CORPORATE TRUST
business risk & crisis management

Studie: Gefahrenbarometer 2010

Sicherheitsrisiken für den deutschen Mittelstand

Begleitet durch: TaylorWessing MAZARS RSA SECURITY

Inhalt

„Sicherheit erreicht man nicht, indem man Zäune errichtet, Sicherheit gewinnt man, indem man Tore öffnet."

Urho Kekkonen,
finnischer Staatspräsident (1956-1981)

Vorwort

Christian Schaaf
Geschäftsführer
CORPORATE TRUST,
Business Risk &
Crisis Management GmbH

„Obwohl die weltweite Bedrohung durch politische Unruhen oder Kriminalität steigt, schützen sich deutsche Mittelständler noch zu wenig gegen die Risiken.“

Mittelständische Unternehmen bilden das Rückgrat der deutschen Industrie. Viele von ihnen sind so genannte Hidden Champions - also Unternehmen, die zwar in ihrem Segment oder ihrer Branche Weltmarktführer sind, aber in der Öffentlichkeit eher am Rande wahrgenommen werden. Diese heimlichen Gewinner haben viel zum Prädikat „Made in Germany“ beigetragen. Sie sind weltweit geschätzt und stehen als Synonym für deutsches Unternehmertum - innovativ, zuverlässig, erfolgreich.

Deutschland war 2008 wieder einmal Exportweltmeister. Somit sind deutsche Mittelständler weltweit präsent und liefern ihre Produkte überall hin. Mit dieser internationalen Ausrichtung verbinden sich zahlreiche grenzüberschreitende Aktivitäten und Aspekte: Geschäftsreisen, weltweite Geschäfts- oder Joint-Venture-Partner, Vertriebsniederlassungen oder Produktionsstandorte im Ausland, Mitarbeiter aus anderen Ländern sowie rechtliche und steuerliche Herausforderungen.

Das alles bedeutet auch, dass sich diese Unternehmen verstärkt mit den wirtschaftlichen, politischen und gesellschaftlichen Gegebenheiten im jeweiligen Land auseinandersetzen müssen. Vor möglichen kriminellen Strukturen darf man dabei nicht die Augen verschließen: Religiöser Fanatismus, ethnische Auseinandersetzungen und besondere Formen der Kriminalität können sehr schnell eine Rolle spielen - bis hin zur erhöhten Bedrohung durch Terrorismus. Die Sicherheitsmaßnahmen müssen entsprechend angepasst sein. Sie sollten nicht nur auf den Erhalt von Sachwerten oder dem Know-how des Unternehmens abzielen, sondern auch und zuerst auf den Schutz von Mitarbeitern.

Kriminelle Risiken für Unternehmen gibt es aber nicht nur im Ausland, sondern zunehmend auch in Deutschland. Zwar ist die allgemeine Bedrohung durch Kriminalität hierzulande seit Jahren relativ konstant, für die Wirtschaft liegen die Dinge jedoch anders. Während die Polizeiliche Kriminalstatistik (PKS)[1] 2007 für die letzten Jahre sogar einen leicht rückläufigen Trend ausweist, machen manche Formen von Kriminalität den mittelständischen Unternehmen vermehrt zu schaffen. Dazu gehören Straftaten der Wirtschaftskriminalität oder Industriespionage genauso wie Überfälle auf Mitarbeiter im Ausland, Produkterpressungen, organisierte Diebstähle und Bedrohungen des Managements oder der vermögenden Eigentümer.

Große Konzerne haben häufig die nötigen Sicherheitsstrukturen aufgebaut. Mittelständler hingegen sind zum Teil unzureichend auf diese veränderten Sicherheitsherausforderungen vorbereitet. Dies führt dazu, dass sie leichter Opfer werden und manche Schäden erst zu spät entdecken. Wenn ein krimineller Angriff bemerkt wird und es im Unternehmen keine geeigneten Strukturen gibt, um ihn abzuwehren oder Schäden schnellstmöglich aufzudecken, kann sich ein solcher Vorfall sehr schnell zu einer Krise ausweiten.

Leider werden viele der Vorfälle - zum Beispiel im Bereich Wirtschaftskriminalität oder Industriespionage - gar nicht erst aufgedeckt bzw. von den Unternehmen vertuscht. Zu groß ist die Angst vor einem Reputationsschaden. Anzeige wird häufig nur dann erstattet, wenn man den finanziellen Schaden bei einer Versicherung geltend machen möchte. Dies führt dazu, dass die Kriminalstatistik nur einen Bruchteil der tatsächlichen Vorkommnisse und finanziellen Schäden widerspiegelt. Ein Großteil bleibt verborgen und wird dem so genannten Dunkelfeld[2] zugerechnet.

Was aber geschieht, wenn die Zahlen nur einen geringen Teil der Realität wiedergeben und man nichts darüber in den Medien liest oder hört? Das Bewusstsein für die Gefahren bleibt aus, und die tatsächlichen Bedrohungen werden nicht erkannt oder nicht richtig eingeschätzt. Corporate Trust hat daher zusammen mit dem Handelsblatt die Studie „Gefahrenbarometer 2010“ erarbeitet, um die tatsächlichen Schäden und aktuellen Risiken für den deutschen Mittelstand genau zu erfassen. Sie soll einen Ausblick darauf geben, welche Bedrohungen mittelständische Unternehmen in den nächsten Jahren zu erwarten haben und in welche Sicherheitsvorkehrungen man investieren sollte. Begleitet und unterstützt wurde die Studie durch die Rechtsanwaltskanzlei TAYLOR WESSING, das Wirtschaftsprüfungsunternehmen MAZARS Hemmelrath und die IT-Security-Spezialisten RSA, The Security Division of EMC. Damit sich Unternehmen auch zukünftig besser auf Risiken vorbereiten können, wird das Corporate Trust Gefahrenbarometer in regelmäßigen Abständen erscheinen.

Ihr

Christian Schaaf

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

2) Dunkelfeld In der Kriminologie bezeichnet das Dunkelfeld die Differenz zwischen den amtlich registrierten Straftaten - dem so genannten Hellfeld - und der vermutlich begangenen Kriminalität.

VORWORT

Jörg Ziercke
Präsident
Bundeskriminalamt

„Das Risiko, selbst Opfer von Wirtschaftskriminalität zu werden, wird vielfach unterschätzt.“

Wirtschaftskriminalität wird zunehmend als Problem erkannt und in ihren Auswirkungen diskutiert. Das Gefahrenpotenzial der Wirtschaftskriminalität zeigt sich vor allem in den Schäden, die sie verursacht: Der zahlenmäßige Anteil der Wirtschaftskriminalität an den insgesamt polizeilich bekannt gewordenen Straftaten betrug in den vergangenen Jahren im Schnitt nur ein bis zwei Prozent. Betrachtet man jedoch den Gesamtschaden aller mit Schadenssumme erfassten Delikte, so geht auf das Konto der Wirtschaftskriminalität regelmäßig rund die Hälfte davon. Im Jahr 2007 waren dies etwa vier Milliarden Euro. Gerade bei der Wirtschaftskriminalität gehen die Strafverfolgungsbehörden zudem von einem großen Dunkelfeld mit einem erheblichen volkswirtschaftlichen Schadenpotenzial aus. Die möglichen Folgen sind Wettbewerbsverzerrungen, Aushebelung von Marktmechanismen, Vertrauensverluste im internationalen Wettbewerb und damit Auftragsrückgänge - um nur einige der wichtigsten zu nennen.

Aktuelle Studien lassen in Unternehmen zwar ein wachsendes Problembewusstsein für die Bedrohungen durch Wirtschaftskriminalität erkennen. Gleichwohl räumen viele Unternehmen ein, nur geringe Kenntnisse über wirtschaftskriminelle Handlungsmuster zu haben. Infolgedessen wird das Risiko, selbst Opfer von Wirtschaftskriminalität zu werden, vielfach unterschätzt und zu wenig in Präventionsmaßnahmen investiert.

Wirtschaftskriminalität umfasst eine Vielzahl verschiedenster Deliktbereiche und Tathergänge. Neben Kriminalität rund um den Kapitalmarkt und Korruption geht es auch um Industriespionage, Produkt- und Markenpiraterie sowie Insolvenzdelikte. Etwa zehn Prozent der polizeilich registrierten Fälle von Wirtschaftskriminalität wurden im Jahr 2007 mit Hilfe des Internets verübt. Das Internet als Tatmittel gewinnt dabei in allen Bereichen der Wirtschaftskriminalität an Bedeutung: So bietet es zum Beispiel neue Angriffspunkte für Wirtschafts- und Konkurrenzspionage - das Einfallstor für Produkt- und Markenpiraterie. Die Registrierung der Fälle von Kriminalität im Zusammenhang mit Informations- und Kommunikationstechnologie zeigt, dass gezielte Angriffe gegen die IT-Infrastruktur von Unternehmen immer häufiger werden.

