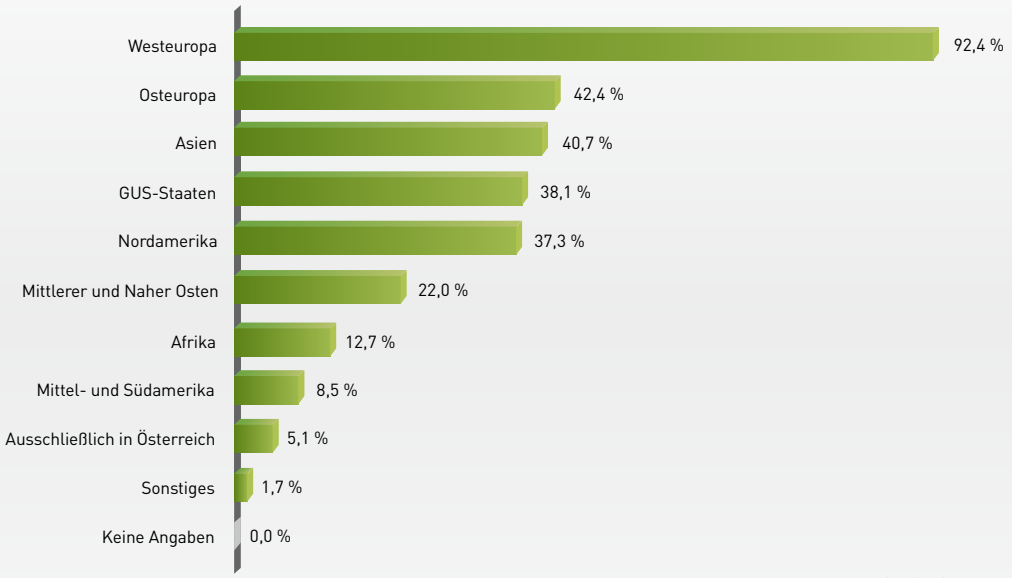


GRAFIK 8

Quelle: Corporate Trust 2014

In welchen Regionen haben Sie Geschäftsbeziehungen?
(Mehrfachnennungen möglich)

Österreich



GRAFIK 9

Quelle: Corporate Trust 2014

Betroffene Unternehmen

Deutsche und österreichische Unternehmen werden vor allem in Asien, Osteuropa und den GUS-Staaten durch Spionage geschädigt.

Bei den meisten Angriffen fällt es schwer, genau zu identifizieren, wo der Informationsabfluss bzw. die Spionage stattfand. Dort, wo es möglich war, die Angriffe einzugrenzen, konnten von deutschen Unternehmen vor allem Asien mit 38,8 Prozent, die GUS-Staaten mit 32,6 Prozent und Osteuropa mit 31,7 Prozent benannt werden. Österreichische Unternehmen hatten mit 36,4 Prozent am häufigsten in Osteuropa mit Industriespionage zu kämpfen. Dies war erwartungsgemäß, da hier neben Westeuropa auch die meisten Geschäftsbeziehungen stattfanden. Am zweithäufigsten, mit 30,9 Prozent, fand die Spionage zum Nachteil österreichischer Firmen in den GUS-Staaten sowie in Österreich selbst statt. Mit 27,3 Prozent an vierter Stelle lag Asien.

Dies belegt eindeutig, dass die Unternehmen am häufigsten in solchen Ländern mit Angriffen konfrontiert waren, wo es einen klaren staatlichen Auftrag zur Wirtschaftsspionage gibt. Auffällig ist darüber hinaus, dass auch Nordamerika in rund einem Fünftel der Fälle (Deutschland: 21,9 Prozent; Österreich: 21,8 Prozent) als Ausgangspunkt der Spionage identifiziert wurde. Unternehmen sollten sich bewusst sein, dass Industriespionage aufgrund des starken globalen Wettbewerbsdrucks sowie der permanent steigenden Möglichkeiten für Datenausspähung auch in „befreundeten" Staaten stattfinden kann. Obwohl Deutschland und Österreich einen Großteil ihrer Geschäftsbeziehungen in Westeuropa unterhalten, gab es dort mit 8,0 Prozent (Deutschland) und 9,1 Prozent (Österreich) nur vergleichsweise geringe Spionagevorfälle.

Die Zuordnung des Ausgangspunkts für die Spionage wird vermutlich in Zukunft aufgrund der Möglichkeiten in einer zunehmend digitalisierten Welt noch wesentlich schwieriger. Nicht nur Staaten agieren bei der klassischen Wirtschaftsspionage[1] im Verbund, sondern auch die Organisierte Kriminalität[2] wirkt meist arbeitsteilig zusammen und führt ihre Angriffe quer über den Globus aus.

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

2) Organisierte Kriminalität: So werden Tätergruppierungen (Banden) bezeichnet, bei der mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig zusammenwirken, um die von Gewinn- und Machtstreben bestimmte planmäßige Begehung von Straftaten durchzuführen, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind und dabei gewerbliche oder geschäftsähnliche Strukturen verwenden, Gewalt oder andere zur Einschüchterung geeignete Mittel anwenden und Einfluss auf Politik, Massenmedien, öffentliche Verwaltungen, Justiz oder die Wirtschaft nehmen.

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

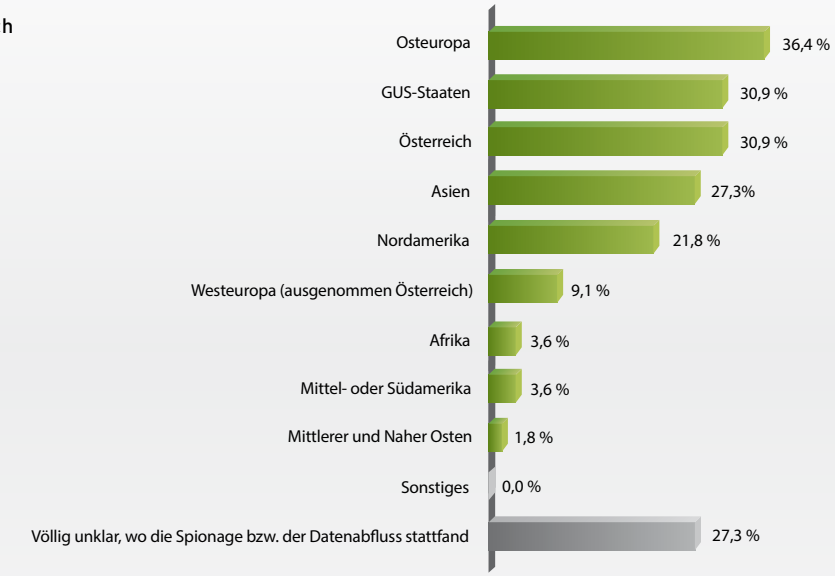
Deutschland

GRAFIK 10

Quelle: Corporate Trust 2014

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

Österreich



GRAFIK 11

Quelle: Corporate Trust 2014


VIRUS
alert

Schäden durch Spionage

Die Wirtschaft wird in beiden Ländern massiv durch Industriespionage geschädigt.

Es wäre zu vermuten, dass Unternehmen durch die gestiegene Berichterstattung über Informationsdiebstähle, Datenausspähung ausländischer Nachrichtendienste oder Know-how-Abfluss durch eigene Mitarbeiter in den letzten Jahren stark sensibilisiert worden sein müssten. Doch die Awareness[1] scheint noch nicht hoch genug und die Schutzmaßnahmen in Unternehmen bei weitem noch nicht ausreichend. Der finanzielle Schaden durch Industriespionage beläuft sich in Deutschland jährlich auf 11,8 Milliarden Euro und in Österreich auf 1,6 Milliarden Euro.

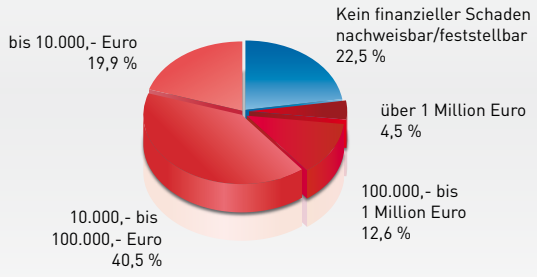
Nach einer Definition der Europäischen Union[2] sind Unternehmen mit weniger als 10 Mitarbeitern bzw. einem Umsatzerlös oder einer Bilanzsumme von weniger als 2 Millionen Euro als Kleinstunternehmen einzustufen. Laut dem deutschen Statistik-Portal[3] gibt es in Deutschland insgesamt ca. 8,4 Millionen umsatzsteuerpflichtige Unternehmen, davon sind ca. 6,3 Millionen Kleinstunternehmen. In Österreich gibt es nach Angaben von Statistik Austria[4] ca. 620.000 umsatzsteuerpflichtige Unternehmen, davon sind ca. 330.000 Kleinstunternehmen. In Österreich wird die Definition von Kleinstunternehmen abweichend von der Definition der Europäischen Union auf Unternehmen mit weniger als 5 Mitarbeitern festgelegt. Bei dem Rest handelt es sich demnach um Konzerne, Mittelständler oder Kleinunternehmen.

Da die Befragung in beiden Ländern nur bei Firmen ab einer Größe von mindestens 10 Mitarbeitern sowie einem Umsatz bzw. einer Bilanzsumme von über einer Million Euro durchgeführt wurde, wurde für die Berechnung des Gesamtschadens von einer Referenzgröße von rund 300.000 zu berücksichtigenden Unternehmen in Deutschland und von rund 42.000 zu berücksichtigenden Unternehmen in Österreich ausgegangen. Kleinstunternehmen und Kleinunternehmen mit einer zu geringen Mitarbeiterzahl, Umsatzgröße oder Bilanzsumme wurden für die Berechnung des Gesamtschadens nicht berücksichtigt. Die Schäden wurden jeweils nach prozentualem Anteil der betroffenen Firmen auf die Gesamtgröße hochgerechnet. Bei den Schadenssummen wurde analog zu den Studien von 2007 und 2012 jeweils nur ein Mittelwert angenommen, also z. B. 55.000 Euro bei der Kategorie „10.000 bis 100.000 Euro" bzw. 5.500 Euro bei der Kategorie „bis zu 10.000 Euro". Bei der Kategorie „über 1 Million Euro" wurde je Schaden ein Mittelwert von 1,2 Millionen Euro veranschlagt.

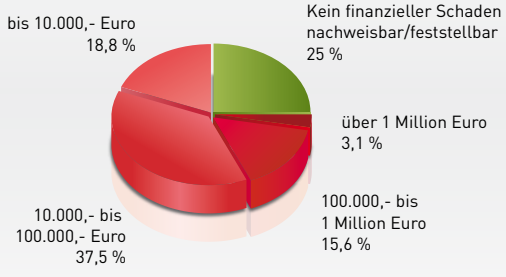
Erstaunlicherweise waren die finanziellen Schäden proportional in Deutschland und Österreich relativ gleich. Dies ist vermutlich darauf zurückzuführen, dass Österreich in den meisten Bereichen mit den gleichen Problemen bzw. den gleichen Know-how-Angriffen wie Deutschland zu kämpfen hat. Es zeigt darüber hinaus auch, dass die Bedrohung für die Wirtschaft in beiden Ländern enorme finanzielle Ausmaße annimmt.

Kann der Schaden finanziell beziffert werden?

Deutschland



Österreich



GRAFIK 12

Quelle: Corporate Trust 2014

1) Awareness: Bewusstsein oder Gewahrsein über die eigene Handlung oder Betonung der aktiven Haltung bzw. Aufmerksamkeit gegenüber einem bestimmten Sachverhalt.
2) siehe http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=uriserv:OJ.L_.2003.124.01.0036.01.DEU
3) siehe www.statista.com
4) siehe www.statistik.at

Schäden durch Spionage

Elektronische Angriffe auf die Unternehmenssysteme nehmen deutlich zu.

Während bei der Studie 2012 vor allem die bewusste Informationsweitergabe bzw. der Datendiebstahl durch eigene Mitarbeiter das größte Problem für Unternehmen darstellte, scheinen sich die Täter aktuell immer mehr auf elektronische Angriffe zu fokussieren. 49,6 Prozent der Unternehmen in Deutschland und 41,8 Prozent der österreichischen Firmen gaben an, dass Hackerangriffe[1] auf EDV-Systeme und Geräte die häufigste Form der Spionage war. An zweiter Stelle lag eine weitere technische Angriffsform, das Abhören bzw. Abfangen von elektronischer Kommunikation. In Deutschland konnte bei 41,1 Prozent der Fälle ein solcher Datenzugriff festgestellt werden, in Österreich bei 40,0 Prozent. Die Antworten zu den konkreten Spionagehandlungen zeigen noch einmal deutlich, wie hoch aktuell das Risiko eines elektronischen Datenangriffs ist.

Social Engineering[2] belegt in der Statistik in Deutschland nur noch den dritten Platz (38,4 Prozent der Fälle), in Österreich gar nur den fünften Platz (18,2 Prozent der Fälle). Dies kann entweder bedeuten, dass tatsächlich in Deutschland wesentlich häufiger versucht wird, über zwischenmenschliche Beeinflussung an Daten zu gelangen, oder dass in Österreich noch ein wesentlich geringeres Bewusstsein für das Risiko von Abschöpfung[3] besteht. Solche Taten zu erkennen ist meistens schwer – und so wäre es nicht verwunderlich, wenn ein Großteil der Angriffe gar nicht erkannt worden ist.

Die Studie bestätigt erneut, dass Unternehmen den Faktor Mensch nicht unterschätzen sollten. In über der Hälfte aller Fälle waren eigene Mitarbeiter oder externe Dritte für den Informationsabfluss verantwortlich. Die bewusste Informations- oder Datenweitergabe bzw. der Datendiebstahl durch eigene Mitarbeiter machte in Deutschland 33,0 Prozent aus und in Österreich 38,2 Prozent. Der Abfluss von Daten durch externe Dritte (wie Zulieferer, Dienstleister, Kunden oder Lieferanten) kam in Deutschland bei 21,9 Prozent der Fälle zum Tragen, in Österreich sogar bei 25,5 Prozent. In der Regel finden solche Handlungen gemeinsam statt – jemand, der gibt, und jemand, der nimmt –, sodass vermutlich in den meisten Fällen von den Unternehmen beide Handlungen für einen Spionagefall angegeben wurden.

Bei der Frage nach den konkreten Handlungen waren zwar Mehrfachnennungen zugelassen, auffällig ist jedoch trotzdem, dass es in beinahe jedem dritten Fall auch zum Diebstahl von Informationen oder Datenträgern gekommen ist. So wurden in Deutschland entweder IT- oder Telekommunikationsgeräte (17,4 Prozent der Fälle) sowie Dokumente, Unterlagen, Muster, Maschinen oder Bauteile (15,2 Prozent der Fälle) entwendet; dies sind insgesamt 32,6 Prozent. In Österreich verhielt es sich ähnlich: Hier handelte es sich in 18,2 Prozent der Fälle um Diebstahl von IT- und Telekommunikationsgeräten und in 16,4 Prozent der Fälle wurden Dokumente, Unterlagen, Muster, Maschinen oder Bauteile gestohlen; die Quote lag damit bei insgesamt 34,6 Prozent.

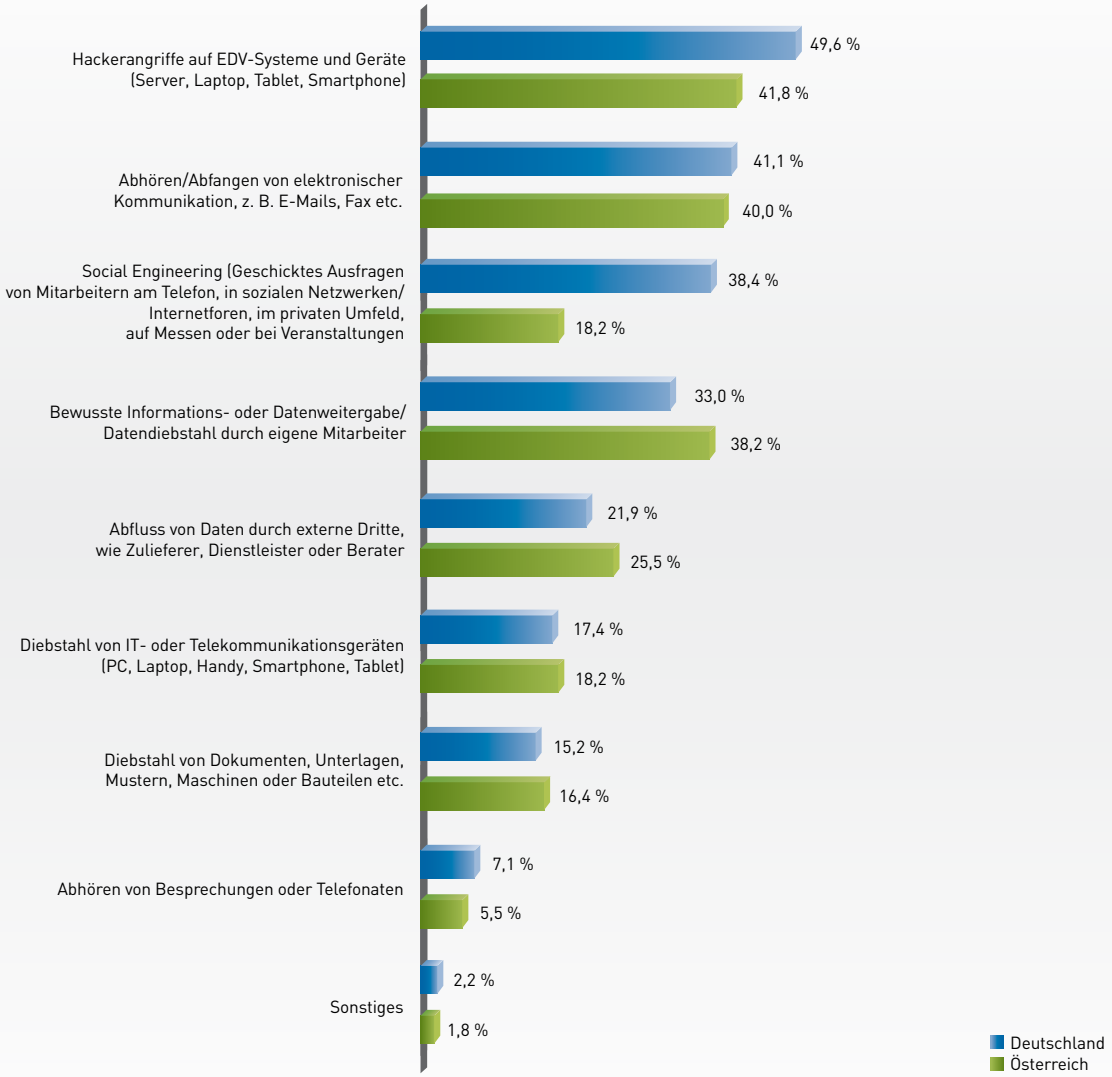
1) Hackerangriff: Unerlaubtes Eindringen in fremde Computer- oder Netzwerksysteme, meist durch das Überwinden von Sicherheitsmechanismen.

2) 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.

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

Welche konkreten Handlungen fanden (vermutlich) statt?

(Mehrfachnennungen möglich)



GRAFIK 13

Quelle: Corporate Trust 2014

Schäden durch Spionage

Die Bereiche Forschung und Entwicklung sowie die IT-Administration sind die begehrtesten Spionageziele.

Auf die Frage, in welchem Bereich spioniert wurde bzw. wo der Informationsabfluss stattfand, gaben 26,3 Prozent der deutschen Firmen den Bereich Forschung und Entwicklung an; an zweiter Stelle lag mit 21,4 Prozent der Bereich IT-Administration bzw. IT-Service. In Österreich waren dies ebenfalls die begehrtesten Ziele, nur mit getauschten Plätzen: Hier wurde in 21,8 Prozent der Fälle bei IT-Administration/IT-Service spioniert und in 18,2 Prozent im Bereich der Forschung und Entwicklung.

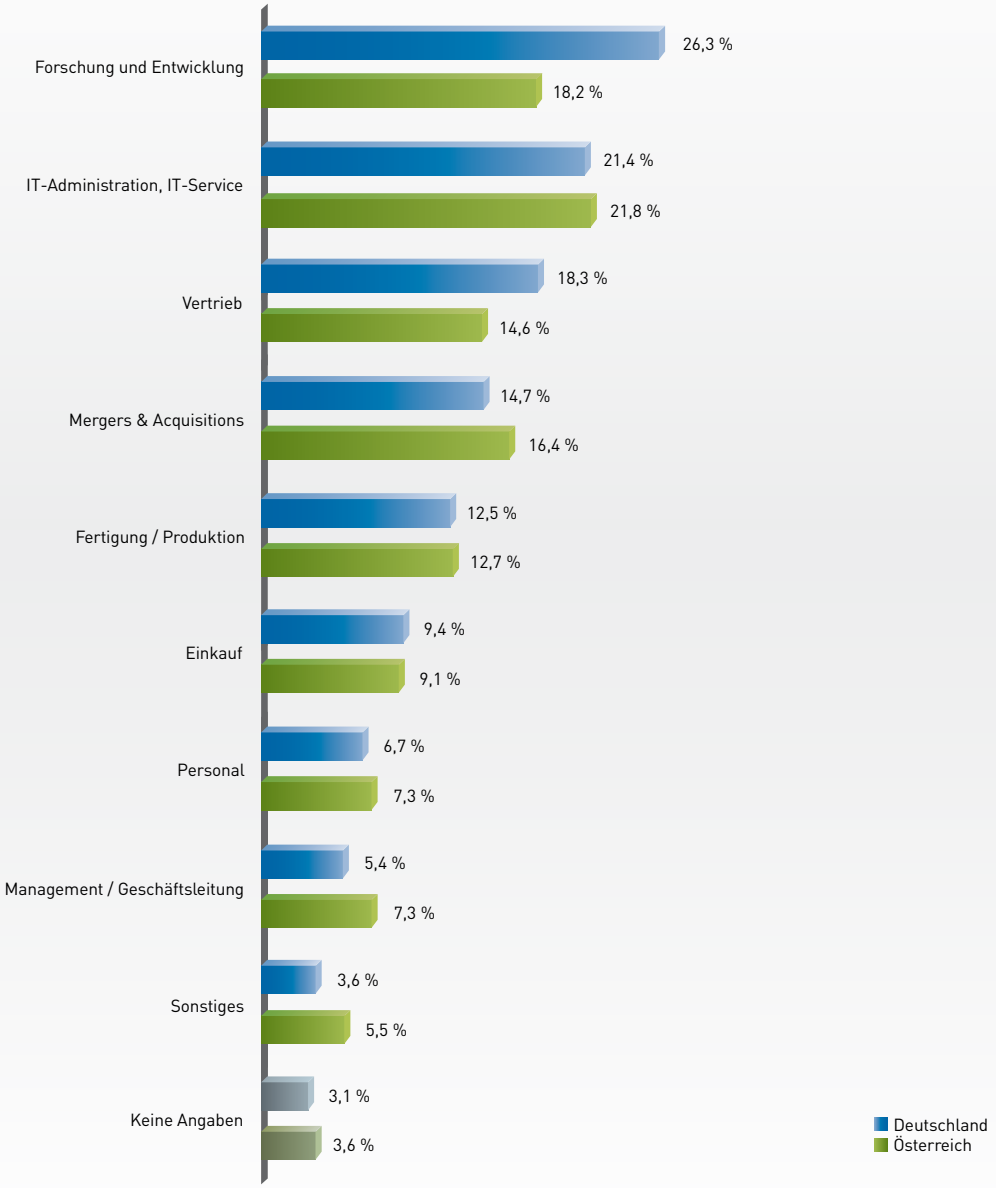
Dies scheint nicht ungewöhnlich. Da die meisten Hackerangriffe[1] in den IT-Abteilungen identifiziert werden, wird die Spionage vermutlich für diese Abteilung gewertet, auch wenn sie unter Umständen ein völlig anderes Ziel verfolgte. Der Bereich Forschung und Entwicklung beherbergt naturgemäß einen Großteil der sensiblen bzw. Know-how-relevanten Informationen. Daher scheint es nur logisch, dass hier ein Großteil der Spionage stattfand.

Während bei der Studie 2012 in Deutschland noch der Vertrieb mit 18,3 Prozent an erster Stelle bei den ausspionierten Bereichen lag, war er bei der aktuellen Studie nur noch auf Platz drei in Deutschland (wiederum 18,3 Prozent) bzw. Platz vier in Österreich (14,6 Prozent) zu finden. Der Bereich Mergers & Acquisitions scheint ebenfalls ein sehr relevanter bzw. interessanter Unternehmensbereich für Spionage gewesen zu sein: Hier wurden in Österreich 16,4 Prozent und in Deutschland 14,7 Prozent der Angriffe registriert. Aufgrund der immer globaleren Unternehmensaktivitäten und weltweiter Geschäftsbeziehungen gewinnen Unternehmenskäufe oder -zusammenschlüsse zunehmend an Bedeutung. Das frühzeitige Wissen um strategische Ausrichtungen, Budgets oder den zeitlichen Horizont für eine Übernahme ist daher begehrtes Know-how.

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

In welchem Bereich wurde spioniert bzw. fand der Informationsabfluss statt?

(Mehrfachnennungen möglich)



GRAFIK 14

Quelle: Corporate Trust 2014

Schäden durch Spionage

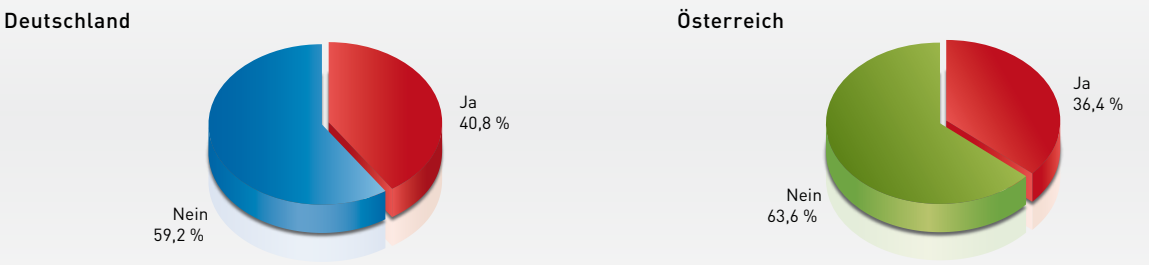
Schäden in der IT und Umsatzeinbußen durch den Verlust von Wettbewerbsvorteilen sind die häufigsten materiellen Folgen von Spionage.

In Deutschland hatten 40,8 Prozent und in Österreich 36,4 Prozent der Firmen einen bezifferbaren Schaden zu verzeichnen. Damit erlitt mehr als jedes dritte Unternehmen einen finanziellen Verlust aufgrund von Spionage. Die häufigsten materiellen Schäden traten durch einen Ausfall, Diebstahl oder die Schädigung von IT- oder Telekommunikationsequipment auf (Deutschland: 53,0 Prozent; Österreich: 58,1 Prozent).

Gerade der Verlust von Wettbewerbsvorteilen kann zu einem unkalkulierbaren finanziellen Risiko für Unternehmen führen: Nicht nur, dass Marktanteile schwinden und damit Umsatzeinbußen einhergehen – in vielen Fällen wird auch die Kundenbindung und damit die Basis einer langfristigen Geschäftsbeziehung geschädigt.

Die Erpressung mit erbeuteten Daten des Unternehmens scheint für die Wirtschaft in beiden Ländern kein Problem darzustellen. Nur in 6,0 Prozent (Deutschland) bzw. 2,3 Prozent (Österreich) aller Fälle hatten Firmen einen finanziellen Schaden durch eine solche Erpressung zu verzeichnen. Diese Deliktsform ist überwiegend der Organisierten Kriminalität[1] zuzurechnen. Da die IT-Systeme der meisten Unternehmen anscheinend gegen deren typische Vorgehensweisen zur Erbeutung von sensiblen Daten geschützt sind, scheint dies eher ein Problem für Privat-PCs zu sein.

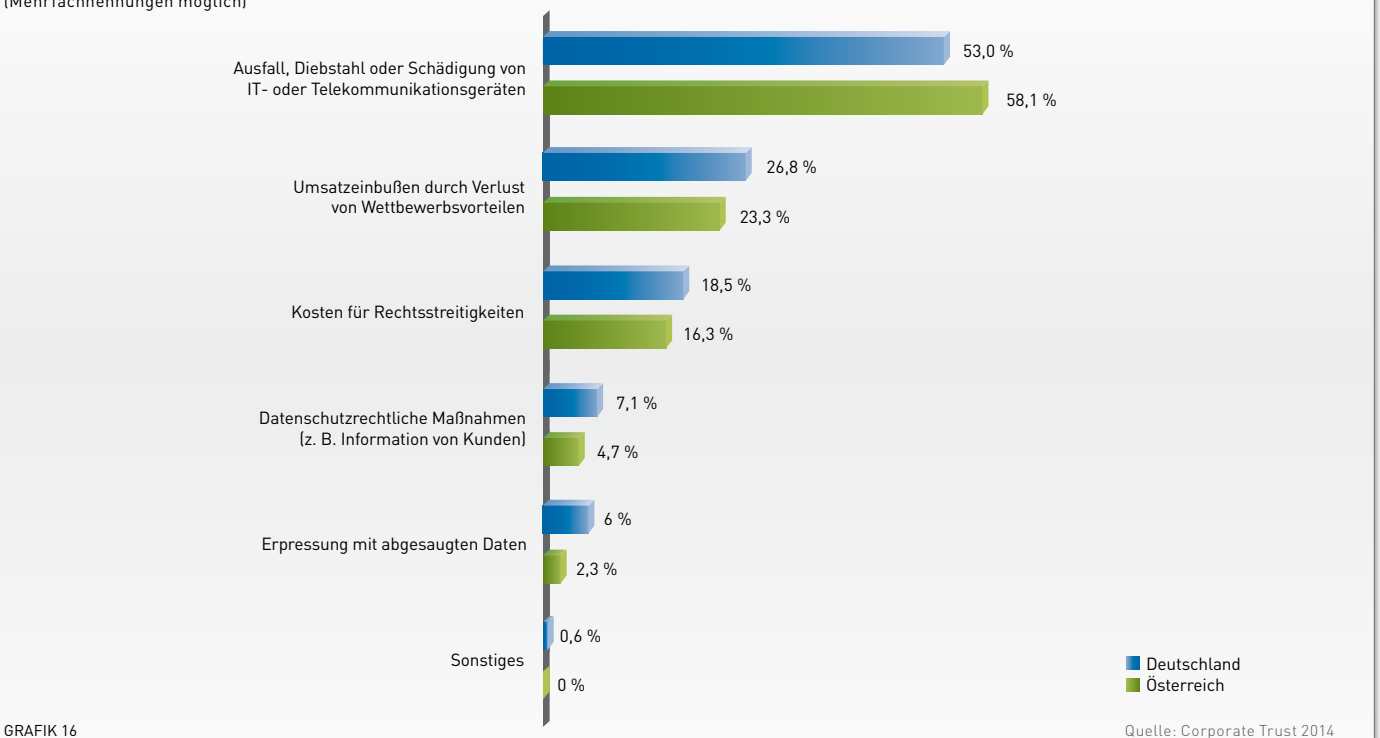
Gab es Hinweise auf konkrete materielle Schäden für das Unternehmen?