Angesichts des vermuteten großen Dunkelfeldes im Bereich der Wirtschaftskriminalität haben es sich die Strafverfolgungsbehörden zum Ziel gesetzt, die Anzeigebereitschaft betroffener Unternehmen zu fördern. Noch immer fürchten viele Verantwortliche einen Imageverlust und sind daher versucht, „interne“ Lösungen vorzuziehen. Erschwerend kommt hinzu, dass vielen Unternehmen die Arbeit der Sicherheitsbehörden noch immer nicht hinreichend bekannt ist. Um das zu ändern, führt das Bundeskriminalamt - in Kooperation mit der Arbeitsgemeinschaft für Sicherheit in der Wirtschaft (ASW) - regelmäßige Informationsveranstaltungen für Wirtschaftsvertreter zu aktuellen Sicherheitsthemen durch. Parallel dazu hat das Bundeskriminalamt eine Initiative zur Zusammenarbeit mit weltweit tätigen deutschen Unternehmen gestartet. Im Mittelpunkt steht neben dem Informationsaustausch die Entwicklung umfassender Sicherheitskonzepte, die zwischen den Wirtschaftsunternehmen und den Sicherheitsbehörden abgestimmt sind.

Vor diesem Hintergrund ist die Studie „Gefahrenbarometer 2010“ auch für die Strafverfolgungsbehörden von großem Interesse. Sie enthält sehr überzeugende Ansätze und dokumentiert eindrucksvoll die Bestrebungen innerhalb der Wirtschaft, Sicherheitsrisiken zu erfassen und zu analysieren, um wirksam und nachhaltig dagegen vorgehen zu können. Effektive Schutzmaßnahmen gegen Wirtschaftskriminalität setzen valide Erkenntnisse dieses Phänomens voraus - Erkenntnisse, die wir derzeit noch nicht in ausreichendem Maße besitzen. Die vorliegende Studie ist ein weiterer entscheidender Schritt, um diese Lücke zu schließen.

Ihr

Jörg Ziercke
Präsident
Bundeskriminalamt

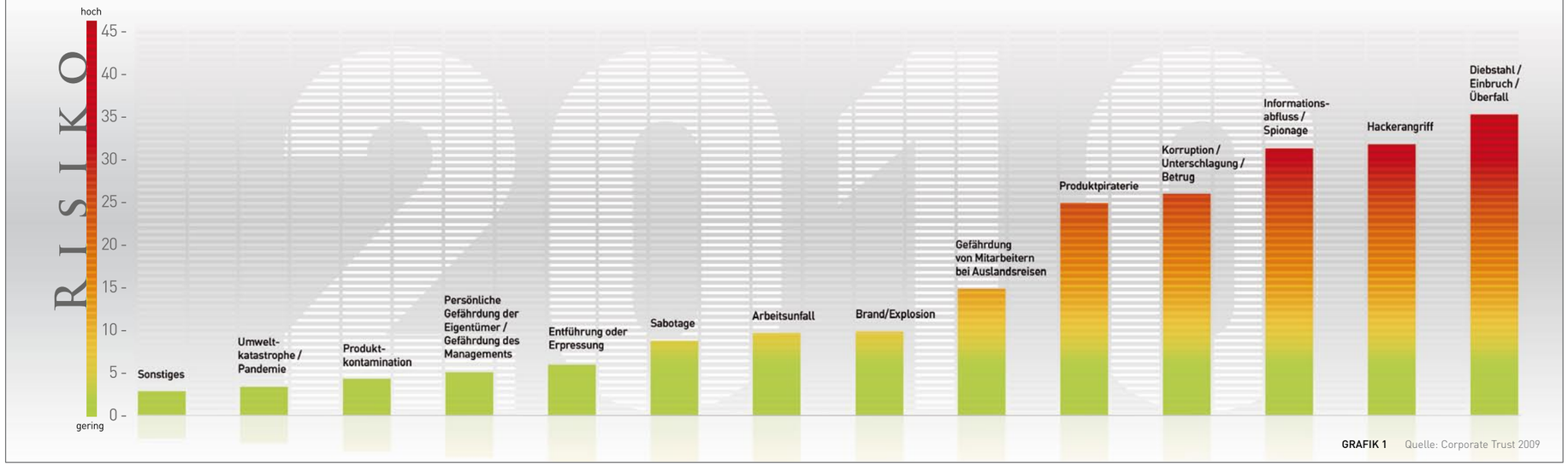
Ergebnisse in Kürze

Gefahrenbarometer 2010

Das Gefahrenbarometer 2010 spiegelt die weltweiten Sicherheitsrisiken für den deutschen Mittelstand wider. Bei der Bewertung des jeweiligen Risikos handelt es sich um einen Mittelwert aus folgenden zwei Kategorien:

- Schäden in den letzten drei Jahren (siehe Seite 17, Grafik 8)
- Einschätzung der zukünftigen Gefahren für Deutschland und bei den ausländischen Gesellschaften (siehe Seite 45, Grafik 35)

Gefahrenbarometer 2010:



GRAFIK 1 Quelle: Corporate Trust 2009

Zusammenfassung

- Auch sehr große Unternehmen mit mehr als 10.000 Mitarbeitern und über 1 Milliarde Euro Umsatz rechnen sich häufig noch zum Mittelstand.
- Größere mittelständische Unternehmen sind häufiger von einem Schaden durch Kriminalität, eine Natur- oder Umweltkatastrophe, eine Pandemie[3], ein Feuer, eine Explosion oder einen Arbeitsunfall betroffen als kleinere Unternehmen. Das größte Schadenrisiko - mit 36,7 Prozent aller betroffenen Unternehmen - haben demnach Mittelständler aus dem Segment 50 bis 250 Millionen Euro Umsatz bzw. 250 bis 1.000 Mitarbeiter.
- 71,6 Prozent aller befragten Unternehmen gaben an, auch im Ausland tätig zu sein. Sie verfügen dort nicht nur über Kunden oder Lieferanten, sondern häufig auch über eigene Niederlassungen, Tochterunternehmen, Joint-Venture-Partner, Produktionsstätten sowie Vertriebs- oder Handelsvertretungen.
- Nach Europa - mit 75,6 Prozent aller Unternehmen - ist Asien mit 50,2 Prozent die zweitstärkste Region bei den Geschäftsbeziehungen der Mittelständler im Ausland.
- Die Mehrzahl der Schäden - 20,1 Prozent - entsteht den mittelständischen Unternehmen durch Diebstahl, Einbruch und Überfall. Korruption, Betrug und Untreue landeten mit 15,1 Prozent auf Platz zwei, dicht gefolgt von Hackerangriffen[4] mit 14,1 Prozent.
- Die meisten Mittelständler haben keine ausreichenden Sicherheitsstrukturen, um die verschiedenen Bedrohungen zu bewältigen. Obwohl Korruption das zweithöchste Risiko darstellt, verfügt nur etwa ein Fünftel aller Unternehmen über einen eigenen Compliance[5]-Verantwortlichen.
- Auch das finanzielle Risiko wird zu wenig beachtet. Nur 47,8 Prozent der Unternehmen gaben an, eine Versicherung gegen die jeweiligen kriminellen Risiken zu haben.
- Genau ein Drittel der Mittelständler gab an, auch in sicherheitskritischen Ländern oder Krisenregionen[6] präsent zu sein. Trotzdem haben nur 15,1 Prozent entsprechende Standards für die Reisesicherheit von Management und Mitarbeitern definiert.
- Korruption[7], Industriespionage[8] und organisierte Kriminalität[9] sind die größten Risiken im Ausland. Zwei Drittel aller Unternehmen - genau 66,4 Prozent - sehen Korruption als Problem an. Dennoch führen nur 21,2 Prozent einen intensiven Background-Check[10] beim Geschäftspartner durch.
- Nur 17,7 Prozent aller befragten Unternehmen verfügen über ein professionelles Krisenmanagement[11]. Zwar haben 26,5 Prozent einen Krisenplan für verschiedene Bedrohungsszenarien, eine vorbereitete Krisen-PR[12] können aber nur die wenigsten vorweisen.
- Die meisten Mittelständler sind nicht ausreichend gegen Wirtschaftskriminalität gewappnet. Compliance-Richtlinien (19,5 Prozent), Fachseminare für die Revision (6,2 Prozent) oder Whistle-Blowing-Systeme[13] (5,3 Prozent) gibt es nur selten.
- Mehr als die Hälfte aller Unternehmen macht ihren Mitarbeitern oder Geschäftspartnern keine klaren Vorgaben zum Umgang mit vertraulichen Informationen, Daten oder Dokumenten. Nur bei 39,8 Prozent gibt es eine Klassifizierung der Geheimhaltungsstufe[14].
- Eigene Mitarbeiter stellen das größte Risiko für einen Informationsabfluss dar. 58,4 Prozent der Unternehmen glauben, dass der leichtfertige Umgang von Mitarbeitern mit Sicherheitsstandards die größte Bedrohung für IT und Telekommunikation darstellt.
- Rund 60 Prozent aller Unternehmen haben sowohl USB-Ports an verschiedenen EDV-Geräten als auch einen offenen Zugang ins Internet für alle Mitarbeiter. Damit eröffnen sich viele Gelegenheiten zum Datenmissbrauch.
- Nur die wenigsten Mittelständler legen bei den Kommunikationsmitteln Wert auf eine Verschlüsselung[15]. Vertrauliche Informationen können dadurch leicht in falsche Hände geraten.
- Die meisten Unternehmen verfügen über ausreichende Vorkehrungen für die Objektsicherheit, den Brandschutz sowie die Möglichkeit einer schnellen Evakuierung[16] bei einer Bombendrohung oder einem Großschaden.
- Das weltweite Risiko durch Kriminalität, Terrorismus, Pandemien, Natur- oder Umweltkatastrophen wird laut der Befragung steigen. Mittelständler bewerten den zukünftigen Anstieg bei den allgemeinen Sicherheitsrisiken im Ausland höher als in Deutschland.
- Befragt nach dem eigenen Unternehmen sah man hingegen meist eine höhere Bedrohung für die deutschen Standorte als bei den ausländischen Töchtern oder Niederlassungen. Sowohl für Deutschland (53,1 Prozent) als auch weltweit (37,2 Prozent) wurde die Gefahr durch Informationsabfluss oder Spionage am höchsten eingeschätzt.
- Der deutsche Mittelstand hat erkannt, dass Investitionen in das Sicherheitsverhalten der Mitarbeiter den größten Schutz bieten. 53,1 Prozent der Unternehmen wollen ihr Personal künftig besser sensibilisieren[17]. Eigene Strukturen gegen Korruption oder ein professionelles Krisenmanagement wird es aber auch in Zukunft zu selten geben.

3) Pandemie Länder- und kontinentübergreifende Ausbreitung einer Krankheit, im engeren Sinn einer Infektionskrankheit. Im Gegensatz zur Epidemie ist eine Pandemie somit nicht örtlich beschränkt.

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

5) Compliance Ein Verhaltenskodex für gesetzmäßiges, rechtskonformes und verantwortungsbewusstes Handeln im Unternehmen.

6) Krisenregion Als Krisengebiet, Krisenherd oder Krisenregion werden Gegenden bezeichnet, in denen Sicherheitsrisiken ein schwer oder nicht mehr beherrschbares Ausmaß erreicht haben. Dazu gehören politische, ethnische oder wirtschaftliche Konflikte und Probleme oder Schäden durch Umwelt- und Naturkatastrophen.

7) Korruption Der Missbrauch einer Vertrauensstellung in einer bestimmten Funktion, um einen materiellen oder immateriellen Vorteil zu erlangen, auf den kein rechtlich begründeter Anspruch besteht.

8) Industriespionage Umgangssprachlich für Konkurrenzausspähung, teilweise auch für Wirtschaftsspionage. Wird häufig als Oberbegriff für Spionage bei Unternehmen verstanden.

9) Organisierte Kriminalität Von Gewinn- und/oder Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind. Von „organisiert" spricht man, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer zusammenwirken - unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen, unter Anwendung von Gewalt oder anderer einschüchternder Mittel oder unter Einflussnahme auf Politik, Massenmedien, öffentliche Verwaltung, Justiz oder Wirtschaft.

10) Background-Check Überprüfung von Mitarbeitern oder Geschäftspartnern bezüglich der Seriosität, Zuverlässigkeit, finanziellen Verhältnisse, etwaiger Firmenbeteiligungen oder sonstiger verdächtiger Lebensumstände.

11) Krisenmanagement Der systematische Umgang mit Krisensituationen. Dazu gehören die Identifikation und Analyse der jeweiligen Risiken, ein Notfallplan, die Benennung der Mitglieder im Krisenstab sowie präventive Vorkehrungen.

12) Krisen-PR Unter Krisen-PR oder Krisenkommunikation versteht man jenes Teilgebiet der Öffentlichkeitsarbeit, das sich mit der Information und Kommunikation in Krisensituationen beschäftigt.

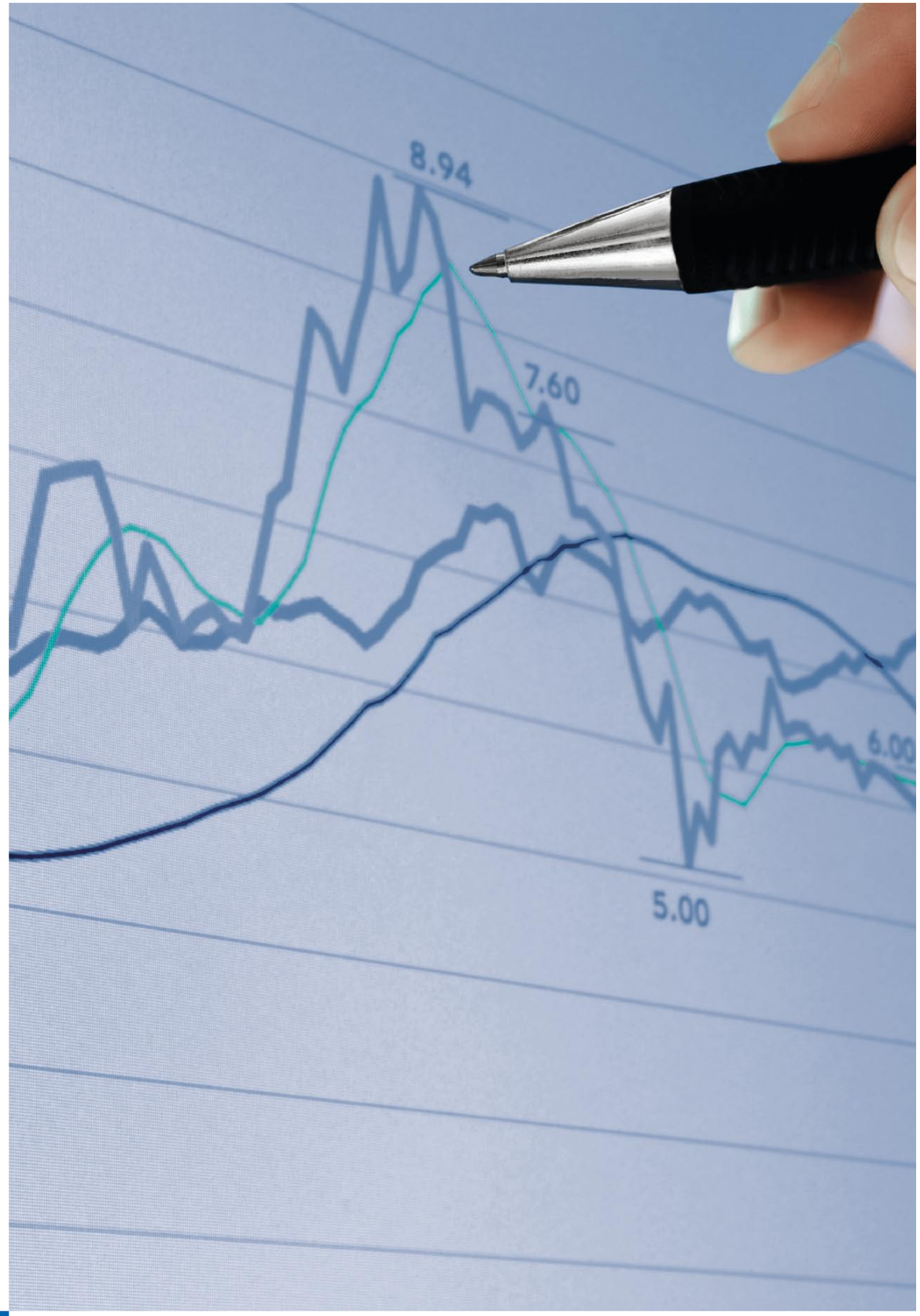
13) Whistle-Blowing Ein Informant bringt Missstände, illegales Handeln oder allgemeine Gefahren, von denen er an seinem Arbeitsplatz erfährt, an die Öffentlichkeit.

14) Geheimhaltungsstufe Festlegung einer Schutzstufe oder Schutzklasse für Daten oder Informationen gemäß der jeweiligen Schutzwürdigkeit und individuellen Gefährdung.

15) Verschlüsselung Vorgang, bei dem klar lesbare Texte oder auch Informationen anderer Art - wie Ton- oder Bildaufzeichnungen - mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine unleserliche, nicht einfach interpretierbare Zeichenfolge umgewandelt werden.