GRAFIK 15

Quelle: Corporate Trust 2014

Wenn ja, welche konkreten materiellen Schäden wurden festgestellt?
(Mehrfachnennungen möglich)



GRAFIK 16

Quelle: Corporate Trust 2014

1) Organisierte Kriminalität: So werden Tätergruppierungen (Banden) bezeichnet, bei der mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig zusammenwirken, um die von Gewinn- und Machtstreben bestimmte planmäßige Begehung von Straftaten durchzuführen, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, und dabei gewerbliche oder geschäftsähnliche Strukturen verwenden, Gewalt oder andere zur Einschüchterung geeignete Mittel anwenden und Einfluss auf Politik, Massenmedien, öffentliche Verwaltungen, Justiz oder die Wirtschaft nehmen.

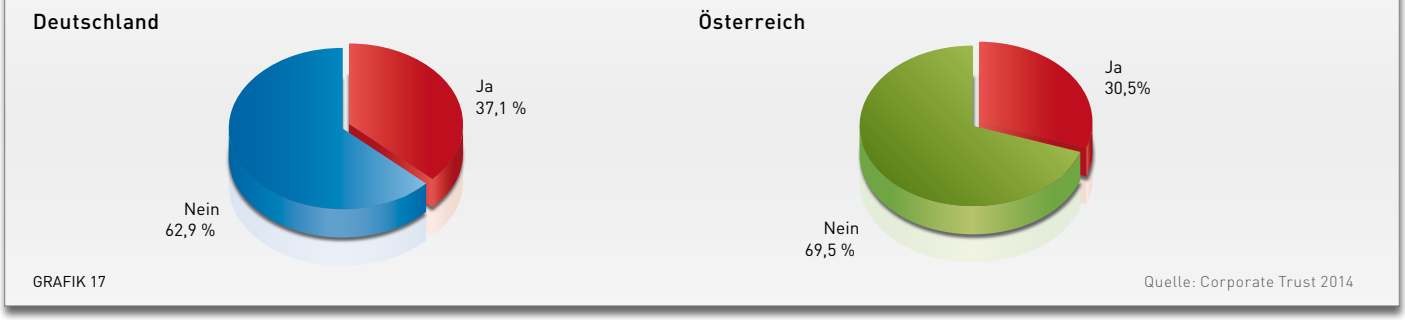
Bei den immateriellen Schäden waren Patentrechtsverletzungen sowie Imageschäden bei Kunden oder Lieferanten die häufigsten Auswirkungen von Spionage.

Informationsabfluss findet häufig unbemerkt statt, sodass manchmal erst reagiert werden kann, wenn festgestellt wird, dass ein Produkt oder eine Dienstleistung schon vom Wettbewerb kopiert wurde. In solchen Fällen führt dies oft zu langwierigen und schwierigen juristischen Auseinandersetzungen. Teilweise verzichten Unternehmen aber im Ausland auf solche Rechtsstreitigkeiten, weil sie aufgrund unklarer Gesetzeslage in manchen Ländern wenig Aussicht auf Erfolg versprechen. Der Reputationsschaden für Unternehmen ist jedoch gerade bei Plagiaten groß, wenn sie von minderwertiger Qualität sind und der Kunde nicht sofort merkt, dass es sich um ein Plagiat handelt.

So hatten in Deutschland 54,3 Prozent und in Österreich sogar 58,3 Prozent der Unternehmen einen immateriellen Schaden durch Patentrechtsverletzungen zu verzeichnen. Imageschäden bei Kunden oder Lieferanten waren mit 26,8 Prozent (Deutschland) bzw. 22,2 Prozent (Österreich) zwar nicht ganz so häufig, stellten aber immerhin noch das zweithöchste Risiko dar.

Anscheinend haben Unternehmen in beiden Ländern nur ganz selten ein Problem mit negativer Medienberichterstattung durch Spionage – in Deutschland nur in 3,3 Prozent und in Österreich nur in 5,6 Prozent der Fälle. Dies scheint jedoch nicht verwunderlich, da Unternehmen mit Vorfällen nur sehr selten an die Öffentlichkeit gehen, auch nicht zu den Behörden. Die Angst vor einem Reputationsschaden ist einfach zu groß.

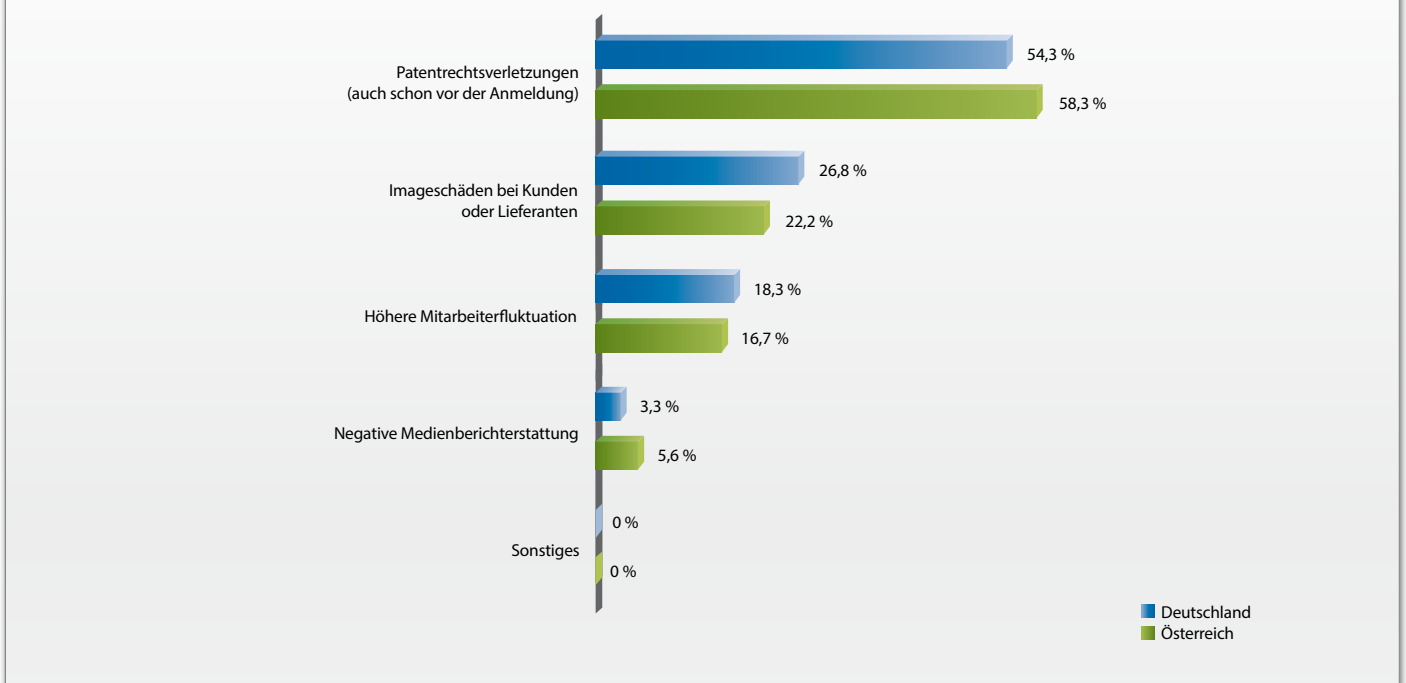
Gab es Hinweise auf immaterielle Schäden?



GRAFIK 17

Quelle: Corporate Trust 2014

Wenn ja, welche immateriellen Schäden wurden festgestellt?
(Mehrfachnennungen möglich)



GRAFIK 18

Quelle: Corporate Trust 2014

Die Täter

Hacker stellen die größte Tätergruppe dar.

Kunden oder Lieferanten sowie eigene Mitarbeiter sind nicht die häufigsten Täter bei Spionage, sondern meist geschieht der Angriff auf das Know-how durch Hacker[1]. In Deutschland gaben 41,5 Prozent und in Österreich 32,7 Prozent aller Unternehmen an, dass sie Hacker als Täter identifiziert hätten. Während in Deutschland Kunden oder Lieferanten mit 26,8 Prozent die zweitgrößte Tätergruppe bei den Unternehmen darstellten, waren es in Österreich mit 30,9 Prozent die eigenen Mitarbeiter (vor den Kunden oder Lieferanten mit 23,6 Prozent).

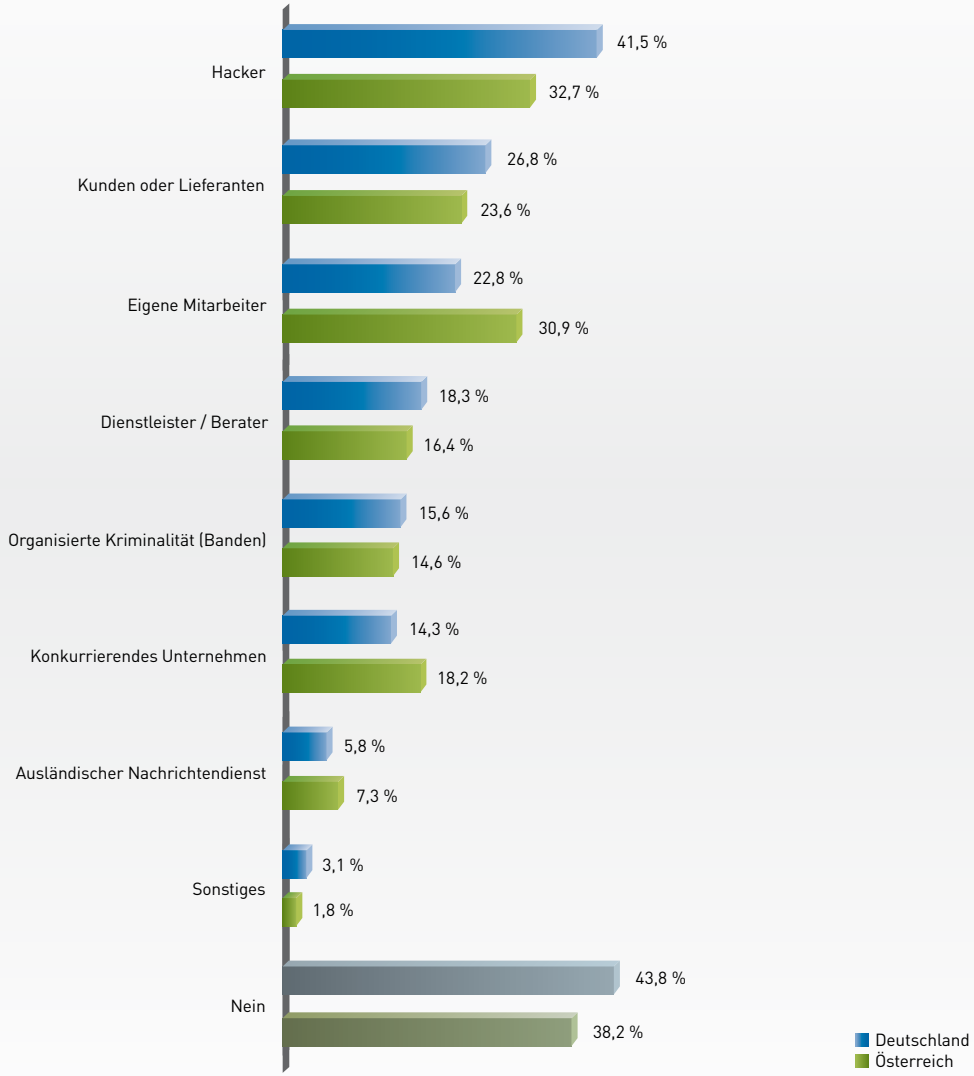
Obwohl die Awareness[2] für amerikanische Spähattacken durch die Enthüllungen von Edward Snowden sehr hoch scheint und das Treiben von NSA[3] und Co. derzeit sehr kritisch beäugt wird, nahmen die Unternehmen ausländische Nachrichtendienste nur konkret in 7,3 Prozent (Österreich) bzw. 5,3 Prozent (Deutschland) der Fälle als Täter wahr. Dies könnte ein deutlicher Beleg dafür sein, dass Spionage durch staatliche Stellen zwar häufig vermutet wird, jedoch nur äußerst selten tatsächlich bewiesen werden kann.

Gerade bei Angriffen in/aus ehemals oder noch kommunistischen Ländern ist es für Unternehmen manchmal schwer zu trennen, wer das Know-how entwendete, da hier oftmals enge Verknüpfungen zwischen Staat und Wirtschaft bestehen bzw. undurchsichtige Beteiligungsstrukturen bei den Gesellschaften herrschen. Bei einem Joint Venture oder einer sonstigen Geschäftsbeziehung mit einem Partner in diesen Ländern kann es daher durchaus vorkommen, dass es sich scheinbar um ein ganz normales Unternehmen handelt, die Verantwortlichen aber tatsächlich einer staatlichen Stelle zuzuordnen sind und der geschäftliche Kontakt vor allem zur Informationsgewinnung initiiert wurde.

Die Organisierte Kriminalität[4] stellt mit ihren massenhaften Spam[5]-E-Mails bzw. gezielten Phishing[6]-Attacken zwar eine ernst zu nehmende Bedrohung für die Sicherheit von Computern dar, dies scheint aber vor allem Privat-PCs und weniger die Unternehmens-IT zu betreffen. Nur 15,6 Prozent in Deutschland und 14,6 Prozent in Österreich gaben an, bei Spionagevorfällen die Organisierte Kriminalität als Täter identifiziert zu haben.

1) Hackerangriff:	Unerlaubtes Eindringen in fremde Computer- oder Netzwerksysteme, meist durch das Überwinden von Sicherheitsmechanismen.
2) Awareness:	Bewusstsein oder Gewahrsein über die eigene Handlung oder Betonung der aktiven Haltung bzw. Aufmerksamkeit gegenüber einem bestimmten Sachverhalt.
3) NSA (National Security Agency):	Größter Auslandsgeheimdienst der Vereinigten Staaten von Amerika. Die NSA ist für die weltweite Überwachung, Entschlüsselung und Auswertung elektronischer Kommunikation zuständig und in dieser Funktion ein Teil der Intelligence Community, in der sämtliche Nachrichtendienste der USA zusammengefasst sind.
4) Organisierte Kriminalität:	So werden Tätergruppierungen (Banden) bezeichnet, bei denen mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig zusammenwirken, um die von Gewinn- und Machtstreben bestimmte planmäßige Begehung von Straftaten durchzuführen, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, und dabei gewerbliche oder geschäftsähnliche Strukturen verwenden, Gewalt oder andere zur Einschüchterung geeignete Mittel anwenden und Einfluss auf Politik, Massenmedien, öffentliche Verwaltungen, Justiz oder die Wirtschaft nehmen.
5) Spam (auch Junk):	Unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten, die dem Empfänger unverlangt zugestellt werden und häufig werbenden Inhalt enthalten.
6) Phishing:	Darunter versteht man Versuche, über gefälschte Internetseiten, E-Mail- oder Kurznachrichten an Daten eines Internet-Nutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Ziel des Betrugs ist es häufig, mit den erhaltenen Informationen beispielsweise auf Kontodaten zuzugreifen.

Gab es Hinweise auf die Täter?



GRAFIK 19

Quelle: Corporate Trust 2014

Ich denke viel an die Zukunft, weil das der Ort ist,
wo ich den Rest meines Lebens verbringen werde.

Woody Allen

Aufklärung der Vorfälle

Unternehmen versuchen Angriffe in der Regel selbst zu lösen, ohne fremde Unterstützung.

Nur bei einem Viertel der Fälle in Deutschland (25,9 Prozent) und nur etwa bei jedem siebten Fall in Österreich (14,6 Prozent) wurden staatliche Stellen oder externe Spezialisten von den Unternehmen hinzugezogen. Zu groß ist anscheinend immer noch die Angst, dass etwas an die Öffentlichkeit durchsickern könnte. Da gerade Hackerangriffe[1] massiv zugenommen haben und die meisten IT-Abteilungen bei ihren täglichen administrativen Tätigkeiten vor allem die Verfügbarkeit der Daten und weniger deren Sicherheit im Fokus haben, verwundert dies.

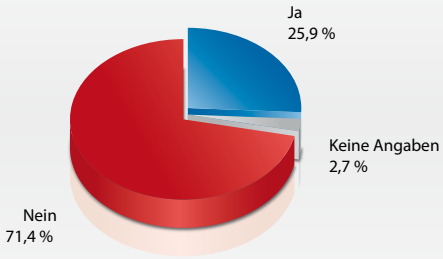
Die Staatsanwaltschaft, Polizeibehörden oder der Verfassungsschutz wurden in Deutschland in nicht einmal zehn Prozent der Fälle involviert (Staatsanwaltschaft oder Polizei: 5,3 Prozent; Verfassungsschutz: 3,6 Prozent). In Österreich wurden sie immerhin noch in 12,8 Prozent der Fälle um Hilfe gebeten (Staatsanwaltschaft oder Polizei: 7,3 Prozent; Verfassungsschutz: 5,5 Prozent). In Deutschland wurde nur in Einzelfällen das Bundesamt für Sicherheit in der Informationstechnik mit ins Boot geholt. Eine solche Behörde gibt es in Österreich jedoch nicht, daher gab es hierzu keine Antworten.

Interessanterweise scheint das Thema Abhören in beiden Ländern für die Unternehmen eine große Bedrohung zu sein. So wurden in 14,7 Prozent (Deutschland) bzw. 13,2 Prozent (Österreich) der Fälle externe Spezialisten für den Abhörschutz eingeschaltet. Sie lagen damit noch vor den Computerspezialisten mit 12,5 Prozent (Deutschland) sowie 12,7 Prozent (Österreich). Dies kann unter Umständen auch bedeuten, dass die IT-Abteilungen entsprechend aufgerüstet wurden und heute in zunehmend mehr Unternehmen eigene Spezialisten für IT-Sicherheit vorhanden sind, die sich um solche Vorfälle kümmern.

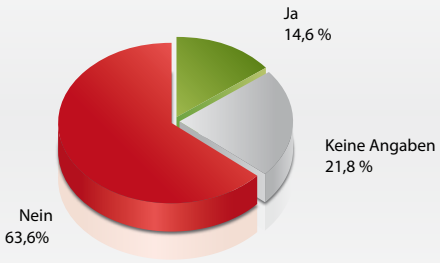
1) Hackerangriff: Unerlaubtes Eindringen in fremde Computer- oder Netzwerksysteme, meist durch das Überwinden von Sicherheitsmechanismen.

Wurden staatliche Stellen oder externe Sicherheitsspezialisten eingeschaltet?

Deutschland



Österreich

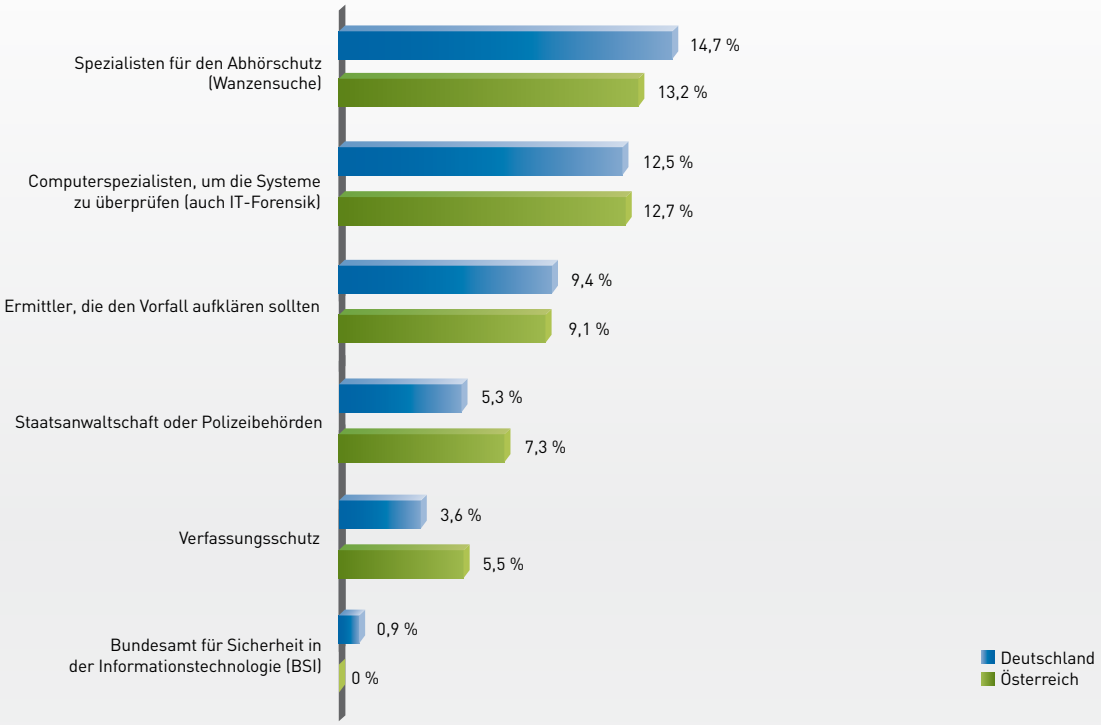


GRAFIK 20

Quelle: Corporate Trust 2014

Welche staatlichen Stellen oder externen Sicherheitsspezialisten wurden eingeschaltet?

(Mehrfachnennungen möglich)



GRAFIK 21

Quelle: Corporate Trust 2014

Sicherheitsvorkehrungen im Unternehmen

Allgemein

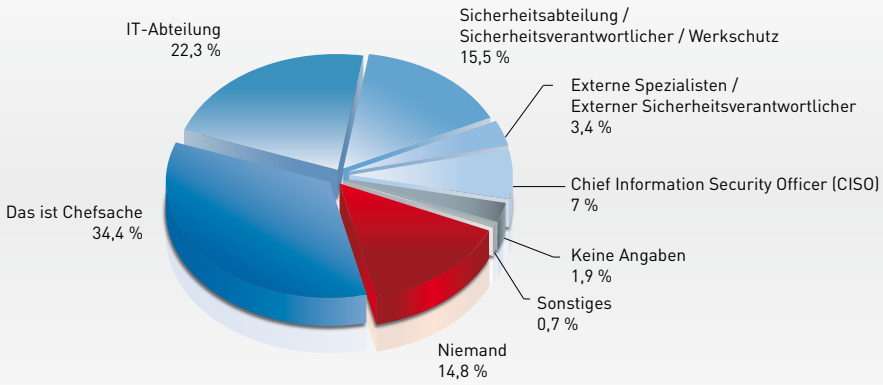
In Deutschland kümmert sich meistens der Chef um den Informationsschutz, in Österreich ist dies überwiegend Aufgabe der IT-Abteilung.

Nicht jedes Unternehmen ist gleich gut gegen Spionage geschützt und nicht jede Firma trifft die gleichen Sicherheitsvorkehrungen. Tatsache ist, dass beim Informationsschutz die verschiedensten Disziplinen zusammenarbeiten müssen, um sowohl einen Schutz der IT-Systeme zu erreichen und die Mitarbeiter zu sensibilisieren als auch die entsprechenden Prozesse für den Umgang mit vertraulichen Daten zu etablieren. Dies sollte zentral von einer Person oder einer Abteilung verantwortet werden, die übergreifend agieren und Einfluss auf die verschiedenen Themen nehmen kann, um keine Lücken beim Schutz der Daten zu haben.

In Deutschland ist an erster Stelle (34,4 Prozent) der Chef für den Informationsschutz verantwortlich. Anders in Österreich: Dort wird diese zentrale Aufgabe in aller Regel von der IT-Abteilung übernommen. Erstaunlich ist, dass in Deutschland 14,8 Prozent der Unternehmen angaben, dass sich niemand um den Informationsschutz kümmert. Dies ist eine Steigerung von 8,1 Prozent im Vergleich zur Studie von 2012; damals gaben nur 6,7 Prozent der deutschen Unternehmen an, dass sich niemand dieses Themas annehme. In Österreich waren es gar 32,2 Prozent der Firmen, die keinen Verantwortlichen für die Belange des Informationsschutzes hatten. Dies ist erstaunlich, weil die Bedrohungen und Schadensfälle annähernd gleich hoch waren wie in Deutschland. Vermutlich gibt es bei österreichischen Firmen noch keine ausreichende Awareness[1] für die Notwendigkeit von Informationsschutz; oder falls doch, dann wird das Thema anscheinend überwiegend als technisches Problem verstanden und der IT-Abteilung übertragen, um die EDV-Systeme entsprechend zu schützen.

Wer kümmert sich in Ihrem Unternehmen um die zentralen Belange des Informationsschutzes?

Deutschland

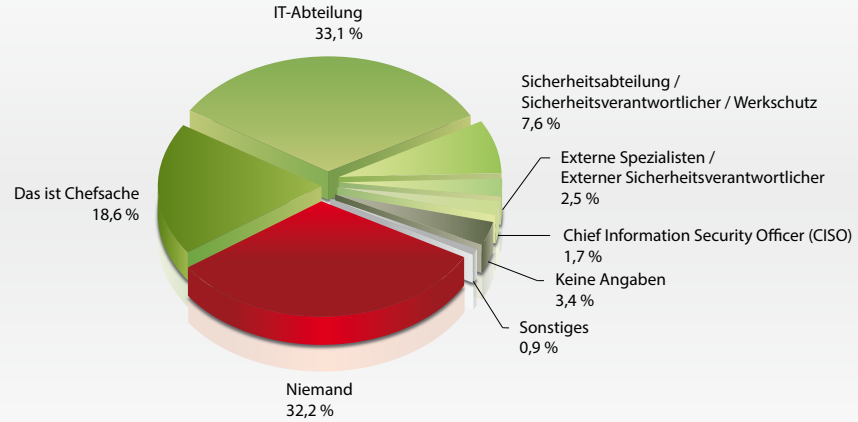


GRAFIK 22

Quelle: Corporate Trust 2014

Wer kümmert sich in Ihrem Unternehmen um die zentralen Belange des Informationsschutzes?

Österreich



GRAFIK 23

Quelle: Corporate Trust 2014

1) Awareness: Bewusstsein oder Gewahrsein über die eigene Handlung oder Betonung der aktiven Haltung bzw. Aufmerksamkeit gegenüber einem bestimmten Sachverhalt.

Sicherheitsvorkehrungen im Unternehmen

Organisation

Regelmäßige Sicherheits-Audits durch externe Spezialisten sowie Background-Checks bei Geschäftspartnern sind immer noch kein Standard.

Während bei der Studie 2012 erst 55,8 Prozent der Unternehmen in Deutschland angaben, eine Geheimhaltungsverpflichtung[1] mit Geschäftspartnern abgeschlossen zu haben, waren es aktuell bereits 62,4 Prozent. Auch in Österreich scheint dies die häufigste Sicherheitsvorkehrung gegen ungewollten Datenabfluss zu sein: Hier gaben 57,6 Prozent an, über eine derartige Vereinbarung mit Geschäftspartnern zu verfügen.

Die Unternehmen vergessen allerdings manchmal, dass Papier geduldig ist und in unterschiedlichen Ländern ganz unterschiedliche Ansichten zum geschäftlichen Gebaren herrschen. Nicht jeder hat einen hohen Ehrenkodex und handelt nach den Grundzügen eines „ehrbaren Kaufmanns". Daher ist es verwunderlich, dass zwar so häufig Geheimhaltungsverpflichtungen abgeschlossen werden, eine sorgfältige Auswahl durch einen Background-Check vor Aufnahme der Geschäftsbeziehung aber allzu oft unterbleibt. So gaben nur 19,7 Prozent der deutschen und 22,9 Prozent der österreichischen Unternehmen an, einen solchen Background-Check durchzuführen. Sicherheits-Audits durch externe Spezialisten scheinen ebenfalls nicht hoch im Kurs zu stehen – sie kamen nur bei 21,8 Prozent (Deutschland) bzw. 17,8 Prozent (Österreich) der Unternehmen zum Einsatz.

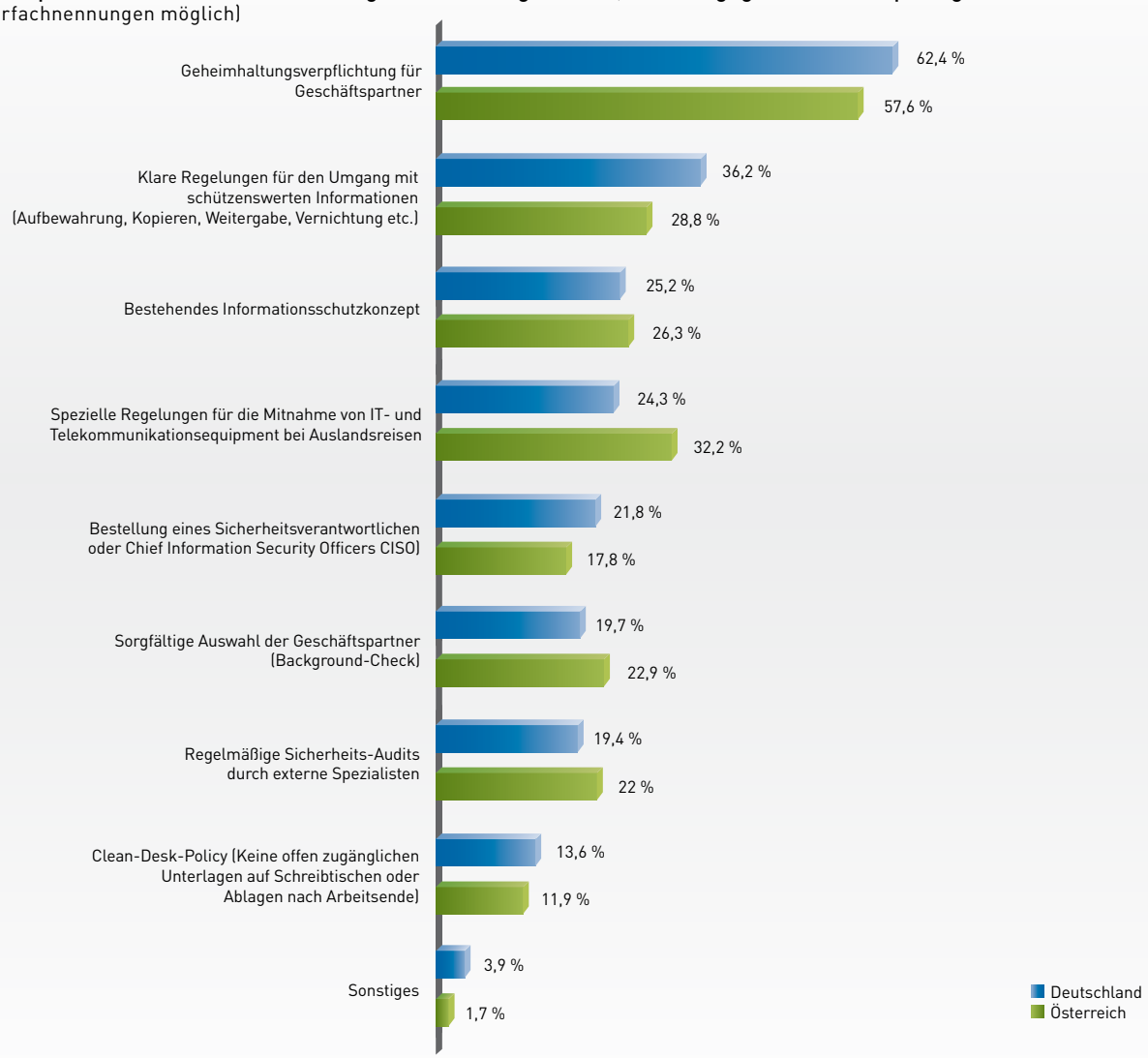
Überraschend war, dass auch der Einsatz einer Clean-Desk-Policy[2] in den Unternehmen rückläufig zu sein scheint. Während bei der Studie 2012 noch 25,6 Prozent der deutschen Unternehmen angaben, eine solche Policy für die Mitarbeiter einzusetzen, waren es aktuell nur noch 13,6 Prozent in Deutschland und 11,9 Prozent in Österreich. Dies kann natürlich auch eine Ursache darin haben, dass es bereits in vielen Unternehmen das papierlose Büro gibt und Informationen heute nur noch auf Datengeräten bearbeitet werden.