16) Evakuierung Die Räumung eines Gebäudes oder Gebiets von Menschen.

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

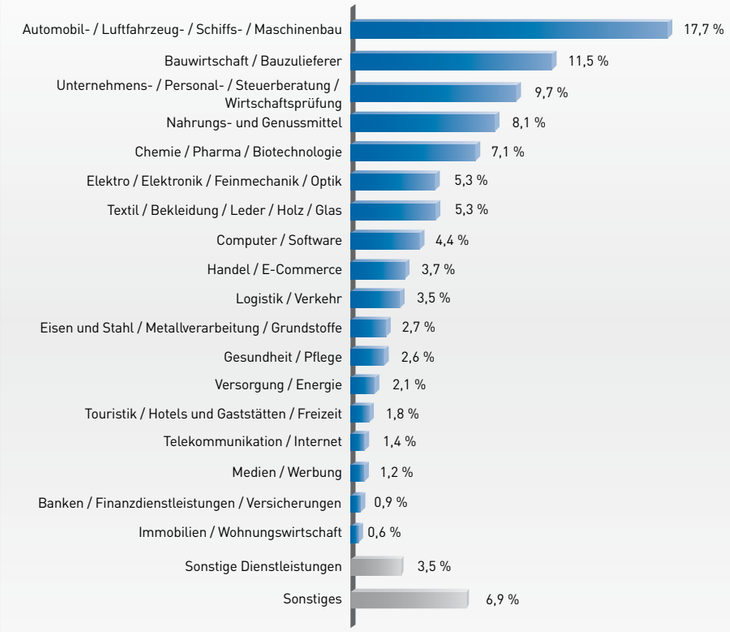


Methodik der Studie

Diese Studie wurde in Zusammenarbeit mit dem Handelsblatt auf Grundlage einer Befragung von 5.154 mittelständischen Unternehmen erstellt. Dafür wurden deutsche Unternehmen anhand ihrer Unternehmensgröße ausgewählt, definiert nach Mitarbeiterzahl und Umsatz. Großer Wert wurde darauf gelegt, dass die Befragung branchenübergreifend durchgeführt wurde.

Laut einer Richtlinie der EU-Kommission gelten Unternehmen mit 50 bis 250 Mitarbeitern und einem Umsatz von 10 bis 50 Millionen Euro bzw. einer Bilanzsumme von 10 bis 43 Millionen Euro als mittelständisch. Davon abweichend bezieht diese Befragung aber auch Unternehmen bis zu einer Größe von 20.000 Mitarbeitern bzw. einem Umsatz von über einer Milliarde Euro ein. Grund dafür ist eine frühere vergleichbare Befragung aus dem Jahr 2007: Sie ergab, dass sich die Mehrheit der Unternehmen in dieser Größenordnung selbst dem Mittelstand zurechnete. Bei den Antworten aller befragten Unternehmen wurden jedoch nur diejenigen berücksichtigt, die sich selbst als Mittelstand bezeichneten.

Teilnahme an der Studie:



GRAFIK 2 Quelle: Corporate Trust 2009

Die Befragung erfolgte in Form eines standardisierten Fragebogens, der sowohl in gedruckter Form als auch online auf einer Website beantwortet werden konnte. Adressaten waren jeweils die Geschäftsführer oder Vorstände, Sicherheitsverantwortliche, Werkschutzleiter, IT-Leiter sowie Personalleiter. Außerdem wurden zusätzlich 30 Unternehmen, die im Januar 2009 von den VDI-Nachrichten als „Hidden Champions" gelistet wurden, in halbstündigen telefonischen Interviews zu eigenen Erfahrungen, erlittenen Schäden und bestehenden Sicherheitsvorkehrungen befragt. Die Telefoninterviews wurden mit Unterstützung des Studiengangs Sicherheits- und Risikomanagement der Hochschule für Öffentliche Verwaltung in Bremen erstellt, für die wir uns nochmals herzlich bedanken möchten!

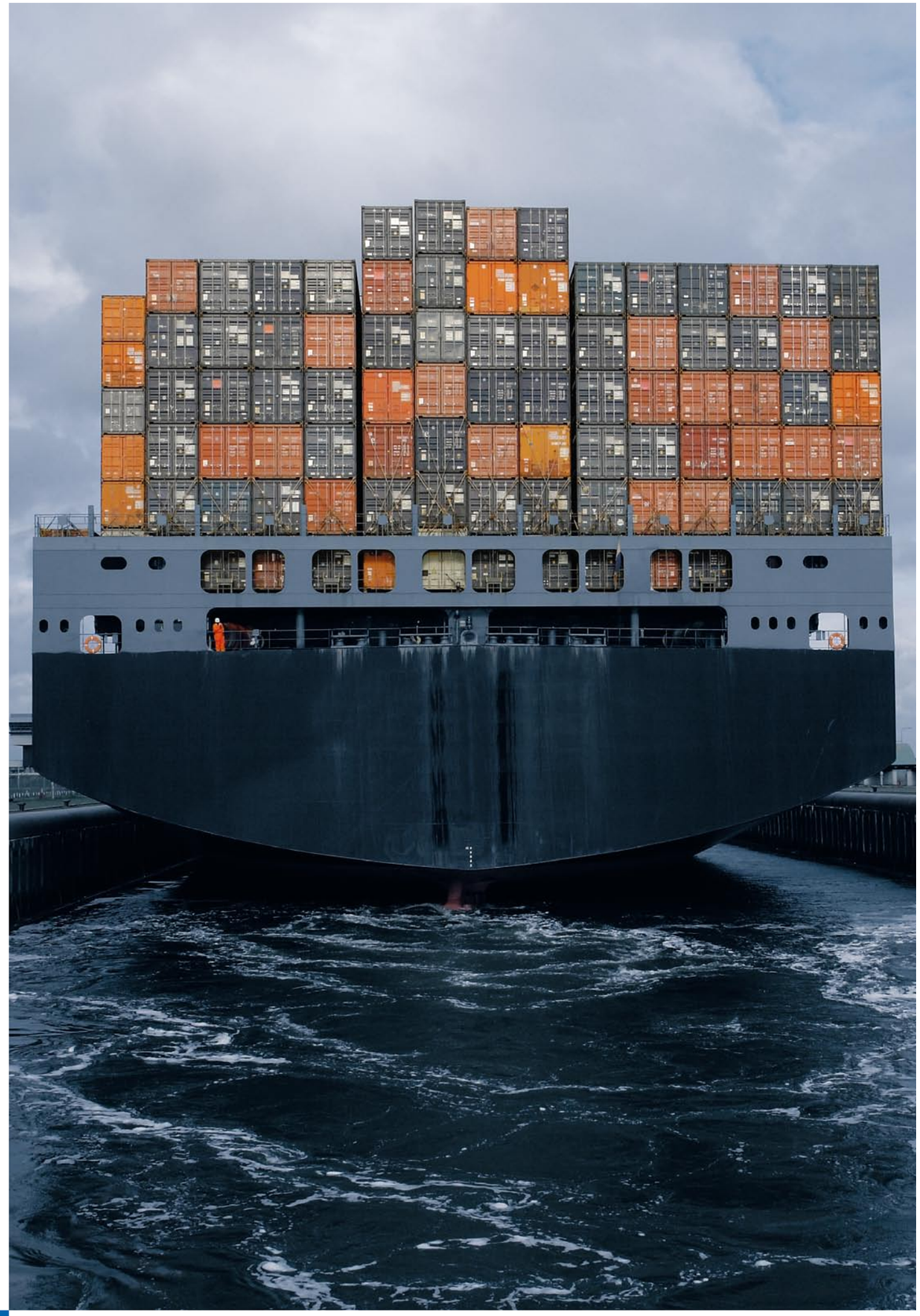
Bei der Erhebung wurden Informationen zum Unternehmen, den kriminellen Vorfällen, Schäden und Sicherheitsvorkehrungen sowie die vermutete Entwicklung von zukünftigen Risiken und geplante Präventionsmaßnahmen abgefragt. Die Fragen waren dabei so angelegt, dass die vorgegebenen Antwortoptionen erfahrungsgemäß 80 Prozent der denkbaren Antworten abdeckten. Für die restlichen 20 Prozent stand es vielfach frei, zusätzliche Texte einzugeben. Bei den meisten Fragen waren außerdem mehrere Antworten möglich.

Im Januar und Februar 2009 wurde der Fragebogen an 2.121 Unternehmen postalisch und an weitere 3.003 Unternehmen per E-Mail versandt. Bei der E-Mail-Aussendung wurden die Teilnehmer eingeladen, an der Befragung online teilzunehmen. Dazu erhielten sie - für alle gleich lautende - Zugangsdaten für eine Website. Auf diese Weise war gewährleistet, dass nur die ausgewählten Unternehmen und keine Zufallsbesucher an der Online-Befragung teilnehmen konnten.

Zum Abschluss bot der Fragebogen jeweils die Möglichkeit, das Unternehmen zu benennen. Es war jedoch allen Teilnehmern freigestellt, auch anonym zu antworten. Der überwiegende Teil machte keinerlei Angaben zum Unternehmen und antwortete anonym. Die meisten Antworten, genau 38,8 Prozent, kamen direkt von der Geschäftsleitung. Zu 15,4 Prozent machten Sicherheits-Ansprechpartner die Angaben, zu 8,9 Prozent der Personalleiter, zu 6,4 Prozent der IT-Leiter und zu 1,8 Prozent der Werkschutzleiter. Von der Möglichkeit der Anonymisierung machten 28,7 Prozent der Teilnehmer Gebrauch und gaben keine Position im Unternehmen an.

Von den 5.154 befragten Unternehmen antworteten 456; das entspricht 8,9 Prozent der Gesamtheit. Die Antwortbereitschaft lag damit zwar im normalen Durchschnitt anderer Befragungen, jedoch unter den 9,9 Prozent bei der Studie zur Industriespionage, die Corporate Trust 2007 erstellt hat.

Begleitet und unterstützt wurde die Studie durch die Rechtsanwaltskanzlei TAYLOR WESSING, das Wirtschaftsprüfungsunternehmen MAZARS Hemmelrath und die IT-Security-Spezialisten RSA, The Security Division of EMC. Allen Partnern und Unterstützern sowie den Führungskräften, IT-, Personal- und Sicherheitsverantwortlichen, die an der Befragung teilgenommen haben, sagen wir auf diesem Wege nochmals herzlichen Dank.



Risiken für den deutschen Mittelstand

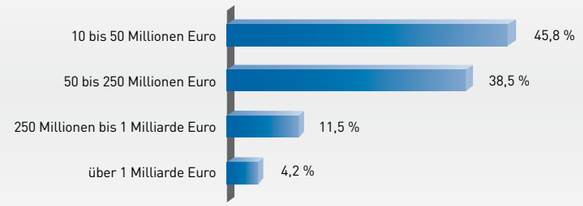
Betroffene Unternehmen

Die meisten mittelständischen Unternehmen kommen aus dem kleinen oder mittleren Segment.

Die meisten Antworten kamen von Unternehmen aus dem typischen Mittelstandssegment, mit 10 bis 50 Millionen Euro Umsatz und 50 bis 250 Mitarbeitern. Die Unternehmen wurden gefragt, zu welcher Kategorie sie sich selbst zählen: Konzern, Mittelstand oder Kleinunternehmen. Es wurde darauf geachtet, dass nur Antworten von Unternehmen gewertet wurden, die sich selbst als Mittelständler bezeichneten.

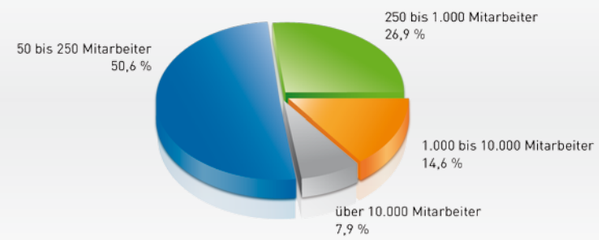
Ein Teil der Antworten kam auch von Unternehmen, die teilweise über 10.000 Mitarbeiter beschäftigen und mehr als 1 Milliarde Euro Umsatz generieren. Dies zeigt, dass die Definition der Europäischen Union[18] alleine nicht ausreichen würde, um den deutschen Mittelstand korrekt zu erfassen.

Wie hoch ist Ihr Jahresumsatz?



GRAFIK 3 Quelle: Corporate Trust 2009

Wie viele Mitarbeiter beschäftigt Ihr Unternehmen?



GRAFIK 4 Quelle: Corporate Trust 2009

18) Definition der EU für KMU
http://ec.europa.eu/enterprise/entrepreneurship/facts_figures.htm
Kleine und Mittlere Unternehmen, wenn sie von größeren Unternehmen unabhängig sind, weniger als 250 Mitarbeiter und weniger als 50 Millionen Euro Umsatz bzw. weniger als 43 Millionen Euro Bilanzsumme haben.

Risiken für den deutschen Mittelstand

Betroffene Unternehmen

Größere Mittelständler sind am stärksten gefährdet.

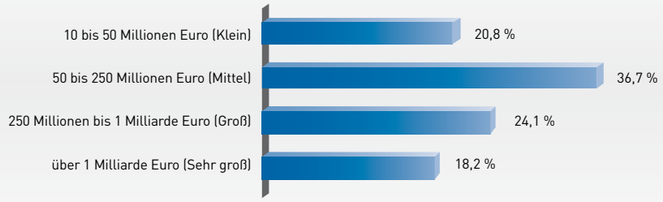
Obwohl die meisten Antworten von den kleineren mittelständischen Unternehmen kamen, war der größte Teil der Schäden bei den etwas größeren Mittelständlern - mit 50 bis 250 Millionen Euro Umsatz bzw. 250 bis 1.000 Mitarbeitern - zu verzeichnen. Die Schäden wurden in vier Größenkategorien jeweils summiert. Anhand der Unternehmensgröße wurde dann abhängig vom Quotienten der Beteiligung die Schadenshäufigkeit errechnet.

Folgende Größenkategorien kamen dabei zur Anwendung:

- 10 bis 50 Millionen Euro Umsatz bzw. 50 bis 250 Mitarbeiter (Klein)
- 50 bis 250 Millionen Euro Umsatz bzw. 250 bis 1.000 Mitarbeiter (Mittel)
- 250 Millionen bis 1 Milliarde Euro Umsatz bzw. 1.000 bis 10.000 Mitarbeiter (Groß)
- Über eine Milliarde Umsatz bzw. über 10.000 Mitarbeiter (Sehr groß)

Unternehmen mittlerer Größe waren mit Abstand am häufigsten betroffen. Das könnte daran liegen, dass sie zwar vermutlich wie ein Großunternehmen agieren und weltweit präsent sind, jedoch oft nicht über die erforderlichen Sicherheitsstrukturen verfügen. Viele der größeren Mittelständler haben sich bereits ähnlich wie Großkonzerne aufgestellt: Sie verfügen über eine Corporate Security[19], ausführliche Notfallpläne oder einen fest verankerten Krisenstab[20], in dem jeder seine Aufgabe genau kennt. Damit besitzen sie die nötigen Strukturen, um Risiken professionell entgegenzutreten. Die kleineren Mittelständler sind teilweise nicht international präsent und haben daher vermutlich ein anderes Bedrohungsspektrum bzw. ein geringeres Risiko.

Verteilung der Schadenshäufigkeit:



GRAFIK 5 Quelle: Corporate Trust 2009

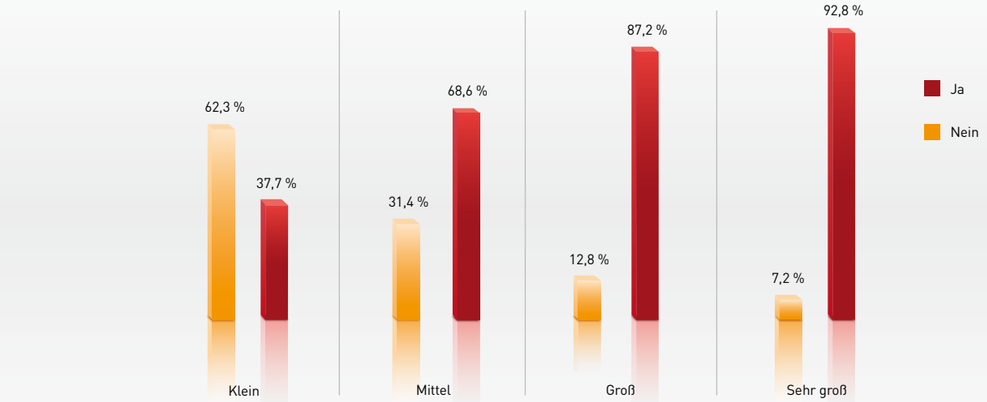
19) Corporate Security Bezeichnung für die Sicherheitsabteilung eines großen Konzerns, in der alle sicherheitsrelevanten Themen bearbeitet werden.

20) Krisenstab Gruppe von Personen innerhalb einer Organisation zum Notfall- oder Katastrophenmanagement. Der Krisenstab selbst übernimmt nicht die Führung, sondern funktioniert nur unter einem führungserfahrenen und alleinverantwortlichen Leiter. Dies stellt sicher, dass auch unter hohem Druck Entscheidungen schnell getroffen und mit vereinten Kräften umgesetzt werden können.

Die Mehrzahl der geschädigten Mittelständler ist auch im Ausland tätig.