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

2) Background-Check (auch Pre-Employment-Screening): Überprüfung von Mitarbeitern bezüglich früherer Arbeitgeber, finanzieller Verhältnisse, Firmenbeteiligungen sowie verdächtiger Lebensumstände.

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

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



GRAFIK 24

Quelle: Corporate Trust 2014

Sicherheitsvorkehrungen im Unternehmen

Organisation

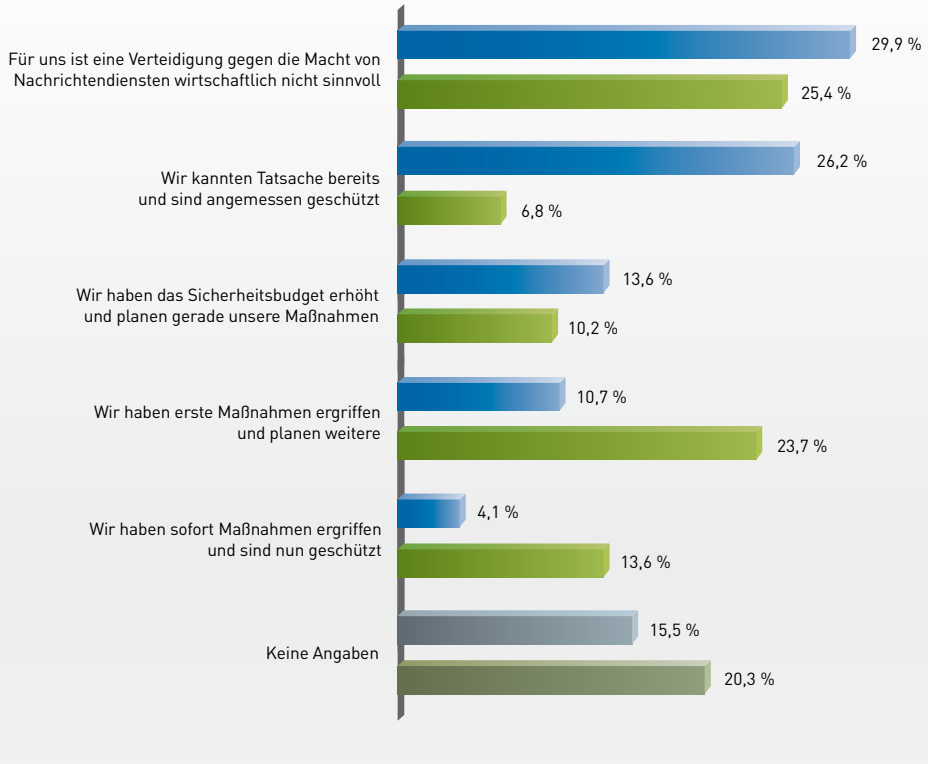
Der NSA-Skandal: Firmen schwanken zwischen Ohnmachtsgefühlen, Unkenntnis, Selbstsicherheit und dem Ringen um die richtigen Gegenmaßnahmen.

Die Enthüllungen des Whistleblowers Snowden wirbeln seit fast einem Jahr Staub auf. Die Geheimdienste werden aus dem Dunkel ins Rampenlicht gezogen – allen voran die NSA. Der Vorwurf in Deutschland ist immer der gleiche: Die Macht der Geheimdienste wird auch zur Wirtschaftsspionage missbraucht.

Die Firmen sind in drei Lager aufgeteilt. Das größte Lager bilden dabei diejenigen, die den Skandal aktiv oder passiv ignorieren: Fast die Hälfte der Unternehmen (Deutschland: 45,4 Prozent; Österreich: 45,8 Prozent) hält eine Verteidigung entweder für wirtschaftlich nicht sinnvoll oder macht keine Angaben über eine Reaktion auf den NSA-Skandal. Das zweite Lager bilden Firmen, die über das Ausmaß der geheimdienstlichen Ermittlungen bereits vor dem Skandal im Bilde waren oder durch erste Sofortmaßnahmen einen für sie ausreichenden Schutz herstellen konnten (Deutschland: 30,3 Prozent; Österreich: 20,4 Prozent). Dabei fällt auf, dass in Deutschland über ein Viertel der Firmen (26,2 Prozent) den NSA-Skandal bereits antizipiert hatten. Dies kann auf eine gute Sensibilisierung hinweisen, aber auch eine Schutzbehauptung der Verantwortlichen sein. Das dritte Lager hat bereits erste Maßnahmen ergriffen bzw. neue Maßnahmen budgetiert und geplant (Deutschland: 24,3 Prozent; Österreich: 33,9 Prozent).

Die Unsicherheit, die der NSA-Skandal an vielen Stellen ausgelöst hat, zeigt sich also auch bei den Firmen – ein echter Trend ist nicht erkennbar. Die Studie verdeutlicht somit einmal mehr die Notwendigkeit, sich mit dem Thema möglichst objektiv und rational im Hinblick auf die eigene Firmenstrategie auseinanderzusetzen. Die Frage, ob man dem richtigen Lager angehört, sollte damit jedes Unternehmen nochmals neu bewerten – es gibt für jede Reaktion auf den Skandal gute Argumente.

Wie hat Ihr Unternehmen auf die Snowden-Enthüllungen reagiert?



GRAFIK 25

Quelle: Corporate Trust 2014

Organisation

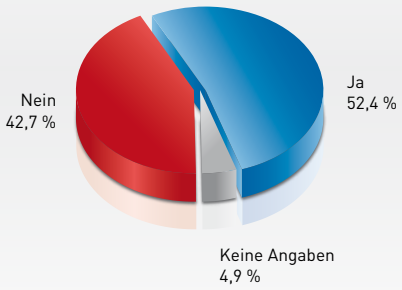
Noch immer hat etwa die Hälfte aller Unternehmen keine eindeutige Sicherheits-Policy für den Schutz sensibler Daten vorgegeben.

Sicherheit versteht jeder anders und nicht alle Mitarbeiter haben den gleichen Ansatz, was sensibel ist und wie sie vertrauliche Informationen aufbewahren müssen. Daher sollten Unternehmen klare Vorgaben machen, welche Daten schützenswert sind, wer darauf zugreifen darf und wie damit umzugehen ist. Dies wird in einer Sicherheits-Policy[1] geregelt, in der nicht nur die wichtigsten Assets des Unternehmens beschrieben sind, die sogenannten „Kronjuwelen", sondern auch die verschiedenen Schutzstufen (z. B. geheim, vertraulich oder offen zugänglich) sowie die Maßnahmen zur Sicherung gegen fremden Zugriff.

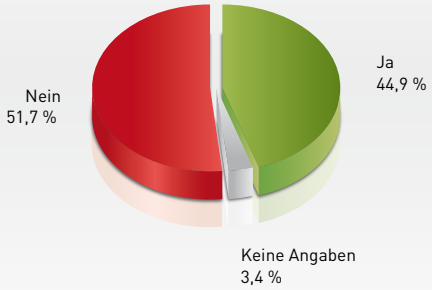
Beim Informationsschutz ist die Sicherheits-Policy eine der ersten und wichtigsten Maßnahmen, um von der Unternehmensleitung einmal ganz klar die Richtung für den Know-how-Schutz vorzugeben. Trotzdem gibt es nur in annähernd jedem zweiten Unternehmen eine solche Regelung. In Deutschland gaben 52,4 Prozent der Unternehmen an, über eine Sicherheits-Policy zu verfügen. Zum Vergleich: Bei der Studie 2012 hatten erst 46,4 Prozent eine solche Vorgabe. Österreich hinkt noch etwas hinterher: Hier gaben 51,7 Prozent der Unternehmen zu, noch keine klaren Regelungen in einer Sicherheits-Policy erstellt zu haben.

Gibt es für das Unternehmen eine Sicherheits-Policy mit klaren Regelungen für den Informationsschutz, die allen Mitarbeitern bekannt ist und Externe miteinbezieht?

Deutschland



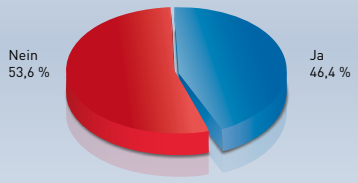
Österreich



GRAFIK 26

Quelle: Corporate Trust 2014

Stand: 2012



Quelle: Studie Industriespionage 2012

1) Sicherheits-Policy: Auch Sicherheitsrichtlinie oder Sicherheitsleitlinie. Beschreibt den angestrebten Sicherheitsanspruch eines Unternehmens und konzeptionell die Maßnahmen, um dorthin zu kommen.

Sicherheitsvorkehrungen im Unternehmen

Organisation

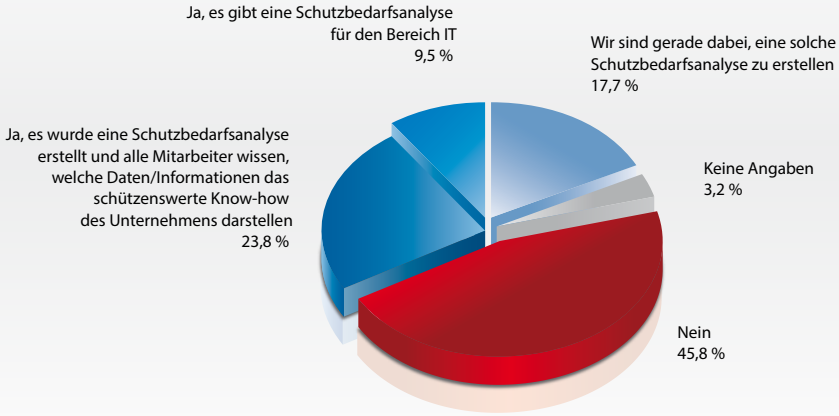
Unternehmen führen viel zu selten eine Schutzbedarfsanalyse durch, um klar zu definieren, welche Daten sensibel sind.

Der individuelle Schutzbedarf einer Information ist nicht selbsterklärend. Er kann nur deshalb entstehen, weil ein Verantwortlicher für die jeweilige Information ihren Wert für das Unternehmen bemisst und entsprechend festlegt, wie damit künftig umzugehen ist. Die verschiedenen Einstufungskriterien und relevanten Bereiche sollten für alle gültig sein und müssen daher einmal definiert werden. Unternehmen, die dies nicht tun, überlassen es jedem einzelnen Mitarbeiter, der mit der Information umgeht, ob und wie er sie aus seiner Sicht für schützenswert hält. Da es den am Rande beteiligten Mitarbeitern in vielen Fällen gar nicht möglich ist, den Wert einer Information zu bemessen, kann diese Bewertung daher sehr unterschiedlich ausfallen.

Wer alles schützen will, kann in der Regel gar nichts schützen, weil dies bei der schieren Masse von Informationen in der heutigen Arbeitswelt nicht mehr möglich ist. Deswegen muss sich der Informationsschutz auf das Wesentliche konzentrieren. Unternehmen sollten durch eine Schutzbedarfsanalyse ganz klar festlegen, welche Daten/Informationen für sie relevant sind. Trotzdem haben in Deutschland 45,8 Prozent und in Österreich 41,5 Prozent noch keine solche Schutzbedarfsanalyse erstellt. Lediglich 23,8 Prozent in Deutschland und 21,2 Prozent in Österreich haben sich hier bereits professionell aufgestellt. 14,4 Prozent (Österreich) bzw. 9,5 Prozent (Deutschland) der Unternehmen haben dies zumindest schon einmal für den Bereich IT getan.

Wurde für das Unternehmen eine Schutzbedarfsanalyse erstellt, die klar und verständlich regelt, welche Daten/Informationen geheim, vertraulich oder offen zugänglich sind?

Deutschland

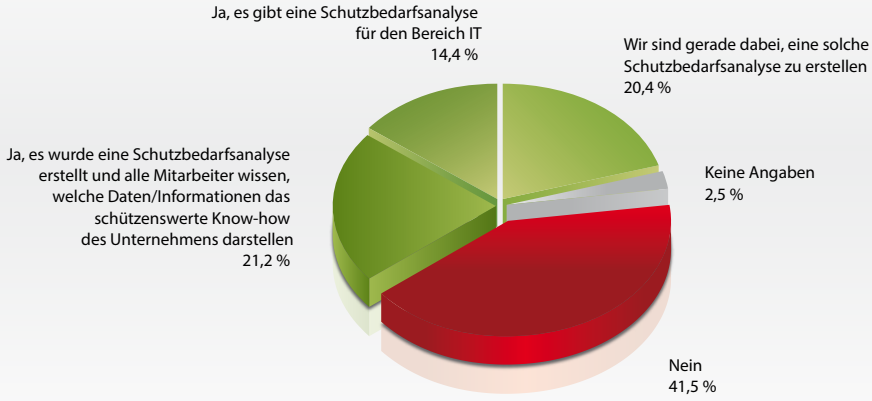


GRAFIK 27

Quelle: Corporate Trust 2014

Wurde für das Unternehmen eine Schutzbedarfsanalyse erstellt, die klar und verständlich regelt, welche Daten/Informationen geheim, vertraulich oder offen zugänglich sind?

Österreich



GRAFIK 28

Quelle: Corporate Trust 2014

Ich möchte nicht in einer Welt leben,
in der alles, was ich sage, alles, was ich tue,
jedes Gespräch, jeder Ausdruck von Kreativität,
Liebe oder Freundschaft aufgezeichnet wird.

Edward Snowden

Sicherheitsvorkehrungen im Unternehmen

IT-Sicherheit

Trotz der Flut an Angriffen werden wichtige IT-Sicherheitsfunktionen nur unzureichend eingesetzt.

Es gibt ständig steigende Zahlen von Angriffen durch Malware[1], Trojaner[2], Viren[3] oder sonstige Schadsoftware. Trotzdem sind viele IT-Systeme in Unternehmen nicht ausreichend geschützt, um sich gegen diese Flut und moderne Art der Spionage zu schützen. Industriespionage richtet sich meist gegen ein ganz bestimmtes Ziel. Dabei werden die Angriffe so lange durchgeführt, bis der Zweck erreicht ist und die nötigen Informationen aus dem Unternehmen abgesaugt wurden. Man spricht in diesem Zusammenhang heute von sogenannten Advanced Persistent Threats (APT)[4], also einer fortgeschrittenen, andauernden Bedrohung, bei der die Täter nicht aufhören, bis sie am Ziel sind.

So werden zwar die klassischen Sicherheitsvorkehrungen wie Firewalls[5] gegen Angriffe von außen oder Passwortschutz auf den IT- und Kommunikationsgeräten eingesetzt, aber ein Verbot von USB-Sticks, portablen Festplatten, CD-Brennern oder Ähnlichem an den PCs oder Laptops gibt es nur in etwa jedem fünften Unternehmen (Deutschland: 19,4 Prozent; Österreich: 22,0 Prozent). Vor allem die Absicherung des Firmennetzwerks gegen Datenabfluss von innen (z. B. durch Data Leakage Prevention[6]) wird in Deutschland nur bei 12,9 Prozent der Unternehmen und in Österreich gar nur in 5,9 Prozent aller Firmen eingesetzt.

Interessant bei den Sicherheitsvorkehrungen zum Schutz der IT-Systeme ist darüber hinaus, dass der Passwortschutz auf allen Geräten anscheinend ein großes Problem darstellt und zumindest in Deutschland nominal zurückgeht. Während bei der Studie 2012 noch 90,6 Prozent der Unternehmen angaben, auf allen Geräten Passwortschutz einzusetzen, waren es bei der aktuellen Studie nur noch 61,4 Prozent. In Österreich waren es ebenfalls nur 55,9 Prozent der Unternehmen, die über einen entsprechenden Geräteschutz verfügten. Dies kann ein Indikator dafür sein, dass den Sicherheitsverantwortlichen der Unternehmen bewusst ist, dass sich durch die zunehmende Mobilität der Daten große Risiken ergeben. Während es bei PCs in Unternehmen fast überall zum Standard gehören dürfte, dass sie mit einem Passwort verschlüsselt sind, kann dies bei der Vielzahl von Smartphones, Tablets, Ultrabooks oder sonstigen Datengeräten vermutlich nicht mehr garantiert werden. Die Angaben zum Passwortschutz waren deswegen wahrscheinlich auch wesentlich vorsichtiger als noch 2012.

1) Malware:	Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Malware ist ein Oberbegriff, der u. a. auch den Computervirus umfasst.
2) Trojaner:	Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund jedoch ohne Wissen des Anwenders eine andere Funktion ausführt.
3) Virus (Computervirus):	Ein sich selbst verbreitendes Computerprogramm, welches sich in andere Computerprogramme einschleust und sich damit reproduziert. Die Klassifizierung als Virus bezieht sich hierbei auf die Verbreitungs- und Infektionsfunktion. Einmal gestartet, kann es vom Anwender nicht kontrollierbare Veränderungen am Status der Hardware, am Betriebssystem oder an der Software vornehmen (Schadfunktion). Viren zählen zur Malware.
4) Advanced Persistent Threat: (APT)	Ein häufig im Bereich der Cyber-Bedrohungen verwendeter Begriff für einen komplexen, zielgerichteten und effektiven Angriff auf kritische IT-Infrastrukturen und vertrauliche Daten von Behörden und Unternehmen. Die Angreifer gehen sehr zielgerichtet und mit großem Aufwand vor, um nach dem Eindringen in einen Rechner weiter in die lokale Infrastruktur des Rechners/Netzwerks vorzudringen. Ziel des APT ist es, möglichst lange unentdeckt zu bleiben, um über einen längeren Zeitraum sensible Informationen auszuspähen oder anderweitig Schaden anzurichten.
5) Firewall:	Ein System (meist Hard- und Software), welches dazu dient, den Netzwerkzugriff zu beschränken, basierend auf Absender- oder Zieladresse und genutzten Diensten. Die Firewall 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.
5) Data Leakage Prevention:	Manchmal auch Data Loss Prevention, Begriff aus dem Bereich der Informationssicherheit, mit dem der Schutz gegen den unerwünschten Abfluss von Daten aus dem Unternehmen gemeint ist, manchmal auch nur gegen eine vermutete, aber nicht mess- oder feststellbare Weitergabe von Informationen an unerwünschte Empfänger.

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

(Mehrfachnennungen möglich)

GRAFIK 29

Quelle: Corporate Trust 2014

Sicherheitsvorkehrungen im Unternehmen

IT-Sicherheit

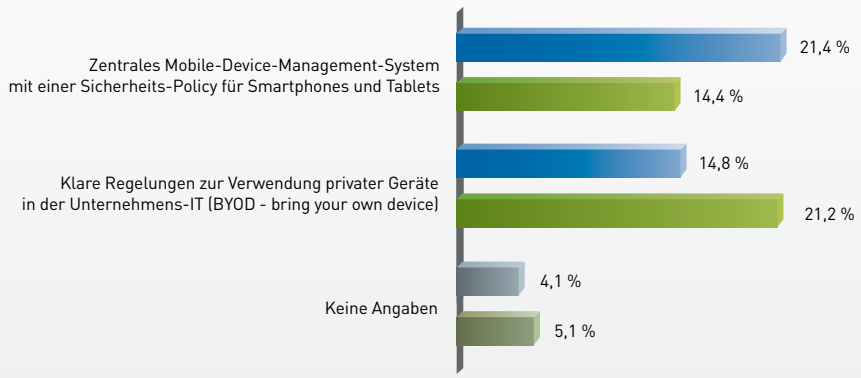
Der zunehmende Einsatz von Mobilgeräten stellt die Unternehmen vor große Herausforderungen, denen sie noch nicht gewachsen sind.

Laptops, Ultrabooks, Smartphones oder Tablets gehören immer häufiger zum Unternehmensalltag. Die vertraulichen Daten sind damit nicht mehr von den Unternehmensmauern geschützt, sondern werden mobil überall mit hingetragen. Mitarbeiter bringen heute immer öfter ihr Privatgerät mit, Stichwort „BYOD – Bring Your Own Device[1]", und erhalten darauf sensible Firmen-E-Mails. Für die Studie sollte erhoben werden, wie Unternehmen mit diesen neuen Herausforderungen umgehen. Zum einen ist es rechtlich gar nicht einfach zu klären, wer Eigentümer der Daten ist, wenn strategische Zahlen, neue Bauteilzeichnungen oder vertrauliche Schreiben auf privaten Geräten gespeichert werden. Zum anderen wird es immer schwieriger, solche Privatgeräte gegen unbefugten Zugriff zu sichern.

Ohne klare Regelungen zum Einsatz von Mobilgeräten bzw. für den sicheren Umgang mit ihnen wird es immer schwieriger, den Verbleib von Unternehmens-Know-how nachzuvollziehen. Nur in den wenigsten Fällen gehen Unternehmen bereits professionell an das Thema heran und haben entsprechende Strukturen geschaffen. In Österreich gab wenigstens noch jedes fünfte Unternehmen (21,2 Prozent) an, klare Regelungen zur Verwendung von privaten Geräten in der Unternehmens-IT aufgestellt zu haben. In Deutschland war dies nur in jedem siebten Unternehmen (14,8 Prozent) der Fall.

Ein zentrales Mobile-Device-Management-System[2] mit einer Sicherheits-Policy[3] für den Einsatz von Mobilgeräten gewährleistet eine vernünftige Sicherung der Geräte gegen fremde Zugriffe, unerwünschte Schadsoftware oder Hackerattacken und damit den Schutz der vertraulichen Unternehmensdaten. Hier haben die Unternehmen in Deutschland bisher etwas mehr getan: 21,4 Prozent gaben an, dass sie über ein solches MDM-System verfügen. In Österreich setzen es bisher nur 14,4 Prozent aller Unternehmen ein. Dies dürfte in beiden Ländern viel zu wenig sein, um das kritische Know-how auch in Zukunft vor Abfluss zu schützen. Die Nachrichtendienste werden auch weiterhin weltweit Daten ausspähen und dabei vor Unternehmensdaten keinen Halt machen. Daher wäre es für Unternehmen ratsam, sich diesen Herausforderungen zu stellen, um nicht im „Cybergeddon[4]" wertvolles Firmen-Know-how zu verlieren.

Welche Sicherheitsvorkehrungen haben Sie für den Einsatz von Mobilgeräten getroffen?
(Mehrfachnennungen möglich)



GRAFIK 30

Quelle: Corporate Trust 2014

1) Bring Your Own Device: (BYOD) Bezeichnung für die Integration von privaten mobilen Endgeräten wie Laptops, Ultrabooks, Tablets oder Smartphones in die Netzwerke bzw. IT-Architektur von Unternehmen. Firmen-E-Mails können damit auch auf den Privatgeräten empfangen werden; angehängte Dokumente werden damit jedoch auch dort gespeichert.

2) Mobile-Device-Management: (MDM) Begriff für die zentralisierte Verwaltung von Mobilgeräten wie Smartphones, Sub-Notebooks, PDAs oder Tablets durch einen oder mehrere Administratoren mithilfe einer Software. Die Verwaltung bezieht sich auf die Inventarisierung der Hardware, die Verteilung der Software und Daten sowie den Schutz der Daten auf diesen Geräten.

3) Sicherheits-Policy: Auch Sicherheitsrichtlinie oder Sicherheitsleitlinie; Beschreibt den angestrebten Sicherheitsmaßstab eines Unternehmens und konzeptionell die Maßnahmen, um dorthin zu kommen.

4) Cybergeddon: An „Armageddon" oder „Harmagedon" angelehnter Begriff, der eine finale oder endzeitliche Entscheidungsschlacht im Cyberraum (virtueller Raum aller auf Datenebene vernetzten IT-Systeme im globalen Internet) bezeichnen soll.

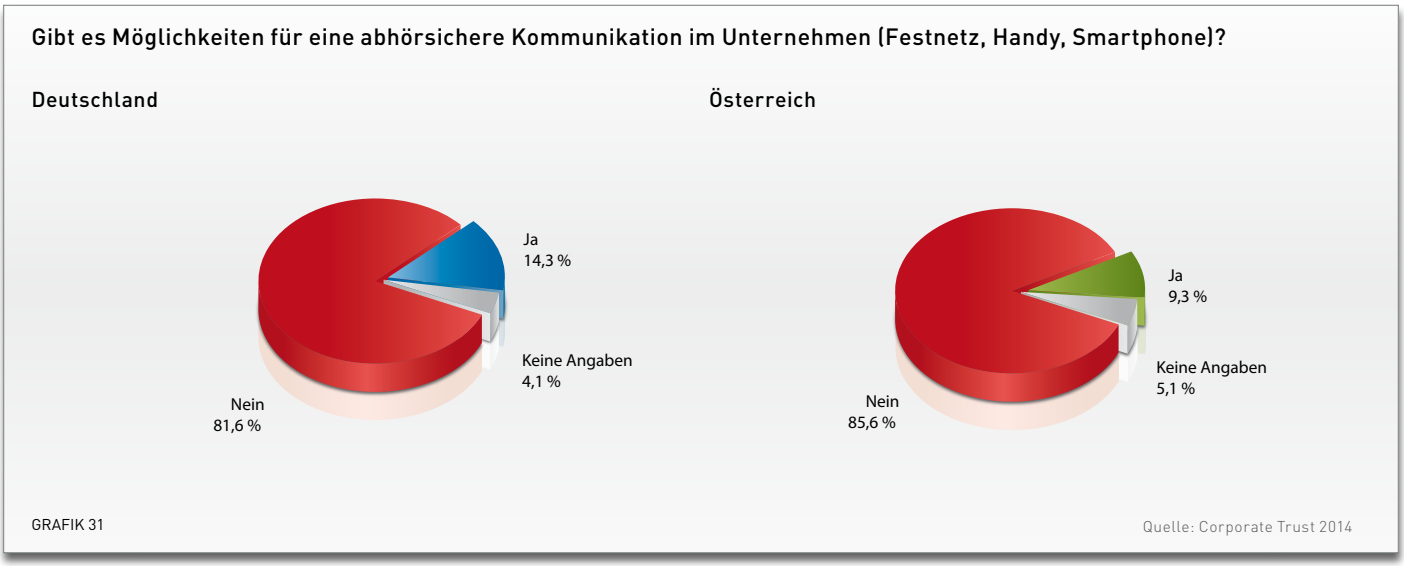
Eine abhörsichere Kommunikation ist nur in den wenigsten Unternehmen möglich.

Vor allem durch die Aussagen von Edward Snowden wurde deutlich, dass nicht nur Russland und China verstärkt Wirtschaftsspionage betreiben, sondern auch die amerikanische NSA[1] sowie das englische GCHQ[2] massenhaft Daten ausspähen. Jede Unternehmenskommunikation läuft damit Gefahr, abgehört zu werden. Wollen deutsche und österreichische Unternehmen hier langfristig keine Wettbewerbsvorteile verlieren, sollten sie dringend technisch aufrüsten, um den Abfluss von Informationen zu verhindern.

Leider gibt es in den Unternehmen nur unzureichend Möglichkeiten, sich gegen diesen Informationsverlust zu schützen. Nur 14,3 Prozent der Unternehmen in Deutschland und 9,3 Prozent der Unternehmen in Österreich hatten die Möglichkeit einer abhörsicheren Kommunikation. Dies ist völlig unzureichend, da somit schnell Wettbewerbsvorteile verloren gehen können.

Es ist verständlich, dass bei den vielfältigen Einsatzmöglichkeiten von modernen Mobilgeräten heute niemand mehr ein zusätzliches Gerät für die abhörsichere Telefonie mitnehmen möchte und ein allzeit verfügbares und in jeder Situation hilfreiches Smartphone nicht gegen ein großes, unhandliches „Handy" eintauschen will. Die Technik für abhörsichere Kommunikation hat sich in den letzten Jahren aber enorm weiterentwickelt und steht nun auch für den Einsatz auf Smartphones zur Verfügung. Unternehmen sollten sich zuerst überlegen, wie hoch die Sicherheit angesetzt werden sollte. Sind die Daten so wichtig, dass es ein höchst verschlüsseltes „Kanzler-Handy" sein muss, oder reicht eine „vernünftige" Verschlüsselung, die zwar nicht ganz so hoch ist, dafür aber noch maximalen Komfort bietet?

Gibt es Möglichkeiten für eine abhörsichere Kommunikation im Unternehmen (Festnetz, Handy, Smartphone)?



GRAFIK 31

Quelle: Corporate Trust 2014

1) NSA (National Security Agency): Größter Auslandsgeheimdienst der Vereinigten Staaten von Amerika. Die NSA ist für die weltweite Überwachung, Entschlüsselung und Auswertung elektronischer Kommunikation zuständig und in dieser Funktion ein Teil der Intelligence Community, in der sämtliche Nachrichtendienste der USA zusammengefasst sind.

2) GCHQ (Government Communications Headquarters): Eine britische Regierungsbehörde (Nachrichtenbehörde und Sicherheitsdienst), die sich mit Kryptografie, Verfahren zur Datenübertragung und mit der Fernmeldeaufklärung befasst.

IT-Sicherheit

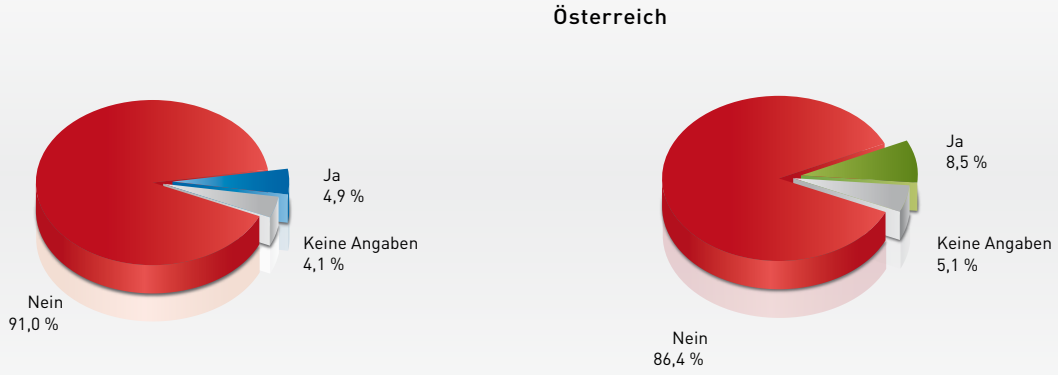
Die Risiken für einen Informationsabfluss in den Social Media wie Facebook, Twitter & Co. werden völlig außer Acht gelassen.

Nur die wenigsten Unternehmen berücksichtigen Social Media[1] als Plattform für einen Informationsabfluss. In Österreich waren es nur 8,5 Prozent, die ein Monitoring von sozialen Medien betrieben, und in Deutschland gar nur 4,9 Prozent, also nicht einmal jedes zwanzigste Unternehmen. Obwohl die sozialen Medien von vielen Firmen zunehmend als Vertriebskanal genutzt werden, betrachten sie diese nur sehr einseitig und erkennen nicht den vollen Umfang. Die Möglichkeit, dass unzufriedene Mitarbeiter dort wertvolles Unternehmens-Know-how preisgeben oder Plagiate frühzeitig erkannt werden könnten, lassen sie meist völlig außer Acht.

Jedes Unternehmen will sich und seine Produkte möglichst positiv darstellen. Was aber, wenn ein „Shitstorm"[2] plötzlich und unerwartet das Image in Gefahr bringt? Wie schnell kann dies erkannt und darauf reagiert werden? Im Rahmen der aktuell festzustellenden Angriffe bei Industriespionage geht es nicht mehr nur darum, Daten zu beschaffen, sondern auch darum, Produktionsprozesse, Lieferketten oder die Kommunikation mit Kunden und Lieferanten zu sabotieren. Wird so etwas gezielt in sozialen Medien dargestellt und die Entrüstung „angefacht", kann dies schnell zu einem Reputationsverlust führen.

Unternehmen sollten daher ein zielgerichtetes Monitoring von Social Media betreiben. Dies beinhaltet auch, dass wichtige und für das Unternehmen relevante Blogs regelmäßig mitgelesen werden, die klassischen Karriere-Plattformen für Mitarbeiter (wie XING, LinkedIn oder Stepstone) auf Datenabfluss gescreent[3] werden und bei Facebook, Twitter & Co. überprüft wird, ob es Negativmeinungen zum Unternehmen oder zu den Produkten gibt.

Gibt es ein Monitoring von Social Media bezüglich Informationsabfluss?



GRAFIK 32

Quelle: Corporate Trust 2014

1) Social Media (auch soziale Medien): Digitale Medien oder Technologien, die es Nutzern im Internet ermöglichen, sich untereinander auszutauschen und mediale Inhalte einzeln oder in Gemeinschaft zu erstellen. Als Kommunikationsmittel werden dabei Text, Bild, Audio oder Video verwendet.

2) Shitstorm: Bezeichnet im Deutschen das Auftreten eines Phänomens bei Diskussionen im Rahmen von sozialen Netzwerken, Blogs oder Kommentarfunktionen von Internetseiten; meist ein Sturm der Entrüstung, der zum Teil mit beleidigenden Äußerungen einhergeht.

3) Screening: Ein systematisches Testverfahren, das eingesetzt wird, um innerhalb eines definierten Prüfbereichs Elemente herauszufiltern, die bestimmte Eigenschaften aufweisen. Das Verfahren kann aus einem Test oder einer Abfolge von aufeinander abgestimmten Tests bestehen.

Es ist nicht genug zu wissen - man muss auch anwenden.
Es ist nicht genug zu wollen - man muss auch tun.

Johann Wolfgang von Goethe

Sicherheitsvorkehrungen im Unternehmen

Personal

Die Loyalität der Mitarbeiter ist für viele Unternehmen schwer einschätzbar. Sie gehen jedoch davon aus, dass sie abnimmt.

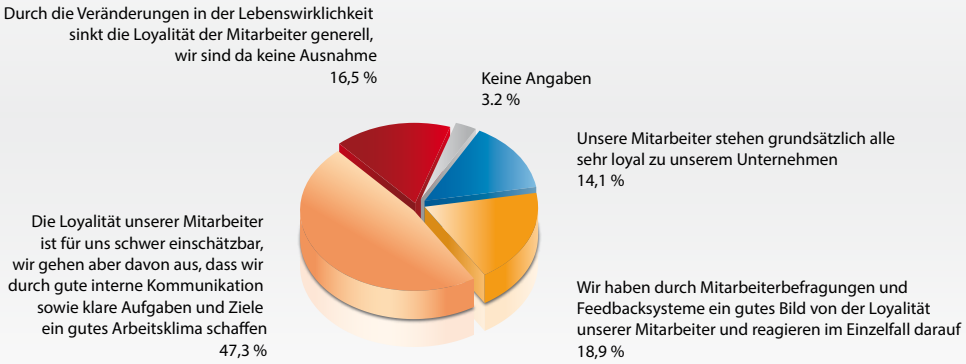
Die Loyalität der Mitarbeiter ist ein wichtiger Faktor für den Schutz von vertraulichem Know-how. Durch eine zunehmende Globalisierung, immer stärker werdenden Erfolgsdruck und härtere Bandagen im täglichen Geschäft nimmt jedoch oftmals die Loyalität zum Unternehmen ab. Während es früher vielleicht normal war, dass man sein ganzes Leben bei nur einem Arbeitgeber verbrachte, gibt es heute kaum noch eine emotionale Bindung der Mitarbeiter an das Unternehmen. Vorgesetzte müssen heute mehr fordern und stehen oftmals selbst unter Druck, die Zielvorgaben einzuhalten. Gemeinsame soziale Aktivitäten oder ein „offenes Ohr" für die Nöte und Sorgen der Mitarbeiter rücken da meist in den Hintergrund.

So scheint es auch nicht verwunderlich, dass sich Unternehmen schwer tun, die Loyalität ihrer Mitarbeiter einzuschätzen. Fast die Hälfte aller Unternehmen in Deutschland, exakt 47,3 Prozent, gaben an, dass die Loyalität ihrer Mitarbeiter für sie schwer einschätzbar sei. In Österreich waren es immerhin nur 27,2 Prozent, also etwa ein Viertel der Firmen. 16,5 Prozent in Deutschland und 19,5 Prozent in Österreich sind sich bereits völlig bewusst, dass die Loyalität der Mitarbeiter zum Unternehmen durch die Veränderungen in der Lebenswirklichkeit permanent sinkt. Interessanterweise glaubten nur noch 14,1 Prozent der Unternehmen in Deutschland und 23,7 Prozent der österreichischen Firmen, dass ihre Mitarbeiter sehr loyal zum Unternehmen stehen.

Dies sollte ein deutliches Signal für die Unternehmen in beiden Ländern sein, den Faktor Mensch nicht auf die leichte Schulter zu nehmen. Zuerst wäre es wichtig, die aktuelle Situation im Unternehmen zu erfassen und zu analysieren, wo die Gründe für einen etwaigen Mangel an Loyalität liegen. Dann sollten entsprechende Maßnahmen ergriffen werden, um die Loyalität der Mitarbeiter zu steigern. Dafür gibt es sicherlich keine Musterlösungen; es erfordert aber auf jeden Fall ein Umdenken in den Köpfen des Managements, denn ein gutes Betriebsklima und vernünftige Mitarbeiterführung gehören definitiv dazu. Mitarbeiter sind auch beim Informationsschutz ein sehr wichtiges Kapital!

Für wie hoch halten Sie die Loyalität Ihrer Mitarbeiter?

Deutschland

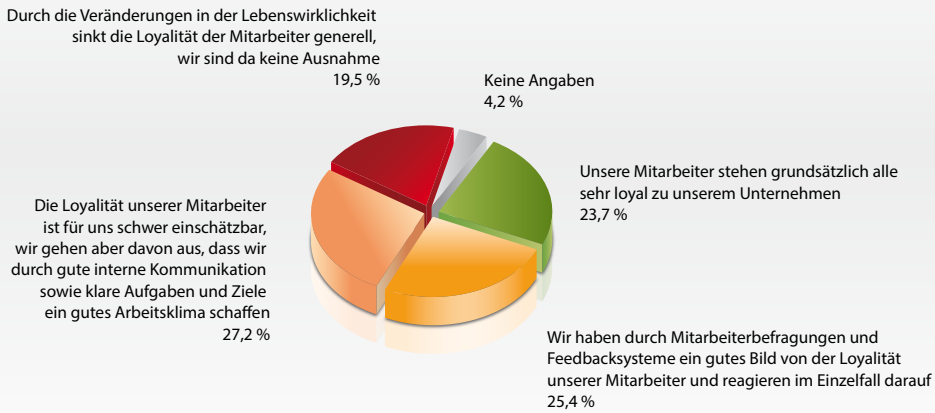


GRAFIK 33

Quelle: Corporate Trust 2014

Für wie hoch halten Sie die Loyalität Ihrer Mitarbeiter?

Österreich



GRAFIK 34

Quelle: Corporate Trust 2014

Sicherheitsvorkehrungen im Unternehmen

Personal

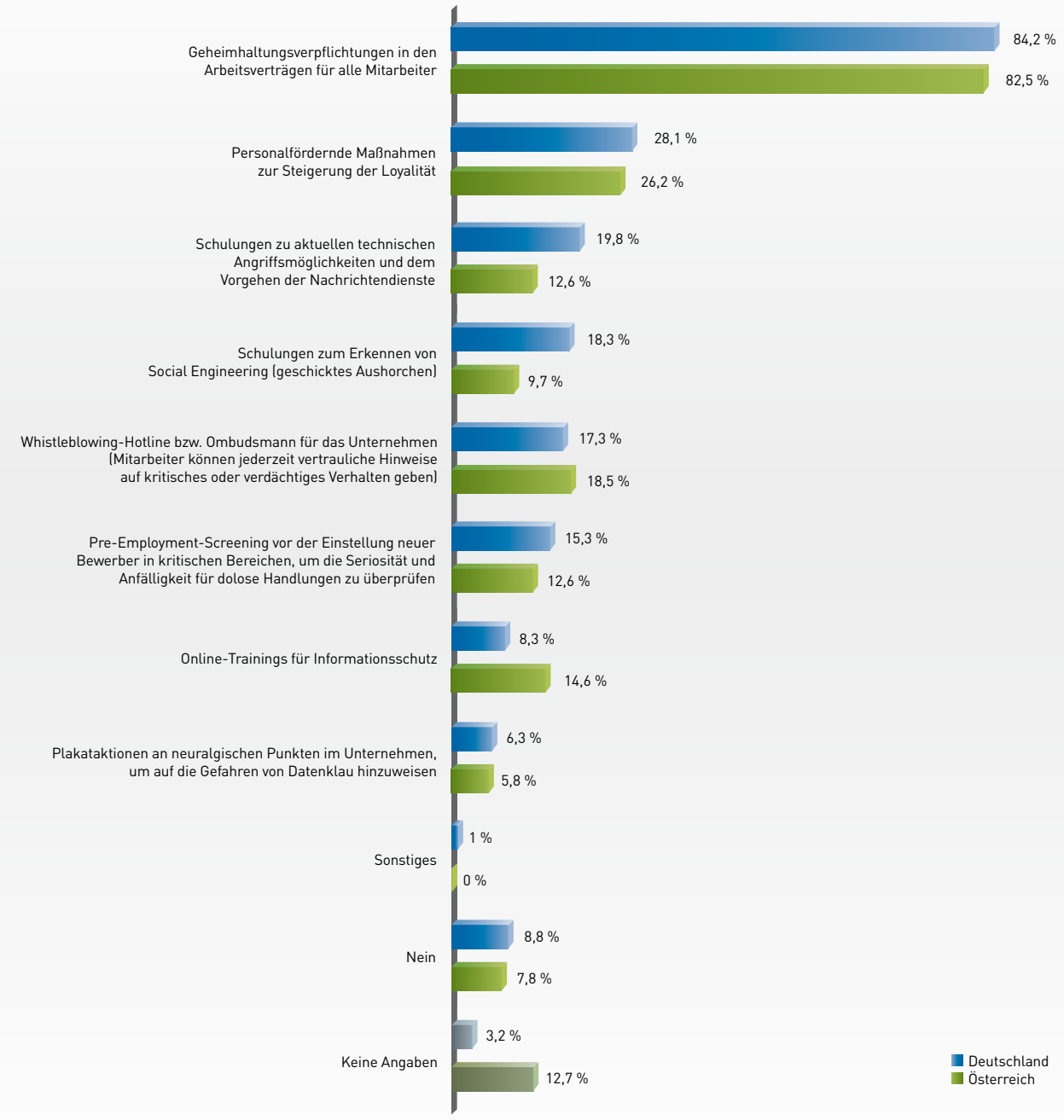
Mitarbeiter müssen stärker sensibilisiert werden, um für die Gefahren im „Cybergeddon“ gerüstet zu sein.

Die überwiegende Mehrzahl der Unternehmen hat zwar in den Arbeitsverträgen Geheimhaltungsverpflichtungen[1] mit den Mitarbeitern (in Deutschland waren es 84,2 Prozent und in Österreich 82,5 Prozent), die Sensibilisierung[2] für die Gefahren durch Industriespionage bleibt jedoch in den meisten Fällen aus. Schulungen zu aktuellen technischen Angriffsmöglichkeiten oder zum Erkennen von Social Engineering[3] gab es in Deutschland nur in 19,8 Prozent bzw. 18,3 Prozent und in Österreich nur in 12,6 Prozent bzw. 9,7 Prozent der Unternehmen. Vor allem Online-Trainings für den Informationsschutz wären heute einfach umzusetzen und würden die Mitarbeiter zeitlich nur gering binden. Aber auch dies gibt es nur in 8,3 Prozent (Deutschland) bzw. 14,6 Prozent (Österreich) aller Firmen. Um die Mitarbeiter künftig für die Gefahren im „Cybergeddon[4]“ zu rüsten, sollten sie dringend mehr Schulungen und Informationen zum Vorgehen bei Spionage erhalten.

Neben den Geheimhaltungsverpflichtungen setzen die Unternehmen beider Länder vor allem auf personalfördernde Maßnahmen zur Steigerung der Loyalität. Ein Pre-Employment-Screening[5] vor der Einstellung neuer Bewerber in kritischen Bereichen wird dagegen nur in 15,3 Prozent (Deutschland) bzw. 12,6 Prozent (Österreich) der Fälle eingesetzt. Gerade für neue Bewerber im Ausland ist ein solcher Background-Check[6] wichtig, weil er bereits im Vorfeld Auffälligkeiten ans Tageslicht bringt, die bei einer Einstellung schnell zu einem Informationsabfluss führen könnten. Über eine Whistleblowing[7]-Hotline verfügen ebenfalls nur 18,5 Prozent der deutschen bzw. 17,3 Prozent der österreichischen Unternehmen. Hinweise auf frühere kritische Handlungen von Mitarbeitern, mangelnde Integrität oder sonstige negativen Charaktereigenschaften können so oftmals nicht rechtzeitig erkannt werden. Dies kann dem Unternehmen langfristig schaden.

1) Geheimhaltungsverpflichtung (auch Vertraulichkeitsvereinbarung):	Schriftliche Vereinbarung über den Umgang mit vertraulichen Informationen.
2) Sensibilisierung:	Unterweisung bzw. Schulung der Mitarbeiter zu einer bestimmten Gefahrenlage mit Bezugnahme auf eine aktuelle Bedrohung.
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) Cybergeddon:	An „Armageddon“ oder „Harmagedon“ angelehnter Begriff, der eine finale oder endzeitliche Entscheidungsschlacht im Cyberraum (virtueller Raum aller auf Datenebene vernetzten IT-Systeme im globalen Internet) bezeichnen soll.
5) Pre-Employment-Screening:	Legale Überprüfung von Bewerbern im Personalauswahlverfahren vor der Einstellung bzw. Unterzeichnung des Arbeits-/Anstellungsvertrags zur Vermeidung von Risiken. Es soll vor allem Erkenntnisse über Charakter, Zuverlässigkeit und Integrität des jeweiligen Bewerbers liefern.
6) Background-Check (auch Pre-Employment-Screening):	Überprüfung von Mitarbeitern bezüglich früherer Arbeitgeber, finanzieller Verhältnisse, Firmenbeteiligungen sowie verdächtiger Lebensumstände.
7) Whistleblowing:	Ein Informant bringt Missstände, illegales Handeln oder allgemeine Gefahren, von denen er an seinem Arbeitsplatz erfährt, an die Öffentlichkeit.

Gibt es regelmäßige Informationen, Schulungen oder Sicherheitsvorkehrungen für Ihre Mitarbeiter, um sie für die Gefahren von Spionage zu sensibilisieren?
(Mehrfachnennungen möglich)



GRAFIK 35

Quelle: Corporate Trust 2014

Sicherheitsvorkehrungen im Unternehmen

Objektsicherheit

Die Awareness steigt zwar, aber es gibt nur wenige Unternehmen, die den baulichen Abhörschutz ernst nehmen.

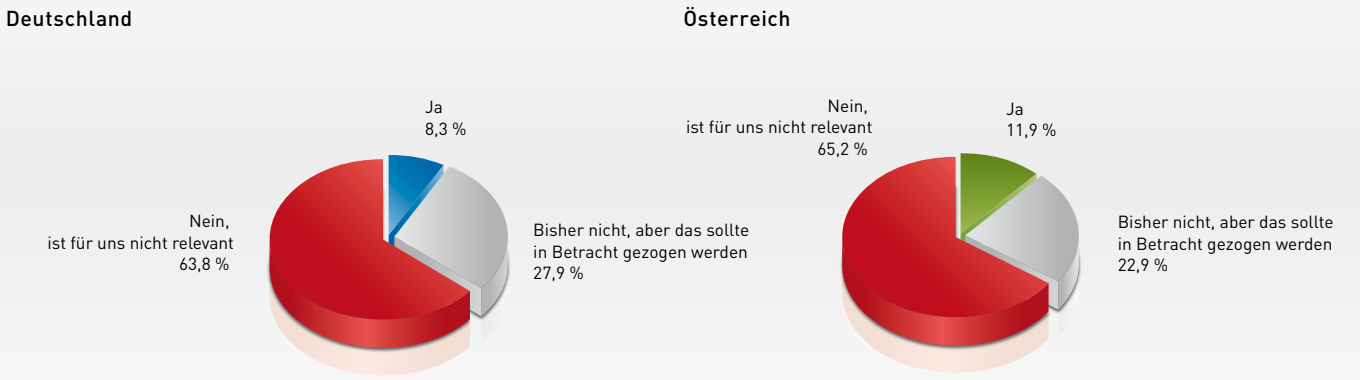
Wanzen[1] oder sonstige Abhörtechnologie werden immer noch von Industriespionen eingesetzt, um Firmengeheimnisse oder vertrauliche Besprechungen abzuhören. Ein solcher Lauschangriff[2] kann nur mit geeigneten Maßnahmen verhindert werden. Am leichtesten fällt es den Tätern, ihr Equipment bereits in der Bauphase in Wände, doppelte Böden oder abgehängte Decken einzubringen. Daher sollte es gerade bei Neu- oder Umbaumaßnahmen im Unternehmen einen Prozess geben, um sicherzustellen, dass keine Spionage-Technologie installiert werden kann.

Die Befragung hat zumindest gezeigt, dass die Awareness[3] der Unternehmen steigt. Annähernd jedes vierte Unternehmen (Deutschland: 27,9 Prozent; Österreich: 22,9 Prozent) gab an, dass man dies bisher zwar nicht getan habe, es zukünftig aber in Betracht gezogen werden sollte.

Vielleicht haben die Erkenntnisse aus den Aussagen von Edward Snowden dazu geführt, dass es ein verstärktes Bewusstsein für die Aktivitäten der Nachrichtendienste bzw. bei professioneller Spionage gibt.

Um sich gegen solche Täter zu schützen, wird es künftig noch viel wichtiger sein, strategische Entscheidungen in einem sicheren Umfeld zu treffen und als geheim eingestufte Besprechungen in abhörgeschützten Räumen[4] durchzuführen. Der Aufwand scheint zwar hoch, die Investitionen amortisieren sich aber meist nach kurzer Zeit, denn einmal verlorenes Know-how kann nicht wieder zurückgeholt werden. Der Aufwand für die Unternehmen, ständig noch schneller neue Innovationen zu schaffen, ist meist deutlich höher, als die Ausgaben für einen vernünftigen baulichen Abhörschutz.

Stellen Sie sicher, dass im Rahmen von Neu- oder Umbaumaßnahmen keine Spionage-Technologie in die Firmenräume eingebracht wird?



GRAFIK 36

Quelle: Corporate Trust 2014

1) Wanzen: Technische, meist miniaturisierte Bauteile bzw. Funksender zum Abhören von Gesprächen oder Aufzeichnen von Informationen.
2) Lauschangriff: Nachrichtendienstlicher Sprachgebrauch für die akustische Überwachung bzw. das Abhören von Gesprächen.
3) Awareness: Bewusstsein oder Gewahrsein über die eigene Handlung oder Betonung der aktiven Haltung bzw. Aufmerksamkeit gegenüber einem bestimmten Sachverhalt.
4) Abhörgeschützter Raum: Architektonische Abschirmung eines Raumes durch technische Maßnahmen, um ungewollte Funkübertragungen zu verhindern.

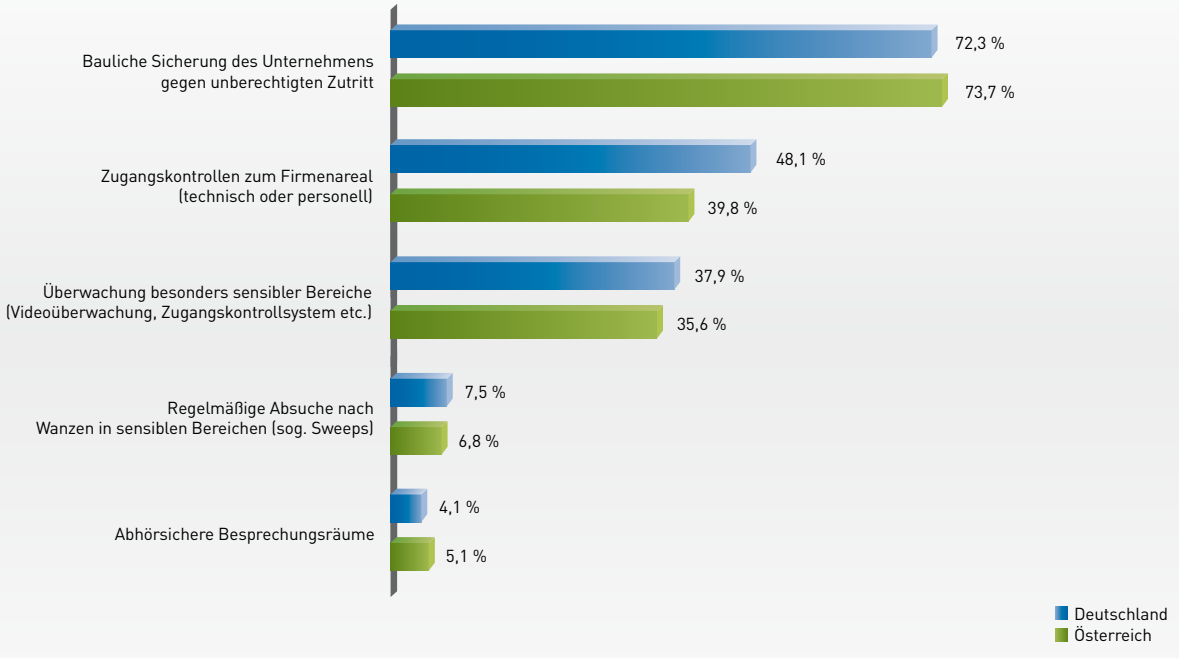
Bauliche Sicherheitsvorkehrungen gegen fremden Zutritt sind Standard, jedoch keine abhörsicheren Besprechungsräume oder Absuchen nach Wanzen.

Zäune, stabile Wände oder verschlossene Tore scheinen die meisten Unternehmen sehr ernst zu nehmen, dies gaben sie auf die Frage nach baulichen Sicherheitsvorkehrungen am häufigsten an. Technische oder personelle Zugangskontrollen zum Firmenareal gibt es jedoch nicht einmal mehr bei der Hälfte aller Unternehmen: In Deutschland hatten nur 48,1 Prozent eine solche Sicherung, in Österreich gar nur 39,8 Prozent.

Die Überwachung besonders sensibler Bereiche ist nur noch in etwas mehr als einem Drittel der Unternehmen gegeben (Deutschland: 37,9 Prozent; Österreich: 35,6 Prozent) und abhörsichere Besprechungsräume existieren praktisch fast nirgends. Auch das regelmäßige Absuchen nach Wanzen unterbleibt in den allermeisten Unternehmen; nur 7,5 Prozent der deutschen und 6,8 Prozent der österreichischen Firmen hatten diese Frage mit Ja beantwortet.

Täter haben damit kein hohes Entdeckungsrisiko, weil sich die Firmen weder entsprechend schützen, noch überprüfen, ob ein Lauschangriff[1] durchgeführt bzw. verdächtige Gegenstände eingebracht wurden. Abhören funktioniert heute noch sehr viel einfacher als vor ein paar Jahren, weil gerade die Kommunikationstechnik via GSM[2] immer kleiner wird. Über diverse Elektronik-Shops kann jedermann für geringes Geld unauffällig erscheinende Bauteile kaufen, in denen sich GSM-Module zum Abhören der Gespräche im Raum befinden.

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



GRAFIK 37

Quelle: Corporate Trust 2014

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

2) GSM (Global System for Mobile Communications): Ein Standard für volldigitale Mobilfunknetze, der hauptsächlich für Telefonie, aber auch für leitungsvermittelnde und paketvermittelnde Datenübertragungen sowie Kurzmitteilungen (Short Messages) genutzt wird.

Sicherheitsvorkehrungen im Unternehmen

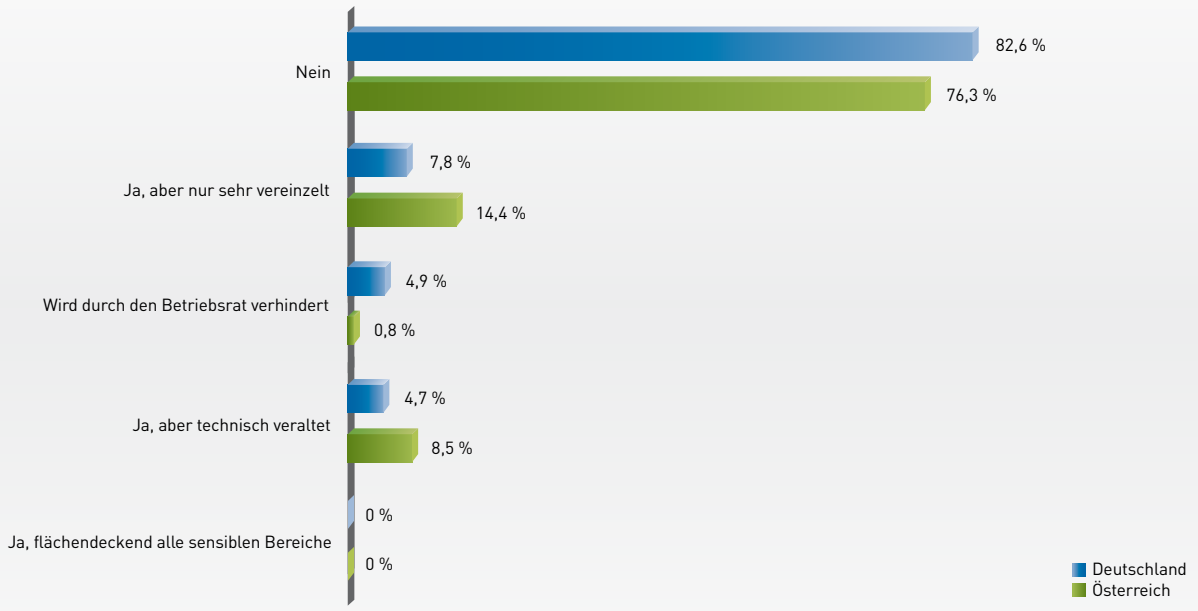
Objektsicherheit

Besonders sensible Bereiche sollten viel häufiger mit Videotechnik gesichert werden, um vertrauliche Daten besser zu schützen.

Vertrauliche Daten müssen besonders geschützt werden. Zum einen sollte durch aufeinander abgestimmte Sicherheitsvorkehrungen der Zugang erheblich erschwert werden, zum anderen sollte eine hohe Abschreckung gegen unberechtigten Zugriff bestehen. Besonders sensible Bereiche, in denen die „Kronjuwelen" des Unternehmens erzeugt, bearbeitet oder gelagert werden, sollten daher nicht nur ordentlich verschlossen, sondern der Zugang dazu auch mit Videotechnik überwacht werden.

Mehr als drei Viertel aller Unternehmen erklärten, dass sie keine Sicherung der besonders sensiblen Bereiche mittels Videoüberwachung durchführen. Praktisch kein Unternehmen nutzte diese Form der Abschreckung flächendeckend für alle sensiblen Örtlichkeiten. Dabei gaben nur 4,9 Prozent der Unternehmen in Deutschland und 0,8 Prozent der Unternehmen in Österreich an, dass dies durch den Betriebsrat verhindert werde. Bei einigen Firmen wird Videoüberwachung nur sehr sporadisch eingesetzt und 4,7 Prozent in Deutschland bzw. 8,5 Prozent in Österreich sagten aus, dass sie zwar Videokameras im Einsatz hätten, diese aber technisch veraltet seien.

Wird in Ihrem Unternehmen bereits Videotechnik zur Sicherung besonders sensibler Bereiche eingesetzt?



GRAFIK 38

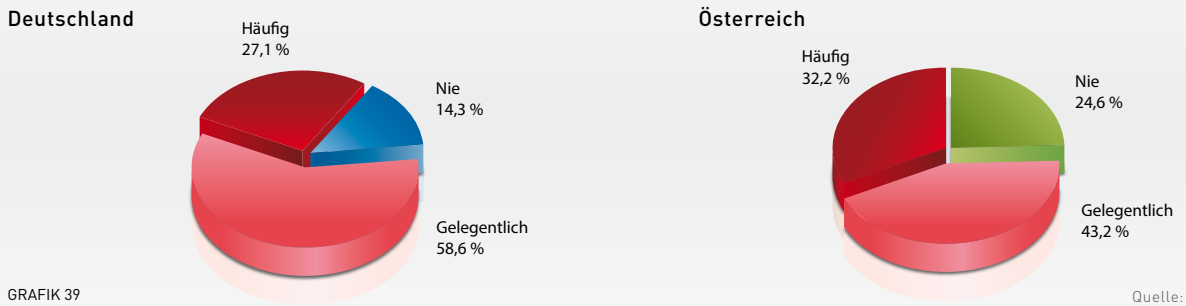
Quelle: Corporate Trust 2014

Obwohl geschäftlich relevante Daten häufig im privaten Umfeld bearbeitet werden, gibt es dort nur selten Sicherheitsvorkehrungen.