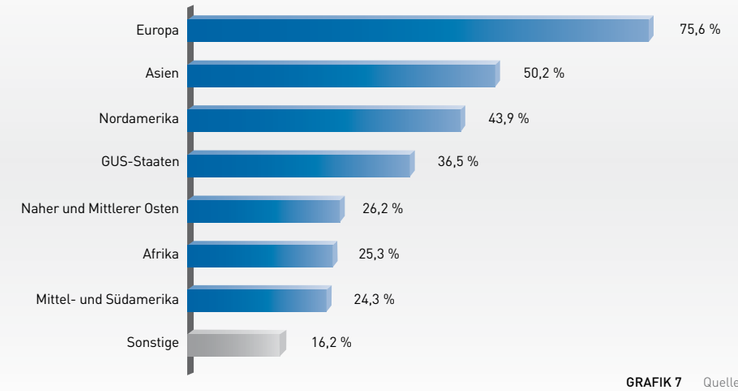
Die überwiegende Mehrzahl aller mittelständischen Unternehmen, ist international präsent und verfügt über Auslandsniederlassungen, Tochterunternehmen, Joint-Venture-Partner, Produktionsstätten, Vertriebs- oder Handelsvertretungen. Je größer das Unternehmen, desto stärker ist anscheinend das internationale Engagement. Für die detaillierte Auswertung wurde bei der Unternehmensgröße nach den Segmenten „Klein", „Mittel", „Groß" und „Sehr groß" anhand des Umsatzes und der Mitarbeiterzahl unterschieden.

Haben Sie Geschäftsbeziehungen im Ausland?



GRAFIK 6 Quelle: Corporate Trust 2009

In welchen Regionen haben Sie Ihre Geschäftsbeziehungen? (Mehrfachnennungen möglich)



GRAFIK 7 Quelle: Corporate Trust 2009

Nach Europa mit 75,6 Prozent war Asien die zweitstärkste Region bei den Geschäftsbeziehungen. Über die Hälfte der mittelständischen Unternehmen - 50,2 Prozent - hat dort geschäftliche Kontakte. Es folgen Nordamerika mit 43,9 Prozent und die GUS-Staaten mit 36,5 Prozent. Auch in die riskanteren Regionen wie Naher und Mittlerer Osten, Mittel- und Südamerika sowie Afrika gehen annähernd ein Viertel aller befragten Unternehmen. Das bedeutet: Mehr oder weniger regelmäßig reisen Mitarbeiter dorthin; man tauscht Daten und Informationen aus, und es befinden sich Mitarbeiter, Gebäude oder sonstige Sachwerte in der jeweiligen Region.

Risiken für den deutschen Mittelstand

DIE SCHADENSQUOTE

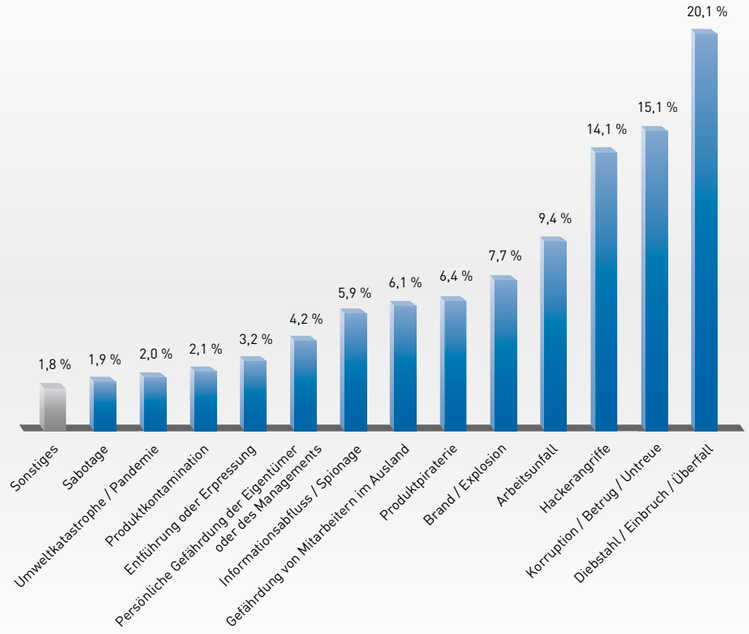
Die häufigsten Schäden entstehen den Unternehmen durch Diebstahl, Einbruch oder Überfall.

Zahlenmäßig liegen die Eigentumsdelikte Diebstahl, Einbruch und Überfall deutlich an der Spitze der schädigenden Ereignisse für Unternehmen. Mit 20,1 Prozent war diese Deliktgruppe sogar um ein Viertel größer als das nächstplatzierte Risiko Korruption, Betrug und Untreue mit 15,1 Prozent. An dritter Stelle kamen bereits Hackerangriffe, auf Platz vier lagen Arbeitsunfälle.

Diese klare Dominanz der Eigentumsdelikte dürfte darauf zurückzuführen sein, dass solche Fälle relativ schnell festgestellt werden und es eine hohe Bereitschaft der Unternehmen gibt, sie anzuzeigen. Delikte wie Sabotage, Produktkontamination, Hackerangriffe oder ein Informationsabfluss kommen hingegen oft nur durch Zufall ans Licht. Wo geeignete Sicherheitsstrukturen oder regelmäßige Überprüfungen fehlen, bleiben sie daher manchmal über Jahre unentdeckt. Die Wahrnehmung richtet sich vermutlich nur auf die Delikte, für die es standardisierte Abläufe gibt - zum Beispiel, weil man sie der Versicherung melden muss oder steuerlich abschreiben kann.

Für die unterschiedlichen Branchen ließ sich aufgrund der Vielzahl der Unterscheidungen - sowohl bei den Branchen als auch bei den Delikten - nicht detailliert zuordnen, welche Branche von welchem Deliktbereich wie stark betroffen war. Zwar wurden die Spitzenreiter mit den häufigsten Schäden bei den einzelnen Risiken ermittelt, aber die unterschiedlich hohe Beteiligung der verschiedenen Branchen lässt keine seriöse Aussage zu: Verständlicherweise kamen die Spitzenreiter ausschließlich aus den Branchen mit der höchsten Beteiligung. Auf eine Einzelwertung wird daher an dieser Stelle verzichtet.

Von welchen Schäden war Ihr Unternehmen in den letzten drei Jahren betroffen?



GRAFIK 8 Quelle: Corporate Trust 2009

Risiken für den deutschen Mittelstand

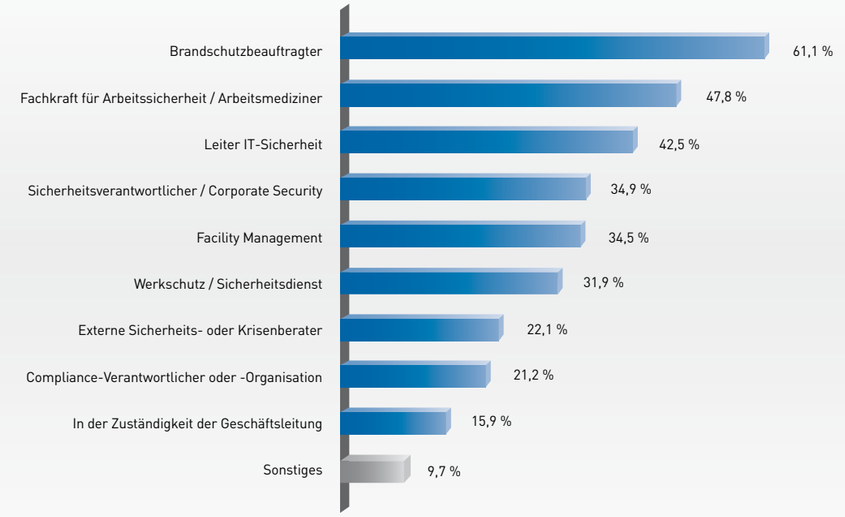
Sicherheitsvorkehrungen im Unternehmen

Viele Mittelständler haben keine ausreichenden Sicherheitsstrukturen zur Bewältigung der verschiedenen Bedrohungen.

Gegen die größten Risiken für ein Unternehmen bestehen oft nur ungenügende Sicherheitsvorkehrungen. Bei den meisten Mittelständlern gibt es zwar einen Brandschutzbeauftragten bzw. eine Fachkraft für Arbeitssicherheit, jedoch keine ausreichenden Strukturen zur Bekämpfung von Diebstahl, Einbruch und Überfall bzw. Unterschlagung, Korruption und Betrug. Obwohl gerade durch diese Risiken mit 20,1 Prozent bzw. 15,1 Prozent aller Vorfälle die meisten Schäden entstehen (vgl. Seite 17, Grafik 8), gibt es nur in einem Drittel der Unternehmen einen Sicherheitsverantwortlichen, und nur jedes fünfte Unternehmen hat eine Compliance[21]-Organisation oder einen Compliance-Verantwortlichen.