Ein Großteil des Managements und der Mitarbeiter nahm geschäftlich relevante Daten mit nach Hause, um die Unterlagen dort zu bearbeiten. 27,1 Prozent in Deutschland und 32,2 Prozent in Österreich gaben an, dies sogar häufig zu tun. Lediglich in 14,3 Prozent der deutschen und 24,6 Prozent der österreichischen Unternehmen kommt es niemals vor, dass Informationen aus dem Büro zu Hause bearbeitet werden.

Die Daten/Informationen sind damit nicht durch die Firmenmauern, Zugangskontrollen oder besonderen Verschluss geschützt. Auch Industriespione wissen das und versuchen immer häufiger, das vertrauliche Know-how an Orten abzugreifen, an denen es viel leichter zugänglich ist, nämlich im privaten Bereich. Trotzdem gaben 69,7 Prozent der deutschen Unternehmen und 71,2 Prozent der österreichischen Firmen an, keine Sicherheitsvorkehrungen zu treffen, damit geschäftliche Unterlagen oder Daten im privaten Umfeld vor unbefugtem Zugriff geschützt sind. Am ehesten scheinen noch Vorgaben gemacht zu werden, dass sensible Daten nicht zu Hause bearbeitet oder aufbewahrt werden dürfen (Deutschland: 24,5 Prozent; Österreich: 32,2 Prozent).

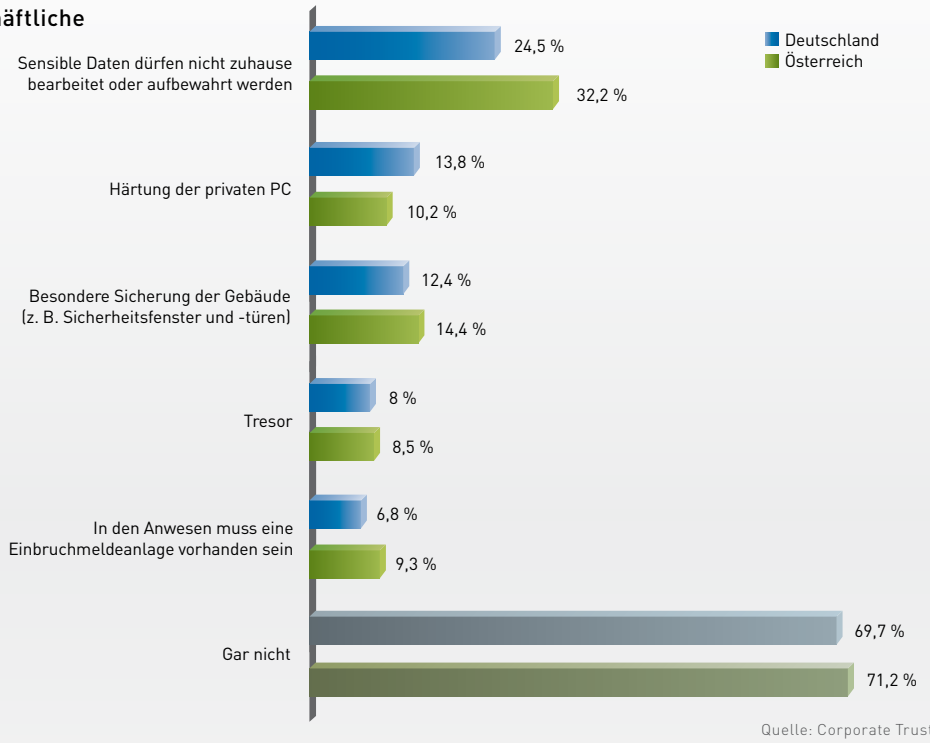
Bearbeiten Mitarbeiter oder das Management geschäftlich relevante Daten auch im privaten Umfeld (z.B. Home-Office)?



GRAFIK 39

Quelle: Corporate Trust 2014

Wie stellen Sie sicher, dass geschäftliche Unterlagen oder Daten im privaten Umfeld vor unbefugtem Zugriff geschützt sind?
(Mehrfachnennungen möglich)



GRAFIK 40

Quelle: Corporate Trust 2014

Sicherheitsvorkehrungen im Unternehmen

Sicherheit bei Auslandsreisen

Geschäftliche Daten sind im Ausland größtenteils nicht ausreichend geschützt.

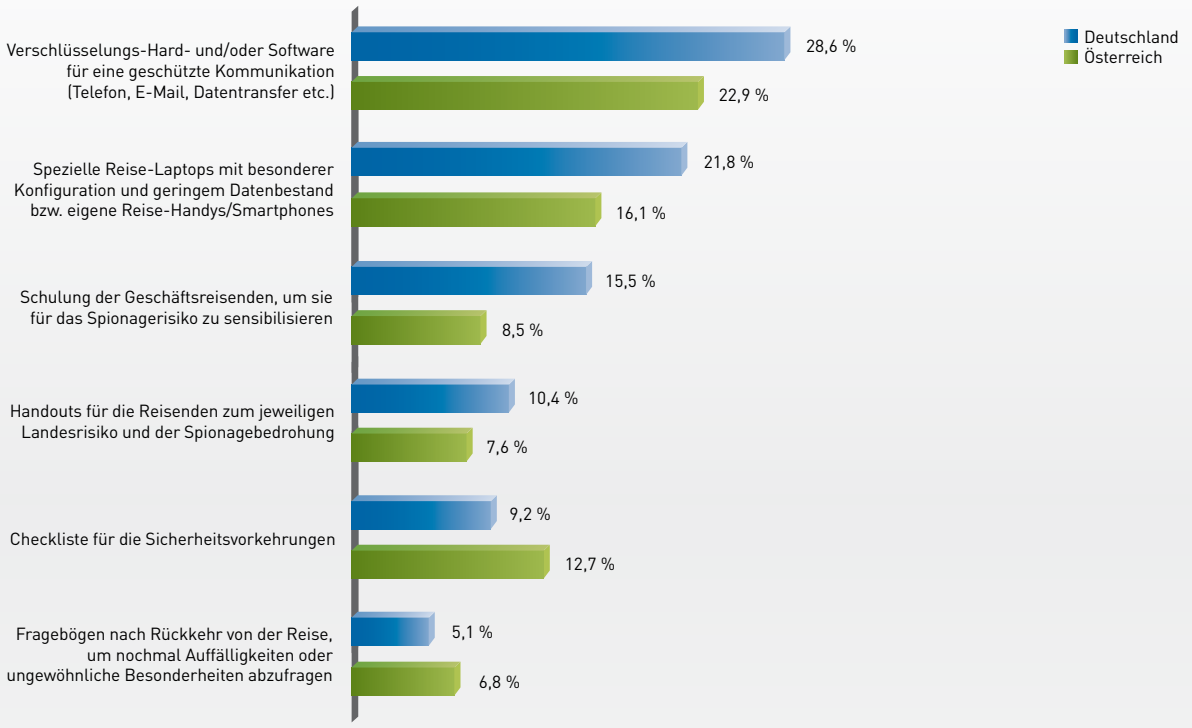
Gerade bei Geschäftsreisen ins Ausland besteht eine erhöhte Bedrohung für den Abfluss von sensiblem Unternehmens-Know-how. Nur wer sich ausreichend schützt, kann verhindern, dass auf die Datengeräte oder vertraulichen Unterlagen zugegriffen wird. Aber nicht jeder Mitarbeiter ist ein Profi in Sicherheitsangelegenheiten, und so ist es eine wichtige Aufgabe der Unternehmensleitung bzw. des Sicherheitsverantwortlichen, die Geschäftsreisenden auf ihren Aufenthalt vorzubereiten und sie mit entsprechenden Vorkehrungen zu unterstützen.

Am häufigsten wird Verschlüsselungs-Hard- und/oder Software eingesetzt, um eine vertrauliche Kommunikation zu gewährleisten. In Deutschland waren es 28,6 Prozent der Unternehmen und in Österreich 22,9 Prozent, die angaben, den Telefon- und E-Mail-Verkehr bzw. den Datentransfer bei Auslandsreisen zu verschlüsseln. Leider gaben nur 15,5 Prozent der deutschen Unternehmen ihren Mitarbeitern eine Schulung zur Sensibilisierung mit auf den Weg. In Österreich waren es gar nur 8,5 Prozent der Firmen, die dies für nötig befanden. Ein Handout[1] für die Reisenden zum jeweiligen Landesrisiko gab es fast ebenso selten.

Um kritische Anbahnungsversuche, versuchte Datenzugriffe oder sonstige Auffälligkeiten schnellstmöglich zu erfahren, bieten sich Fragebögen nach der Rückkehr von Geschäftsreisen geradezu an. Da auf einer Reise einiges passiert und die Mitarbeiter vor allem ihren geschäftlichen Auftrag im Fokus haben, kann so etwas schnell in Vergessenheit geraten. Ein Fragebogen ist da oft ein gutes Hilfsmittel, um die Reise noch einmal Revue passieren zu lassen und an die Auffälligkeiten erinnert zu werden. Leider nutzen nur 5,1 Prozent in Deutschland und 6,8 Prozent in Österreich diese Chance, mögliche Spionageversuche rasch zu erkennen.

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

Welche Sicherheitsvorkehrungen haben Sie getroffen, um Ihre Daten auf Auslandsreise zu schützen?
(Mehrfachnennungen möglich)



GRAFIK 41

Quelle: Corporate Trust 2014

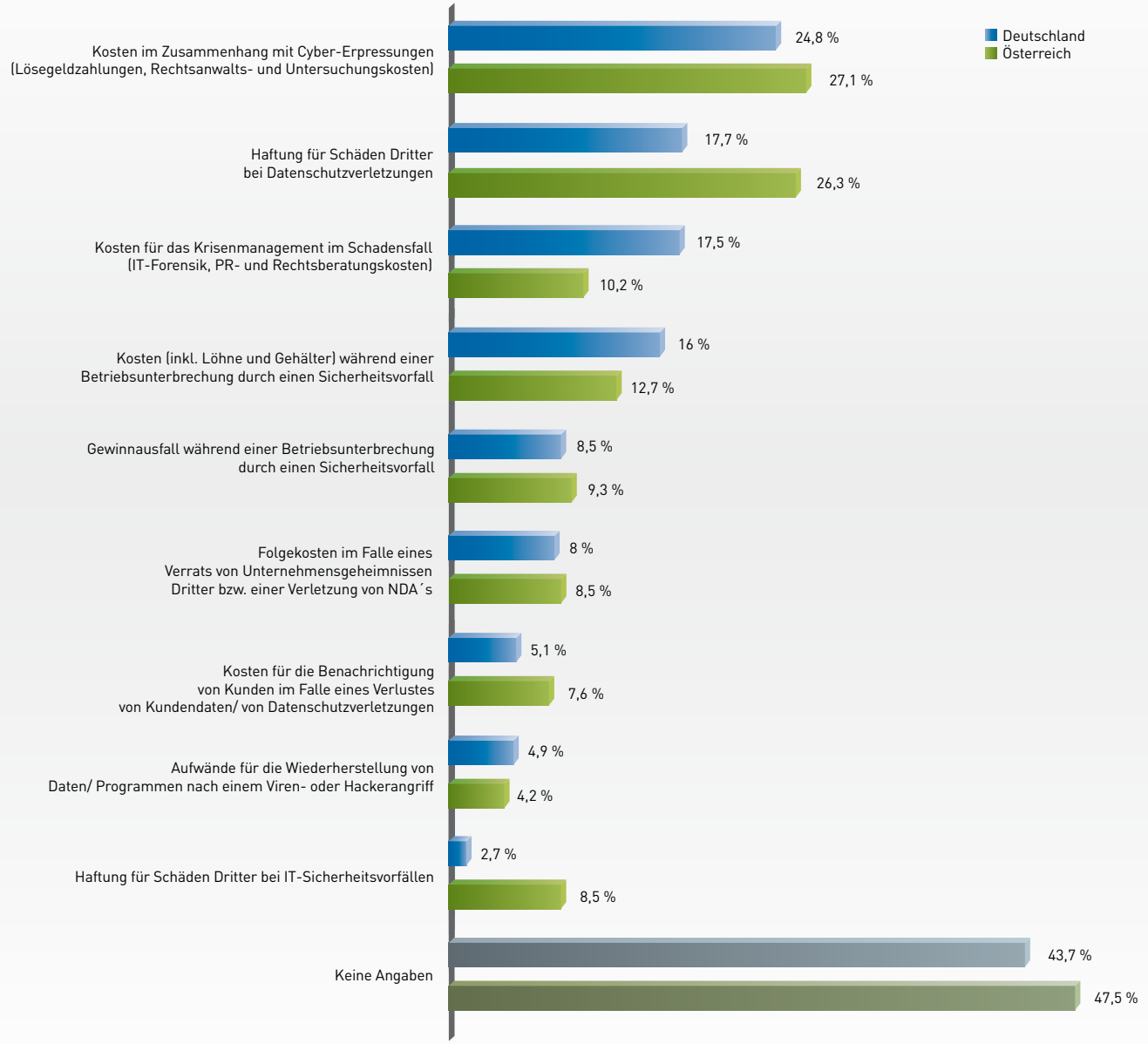
Finanzielle Risiken

Unternehmen sind sich der finanziellen Auswirkungen von Cyber-Risiken noch nicht ausreichend bewusst.

Fast die Hälfte der befragten Unternehmen machte bei dieser Frage keine Angaben. Die andere Hälfte sieht das größte Risiko in potenziellen Erpressungsversuchen. Bei österreichischen Unternehmen spielt zudem die Versicherung von Haftpflichtansprüchen Dritter wegen einer Datenschutzverletzung eine bedeutende Rolle.

Auffällig an dem Ergebnis ist, dass der Absicherung von Eigenschäden anscheinend kaum Bedeutung zukommt. Beispielsweise würden in Deutschland nur 8,5 Prozent und in Österreich nur 9,3 Prozent der Unternehmen den Gewinnausfall durch eine Betriebsunterbrechung versichern wollen. Dabei sind es gerade die Kosten infolge von Datenverlusten und Hackerangriffen[1], die den Großteil eines Schadens ausmachen können. Unternehmen scheinen also die Kosten eines Datenverlustes zu unterschätzen. Die Zahlen zeigen zudem, dass eine große Unsicherheit bezüglich der möglichen Schäden besteht und Unternehmen nicht wissen, welche Schäden abgesichert werden können.

Welche Risiken würden Sie gerne versichern oder haben Sie bereits versichert?
(Mehrfachnennungen möglich)



GRAFIK 42

Quelle: Corporate Trust 2014

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

Finanzielle Risiken

Nicht einmal jedes zwanzigste Unternehmen hat die finanziellen Risiken vernünftig abgesichert.

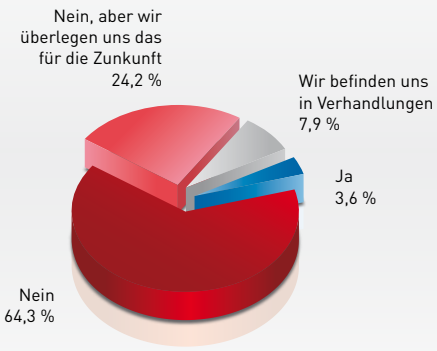
Cyber-Versicherungen sind seit wenigen Jahren auch in Deutschland erhältlich. Bereits zuvor war es schon möglich, einzelne Cyber-Risiken in bestehende Deckungen zu integrieren. Die steigende Bedrohung durch Hackerangriffe[1] sowie Datenverluste und die Komplexität der Materie machten es jedoch notwendig, Cyber-Risiken getrennt von anderen Versicherungssparten zu betrachten.

Nach wie vor scheinen Unternehmen den neuen Versicherungsprodukten aber skeptisch gegenüberzustehen. Ein Grund dafür mag sein, dass den für das Risikomanagement zuständigen Personen das Verständnis für die Risiken und möglichen Schäden fehlt. Allzu oft verlassen sich die Verantwortlichen dabei auf die Aussage der IT-Abteilung, dass kein Grund zur Sorge bestehe. Dabei können IT-Abteilungen das finanzielle Ausmaß eines Schadens in der Regel gar nicht abschätzen. Zudem sind im Hinblick auf Cyber-Risiken nicht nur die technischen Risiken zu bewerten; auch die Verträge mit Kunden und Geschäftspartnern sind zu prüfen. Relevant ist hier beispielsweise, ob Haftungsbeschränkungen bestehen oder das Unternehmen bei einem Verlust sensibler Daten voll haftet.

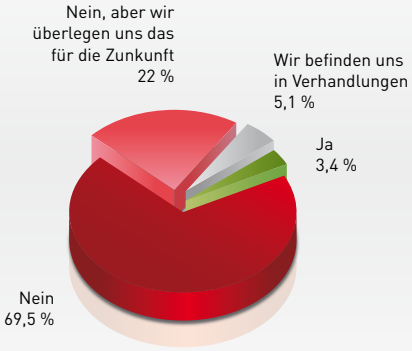
All diese zu berücksichtigenden Umstände führen dazu, dass Unternehmen sich nicht mit den Risiken beschäftigen wollen oder können. Aufgrund des mangelnden Verständnisses für das Risiko sehen viele Unternehmen dementsprechend auch noch keine Notwendigkeit für den Abschluss einer Cyber-Versicherung. Immerhin knapp ein Viertel der Unternehmen in Deutschland (24,2 Prozent) und Österreich (22,0 Prozent) denkt zumindest darüber nach, eine Cyber-Versicherung abzuschließen.

Hat Ihr Unternehmen bereits eine Cyber-Versicherung abgeschlossen?

Deutschland



Österreich



GRAFIK 43

Quelle: Corporate Trust 2014

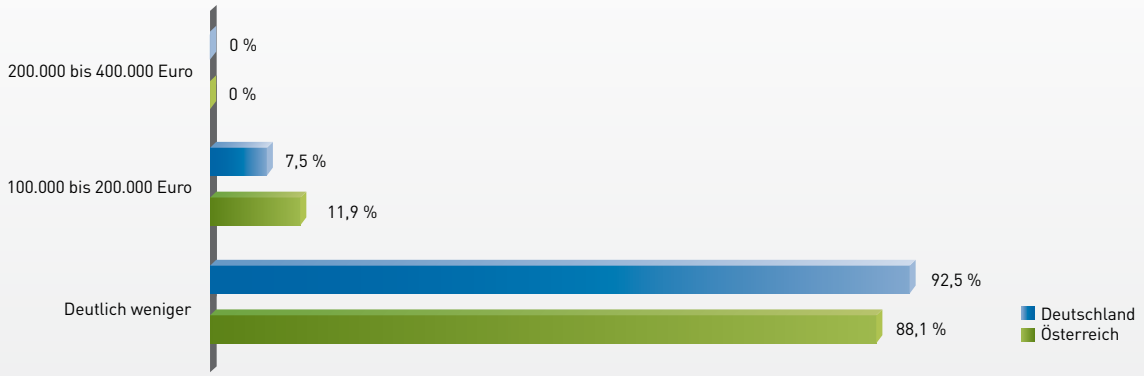
1) Hackerangriff: Unerlaubtes Eindringen in fremde Computer- oder Netzwerksysteme, meist durch das Überwinden von Sicherheitsmechanismen.

Die überwiegende Mehrheit der Unternehmen ist nicht bereit, mehr als 100.000 Euro für eine Cyber-Versicherung zu zahlen.

Der Wert einer Cyber-Versicherung wird offensichtlich als gering eingeschätzt. Dementsprechend sind Firmen nicht bereit, hohe Prämien zu zahlen. 92,5 Prozent der Unternehmen in Deutschland und 88,1 Prozent in Österreich gaben an, dass sie nur bereit wären, deutlich weniger als 100.000 bis 200.000 Euro dafür auszugeben.

Sicherlich ist dieses Ergebnis auch darauf zurückzuführen, dass gerade kleine und mittelständische Unternehmen selten mehrere Hunderttausend Euro für eine Versicherung ausgeben. Aber auch Großunternehmen scheinen nicht mehr als 200.000 Euro investieren zu wollen. Ein Grund dafür könnte sein, dass der Mehrwert einer Cyber-Versicherung schwer zu bemessen ist, insbesondere dann, wenn dem Unternehmen der Deckungsumfang und die Leistungen des Versicherers im Schadensfall nicht bekannt sind. Die Wahrscheinlichkeit, Opfer eines Hackerangriffes[1] zu werden oder durch Fahrlässigkeit Daten zu verlieren, ist zwar wesentlich höher als zum Beispiel ein Brand eines Fabrikgebäudes – der Wert einer Feuerversicherung lässt sich jedoch relativ leicht am Wert der zu versichernden Gebäude und Gegenstände beurteilen. Hier fehlt es den Unternehmen noch an klaren Fakten, welche Schadenssummen durch eine Cyberattacke[2] entstehen könnten.

Wie viel wäre Ihnen eine Deckungssumme von 10 Mio. Euro wert?



Grafik 44

Quelle: Corporate Trust 2014

1) Hackerangriff: Unerlaubtes Eindringen in fremde Computer- oder Netzwerksysteme, meist durch das Überwinden von Sicherheitsmechanismen.
2) Cyberattacke: Der gezielte Angriff von außen auf größere, für eine spezifische Infrastruktur wichtige Computernetzwerke.

Finanzielle Risiken

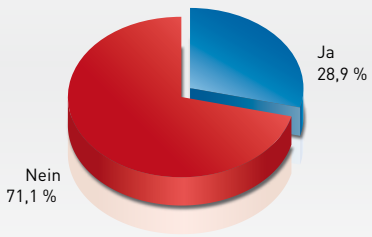
Unternehmen fühlen sich nicht ausreichend über die am Markt erhältlichen Versicherungslösungen informiert.

71,1 Prozent der deutschen und 63,6 Prozent der österreichischen Unternehmen haben das Gefühl, nicht ausreichend über die am Markt erhältlichen Versicherungslösungen informiert zu sein. Diese Zahlen belegen zum einen, dass Versicherer und Versicherungsmakler deutlich mehr Aufklärungsarbeit leisten müssen, um Unternehmen über die verfügbaren Versicherungskonzepte zu informieren. Zum anderen bestätigen sie die Annahme, dass aufseiten der Unternehmen immer noch das Bewusstsein für Cyber-Risiken fehlt. In der Konsequenz bedeutet das, dass man sich nicht mit entsprechenden Versicherungsprodukten beschäftigt.

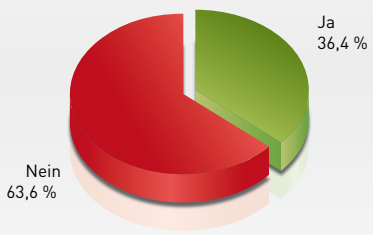
Die Versicherungsbranche hält inzwischen umfangreiches Informationsmaterial bereit, das von Unternehmen lediglich abgerufen werden muss. Speziell entwickelte Cyber Diagnostic Tools können zudem dabei helfen, einen ersten Einblick in die eigenen Risiken zu gewinnen und erste Schritte zur Risikovermeidung einzuleiten. Vor allem bei den aktuellen Risiken eines „Cybergeddon"[1] kann den Unternehmen in beiden Ländern nur geraten werden, die umfangreichen Beratungsangebote wahrzunehmen.

Haben Sie das Gefühl, ausreichend über die am Markt erhältlichen Versicherungslösungen informiert zu sein?

Deutschland



Österreich



GRAFIK 45

Quelle: Corporate Trust 2014

1) Cybergeddon: An den Begriff Armageddon oder Harmagedon angelehnter Begriff, der eine finale oder endzeitliche Entscheidungsschlacht im Cyberraum (virtueller Raum aller auf Datenebene vernetzten IT-Systeme im globalen Internet) bezeichnen soll.

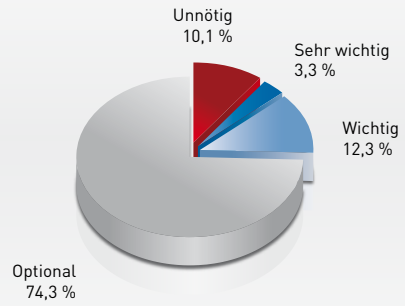
Unternehmen unterschätzen den Wert von Cyber-Versicherungen für den Risikotransfer.

Auf die Frage, wie wichtig Cyber-Versicherungen zukünftig für sie wären, gaben zumindest 74,3 Prozent (Deutschland) bzw. 72,0 Prozent (Österreich) der Unternehmen an, dass sie dies für optional hielten. Etwa jedes zehnte Unternehmen hält sie leider für unnötig. Dieses Ergebnis spiegelt letztendlich das teilweise mangelnde Risikobewusstsein der Entscheider wider. In zahlreichen Umfragen zu den größten Bedrohungen für die Gesamtwirtschaft belegen Cyber-Risiken stets die ersten Plätze. Auf das eigene Unternehmen werden diese Risiken jedoch noch nicht ausreichend bezogen.

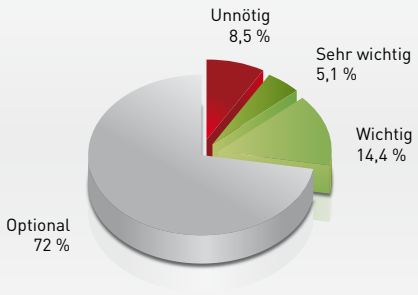
Neben den bereits genannten Gründen für diese fatale Fehleinschätzung ist sicherlich auch die Mentalität der Bürger im deutschsprachigen Raum ausschlaggebend. Deutschland ist weltweit bekannt für seine Innovationskraft und Ingenieurleistungen sowie die Zuverlässigkeit seiner Produkte. Die Menschen sind es gewohnt, auf Technik „Made in Germany" oder „Made in Austria" zu vertrauen. Dieses Vertrauen überwiegt anscheinend die Angst, Opfer eines Hackerangriffes[1] zu werden. Dabei wird jedoch übersehen, dass Deutschland gerade in diesem Bereich keine Führungsposition einnimmt

Für wie wichtig halten Sie Cyber-Versicherungen in Zukunft?

Deutschland



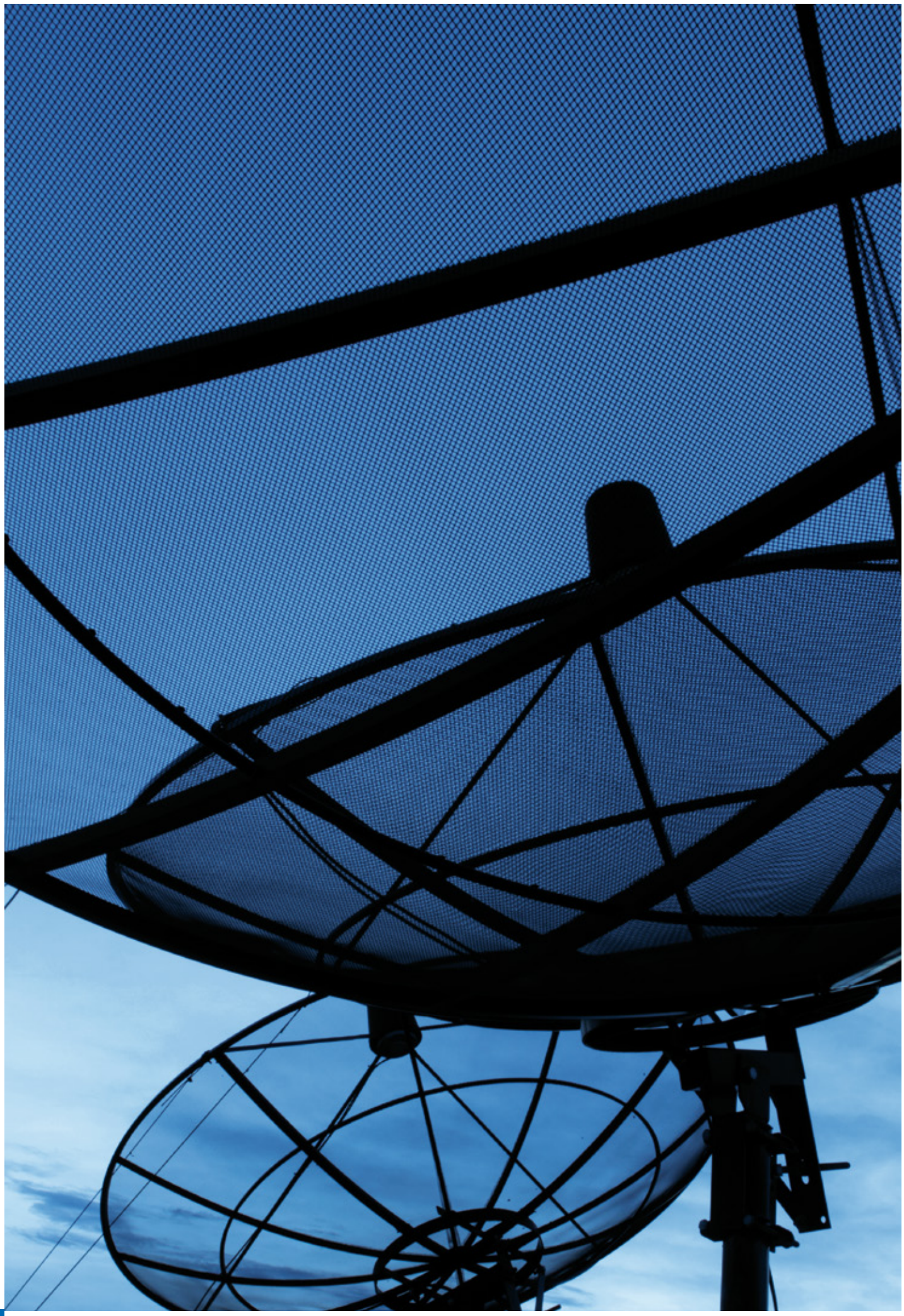
Österreich



GRAFIK 46

Quelle: Corporate Trust 2014

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



Einschätzung der künftigen Risiken

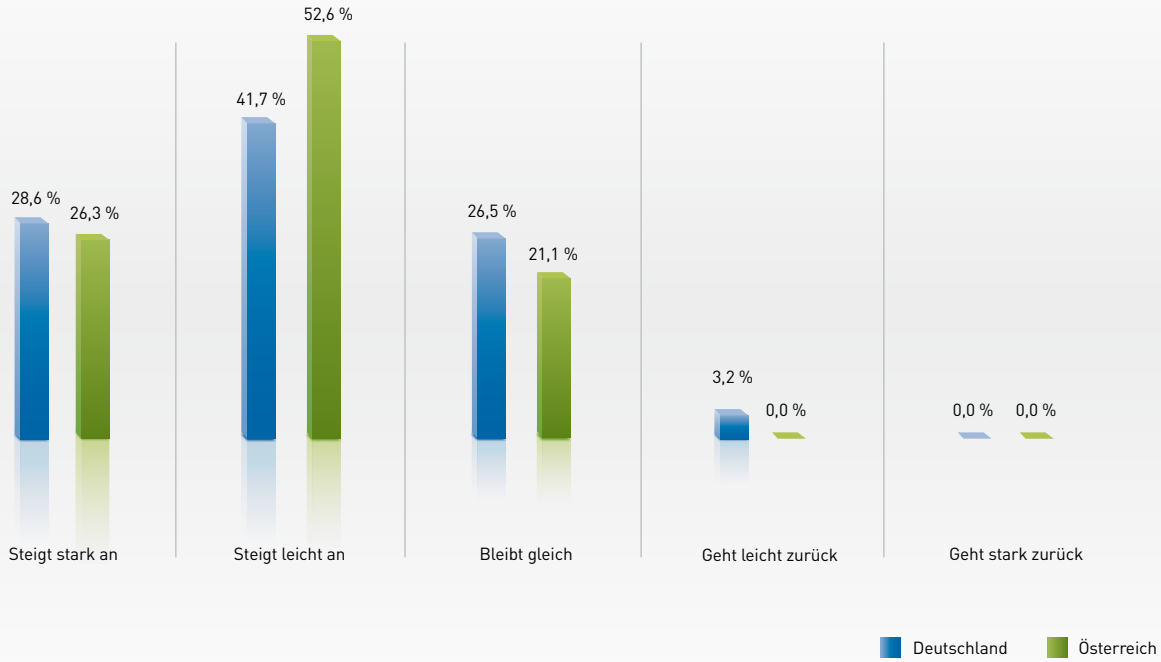
Den Unternehmen ist bewusst, dass Industriespionage noch deutlich zunehmen wird.

In Deutschland gab es nur wenige Unternehmen, die glauben, dass Industriespionage zurückgehen wird; in Österreich glaubt dies sogar niemand. Die meisten Unternehmen sind sich bewusst, dass ihr Risiko, Opfer eines Spionageangriffs zu werden, ansteigt. 52,6 Prozent in Deutschland und 41,7 Prozent in Österreich denken, dass die Industriespionage in den nächsten Jahren leicht zunehmen wird. Einen starken Anstieg vermuten sogar 28,6 Prozent (Deutschland) bzw. 26,3 Prozent (Österreich).

Bei der Befragung 2012 glaubten noch 47,7 Prozent der deutschen Unternehmen, dass ihr eigenes Risiko, ausspioniert zu werden, gleich bleiben werde. Hier haben die Unternehmen in den letzten Jahren vermutlich dazugelernt. Vor allem in Österreich scheint es ein hohes Bewusstsein dafür zu geben, dass Spionage auf dem Vormarsch ist und in den nächsten Jahren noch zulegen könnte.

Den Unternehmen ist bewusst, dass die technischen Möglichkeiten der weltweiten Überwachung permanent zunehmen und sie daher überall ausgeforscht werden können. Angriffe durch Stuxnet[1], Flame[2], Duqu[3] oder Uroburos[4] haben gezeigt, dass Nachrichtendienste heute mit allen zur Verfügung stehenden technischen Möglichkeiten ihre strategischen Ziele verfolgen. Vermutlich befinden wir uns bereits im „Cybergeddon"[5]. Es bleibt zu hoffen, dass sich die Unternehmen darauf einstellen, die Einschätzung der künftigen Gefährdung auf ihre eigene Firma übertragen und deshalb entsprechende Sicherheitsmaßnahmen ergreifen.

Wie ist Ihre Einschätzung für die künftige Entwicklung von Industriespionage?



GRAFIK 47

Quelle: Corporate Trust 2014

1) Stuxnet: Computerwurm, der im Juni 2010 entdeckt wurde. Er wurde speziell für das System Simatic S7 zur Überwachung und Steuerung technischer Prozesse entwickelt, um damit in die Steuerung von Frequenzumrichtern einzugreifen.

2) Flame: Komplexes Schadprogramm für Angriffe in Rechnernetzen, um sie fernzusteuern oder auszuspionieren. Damit können z. B. angeschlossene oder integrierte Mikrofone eingeschaltet und abgehört oder Tastaturen und Bildschirme ausgewertet werden.

3) Duqu: Vermutlich auf dem Quelltext von Stuxnet aufbauende Nachfolge-Malware zur Sammlung von Informationen in Computersystemen, um damit künftige Angriffe vorzubereiten.

4) Uroburos: Mutmaßliche Geheimdienstsoftware zum Absaugen hochsensibler und geheimer Informationen von staatlichen Einrichtungen, Nachrichtendiensten und Großunternehmen, welche autonom arbeitet, sich selbstständig im infizierten Rechner verbreitet und auch Rechner angreift, die nicht direkt mit dem Internet verbunden sind. Damit soll die Kontrolle über den PC erlangt und Daten vom Computer gestohlen werden.

5) Cybergeddon: An „Armageddon" oder „Harmagedon" angelehnter Begriff, der eine finale oder endzeitliche Entscheidungsschlacht im Cyberraum (virtueller Raum aller auf Datenebene vernetzten IT-Systeme im globalen Internet) bezeichnen soll.

Einschätzung der künftigen Risiken

Das Verhalten von Mitarbeitern und die Verwendung von Mobilgeräten machen Unternehmen für die Zukunft am meisten Sorgen.

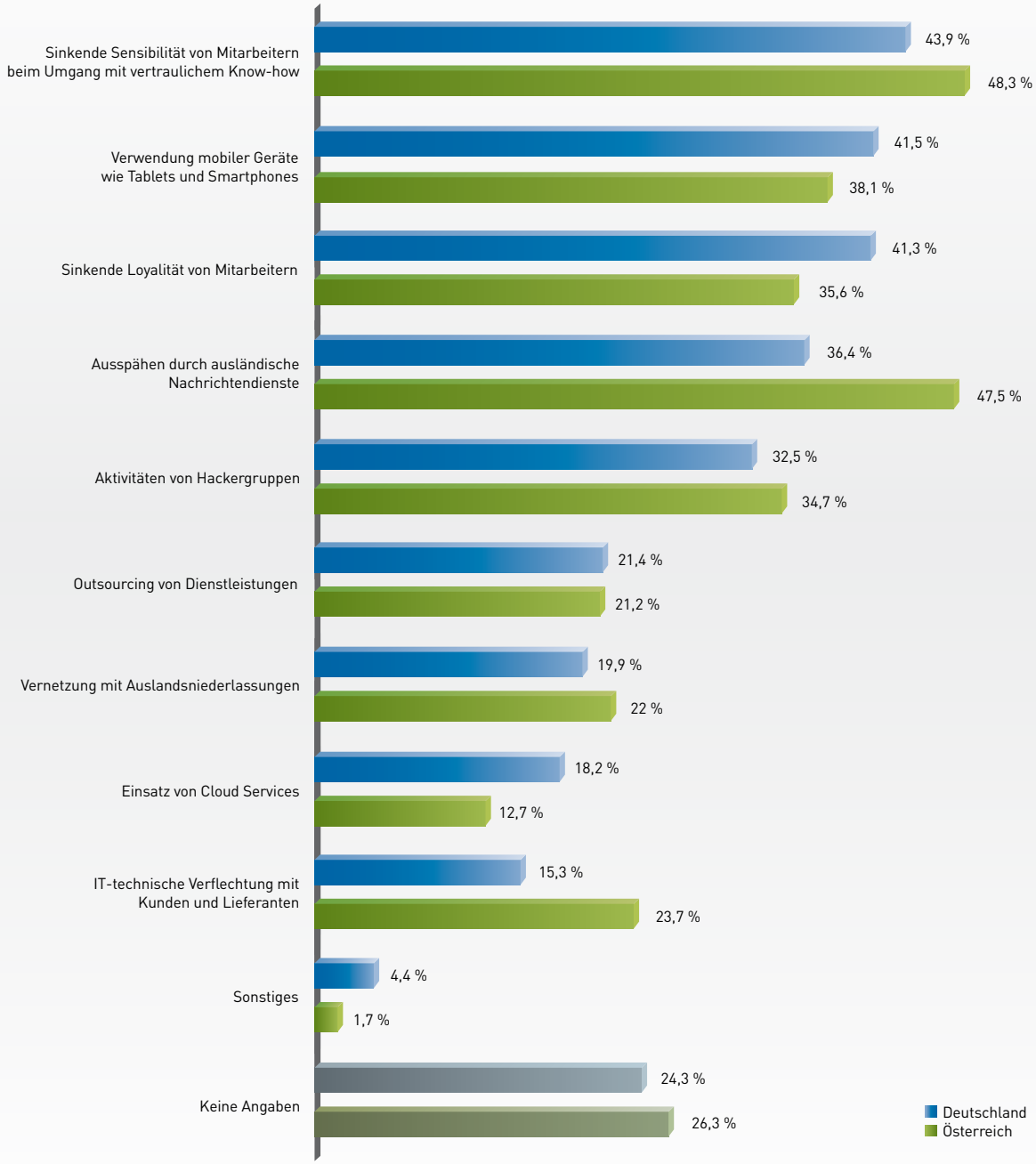
43,9 Prozent in Deutschland und 48,2 Prozent in Österreich gaben an, dass ihnen die sinkende Sensibilität von Mitarbeitern beim Umgang mit vertraulichem Know-how am meisten Sorge bereite. Dies ist nicht verwunderlich, stand doch an zweiter Stelle die Verwendung mobiler Geräte wie Tablets und Smartphones (Deutschland: 41,5 Prozent; Österreich: 38,1 Prozent). Immer mehr Mitarbeiter sind mit Tablets oder Smartphones ausgestattet und tragen damit sensible Unternehmensinformationen mit sich herum. Je fahrlässiger sie damit umgehen, umso häufiger kommt es vor, dass Geräte verloren werden oder die Informationen in fremde Hände fallen.

Ebenfalls an einer der vorderen Stellen rangiert die Angst vor der sinkenden Loyalität der Mitarbeiter. 41,3 Prozent der deutschen und 35,6 Prozent der österreichischen Firmen sind sich durchaus bewusst, dass ihre Mitarbeiter häufig keine allzu hohe Verbundenheit mit dem Unternehmen haben. Daraus ergeben sich Chancen für Angreifer. Es gilt das leichteste Opfer zu finden. Wer hat Schulden? Wer äußert sich in sozialen Netzwerken kritisch über seinen Arbeitgeber und hat daher evtl. schon die innere Kündigung vollzogen? Einem solchen Mitarbeiter Geld für sensible Informationen zu bieten, kann deutlich günstiger sein, als zu versuchen langwierig über einen Hackerangriff[1] in das Netzwerk einzudringen.

In Österreich lag an zweiter Stelle (47,5 Prozent) der Verdacht, dass Nachrichtendienste zukünftig noch viel mehr das vertrauliche Wissen der Unternehmen ausspionieren werden. Dies sahen deutsche Unternehmen erst an vierter Stelle (36,4 Prozent) der künftigen Risiken. Hier haben die Enthüllungen von Edward Snowden sicherlich ihren Teil dazu beigetragen, dass die Arbeit der Nachrichtendienste zunehmend kritisch beurteilt wird. Interessanterweise wurde in beiden Ländern das Risiko beim Einsatz von Cloud Services nur von knapp jeder fünften Firma als Bedrohung eingestuft.

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

Welche Entwicklungen sehen Sie als zunehmende Risiken für Ihr Know-how?
(Mehrfachnennungen möglich)



GRAFIK 48

Quelle: Corporate Trust 2014

Einschätzung der künftigen Risiken

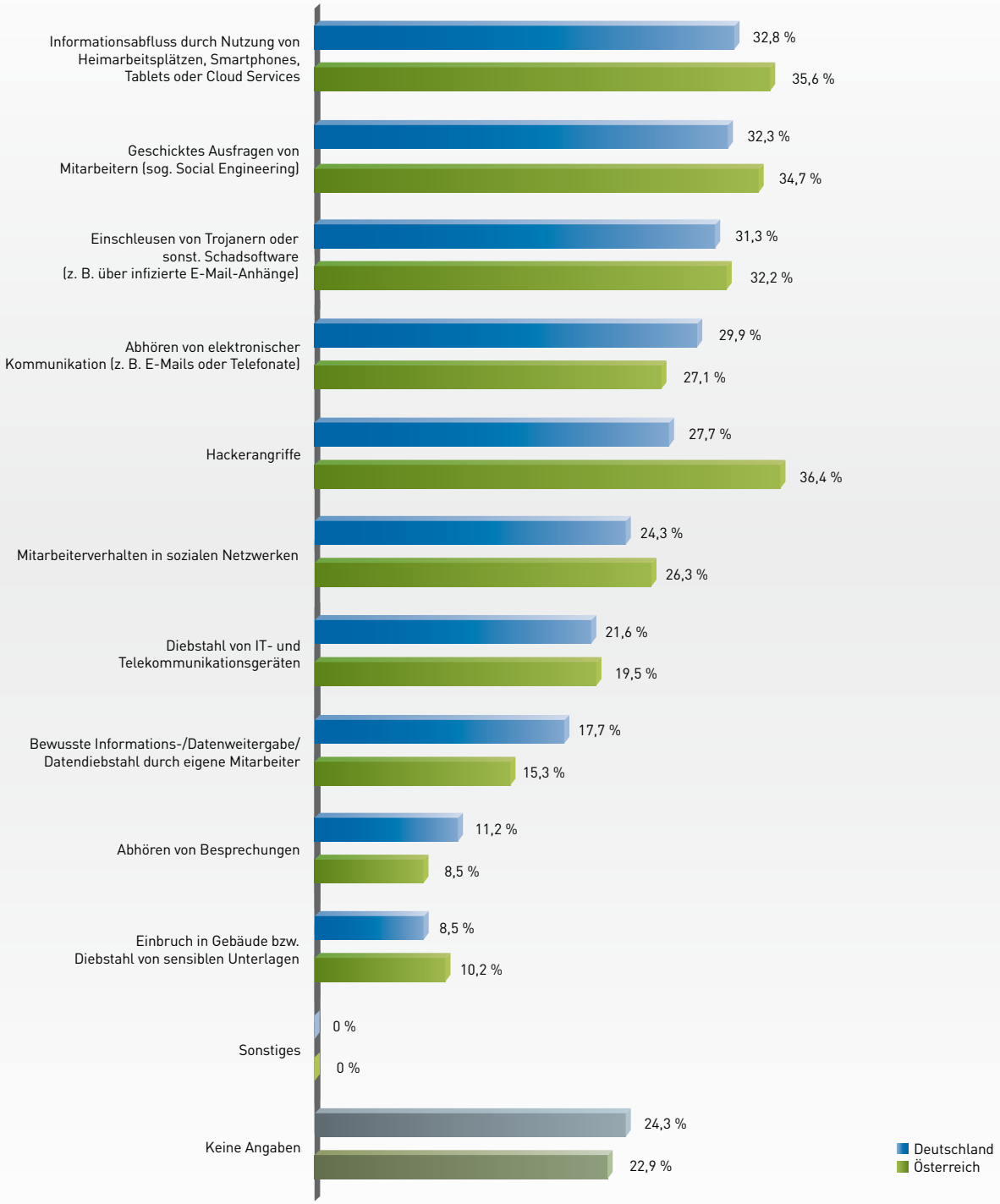
Unternehmen sind sich ziemlich sicher, dass ihre Schutzmaßnahmen für die aktuellen Bedrohungen nicht ausreichen.

Die Einschätzung der Bedrohungen, für die ihre Schutzmaßnahmen nicht ausreichten, war in beiden Ländern teilweise unterschiedlich. Während in Österreich die meisten Unternehmen (36,4 Prozent) davon ausgehen, dass sie nicht genug getan haben, um Hackerangriffe[1] zu verhindern, war es in Deutschland am häufigsten (32,8 Prozent) die Befürchtung, dass keine ausreichenden Sicherheitsvorkehrungen bestehen, um bei der Nutzung von Heimarbeitsplätzen, Smartphones, Tablets oder Cloud Services[2] einen Informationsabfluss zu verhindern. Das geschickte Ausfragen von Mitarbeitern (sogenanntes Social Engineering[3]) sahen die Unternehmen in beiden Ländern (Deutschland: 32,3 Prozent; Österreich: 34,7 Prozent) als starke Bedrohung, für die sie nicht ausreichend gerüstet seien. Ebenfalls in der oberen Hälfte der gefühlten Risiken ohne entsprechende Gegenmaßnahmen lagen das Einschleusen von Trojanern[4] oder sonstiger Schadsoftware sowie das Abhören von elektronischer Kommunikation.

Alle genannten Risiken beschränken sich nicht nur auf einen Unternehmensbereich: Der Schutz gegen die Bedrohungen eines Hackerangriffs oder des Abhörens der Kommunikation wird zwar in vielen Firmen als technische Disziplin der IT-Abteilung verstanden, dem ist aber nicht so. Nur wenn Mitarbeiter durch adäquate Sensibilisierung[5] entsprechend mit IT-Equipment umgehen, wird Informationsschutz beim Einsatz von modernen Kommunikationsgeräten auch funktionieren. Darüber hinaus stellt gerade die Prävention gegen Social Engineering die Personalabteilungen vor große Herausforderungen. Sie sind zwar zuständig für die Mitarbeiterqualifizierung, tun sich aber schwer, das sehr IT-lastige Thema eigenständig umzusetzen. Es ist also nötig, dass alle Disziplinen zusammenwirken, damit der Informationsschutz durch ein vernünftiges Zusammenspiel von Mensch, Technik und Prozess gewährleistet werden kann.

1) Hackerangriff:	Unerlaubtes Eindringen in fremde Computer- oder Netzwerksysteme, meist durch das Überwinden von Sicherheitsmechanismen.
2) 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.
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) Trojaner:	Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund jedoch ohne Wissen des Anwenders eine andere Funktion ausführt.
5) Sensibilisierung:	Unterweisung bzw. Schulung der Mitarbeiter zu einer bestimmten Gefahrenlage mit Bezugnahme auf eine aktuelle Bedrohung.

Gibt es Bedrohungen, für die Sie die Schutzmaßnahmen Ihres Unternehmens nicht für ausreichend halten?
(Mehrfachnennungen möglich)



GRAFIK 49

Quelle: Corporate Trust 2014

Schlussfolgerungen

Bewertung der Ergebnisse

Industriespionage ist auf dem Vormarsch. Vor allem technische Angriffe nehmen permanent zu und gefährden die Wirtschaft in beiden Ländern.

Erstmals wurde der Schaden durch Industriespionage sowohl für die deutsche als auch die österreichische Wirtschaft erhoben. Dabei hat sich herausgestellt, dass in beiden Ländern die Häufigkeit und das Volumen an Schäden ziemlich identisch sind. Der finanzielle Gesamtschaden beläuft sich jährlich in Deutschland auf ca. 11,8 Milliarden Euro und in Österreich auf ca. 1,6 Milliarden Euro. Bei den zugrunde gelegten Unternehmen wurde dieses Mal zwar eine breitere Basis veranschlagt, sodass auch kleinere Unternehmen berücksichtigt werden konnten, dies dürfte sich auf das tatsächliche finanzielle Ergebnis jedoch nicht gravierend ausgewirkt haben.

Annähernd jedes zweite Unternehmen ist betroffen, sei es durch einen konkreten Schaden (Deutschland: 26,9 Prozent; Österreich: 27,1 Prozent) oder den Verdacht auf Spionage (Deutschland: 27,4 Prozent; Österreich: 19,5 Prozent). Bei den betroffenen Unternehmen hatten 77,5 Prozent in Deutschland und 75,0 Prozent in Österreich auch einen finanziellen Schaden zu verzeichnen. Im Vergleich zur letzten Studie, bei der die Datenweitergabe bzw. der Datendiebstahl durch eigene Mitarbeiter die größte Bedrohung für Unternehmen darstellte, waren es bei dieser Befragung eher technische Angriffe.

Vor allem die Hackerangriffe[1] auf EDV-Systeme waren mit 49,6 Prozent in Deutschland und 41,8 Prozent in Österreich die am häufigsten festgestellten Handlungen. Berücksichtigt man, dass bei einem Großteil der Firmen Mitarbeiter auch zu Hause geschäftlich relevante Daten bearbeiten (Deutschland: 85,7 Prozent; Österreich: 75,4 Prozent), so ist es verwunderlich, dass in beiden Ländern annähernd 70 Prozent der Unternehmen angaben, keinerlei Sicherheitsvorkehrungen dafür zu treffen. Die Firmen verstehen aber, dass dies zu einem Problem werden könnte: Auf die Frage, welche Entwicklung sie zukünftig als Risiko für die „Kronjuwelen" ihres Unternehmens sehen, nannten 48,3 Prozent in Österreich und 43,9 Prozent in Deutschland die sinkende Sensibilität von Mitarbeitern beim Umgang mit vertraulichem Know-how.

Trotz der vielen Fälle und hohen Schäden haben die wenigsten Unternehmen Vorkehrungen für ihr finanzielles Risiko in Form einer entsprechenden Cyber-Versicherung getroffen. Zwar überlegen sich 24,2 Prozent in Deutschland und 22,0 Prozent in Österreich, eine solche Versicherung abzuschließen, bisher haben dies aber nur die allerwenigsten umgesetzt (Deutschland: 3,6 Prozent; Österreich: 3,4 Prozent).

Die Möglichkeiten für Nachrichtendienste, weltweite Datenströme zu überwachen, nehmen ständig zu. Spioniert wird aber nicht nur durch NSA & Co., sondern auch durch Konkurrenten oder die Organisierte Kriminalität[2]. Durch das Internet haben sich vielfältige Chancen für die Wirtschaft ergeben, jedoch auch ganz reale Bedrohungen. Information ist heute die zentrale Währung im Netz – über individuelle Interessen, das Kaufverhalten sowie die geschäftlichen Kontakte. Wer Informationen hat, verfügt über Macht. Darüber hinaus werden Geschäfte immer häufiger digital abgewickelt und sind somit leicht auszuforschen. Ein Informationsvorsprung, und sei er auch noch so klein, kann bei relevanten Entscheidungen ausschlaggebend sein.

Die Datenausspähung wird jedoch nicht nur zur Durchsetzung von staatspolitischen Zielen genutzt, sondern sie nimmt auch im Bereich der Wirtschaftsspionage ständig zu. Nachrichtendienste und Cyber-Kriminelle rüsten permanent auf, um einen Informationsvorsprung beim Kampf um wichtige Technologien, begrenzte Ressourcen oder neue Absatzstrategien zu erlangen. Daher stellt sich die Frage, ob wir uns nicht bereits im „Cybergeddon[3]" befinden. Die Wirtschaft sollte sich auf jeden Fall darauf vorbereiten, dass die Angriffe noch deutlich zunehmen werden.

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

2) Organisierte Kriminalität: So werden Tätergruppierungen (Banden) bezeichnet, bei denen mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig zusammenwirken, um die von Gewinn- und Machtstreben bestimmte planmäßige Begehung von Straftaten durchzuführen, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, und dabei gewerbliche oder geschäftsähnliche Strukturen verwenden, Gewalt oder andere zur Einschüchterung geeignete Mittel anwenden und Einfluss auf Politik, Massenmedien, öffentliche Verwaltungen, Justiz oder die Wirtschaft nehmen.

3) Cybergeddon: An „Armageddon" oder „Harmagedon" angelehnter Begriff, der eine finale oder endzeitliche Entscheidungsschlacht im Cyberraum (virtueller Raum aller auf Datenebene vernetzten IT-Systeme im globalen Internet) bezeichnen soll.

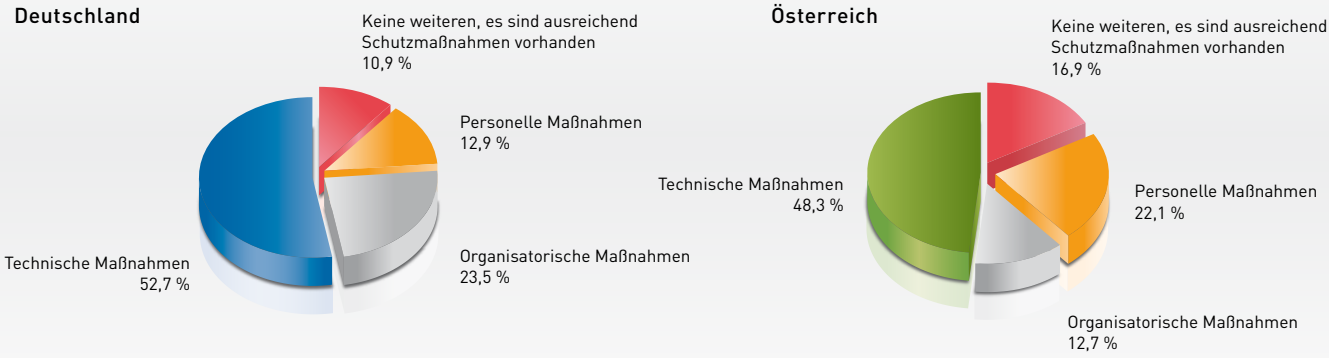
PRÄVENTION

Technische Sicherungsmaßnahmen stehen für die Prävention nach wie vor am höchsten im Kurs.

Um sich gegen die zunehmenden Bedrohungen durch ausländische Nachrichtendienste, versierte Hacker[1], Konkurrenten oder die Organisierte Kriminalität[2] zu wehren, setzen die Unternehmen beider Länder auf Prävention. Nach wie vor werden dabei technische Maßnahmen als am wichtigsten erachtet. Bezüglich der Frage, welche Vorkehrungen die Unternehmen in Zukunft treffen wollen, um auf die Risiken durch Industriespionage vorbereitet zu sein, waren in Deutschland 52,7 Prozent und in Österreich 48,3 Prozent der genannten Maßnahmen technischer Natur.

Während die deutschen Unternehmen verstärkt auf die Implementierung organisatorischer Maßnahmen (23,5 Prozent) Wert legen, setzen die Firmen in Österreich mit 22,1 Prozent am zweithäufigsten auf personelle Prävention. Etwa jedes zehnte Unternehmen in Deutschland und jedes sechste in Österreich glaubt, dass die bereits vorhandenen Sicherheitsvorkehrungen völlig ausreichend sind, um sich gegen Spionage zu schützen.

Wie verteilen sich die von den Unternehmen geplanten Maßnahmen?



GRAFIK 50

Quelle: Corporate Trust 2014

Detailliert befragt nach den Maßnahmen in den einzelnen Bereichen, benannten 38,1 Prozent der deutschen und 33,1 Prozent der österreichischen Unternehmen die verbindlichen Richtlinien für alle Mitarbeiter zum Umgang mit sensiblen Informationen (Sicherheits-Policy[3]) als probatestes Mittel im organisatorischen Bereich. Darüber hinaus wollen die Unternehmen beider Länder zukünftig häufiger eine Schutzbedarfsanalyse erstellen (Deutschland: 36,2 Prozent; Österreich: 27,1 Prozent) bzw. regelmäßig Gefährdungsanalysen durchführen (Österreich: 31,4 Prozent; Deutschland: 28,2 Prozent).

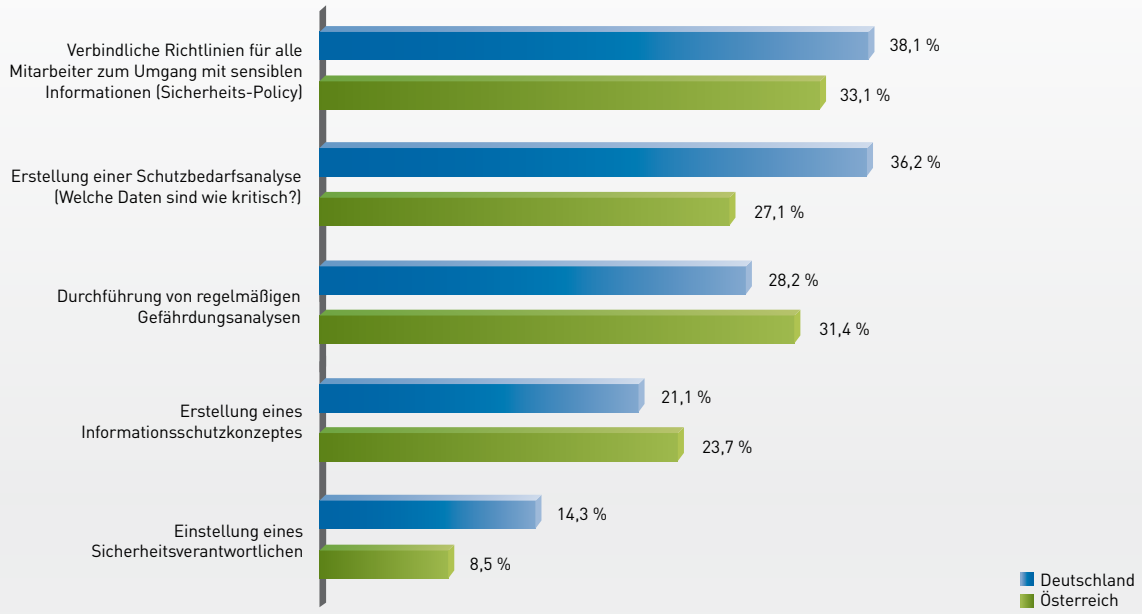
Einen Sicherheitsverantwortlichen wollen nur die wenigsten Unternehmen einstellen. Dies kann bedeuten, dass sie entweder schon einen haben oder ein solcher immer noch mehr der klassischen Sicherheit, also den Themen Objektschutz oder interne Ermittlungen etc., zugeordnet wird. Auch wenn es sich bei den Vorkehrungen zum Schutz gegen Industriespionage um organisatorische Maßnahmen handelt, so sind sie doch in vielen Fällen IT-lastig. Daher wird der Bedarf vermutlich mehr in Richtung eines qualifizierten Verantwortlichen für IT-Sicherheit gesehen.

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

2)Organisierte Kriminalität: So werden Tätergruppierungen (Banden) bezeichnet, bei denen mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig zusammenwirken, um die von Gewinn- und Machtstreben bestimmte planmäßige Begehung von Straftaten durchzuführen, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, und dabei gewerbliche oder geschäftsähnliche Strukturen verwenden, Gewalt oder andere zur Einschüchterung geeignete Mittel anwenden und Einfluss auf Politik, Massenmedien, öffentliche Verwaltungen, Justiz oder die Wirtschaft nehmen.

3) Sicherheits-Policy: Auch Sicherheitsrichtlinie oder Sicherheitsleitlinie. Beschreibt den angestrebten Sicherheitsanspruch eines Unternehmens und konzeptionell die Maßnahmen, um dorthin zu kommen.