Das Risiko bei der IT scheint dagegen ernst genommen zu werden. Immerhin verfügen 42,5 Prozent aller befragten Unternehmen über einen eigenen Leiter für IT-Sicherheit. Da die tatsächlichen Schäden durch Hackerangriffe mit 14,1 Prozent immerhin am dritthäufigsten auftreten (vgl. Seite 17, Grafik 8), kommt der IT-Sicherheit eine angemessene Aufmerksamkeit zu.

Welche Verantwortlichen bzw. Strukturen haben Sie im Unternehmen, um sich mit Sicherheitsrisiken auseinanderzusetzen? (Mehrfachnennungen möglich)



GRAFIK 9 Quelle: Corporate Trust 2009

21) Compliance Ein Verhaltenskodex für gesetzmäßiges, rechtskonformes und verantwortungsbewusstes Handeln im Unternehmen.

Risiken für den deutschen Mittelstand

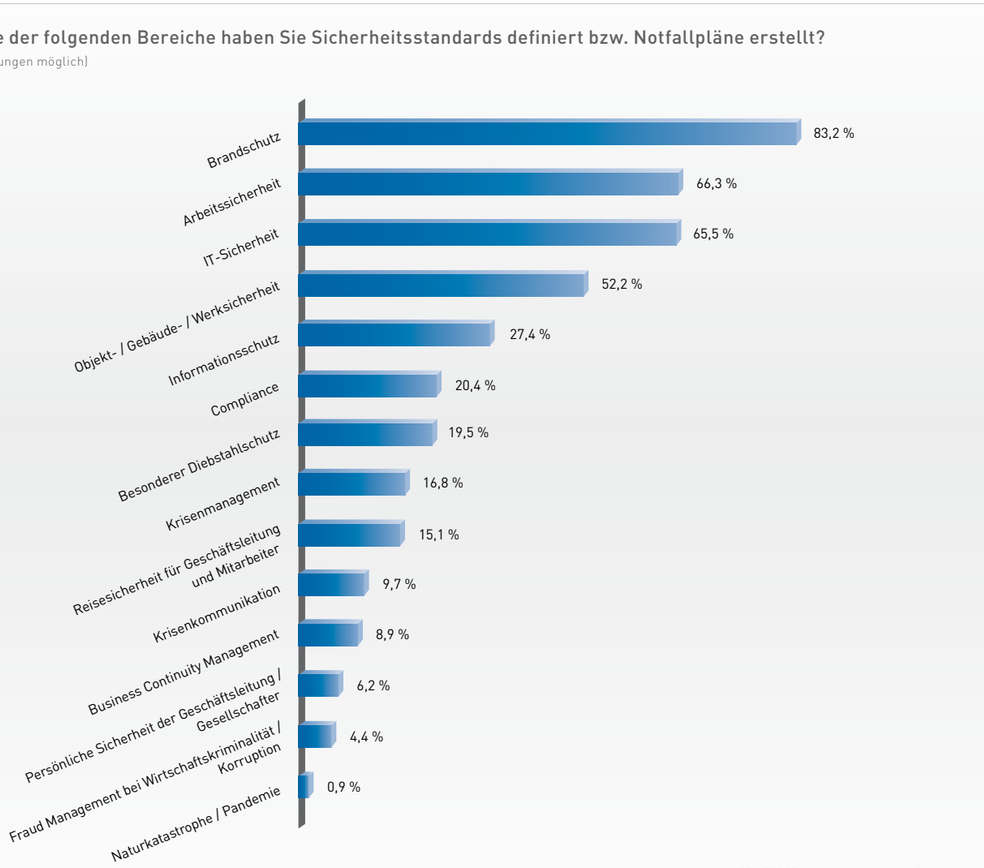
Sicherheitsvorkehrungen im Unternehmen

Präventive Reaktionspläne sollten zum Standard mittelständischer Unternehmen gehören.

Sicherheitsprobleme treten in der Regel unerwartet auf. Oft sind die vorhandenen Informationen anfangs unzureichend, und trotzdem ist schnelles Handeln erforderlich, damit sich das Problem nicht zu einer Krise ausweitet. Umso mehr verwundert es, dass nur 22,1 Prozent aller Unternehmen über einen externen Sicherheits- oder Krisenberater verfügen, der eine schnelle Reaktion und professionelle Problembewältigung ermöglichen würde.

Gerade bei mittelständischen Unternehmen, die keine eigene Corporate Security[22)] besitzen, auf dem Weltmarkt aber den gleichen Gefahren und Bedrohungen ausgesetzt sind wie Konzerne, sollten zumindest präventive Reaktionspläne zum Standard gehören. Die wenigsten Unternehmen haben sich jedoch strukturierte Gedanken zu Ablauf und Reaktionsmöglichkeiten bei einem solchen Vorfall gemacht. Am häufigsten gibt es Sicherheitsstandards oder Notfallpläne für den Brandschutz (83,2 Prozent der befragten Unternehmen), die Arbeitssicherheit (66,3 Prozent) und die IT-Sicherheit (65,5 Prozent). Gerade das Fraud Management - also die klare Regelung von Zuständigkeiten oder periodischen Prüfungen zur Bekämpfung von Wirtschaftskriminalität - wäre wichtig. Es ist jedoch nur bei 4,4 Prozent der Unternehmen in Form eines Reaktionsplans oder von Standards festgelegt.

Für welche der folgenden Bereiche haben Sie Sicherheitsstandards definiert bzw. Notfallpläne erstellt?
(Mehrfachnennungen möglich)



GRAFIK 10 Quelle: Corporate Trust 2009

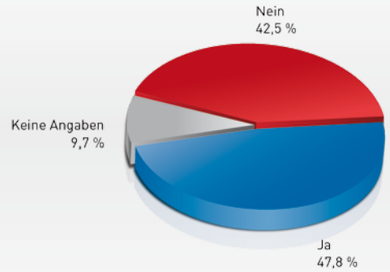
Unternehmen sichern sich noch zu wenig gegen die finanziellen Risiken ab.

Gerade für mittelständische Unternehmen ist es wichtig, zumindest gegen den finanziellen „Super-GAU" abgesichert zu sein. Bei Großschadensereignissen werden häufig Geschäftsprozesse beeinträchtigt. Nicht selten sind dann das Management oder wichtige Führungsverantwortliche fast ausschließlich mit diesem Vorfall beschäftigt, was weitere finanzielle Belastungen mit sich bringt.

Späht ein Konkurrent geheime Konstruktionspläne aus, manipuliert ein interner Täter die Buchhaltungsdaten oder wird ein Mitarbeiter auf einer Geschäftsreise entführt, kann dies unter Umständen zu einer finanziellen Schieflage führen. Die Kosten für einen Rückruf nach einer Produktkontamination - sei sie ungewollt oder von einem Kriminellen absichtlich herbeigeführt worden - können sehr schnell in die Millionen gehen. Veruntreut ein Mitarbeiter über Jahre Geld oder wird ein Unternehmen erpresst, handelt es sich in der Regel ebenfalls um hohe Summen.

Die Rückforderung des Geldes bedeutet oft einen langwierigen und schwierigen zivilrechtlichen Prozess - wenn überhaupt ein Täter ermittelt werden kann. Mittelständische Unternehmen sollten sich daher absichern, um durch solche Schäden nicht in einen finanziellen Engpass zu geraten. Leider haben nur 47,8 Prozent aller befragten Unternehmen entsprechende Versicherungen abgeschlossen.

Haben Sie für verschiedene Risiken, zum Beispiel Wirtschaftskriminalität, Industriespionage, Produktkontamination, Entführung oder Erpressung, eine Versicherung abgeschlossen, um das finanzielle Risiko zu vermindern?



GRAFIK 11 Quelle: Corporate Trust 2009

22) Corporate Security Bezeichnung für die Sicherheitsabteilung eines großen Konzerns, in der alle sicherheitsrelevanten Themen bearbeitet werden.

Risiken für den deutschen Mittelstand

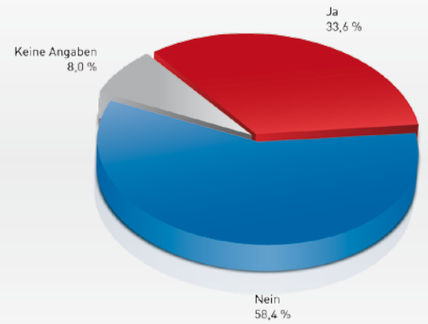
Risiken im Einzelnen

Das Risiko bei der Geschäftstätigkeit im Ausland wird zwar hoch eingeschätzt, die nötige Prävention unterbleibt aber allzu oft.