Welche organisatorischen Maßnahmen werden Sie treffen?
(Mehrfachnennungen möglich)



GRAFIK 51

Quelle: Corporate Trust 2014

Wie bereits festgestellt, legen die meisten Unternehmen großen Wert auf die Sicherung gegen Angriffe von außen; dies wird auch in Zukunft so bleiben. 52,5 Prozent der österreichischen und 48,3 Prozent der deutschen Unternehmen wollen künftig ihr Augenmerk noch mehr auf die Sicherung der Netzwerkinfrastruktur richten. Die Verbesserung der Gebäudesicherheit steht mit 33,1 Prozent in Österreich und 28,4 Prozent in Deutschland erst an dritter Stelle der wichtigsten Maßnahmen für die nächsten Jahre.

Obwohl es dringend nötig wäre, die Täter künftig auch durch einen höheren Repressionsdruck abzuschrecken, wollen nur 11,9 Prozent der österreichischen und 8,3 Prozent der deutschen Firmen eine Logfile-Protokollierung zur Verbesserung der Nachverfolgungs- bzw. Ermittlungsmöglichkeiten installieren. Dies wäre jedoch wichtig, um nach einem Informationsabfluss schnell feststellen zu können, woher der Angriff kam und welche Daten betroffen sind. Solange Zugriffe gar nicht nachvollzogen werden können, wird sich bei der Repression nichts ändern. Wenn die Täter aufgrund dürftiger Spurenlage keinen Verfolgungsdruck zu befürchten haben, wird das Thema Industriespionage nicht in den Griff zu bekommen sein.

PRÄVENTION

Welche technischen Maßnahmen werden Sie treffen?
(Mehrfachnennungen möglich)

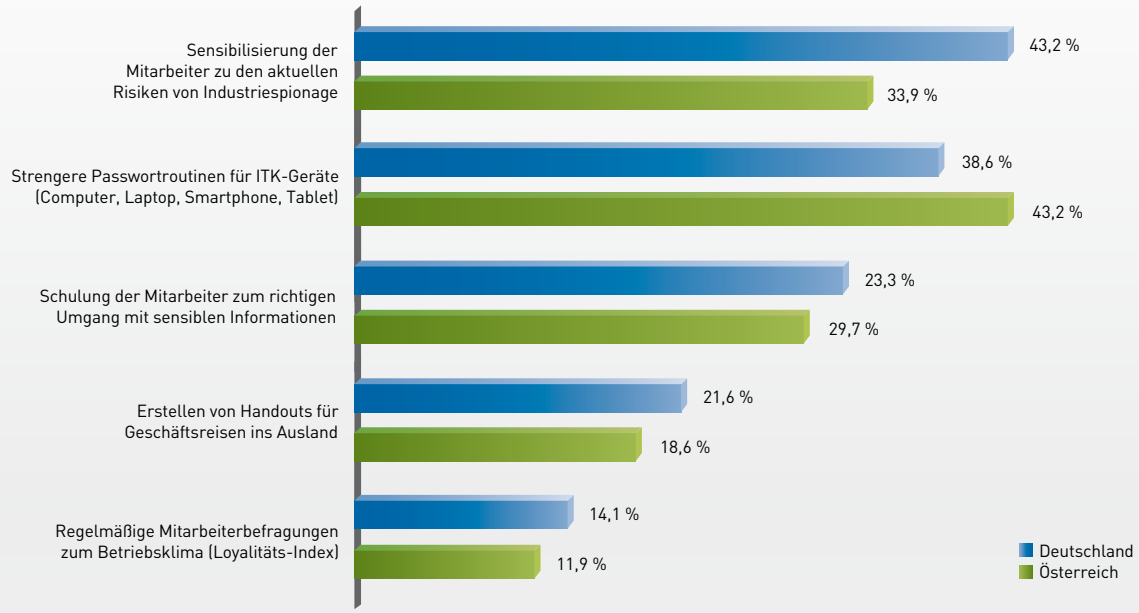
GRAFIK 52

Quelle: Corporate Trust 2014

Als Letztes wurden auch die personellen Maßnahmen abgefragt, mit denen die Unternehmen künftig mehr Prävention betreiben wollen. Gerade Österreich setzt hier verstärkt auf strengere Passwortroutinen für ITK-Geräte (Computer, Laptop, Smartphone, Tablet etc.). In Deutschland wurde die Sensibilisierung der Mitarbeiter zu den aktuellen Risiken von Industriespionage präferiert.

In beiden Ländern wurde das Betriebsklima als wesentlich weniger wichtig im Kampf gegen Industriespionage erachtet: Nur 14,1 Prozent der deutschen und 11,9 Prozent der österreichischen Unternehmen gaben an, in Zukunft regelmäßig eine solche Befragung durchführen zu wollen.

Welche personellen Maßnahmen werden Sie treffen?
(Mehrfachnennungen möglich)



GRAFIK 53

Quelle: Corporate Trust 2014

Florian Oelmaier
Leiter IT-Sicherheit und
Computerkriminalität
Corporate Trust GmbH

Ist die Kriminalität im IT-Bereich noch beherrschbar? Hat die Bevölkerung noch Vertrauen in die Sicherheit des Internets? Die Sicherheitsbranche hat große Aufgaben vor sich.

CORPORATE TRUST
business risk & crisis management

Die vorliegende Studie von Corporate Trust greift nun zum dritten Mal das Thema Industriespionage auf. Und zum wiederholten Mal hat sich die Sicherheitslage in den vergangenen Jahren nicht signifikant verbessert. Viele werden nun denken: „Das war mir klar." Aber kann das unser Anspruch sein? Trotz steigender Budgets im Sicherheitsbereich, trotz der verbesserten staatlichen Unterstützung durch Cybercrime-Einheiten und Schwerpunktstaatsanwaltschaften, trotz aller Innovationen im Sicherheitsbereich konnten wir keine Verbesserung der Sicherheitslage erreichen?

Auf der einen Seite muss hier eine Lanze für die Sicherheitsbranche gebrochen werden: Natürlich haben uns all diese Anstrengungen weitergebracht. Aber neue Technologien wie Cloud Computing, mobile Geräte und eine zunehmende Professionalisierung aufseiten der Angreifer haben unsere Weiterentwicklungen zu statuserhaltenden Maßnahmen degradiert. Und wenn wir ganz ehrlich sind, konnten sie nicht einmal den Status erhalten. Die Bedrohung durch Schadsoftware steigt täglich, bösartige Spam-E-Mails werden wöchentlich besser formuliert und die Anzahl der verlorenen Passwörter steigt von Jahr zu Jahr. Ganz zu schweigen davon, dass jedes Verfahren zur Rücksetzung von Passwörtern, das für einen 65-Jährigen noch akzeptabel ist, von einem 14-Jährigen binnen Minuten überlistet werden kann.

Dennoch baut unsere Gesellschaft mehr und mehr auf die Sicherheit des Internets. Selbstfahrende Autos, Heimautomatisierung und sogar die dezentrale Stromversorgung der Energiewende benötigen eine sichere Internetinfrastruktur. Fragt man aber Experten wie Anwender, ob die derzeitigen IT-Strukturen und deren Vernetzung noch beherrschbar sind, überwiegt die Skepsis. Selbst das Weltwirtschaftsforum spricht von „Cybergeddon"[1] und malt ein düsteres Bild einer Zukunft, in der Firmen und Nutzer das Vertrauen in ein freies Internet verloren haben und sich durch eine „Balkanisierung"[2] verschiedene, von großen Konzernen betriebene Infrastrukturen entwickeln: Sind Sie im Amazon-, im Apple-, im Microsoft- oder im Googlenetz? Hinzu kommt ein durch den NSA-Skandal befeuertes, deutlich gewachsenes Misstrauen der Nutzer gegenüber staatlichen Stellen – brave new world.

Es ist Zeit, einen Anspruch an die Sicherheitsbranche zu formulieren: Wir sorgen dafür, dass die Benutzer IT-Systeme nicht als unbeherrschbar wahrnehmen. Wir

1) Cybergeddon: An „Armageddon" oder „Harmagedon" angelehnter Begriff, der eine finale oder endzeitliche Entscheidungsschlacht im Cyberraum (virtueller Raum aller auf Datenebene vernetzten IT-Systeme im globalen Internet) bezeichnen soll.

2) Balkanisierung: Ursprünglich ein politisches Schlagwort für Sezessionen (Loslösung einzelner Landesteile) von Staatsgebilden; es soll dabei in der Regel eine ablehnende Haltung ausgedrückt werden. Jenseits der Politik werden mit dem Begriff Vorgänge bezeichnet, bei denen große Gebilde in viele kleine zerfallen.

entwerfen IT-Systeme so, dass die Kontrolle darüber klar und transparent geregelt ist und nicht von Dritten ausgehebelt werden kann. Dies setzt hohe Standards im Bereich der Sicherheit und des Datenschutzes voraus. Dazu ist außerdem eine gute Zusammenarbeit der Experten aus klassischer Sicherheit und IT-Sicherheit eine notwendige Voraussetzung – aber nicht ausreichend. Erst wenn dadurch ein umfassender Blick auf die real existierenden Angriffe und Bedrohungen für das eigene Unternehmen entsteht, ist die Sicherheitsbasis geschaffen, die benötigt wird, um die wirtschaftlichen Prozesse minimalinvasiv absichern zu können. Dazu gehört jedoch auch, dass Angriffe zeitnah erkannt werden können, ein umfassender Plan für die forensische Aufklärung existiert und ernsthafte Anstrengungen unternommen werden, Täter auch wirklich zur Rechenschaft zu ziehen.

Wenn es ernst wird mit der Sicherheit: Corporate Trust

Corporate Trust ist einer der wenigen Marktteilnehmer, bei dem ehemalige Polizisten und Sicherheitsverantwortliche aus Konzernen Hand in Hand mit IT-Sicherheitsexperten und Profis für alle Themen rund um den baulichen Schutz oder die Krisenkommunikation arbeiten. Auf diese Weise kann Corporate Trust den Brückenschlag zwischen den Disziplinen verwirklichen und Angriffe von der Erkennung über die Forensik bis hin zur Täterfeststellung aufklären. Dementsprechend sind wir ein gefragter Partner, wenn es um die Aufklärung von Spionagefällen geht.

Diese Tätigkeiten ermöglichen es aber auch, eine neue Dimension von präventiven Dienstleistungsprodukten anzubieten. Eine interdisziplinäre Schutzbedarfsanalyse hilft, die wirklich wertvollen Assets des Unternehmens zu identifizieren. Unsere Erfahrung nutzt Ihnen, um – fernab von standardisierten Audits – die echten Angriffe zu detektieren, die aktuell ausgeführt werden. Um die Einstiegshürde möglich niedrig zu gestalten, bieten wir an, eine Auswahl aus fünf aktuellen Industriespionagefällen bei Ihnen im Unternehmen durchzuspielen. Damit können Sie in kurzer Zeit erfahren, wie Ihre Sicherheitsprozesse auf diese Angriffe reagiert hätten. Oder senden Sie uns einfach Ihren Laptop zur forensischen Untersuchung zum Festpreis – so lernen Sie die notwendigen Ermittlungsprozesse noch vor dem Ernstfall kennen. Denn eines ist klar: Es geht nicht mehr um das „Ob", sondern um das „Wann".

Neben der Verteidigung gegen Angriffe hat die Sicherheit aber auch eine gestaltende Rolle zu übernehmen. Wir unterstützen Sie gerne dabei, die richtige Balance zwischen Sicherheit, Usability und Datenschutz zu schaffen – auch und vor allem bei neuen Themen wie Windows 8, Cloud und Mobile. Da wir sämtliche Angriffsmöglichkeiten und Sicherheitsprobleme der neuesten 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.

Die IT dient den Menschen, nicht umgekehrt. Machen Sie Ihre IT wieder beherrschbar!

Ihr
Florian Oelmaier

Johannes Behrends
Specialty
AON Risk Solutions

Ein effektives Risikomanagement beginnt mit dem Verständnis für die Risiken. Fehlt dieses, wird ein Unternehmen niemals in der Lage sein, die eigenen Unternehmensdaten umfassend vor Angriffen zu schützen.

Das Ergebnis der vorliegenden Studie belegt, dass Unternehmen Cyber-Versicherungen noch nicht als Notwendigkeit ansehen. Dies liegt vor allem daran, dass die abzusichernden Risiken für das eigene Unternehmen unterschätzt oder gar nicht erst wahrgenommen werden. Die zerstörerische Kraft eines Feuers kann sich jeder leicht ausmalen: Der Schaden kann je nach Ausmaß schnell in die Millionen gehen. Es ist somit selbstverständlich, dass sich Unternehmen gegen Feuerschäden absichern. Wenn es jedoch darum geht, sich die Folgen eines Datenverlustes oder Hackerangriffes bewusst zu machen, versagt die Vorstellungskraft. Wie aktuelle Fälle allerdings zeigen, kann auch der bloße Verlust von Kundendaten Kosten im siebenstelligen Bereich verursachen. Selbst wenn Unternehmen bereits Opfer von Hackerangriffen geworden sind, werden die Schäden nicht erfasst und fließen nicht in das Risikomanagement ein. Dieser Fehler wiegt mitunter schwer.

Experten gehen davon aus, dass bereits jedes zweite Unternehmen Opfer eines Hackerangriffes wurde. Es dürfte lediglich eine Frage der Zeit sein, bis jedes Unternehmen mit Cyber-Crime in Berührung gekommen ist. So verzeichnet auch die aktuell erschienene Kriminalstatistik einen erneuten Anstieg im Bereich der Cyber-Kriminalität.

Das mangelnde Bewusstsein für Cyber-Risiken lässt sich demnach nur mit einem mangelnden Verständnis erklären. Nach wie vor tun sich die meisten Unternehmen schwer mit dieser sehr komplexen Materie. Risikomanager verlassen sich auf ihre IT-Abteilungen, obwohl diese nur einen kleinen Teil im Risikomanagement-Puzzle darstellen. Genauso wichtig ist die Einhaltung von Datenschutzgesetzen oder die Überprüfung der Verträge mit Zulieferern, Kunden und Dienstleistern wie Cloud-Service-Providern. Manchen Unternehmen ist beispielsweise nicht bewusst, dass sie gemäß Bundesdatenschutz auch dann für ihre Daten verantwortlich sind, wenn sie Dritte mit der Speicherung oder Verarbeitung beauftragen.

Ein Grundverständnis für Cyber-Risiken ist folglich essenziell für ein effektives Risikomanagement.

Risikoanalyse

Um die Gefahren für das Unternehmen richtig bewerten und einordnen zu können, sollten die konkreten Risiken für den eigenen Betrieb als Erstes genau analysiert werden. Die Risikoanalyse hilft dabei, ein vertieftes Verständnis für Cyber-Risiken zu gewinnen und die Notwendigkeit eines Risikotransfers besser abschätzen zu können.

Wie zuvor angedeutet, sind Cyber-Risiken nicht ausschließlich ein Thema der IT-Sicherheit. Eine Risikoanalyse betrifft deshalb auch den Bereich Recht und Compliance. Für die Analyse sollte dementsprechend ein Team aus den für die genannten Bereiche Verantwortlichen zusammengestellt werden – nur so wird gewährleistet, dass alle erforderlichen Risikoinformationen vorliegen. Bestandteil der Analyse sollte die Frage sein, ob das Unternehmen sensible oder personenbezogene Daten speichert, verarbeitet oder verwaltet. Ist dies der Fall, sollte überprüft werden, ob und wie Dritte an diese Daten gelangen könnten und was für ein Schaden dem Unternehmen oder Dritten durch

einen Datenverlust entstehen könnte. Aber auch Produktionsanlagen, Logistik-, Lager- und andere wichtige Systeme können für Cyber-Kriminelle potenzielle Ziele darstellen. Es sollte deshalb überprüft werden, ob und welche Systeme gestört und außer Funktion gesetzt werden könnten und wie lange der Betrieb stillstehen kann, bis dem Unternehmen ein signifikanter Schaden entsteht.

Auch wenn die IT-Sicherheit nicht die einzige Schwachstelle ist, sollte hierauf trotzdem ein besonderes Augenmerk liegen. Für eine technische Risikoanalyse empfiehlt es sich, spezialisierte IT-Berater zu konsultieren. Die eigene IT-Abteilung mag die Sicherheitsvorkehrungen in- und auswendig kennen; IT-Krisenberater kennen jedoch die Lücken. Sie haben Erfahrung damit, wie Industriespione und andere Cyber-Kriminelle vorgehen und welche Sicherheitslücken sie ausnutzen (zum Beispiel, indem sich der Täter physischen Zugang zum Gebäude verschafft). Dieses sehr spezielle Know-how haben IT-Abteilungen in der Regel nicht.

Durch die Identifizierung der bestehenden Risiken können einige der Gefahren bereits beseitigt oder zumindest gemindert werden.

Risikotransfer

Die Risikoanalyse soll Unternehmen in die Lage versetzen, die bestehenden Risiken zu erfassen und richtig bewerten zu können. Erst mit diesem Wissen kann eine Entscheidung getroffen werden, ob die Restrisiken, die nicht beseitigt werden können, durch eine Versicherungslösung abgesichert werden sollten. Cyber-Versicherungen können dem Bedarf der Unternehmen angepasst werden und decken je nach Vereinbarung den entstandenen Eigen- und Drittschaden.

So sind über den Eigenschadenteil unter anderem die Krisenmanagementkosten gedeckt. Im Schadensfall entstehen dem betroffenen Unternehmen Kosten für IT-Forensiker, die die Schadensursache und den Umfang klären sollen. Rechtsanwälte beraten über einzuhaltende datenschutzrechtliche Regelungen und Meldeverfahren. PR-Berater unterstützen dabei, den Reputationsschaden gering zu halten. Diese Kosten werden von den Versicherern erstattet. Einen nicht zu unterschätzenden Teil der Kosten nimmt die Benachrichtigung der betroffenen Kunden ein. Allein durch die Portokosten für die zu verschickenden Informationsbriefe oder eine ganzseitige Anzeige in der Tagespresse entstehen schnell hohe Beträge. Darüber hinaus deckt die Cyber-Versicherung die Kosten für die Wiederherstellung gelöschter oder beschädigter Daten nach einem Hackerangriff. Kommt es durch einen Angriff zu einer Betriebsunterbrechung, kann ferner der dadurch verursachte Schaden versichert werden. Wird das Unternehmen erpresst und etwa damit bedroht, sensible Daten zu veröffentlichen oder Systeme stillzulegen, werden außerdem die gezahlten Erpressergelder erstattet. Selbst Belohnungen, die zur Ergreifung der Täter führen, können in die Versicherungslösung eingeschlossen werden. Auf der Drittschadenseite sind Ansprüche wegen Verletzung des Datenschutzrechtes, des Persönlichkeitsrechtes und geistiger Eigentumsrechte versichert. Übermittelt ein Unternehmen versehentlich Malware auf Systeme Dritter, zum Beispiel die von Geschäftspartnern, kann der dadurch bei dem Dritten entstandene Schaden ebenfalls mitversichert werden.

Eine Cyber-Versicherung trägt jedoch nicht nur den finanziellen Schaden: Die Bereitstellung der Krisenberater macht einen wesentlichen Teil der Deckung aus. Somit übernimmt der Versicherer nicht nur die Kosten für diese Dienstleistungen. Der Verlust von sensiblen Daten oder die Unterbrechung des Betriebs bedeutet einen echten Krisenfall, mit dem die meisten Unternehmen überfordert sind. In eventuell existierenden Krisenplänen werden Hackerangriffe nur in den seltensten Fällen berücksichtigt. Durch die Krisenberater erhalten Unternehmen somit umgehend kompetente Unterstützung bei der Bewältigung der Krise.

Fazit

In den vergangenen Jahren wurden stetig mehr Fälle von Cyber-Kriminalität verzeichnet. Erbeutete Datensätze können von Hackern im Internet gewinnbringend weiterveräußert werden. Unternehmen müssen erkennen, dass es keinen hundertprozentigen Schutz geben kann. Da die Risiken jedoch sehr komplex sind, scheuen viele Unternehmen die Auseinandersetzung mit dem Thema – dabei können die finanziellen Schäden im schlimmsten Fall das Ende des Geschäftsbetriebes bedeuten. Ein Verständnis für die eigenen Cyber-Risiken ist deshalb unerlässlich: Erst wenn die Risiken identifiziert sind, kann die Notwendigkeit einer Cyber-Versicherung beurteilt werden.

Ihr
Johannes Behrends

Werner Sielenkemper
Senior Consultant
Securiton GmbH

Sicherheit – auch eine Frage der Kommunikation

SECURITON

Das Risiko, durch Industriespionage auf allen gesellschaftlichen und wirtschaftlichen Ebenen tangiert zu werden, entwickelt sich dynamisch. Technische und organisatorische Maßnahmen zur Risikoreduktion werden nur gegen bekannte oder prognostizierte Risikoprofile eingesetzt. Um nicht nur in Bezug auf Vorgehensmuster tätig zu werden, sondern generell präventiv zu wirken, muss auf Entscheidungsprozesse von potenziellen Risikoträgern Einfluss genommen werden. In diesem Zusammenhang ist die Abstrahierung von Risikopotenzialen nicht zielführend, da konkret menschliche Entscheidungsprozesse beeinflusst werden sollen.

Prävention gegen kriminelle und terroristische Übergriffe wird in der Regel bestimmt durch Kosten, Design und Organisation, und nicht durch Effekte auf Entscheidungsprozesse der „Gegenseite". Einzeltäter, Tätergruppen, auch komplexe Täterorganisationen unterliegen bei der Zielselektion und Festlegung von Art und Umfang von Aktionen bestimmbaren Entscheidungskriterien. Die bewusste Beeinflussung dieser Entscheidungsprozesse erfordert ein Umdenken hinsichtlich des Designs und der Organisation von Maßnahmen zur Risikoreduzierung.

Die Kriterien zur Reduzierung von Spionagerisiken sind, bis auf konkrete technische Maßnahmen, für physische und virtuelle Übergriffe identisch. Besonders wenn nicht zielgerichtet ein bestimmtes Unternehmen attackiert werden soll, um definierte Informationen zu erlangen, sondern generell nach Schwachstellen in relevanten Unternehmen gesucht wird, um prophylaktisch Informationen zu sammeln, ist die sicherheitsrelevante Darstellung von großer Bedeutung.

Das Design von Sicherheitskonzepten wird in der Regel durch Unauffälligkeit bestimmt. Technische Einrichtungen wie Kameras, Sensoren oder mechanische Barrieren sollen architektonischen Anforderungen angepasst werden, martialische Tendenzen müssen per se vermieden werden. Besonders Unternehmen bewegen sich in dem Spannungsfeld zwischen Wahrnehmungsanspruch durch die Öffentlichkeit und der Risikoreduzierung durch technische und organisatorische Maßnahmen. Unternehmenszentralen versuchen sich offen und einladend zu präsentieren, Empfangszentralen werden in Glas und Chrom gestaltet, um ihre Kontroll- und Sicherheitsfunktionen zu kaschieren. Im institutionellen und behördlichen Umfeld sind die Einflüsse der Öffentlichkeitsabteilungen eingeschränkter, da Sicherheitsmaßnahmen aufgrund vermutet höherer Risiken akzeptiert werden. Generell wird jedoch einem offenen Öffentlichkeitsbild große Bedeutung beigemessen und das hat Einfluss auf das Selektionsverhalten potenzieller Täter. Ein Industrieunternehmen, das durch einen drei Meter hohen Gitterzaun eingefriedet ist, hinter dem im Abstand von 30 Metern Masten mit Kameras und IR-Scheinwerfer stehen, hat in der Selektionsphase eine andere Wirkung auf mögliche Angreifer, die einen physischen Übergriff planen, als die Darstellung der juristischen Grenze durch einen 1,8 Meter hohen Maschendrahtzaun – auch wenn dieser überwacht sein sollte.

Informationsbeschaffung

Abgesehen von kriminellen Spontantätern werden „qualifizierte" Spionageübergriffe geplant, sowohl mit kriminellem als auch terroristischem Hintergrund. Die Selektion von Angriffsobjekten ist von besonde-

rer Bedeutung und wird bestimmt durch die Zielsetzung, das Risikopotenzial für die Angreifer, die Aufwendung zur Erreichung des Zieles und die erwarteten Ergebnisse der Aktion.

Entscheidend ist jedoch die Erstselektion, die von diversen Faktoren – u. a. auch von der öffentlichen Wahrnehmung – abhängen kann. Naturgemäß sind ungesicherte oder ungesichert erscheinende Objekte in der Täterperspektive relevanter als offensichtlich konsequent gesicherte Anlagen. Deutlich wird das anhand hochwertiger Privatobjekte, selektiert z. B. durch Open-Source-Intelligence (OSINT)-Aktionen. Sind im Zuge der Grundstücksgrenze keine sicherheitstechnischen Einrichtungen zu erkennen, kann angenommen werden, dass die juristische Grenze überwunden werden kann, ohne detektiert zu werden. Auf dem Grundstück können weitere Observationen erfolgen, die das Vorgehen bestimmen.

Finden sich jedoch qualifizierte sicherheitstechnische Einrichtungen bereits im Zuge der Grundstücksgrenze, werden meist weniger oder nicht gesicherte Objekte selektiert. Im privaten Umfeld kann davon ausgegangen werden, dass über Detektionseinrichtungen auf der juristischen Grenze hinaus weitere, nach innen gestaffelte Sicherheitsmaßnahmen durchgeführt wurden.

Für gewerblich-industrielle Objekte ist das üblicherweise nicht zu erwarten. Maximal sind Detektionseinrichtungen mit Videoverifikationstechnik im Zuge der Einfriedung zu finden. Ist diese überwunden, können Angreifer innerhalb des Betriebsgeländes verschwinden und nur mit hohem Aufwand gestellt werden. Technisch besteht zwar die Möglichkeit einer homogenen Täterverfolgung auf dem Betriebsgelände, jedoch verhindern die damit verbundenen Kosten und die Widerstände der Betriebsräte die Einrichtung solcher Techniken. Hier kann intelligente Informationskultur mit der Belegschaft präventiv wirken und Sicherheitsdefizite kompensieren. Schon indem den Mitarbeitern vermittelt wird, dass Sicherheit einen hohen Stellenwert in der Unternehmensphilosophie hat, können Abschöpfungsversuche in der Belegschaft Täterentscheidungen beeinflussen. Die Risikokommunikation mit der Belegschaft sollte fest im Risikomanagement verankert werden.

Offensive Kommunikation von Sicherheitsmaßnahmen

Der im Handel übliche Hinweis „Jeder Diebstahl wird zur Anzeige gebracht!" wird sicher keine Spionageaktion verhindern, deutet aber auf Observationsmaßnahmen hin und zeigt ein gewisses Sicherheitsbewusstsein. Die eindeutige Information über den Stellenwert von Sicherheitsinteressen in der Unternehmenskommunikation nach innen und außen wird von vielen Unternehmen vernachlässigt. Seitens der Presse wird das Thema Industriespionage aus gegebenen Anlässen immer wieder aufgegriffen. Die Industrie erwähnt Industriespionage jedoch maximal in Randnotizen, konkret betroffene Unternehmen scheint es generell nicht zu geben. Allein der Hinweis auf möglicherweise vorhandene Risiken widerspricht dem Anspruch eines omnipotenten Unternehmens und reduziert das Image. Die Öffentlichkeit ist sich heute jedoch darüber im Klaren, dass jedes Unternehmen mit eigenen Produkten und Innovationen Spionageversuchen ausgesetzt sein kann.

Ein Konzern, der ein Programm zur Reduzierung von Ausspährisiken veröffentlichen würde – natürlich ohne konkrete Details zu nennen –, würde von der Öffentlichkeit als zeitgemäß und verantwortungsbewusst wahrgenommen. Für potenzielle Angreifer würde die Hemmschwelle durch den Eindruck der Abwehrbereitschaft erhöht. Durch gelegentliche Erfolgsmeldungen über verhinderte Spionageversuche kann das Image entwickelt werden, wehrhaft gegen Kriminelle zu sein.

Durch kostengünstige Presse- und Öffentlichkeitsarbeit können auch mittelständische Unternehmen ihr Profil in der Wahrnehmung potenzieller Angreifer modifizieren. Wird diese Imagebildung durch konkrete technische und organisatorische Maßnahmen ergänzt, können die Spionagerisiken sowohl durch physische als auch virtuelle Übergriffe eingeschränkt werden.

Ein Unternehmen, das ein offensichtliches Spionageproblem in der öffentlichen Wahrnehmung ignoriert, wird als angreifbar erscheinen und eher attackiert werden als ein Unternehmen, von dem bekannt ist, dass die Spionageabwehr einen hohen Stellenwert in der Sicherheitsphilosophie hat.

Ihr
Werner Sielenkemper

Johann Worm
Head of Broker Management
Zurich Gruppe Deutschland

Cyber & Data Protection: Unternehmen unterschätzen noch immer die Bedeutung einer Absicherung ihrer Daten und Netzwerke. Besonders internationale Programme werden immer wichtiger – und Versicherer bieten passende Lösungen.

ZURICH®

Bereits in den Neunzigerjahren des vergangenen Jahrhunderts entwickelten amerikanische Versicherer erste Absicherungskonzepte gegen eine neue, selbst für viele Experten exotische Risikoart: Cyberkriminalität. Die Assekuranz erkannte schon damals, dass sich durch die zunehmende Digitalisierung und Vernetzung eine neue Angriffsfläche auf Produktions- und Wertschöpfungsprozesse, vor allem aber bei Haftungsfragen, zu entwickeln begann. Im Jahr 2003 verhalf die Gesetzgebung in Kalifornien der Cyber Insurance zum Durchbruch: Unternehmen wurden verpflichtet, Betroffene über den Verlust personenbezogener Daten zu unterrichten – ein Urteil mit teils kostspieligen Konsequenzen für die Unternehmen. Mittlerweile haben 43 US-Bundesstaaten regulatorisch nachgezogen. Die Absicherungslösung wurde auf diese Weise schnell zu einem anerkannten und gefragten Produkt, das wir unseren Kunden in den USA – und mittlerweile auch in Deutschland – unter dem Namen Zurich Cyber & Data Protection (CDP) anbieten. Heute, über 20 Jahre nach den ersten Lösungsansätzen der Versicherer in den USA, scheinen die Gefahren größer denn je: Die globale Vernetzung ermöglicht Spionage, Diebstahl und Sabotage; es drohen Datenverlust, Geheimnisverrat, Produktionsunterbrechungen und Reputationsschäden. Doch in Deutschland besteht noch immer große Unsicherheit über die Risiken, die mit der voranschreitenden Vernetzung einhergehen. Vor allem im Mittelstand wird das Problem teilweise unterschätzt, aber auch in der Konzernlandschaft haben sich die Deckungskonzepte noch nicht überall durchgesetzt. Gemeinsam mit den Versicherungsmaklern haben die Versicherer daher viel Aufklärungsarbeit zu leisten: Welche Absicherungslösungen sind überhaupt verfügbar? Welche ist für das jeweilige Unternehmen sinnvoll? Wie ergänzen sie bestehende Versicherungslösungen, etwa die Vertrauensschadenversicherung sowie Haftplicht- oder Sachversicherungen? Wie schnell kann ich Versicherungsschutz erlangen und in welcher Höhe?

Cyber-Deckung: international und modular

Gespräche mit Unternehmen zeigen oft, dass verwandte Versicherungslösungen nur scheinbar ausreichend Sicherheit erzeugen. Beispielsweise bieten IT-/Tech-Haftpflichtdeckungen lediglich Versicherungsschutz gegen Schäden, die direkt durch IT- und Telekommunikationsdienstleister verursacht wurden. Die Vertrauensschadenversicherung schützt gegen Eigen- und Drittschäden, die durch vorsätzliche, kriminelle Handlungen von Angestellten des eigenen Unternehmens entstehen. Die Zurich Cyber & Data Protection geht weiter: Die Police ist modular aufgebaut und bietet zahlreiche optionale Eigenschadenbausteine; sie schützt weltweit (sofern rechtlich zulässig) und lässt sich auf internationale Programme erweitern. Durch die Einrichtung von Lokalpolicen können Unternehmen auch in sogenannten Non-admitted-Ländern vor Ort Versicherungsschutz erhalten und sogar eine lokale Schadensregulierung in Anspruch nehmen – damit werden auch hohe Compliance-Anforderungen erfüllt. Wichtige Dienstleistungselemente grenzen CDP von bestehenden Versicherungslösungen ab: Zur Prävention und im Schadensfall sind ein sogenanntes Pre-Breach Risk Assessment und eine Post-Breach Remediation vorgesehen. Das bedeutet: Gemeinsam mit einem erfahrenen IT-Dienstleister übernehmen

wir ein Risk Assessment auf Ad-hoc-Basis sowie eine Detailanalyse des unternehmensinternen Risk Managements bezüglich Datenschutz und Vertraulichkeit; im Schadensfall unterstützen wir bei der Sachverhaltsaufklärung und bei der erforderlichen Benachrichtigung Betroffener (z. B. durch Callcenter-Services). Zusätzlich erhalten Versicherungsnehmer im Schadensfall Public-Relations-Beratung zur Eindämmung von Reputationsschäden.

Die wichtigsten Deckungsbausteine im Überblick

Das zentrale Element der Cyber & Data Protection ist die Drittschadenkomponente, also die Haftpflichtversicherung im Zusammenhang mit IT-Sicherheit, Datenschutz und Vertraulichkeit. Sie gewährt Deckung für die Haftpflicht im Zusammenhang mit der Beeinträchtigung von Daten- und Computersystemen, sublimiert auch Verteidigungsaufwendungen im Zusammenhang mit einem behördlichen oder gerichtlichen Verfahren. Hierzu zählt auch das Verhalten von im Auftrag der Versicherungsnehmerin tätigen Serviceprovidern. Darüber hinaus schützt die Versicherungslösung vor verschiedenen Arten von Eigenschäden, zum Beispiel:

- Die Eigenschadenkomponente Verletzung der Vertraulichkeit oder des Datenschutzes gewährt Deckung für Kosten, die aufgrund der Verletzung der Vertraulichkeit oder des Datenschutzes entstehen, beinhaltet Kosten für die Benachrichtigung von Betroffenen, für die Sachverhaltsermittlung und für Beratung im Bereich Public Relations.

- Die Eigenschadenkomponente Ersatz von computergespeicherten Daten und Programmen bietet Deckung für Aufwendungen aufgrund der Beeinträchtigung von Daten und Programmen (Notfallwiederherstellung) und beinhaltet Aufwendungen für die Sachverhaltsermittlung durch einen IT-Sachverständigen.

- Die Eigenschadenkomponente Betriebliche Ertragseinbußen gewährt Deckung für die Betriebsunterbrechung durch einen Sicherheitsvorfall und beinhaltet mittelbare betriebliche Ertragseinbußen.

- Die Eigenschadenkomponente cyberbezogene Erpressungsandrohung gewährt Deckung für Erpressungsgelder, die gezahlt werden aufgrund der glaubhaften Drohung, das Computersystem der Versicherungsnehmerin mit schädlichem Code zu infizieren oder durch einen Denial-of-Service-Angriff zu blockieren. Darüber hinaus schützt sie vor den finanziellen Folgen, die entstehen, wenn personenbezogene Daten oder andere geschäftlich relevante Informationen entwendet und anschließend etwa an nicht autorisierte Personen weitergegeben werden. Schließlich deckt diese Eigenschadenkomponente Belohnungszahlungen für Hinweise, die zur Verhaftung oder Verurteilung von Erpressern führen.

Komplexe Risiken – komplexe Absicherungskonzepte

Durch die zunehmende Vernetzung und Digitalisierung sind Unternehmen heute bis tief in ihre Wertschöpfungsprozesse hinein technologieabhängig – die Bedeutung von Cyberrisiken für das Risikomanagement von Unternehmen steigt damit zwangsläufig. Durch die technologieinhärente Komplexität ist eines jedoch niemals gewährleistet: ein hundertprozentiger technischer oder prozessbezogener Schutz gegen Datenverlust oder -missbrauch. Ein Restrisiko bleibt bestehen – es kann jedoch auf einen Versicherer transferiert werden. Eine ideale Cyber-Deckung ist dabei mehr als eine einfache Erweiterung von Haftpflicht- oder Sachpolicen um den Schutz vor Hackerschäden oder ähnlichen Bedrohungen. Cyber & Data Protection ist vielmehr eine individuell auf den Einzelfall abgestimmte Absicherungslösung, die schon konzeptionell weit über die reine Versicherungsleistung hinausgeht und entscheidende Zusatzleistungen bietet. Besonders größere Unternehmen suchen dabei nach Lösungen, die nicht nur zu ihrem internationalen Geschäft passen, sondern auch in der Absicherungshöhe den Anforderungen entsprechen. Keine leichte Aufgabe für die Versicherer und ihre Vertriebspartner, denn die Deckungssummen übersteigen schnell den Risikoappetit eines einzelnen Versicherers. In partnerschaftlicher Zusammenarbeit können Versicherer die gefragten Kapazitäten oft nur in Konsortien in der länderübergreifenden Kooperation zur Verfügung stellen. Nicht viele Versicherer verfügen über die Erfahrung und das internationale Netzwerk, um diese Komplexität zu meistern; aber immer mehr Unternehmen stellen sich dieser Herausforderung.

Ihr
Johann Worm

Ausblick

Cybergeddon – Wird die Schreckensvision wahr?

Das Weltwirtschaftsforum listet im Jahr 2014 erstmalig den „Cybergeddon“[1] als eines der Top-Risiken für die Weltwirtschaft[2]. Dahinter steckt ein Trend: Sicherheitsüberlegungen und Angriffsszenarien nehmen zunehmend Einfluss auf die Entwicklung unserer Zukunft – und das zu Recht.

CORPORATE TRUST
business risk & crisis management

Während sich unser modernes Geschäftsleben auch in der digitalen Welt bislang hinsichtlich Angriffen als ziemlich widerstandsfähig erwiesen hat, war die zugrunde liegende Dynamik doch immer, dass es Angreifer leichter haben als Verteidiger. Das Vordringen der Digitalisierung in immer mehr Lebensbereiche eröffnet auch immer mehr Angriffspunkte. Außerdem wird sowohl die Vernetzung auf technischer Ebene zwischen Geräten und Programmen als auch zwischen Unternehmen und Wirtschaftszweigen stetig komplexer und vielschichtiger. Die Widerstandsfähigkeit unseres Wirtschaftssystems wird dadurch Schritt für Schritt untergraben.

Dynamik und Folgen von Angriffen werden zunehmend unvorhersehbarer und überraschen auch Sicherheitsprofis immer wieder. Das Weltwirtschaftsforum schreibt: „Eine Zukunft, in der Angreifer (egal ob Hacker, Kriminelle aus dem Bereich des organisierten Verbrechens oder nationales Militär) einen überwältigenden, entscheidenden und dauerhaften Vorteil gegenüber den Verteidigern haben, könnte nur eine zerstörerische Technologie weit entfernt sein. [...] Das Internet wäre nicht länger ein vertrauenswürdiges Medium für Kommunikation oder Handel; Konsumenten und Unternehmen würden es zunehmend meiden. Der Cyberspace wäre nicht mehr unterteilt in Angreifer und Verteidiger, sondern in Räuber und Beute.“

Viele Innovationen der Zukunft – von selbstfahrenden Autos über die Heimautomatisierung bis hin zur dezentralen Stromversorgung im Rahmen der Energiewende – benötigen aber eine vertrauensvolle digital vernetzte Wirtschaft. Hier sind neue Denkmuster und Innovationen im Bereich Sicherheit gefragt: Der Informationsschutz, nicht nur der eigenen Daten, sondern auch der anvertrauten Informationen von Kunden und Partnern, wird mehr und mehr zu einer wettbewerbsentscheidenden Frage. Für diesen Schutz ist heute mehr denn je die gute, auf Vertrauen gegründete Zusammenarbeit von Wirtschaftsakteuren und staatlichen Stellen notwendig. Dieses Vertrauen wurde von den jüngsten Enthüllungen über das Ausmaß, wie nationale Sicherheitsorganisationen Spionage betreiben und Angriffe durchführen, schwer erschüttert – ein Bruch, den es zu überwinden gilt.

Die vorliegende Studie zeigt aber auch, dass in vielen Unternehmen diese neuen Gefahren unter dem Stichwort „Cyberrisiken“ durchaus auf der strategischen Managementebene angekommen sind. Trotz des Namens sind diese Risiken nur teilweise IT-Risiken und haben vor allem mit Vertrauen von Marktteilnehmern, Organisationen, Behörden untereinander sowie mit der Loyalität und dem Zusammenhalt innerhalb von Firmen und Organisationen zu tun. Der Mensch bleibt der entscheidende Faktor. Das Schreckensszenario „Cybergeddon“ wird nur durch gut ausgebildete, motivierte, dem Unternehmen loyal verbundene Arbeitnehmer und eine gute Zusammenarbeit der Verteidiger aus verschiedenen Firmen und staatlichen Organisationen verhindert werden können. Sowohl die deutsche „Allianz für Cybersicherheit“ des BSI als auch das „Kuratorium sicheres Österreich“ leisten hier wertvolle Arbeit und verdienen Ihre Unterstützung.

Die Versicherungsbranche hilft mit neuen Versicherungstypen, die Auswirkungen von Angriffen für Unternehmen beherrschbarer machen sollen. Um diesen Vorteil zu nutzen, bleibt es weiterhin entscheidend, die Angriffe aus dem Dunkelfeld herauszuholen, die Messung der wirtschaftlichen Auswirkungen von Cyberrisiken zu verbessern und die systemischen Wechselbeziehungen im Cyberspace zu verstehen. Dies wiederum ist für die nächsten Jahre die Hauptaufgabe der Sicherheitsexperten und Manager in den Unternehmen: eine faktenbasierte und öffentliche Diskussion über Sicherheitsrisiken zu führen.

1) Cybergeddon: An „Armageddon“ oder „Harmagedon“ angelehnter Begriff, der eine finale oder endzeitliche Entscheidungsschlacht im Cyberraum (virtueller Raum aller auf Datenebene vernetzten IT-Systeme im globalen Internet) bezeichnen soll.

2) siehe http://reports.weforum.org/global-risks-2014

Am Ende werden sich nicht die Unternehmen hervortun, die die fortschrittlichste Technologie besitzen, sondern die Unternehmen, die die Technologie beherrschen und deren Risiken richtig einschätzen.

Die vierte industrielle Revolution wird in den kommenden Jahren mit riesigen Schritten voranschreiten. Moderne Informationstechnologien werden unser Leben tiefgreifend verändern. Leider ist dennoch davon auszugehen, dass sich die meisten Unternehmen – wie bisher auch – wenig bis gar nicht um die notwendige Sicherheit ihrer Daten und kritischen Systeme kümmern. Gleichzeitig wird die Bedrohung durch Cyber-Kriminalität rasant steigen; eine Entwicklung, die besorgniserregend ist. Unternehmen haben zwar längst die Chancen einer Vernetzung ihrer Systeme und Produkte erkannt, die daraus resultierenden Gefahren werden aber häufig ignoriert.

Durch die fortschreitende Technologisierung wird es zukünftig immer einfacher werden, an vertrauliche Daten zu gelangen. Das weltweit abrufbare Datenvolumen steigt exponenziell an und viele Unternehmen stellen auf papierlose Aktenführung um. All diese Daten müssen gespeichert werden und bieten dementsprechend eine potenzielle Angriffsfläche. Schon bald dürfte jedes Unternehmen auf irgendeine Art und Weise mit Cyber-Kriminalität in Berührung gekommen sein. Höchste Zeit also, sich auf den „Cyber War" vorzubereiten.

Industriespione und andere Hacker entwickeln ihre Methoden laufend weiter und sind der Industrie immer ein paar Schritte voraus. Softwarehersteller können auf Bedrohungen deshalb oft nur reagieren und identifizierte Lücken schließen – vorausgesetzt natürlich, die Lücken werden überhaupt identifiziert. Und auch die eigenen Mitarbeiter, die meist ungehinderten Zugang zu Unternehmensdaten haben, stellen eine potenzielle Gefahr dar.

Hackerdienstleistungen wie Datendiebstahl oder Betriebsunterbrechungen können im Internet bereits für wenige Dollar gekauft werden. Man muss heutzutage also kein IT-Experte mehr sein, um an sensible Daten zu gelangen. Doch je einfacher es ist, Unternehmen auszuspionieren und Daten zu stehlen, desto häufiger wird diese Möglichkeit auch genutzt. Cyber-Kriminalität wird die klassischen Delikte deshalb in vielen Bereichen ablösen, da mit weniger Aufwand mehr Gewinn zu erzielen ist.

Cyber-Versicherungen werden daher kurzfristig ein wichtiger Bestandteil des Risikomanagements werden; denn ist es nicht möglich, alle Gefahren zu beseitigen, sollten zumindest die finanziellen Restrisiken abgesichert werden. In den vergangenen Jahren sind dementsprechend immer mehr Versicherer mit eigenen Produkten auf den Markt gekommen. Dabei wird auch der Deckungsumfang stetig ausgebaut und dem technologischen Fortschritt angepasst. Die Vielfalt der Versicherungslösungen ermöglicht es, für jede Branche und Unternehmensgröße das passende Konzept zu finden.

Cybergeddon – Wird die Schreckensvision wahr?

Spionageabwehr – ein Zweifrontenkrieg

SECURITON

Hacker, Einbrecher und Agentenführer teilen sich die Aufgabe, Unternehmensdaten illegal zu beschaffen. Aber es muss auch von Kooperationen ausgegangen werden, durch die die Beschaffung für die Beteiligten einfacher und mit geringerem Risiko behaftet ist. So könnte der Einbrecher mit dem Hacker kooperieren, indem er physisch Zugriff auf Rechnerhardware nimmt, Programmträger platziert oder Geräte installiert, die es dem Hacker ermöglichen, in das Firmennetzwerk zu gelangen.

Agentenführer könnten Kontakte zu relevanten Mitarbeitern knüpfen und Informationen über das private Arbeitsverhalten von Informationsträgern im Unternehmen ermitteln, die wiederum der Einbrecher nutzt, um im privaten Umfeld Zugriff auf Rechner, Netzwerke und Unterlagen zu bekommen. Abwehrmaßnahmen beschränken sich also nicht nur auf das Unternehmen, Niederlassungen und Zweigstellen, sondern sind auch im privaten Umfeld von Informationsträgern nötig. Das betrifft insbesondere die Unternehmensleitung und relevante Informationsträger. Der Zugriff auf Informationen sowie Netzwerk- und Rechnerstrukturen ist in Privathäusern wesentlich einfacher als in Firmengebäuden.

Eine konventionelle Einbruchmeldeanlage (EMA) bietet nur eingeschränkten Schutz vor Übergriffen im Privathaus, besonders dann, wenn die Zielperson anwesend und die EMA unscharf geschaltet ist. Spezielle Sicherungskonzepte zum Personenschutz (Security Level Model) im privaten Umfeld erfüllen auch Sicherungsanforderungen gegen Angreifer mit dem Ziel der Informationsbeschaffung. Das Sicherungsprinzip basiert auf einem Detektionsring im Zuge der juristischen Grenze eines Privatobjektes, der ständig – unabhängig von der An- oder Abwesenheit der Bewohner – scharf geschaltet ist und jede unbefugte Person detektiert.

Weitere Maßnahmen ertüchtigen die Gebäudeaußenhaut und erschweren das Eindringen durch Fenster, Türen und Dachflächen erheblich, sodass Interventionskräfte den Einbruchsversuch nach der Detektion auf der Grundstücksgrenze unterbinden können. Bei langen Interventionszeiten kann ein sicherer Rückzugsraum (Panic Room) sowohl die Bewohner als auch wichtige Unterlagen bis zum Eintreffen der Interventionskräfte schützen. Auch in Firmengebäuden erhöht das Security Level Model den Schutz vor physischen Übergriffen zur Informationsbeschaffung, mit dem Effekt, dass Büros, Etagen oder Gebäude generell einen deutlich größeren Schutz für Personen und Sachgüter bieten.

Die Abwehr von Cyberkriminellen allein zur Verhinderung von Industriespionage greift zu kurz. Je konsequenter Netzwerke geschützt werden, desto wahrscheinlicher werden konzertierte Aktionen zwischen Hackern, Einbrechern und Agentenführern. Erst Abwehrmaßnahmen gegen alle Varianten von Informationsbeschaffern bieten konsequenten Schutz.

Die Gesetzgebungen in der EU und Deutschland verschärfen den Absicherungsbedarf von Cyber-Risiken für Unternehmen.

ZURICH®

Die weitere Entwicklung beim Datenschutz in Deutschland wird – wie bei so vielen Themen – durch die gesetzgeberische Entwicklung auf EU-Ebene beeinflusst. Der aktuelle Stand: In der EU besteht noch ein heterogenes Datenschutzrecht in allen 28 Mitgliedsstaaten. Der gültige Rahmenbeschluss (2008/977/JI) enthält allerdings Regelungen für die Verarbeitung von personenbezogenen Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit grenzüberschreitend übermittelt oder bereitgestellt werden. Bereits im Jahr 1995 wurde zudem die Datenschutzrichtlinie (95/46/EG) erlassen, die in Deutschland erst 2001 nach einem Vertragsverletzungsverfahren umgesetzt wurde. Am 24. Juni 2013 schließlich wurden neue Ausführungsvorschriften zur EU-Datenschutzrichtlinie für elektronische Kommunikation (2009/136/EG, die sogenannte E-Privacy-Richtlinie) erlassen: Telekommunikations- und Internetdienstleister sind bei Verletzungen des Schutzes personenbezogener Daten verpflichtet, die für Datenschutz oder Telekommunikationsregulierung zuständige nationale Behörde zu benachrichtigen.

Auch in Deutschland besteht nach dem Bundesdatenschutzgesetz (§ 42a) eine Informationspflicht bei unrechtmäßiger Übermittlung von personenbezogenen Daten: Die zuständigen Behörden sind innerhalb von 24 Stunden über Störungen zu informieren, um die Auswirkungen des Vorfalls so weit wie möglich zu begrenzen. Ist in dieser Zeit keine vollständige Offenlegung möglich, müssen innerhalb dieser Zeit zumindest erste Teilinformationen bereitgestellt werden. Die restlichen Informationen sind innerhalb von drei Tagen nachzureichen. Die Unternehmen müssen darlegen, welche Daten genau betroffen sind und welche Maßnahmen sie zur Schadensbegrenzung einleiten. Sollte sich ein Unternehmen nicht an diese Spielregeln halten, drohen derzeit Bußgelder von bis zu 300.000 Euro. Diese sollen drastisch erhöht werden.

So viel zur Theorie. Die Praxis zeigt: Gut die Hälfte der meldepflichtigen Fälle bleibt im Verborgenen – mindestens!

Dies soll die gesetzliche Verschärfung durch die Datenschutz-Grundverordnung auf EU-Ebene ändern: Für die Meldung müssen die Unternehmen künftig ein für alle EU-Mitgliedsstaaten einheitliches Onlineformular verwenden. Der Standard soll verhindern, dass die Unternehmen die teils kreuzenden Zuständigkeiten nationaler Gerichte systematisch ausnutzen (forum shopping). Eine zentrale Behörde – die europäische Datenschutzaufsicht – soll nach dem Vorbild der Wettbewerbs- und Bankenaufsicht die Durchsetzung der Verordnung gewährleisten („One-Stop-Shop"-Ansatz). Die vielleicht wichtigste Neuerung betrifft jedoch das Bußgeld: Es soll auf bis zu zwei Prozent des weltweiten Jahresumsatzes festgelegt werden. Gerade auf internationale Konzerne könnten so erhebliche Forderungen zukommen. Unmittelbar geltendes Recht wird die EU-Verordnung so bald allerdings nicht, denn die Justiz- und Innenminister der Mitgliedsstaaten sind sich über Details uneins. Doch eines ist sicher: Der Bedarf nach Absicherung gegen Eigen- und Drittschäden wird nicht nur durch technische Entwicklungen steigen, sondern auch durch den Gesetzgeber. Mit internationalen, rechtssicheren und flexiblen Absicherungskonzepten kommt Zurich diesem Bedarf entgegen.

Glossar

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

- **Abschöpfen**
  Gezieltes Gewinnen von Informationen, oftmals ohne dass der Betroffene merkt, dass er als Datenquelle benutzt wird, oder unter Verwendung einer Legende.

- **Advanced Persistent Threat (APT)**
  Ein häufig im Bereich der Cyber-Bedrohungen verwendeter Begriff für einen komplexen, zielgerichteten und effektiven Angriff auf kritische IT-Infrastrukturen und vertrauliche Daten von Behörden und Unternehmen. Die Angreifer gehen sehr zielgerichtet und mit großem Aufwand vor, um nach dem Eindringen in einen Rechner weiter in die lokale Infrastruktur des Rechners/Netzwerks vorzudringen. Ziel des APT ist es, möglichst lange unentdeckt zu bleiben, um über einen längeren Zeitraum sensible Informationen auszuspähen oder anderweitig Schaden anzurichten.

- **Awareness**
  Bewusstsein oder Gewahrsein über die eigene Handlung oder 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.

- **Balkanisierung**
  Ursprünglich ein politisches Schlagwort für Sezessionen (Loslösung einzelner Landesteile) von Staatsgebilden; es soll dabei in der Regel eine ablehnende Haltung ausgedrückt werden. Jenseits der Politik werden mit dem Begriff Vorgänge bezeichnet, bei denen große Gebilde in viele kleine zerfallen.

- **Bring Your Own Device (BYOD)**
  Bezeichnung für die Integration von privaten mobilen Endgeräten wie Laptops, Ultrabooks, Tablets oder Smartphones in die Netzwerke bzw. IT-Architektur von Unternehmen. Firmen-E-Mails können damit auch auf den Privatgeräten empfangen werden; angehängte Dokumente werden damit jedoch auch dort gespeichert.

- **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.

- **Cyberattacke**
  Der gezielte Angriff von außen auf größere, für eine spezifische Infrastruktur wichtige Computernetzwerke.

- **Cybergeddon**
  An „Armageddon" oder „Harmagedon" angelehnter Begriff, der eine finale oder endzeitliche Entscheidungsschlacht im Cyberraum (virtueller Raum aller auf Datenebene vernetzten IT-Systeme im globalen Internet) bezeichnen soll.

- **Data Leakage Prevention (manchmal auch Data Loss Prevention)**
  Begriff aus dem Bereich der Informationssicherheit, mit dem der Schutz gegen den unerwünschten Abfluss von Daten aus dem Unternehmen gemeint ist, manchmal auch nur gegen eine vermutete, aber nicht mess- oder feststellbare Weitergabe von Informationen an unerwünschte Empfänger.

- **Duqu**
  Vermutlich auf dem Quelltext von Stuxnet aufbauende Nachfolge-Malware zur Sammlung von Informationen in Computersystemen, um damit künftige Angriffe vorzubereiten.

- **Flame**
  Komplexes Schadprogramm für Angriffe in Rechnernetzen, um sie fernzusteuern oder auszuspionieren. Damit können z. B. angeschlossene oder integrierte Mikrofone eingeschaltet und abgehört oder Tastaturen und Bildschirme ausgewertet werden.

- **Firewall**
  Ein System (meist Hard- und Software), welches dazu dient, den Netzwerkzugriff zu beschränken, basierend auf Absender- oder Zieladresse und genutzten Diensten. Die Firewall 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.

- **GCHQ (Government Communications Headquarters)**
  Eine britische Regierungsbehörde (Nachrichtenbehörde und Sicherheitsdienst), die sich mit Kryptografie, Verfahren zur Datenübertragung und mit der Fernmeldeaufklärung befasst.

- **Geheimhaltungsverpflichtung (auch Vertraulichkeitsvereinbarung)**
  Schriftliche Vereinbarung über den Umgang mit vertraulichen Informationen.

- **GSM (Global System for Mobile Communications)**
  Ein Standard für volldigitale Mobilfunknetze, der hauptsächlich für Telefonie, aber auch für leitungsvermittelnde und paketvermittelnde Datenübertragungen sowie Kurzmitteilungen (Short Messages) genutzt wird.

- **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.

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

- **Joint Venture**
  Ein Anglizismus, unter dem im Handelsrecht verschiedene Formen der Unternehmenskooperation zwischen zwei oder mehr Partnerunternehmen verstanden werden.

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

Glossar

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

- **Malware**
  Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Malware ist ein Oberbegriff, der u. a. auch den Computervirus umfasst.

- **Mobile-Device-Management (MDM)**
  Begriff für die zentralisierte Verwaltung von Mobilgeräten wie Smartphones, Sub-Notebooks, PDAs oder Tablets durch einen oder mehrere Administratoren mithilfe einer Software. Die Verwaltung bezieht sich auf die Inventarisierung der Hardware, die Verteilung der Software und Daten sowie den Schutz der Daten auf diesen Geräten.

- **NSA (National Security Agency)**
  Größter Auslandsgeheimdienst der Vereinigten Staaten von Amerika. Die NSA ist für die weltweite Überwachung, Entschlüsselung und Auswertung elektronischer Kommunikation zuständig und in dieser Funktion ein Teil der Intelligence Community, in der sämtliche Nachrichtendienste der USA zusammengefasst sind.

- **Organisierte Kriminalität**
  So werden Tätergruppierungen (Banden) bezeichnet, bei denen mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig zusammenwirken, um die von Gewinn- und Machtstreben bestimmte planmäßige Begehung von Straftaten durchzuführen, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, und dabei gewerbliche oder geschäftsähnliche Strukturen verwenden, Gewalt oder andere zur Einschüchterung geeignete Mittel anwenden und Einfluss auf Politik, Massenmedien, öffentliche Verwaltungen, Justiz oder die Wirtschaft nehmen.

- **Phishing**
  Darunter versteht man Versuche, über gefälschte Internetseiten, E-Mail- oder Kurznachrichten an Daten eines Internet-Nutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Ziel des Betrugs ist es häufig, mit den erhaltenen Daten beispielsweise auf Kontodaten zuzugreifen.

- **Pre-Employment-Screening**
  Legale Überprüfung von Bewerbern im Personalauswahlverfahren vor der Einstellung bzw. Unterzeichnung des Arbeits-/Anstellungsvertrags zur Vermeidung von Risiken. Es soll vor allem Erkenntnisse über Charakter, Zuverlässigkeit und Integrität des jeweiligen Bewerbers liefern.

- **PRISM**
  Ein seit 2005 existierendes und als Top Secret eingestuftes Programm zur Überwachung und Auswertung elektronischer Medien und elektronisch gespeicherter Daten. Es wird von der NSA betrieben und ermöglicht die umfassende Überwachung von Personen, die digital kommunizieren, innerhalb und außerhalb der USA.

- **Screening**
  Ein systematisches Testverfahren, das eingesetzt wird, um innerhalb eines definierten Prüfbereichs Elemente herauszufiltern, die bestimmte Eigenschaften aufweisen. Das Verfahren kann aus einem Test oder einer Abfolge von aufeinander abgestimmten Tests bestehen.

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

- **Shitstorm**
  Bezeichnet im Deutschen das Auftreten eines Phänomens bei Diskussionen im Rahmen von sozialen Netzwerken, Blogs oder Kommentarfunktionen von Internetseiten; meist ein Sturm der Entrüstung, der zum Teil mit beleidigenden Äußerungen einhergeht.

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

- **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.

- **Social Media (auch soziale Medien)**
  Digitale Medien oder Technologien, die es Nutzern im Internet ermöglichen, sich untereinander auszutauschen und mediale Inhalte einzeln oder in Gemeinschaft zu erstellen. Als Kommunikationsmittel werden dabei Text, Bild, Audio oder Video verwendet.

- **Spam (auch Junk)**
  Unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten, die dem Empfänger unverlangt zugestellt werden und häufig werbenden Inhalt enthalten.

- **Stuxnet**
  Computerwurm, der im Juni 2010 entdeckt wurde. Er wurde speziell für das System Simatic S7 zur Überwachung und Steuerung technischer Prozesse entwickelt, um damit in die Steuerung von Frequenzumrichtern einzugreifen.

- **TEMPORA**
  Codename für eine britische Geheimdienstoperation des GCHQ zur Überwachung des weltweiten Telekommunikations- und Internet-Datenverkehrs.

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

- **Uroburos**
  Mutmaßliche Geheimdienstsoftware zum Absaugen hochsensibler und geheimer Informationen von staatlichen Einrichtungen, Nachrichtendiensten und Großunternehmen, welche autonom arbeitet, sich selbstständig im infizierten Rechner verbreitet und auch Rechner angreift, die nicht direkt mit dem Internet verbunden sind. Damit soll die Kontrolle über den PC erlangt und Daten vom Computer gestohlen werden.

- **Virus (Computervirus)**
  Ein sich selbst verbreitendes Computerprogramm, welches sich in andere Computerprogramme einschleust und sich damit reproduziert. Die Klassifizierung als Virus bezieht sich hierbei auf die Verbreitungs- und Infektionsfunktion. Einmal gestartet, kann es vom Anwender nicht kontrollierbare Veränderungen am Status der Hardware, am Betriebssystem oder an der Software vornehmen (Schadfunktion). Viren zählen zur Malware.

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

- **Whistleblowing**
  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

Johannes Behrends
Specialty
AON Risk Solutions

www.aon.de
johannes.behrends@aon.de

Die Studie **„Industriespionage 2014 – Cybergeddon der deutschen Wirtschaft durch NSA & Co.?“** wurde durch die Corporate Trust - Business Risk & Crisis Management GmbH erstellt. Begleitet wurde die Studie durch AON Risk Solutions, die Securiton GmbH und die Zurich Gruppe Deutschland.

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

Werner Sielenkemper
Senior Consultant
Securiton GmbH

www.securiton.de
werner.sielenkemper@securiton.de

Johann Worm
Head of Broker Management
Zurich Gruppe Deutschland

www.zurich.com
johann.worm@zurich.com

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