Etwa ein Drittel aller mittelständischen Unternehmen - exakt 33,6 Prozent - sind auch in sicherheitskritischen Ländern oder Krisenregionen vertreten, um dort fertigen zu lassen oder ihre Produkte zu verkaufen. In diesen Ländern besteht eine deutlich erhöhte Bedrohung. Die meisten Mittelständler wissen um diese Gefahr, treffen aber nicht die nötigen Vorkehrungen, um bei einem überraschend auftretenden Ereignis schnell reagieren zu können.

Zur professionellen Risikobewältigung bei einem Überfall auf einen Mitarbeiter, einer Entführung, einem Terroranschlag, einer Pandemie[23] oder der Explosion einer Produktionsstätte ist es erforderlich, sofort ein gut organisiertes Krisenmanagement durchzuführen. Unabdingbar dafür sind ein Krisenstab[24], in dem jeder seine Zuständigkeit genau kennt, klar definierte Verständigungswege und Erreichbarkeiten sowie eine vorbereitete Strategie für die Krisenkommunikation. Viele Mittelständler haben sich dieser Thematik noch nicht gestellt: Nur 17,7 Prozent verfügen tatsächlich über ein professionelles Krisenmanagement (siehe Seite 29, Grafik 17). 56,6 Prozent gaben an, dass Reisesicherheit für sie gar keine Rolle spielt (siehe Seite 26, Grafik 15). Die nötigen Sicherheitsstandards oder Notfallpläne für das Thema Krisenkommunikation haben sogar nur 9,7 Prozent der befragten Unternehmen geschaffen (siehe Seite 20, Grafik 10).

Sind Sie in sicherheitskritischen Ländern oder Krisenregionen präsent?



GRAFIK 12 Quelle: Corporate Trust 2009

23) Pandemie Länder- und kontinentübergreifende Ausbreitung einer Krankheit, im engeren Sinn einer Infektionskrankheit. Im Gegensatz zur Epidemie ist eine Pandemie somit nicht örtlich beschränkt.

24) Krisenstab Gruppe von Personen innerhalb einer Organisation zum Notfall- oder Katastrophenmanagement. Der Krisenstab selbst übernimmt nicht die Führung, sondern funktioniert nur unter einem führungserfahrenen und alleinverantwortlichen Leiter. Dies stellt sicher, dass auch unter hohem Druck Entscheidungen schnell getroffen und mit vereinten Kräften umgesetzt werden können.

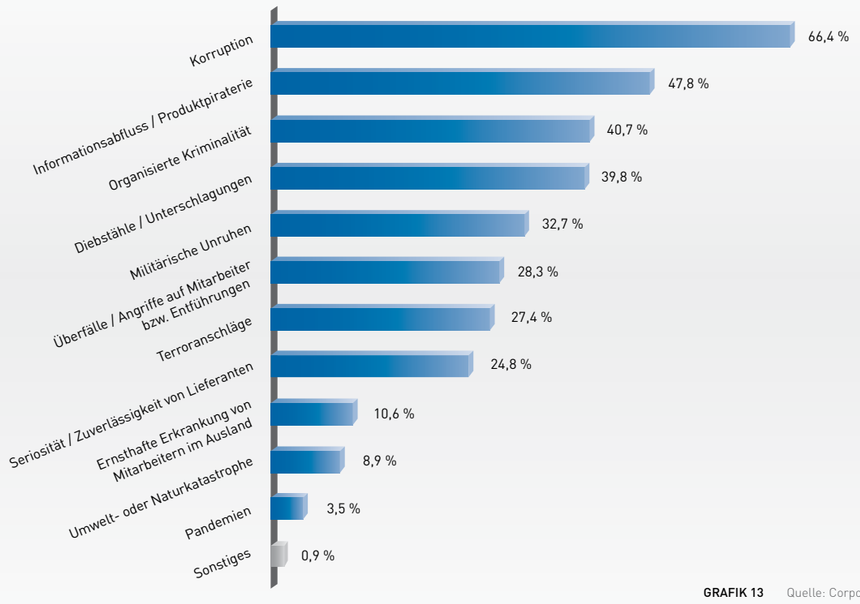
Risiken für den deutschen Mittelstand

Risiken im Einzelnen

Korruption, Industriespionage und die organisierte Kriminalität sind die größten Risiken im Ausland.

Es gibt eine Vielzahl krimineller Risiken im Ausland. Hier scheint vor allem die Korruption als größte Bedrohung eingeschätzt zu werden: 66,4 Prozent der Unternehmen nannten sie bei Geschäften im Ausland an erster Stelle. Auf den nächsten Plätzen folgten Informationsabfluss und Produktpiraterie[25] (47,8 Prozent aller Angaben) sowie organisierte Kriminalität[26] (40,7 Prozent). Am geringsten eingeschätzt wurde das Risiko einer Pandemie[27], einer Umwelt- oder Naturkatastrophe sowie einer ernsthaften Erkrankung eines Mitarbeiters im Ausland.

Wo sehen Sie die größten Risiken bei der Geschäftstätigkeit im Ausland? (Mehrfachnennungen möglich)



GRAFIK 13 Quelle: Corporate Trust 2009

Praxishinweis MAZARS Hemmelrath: Wir gehen davon aus, dass die globale Finanz- und Wirtschaftskrise insbesondere im Ausland zu erhöhten Sicherheitsrisiken führen wird. Eine Verschlechterung der wirtschaftlichen Rahmenbedingungen, verbunden mit potenziellen Restrukturierungsmaßnahmen, kann den Nährboden für wirtschaftskriminelle Handlungen bilden, da sowohl Motivation, Gelegenheit und Rechtfertigung in Verbindung mit der Angst vor dem Arbeitsplatzverlust bei den Betroffenen zu kriminellen Kurzschlusshandlungen führen können. Stellen Sie durch nachhaltig wirksame Maßnahmen sicher, dass in Ihren ausländischen Tochtergesellschaften die für einen reibungslosen Geschäftsbetrieb relevanten Bereiche wie Einkauf, Produktion, Vertrieb und interne Verwaltung auf sich rasch verändernde Rahmenbedingungen vorbereitet werden.

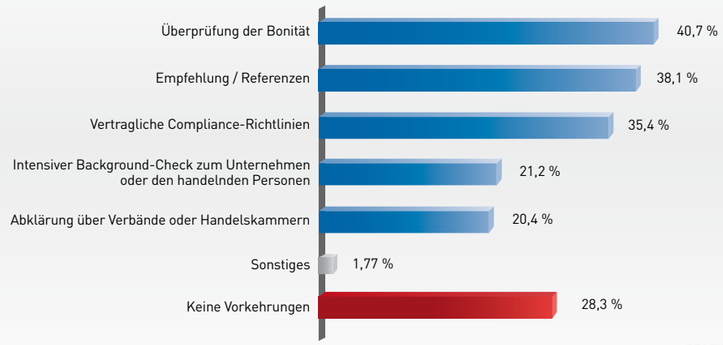
Sorgen Sie für Stabilität der Prozesse und der Kernteams, indem Sie regelmäßig und zeitnah über aktuelle Entwicklungen und Veränderungen im Geschäftsumfeld Ihrer Unternehmensgruppe informieren. Verstärken Sie das lokale Management durch regelmäßige Anwesenheit von Managementkapazitäten aus der Unternehmenszentrale.

MAZARS

Nur die wenigsten führen intensive Background-Checks durch.

Obwohl gerade Risiken wie Korruption, Informationsabfluss oder Produktpiraterie häufig im Zusammenhang mit den ausländischen Geschäftspartnern stehen, treffen nur die wenigsten Unternehmen ausreichende Vorsorge dagegen oder schaffen die nötigen Sicherheitsstrukturen. 28,3 Prozent aller Befragten bleiben sogar völlig untätig. Das scheint erstaunlich, zeigt aber, wie gering die Bedrohung eingeschätzt wird. Zwar überprüfen 40,7 Prozent der befragten Mittelständler die Bonität des ausländischen Geschäftspartners, aber nur ein gutes Fünftel durchleuchtet die Hintergründe des jeweiligen Unternehmens oder der handelnden Personen. Dabei würde ein solcher Background-Check[28] - ebenso wie vertraglich festgelegte Compliance-Richtlinien[29] - erheblich helfen, das Risiko bereits im Vorfeld geschäftlicher Beziehungen zu minimieren.

Welche Vorkehrungen haben Sie getroffen, um die Risiken mit internationalen Geschäftspartnern zu minimieren?
(Mehrfachnennungen möglich)



GRAFIK 14 Quelle: Corporate Trust 2009

Praxishinweis Taylor Wessing: In fremden Ländern kann der Unterschied zwischen Recht haben und Recht bekommen erhebliche Konsequenzen haben – achten Sie daher neben vertraglichen Regelungen zum Umgang mit Know-how sorgfältig auf die Auswahl Ihrer Geschäftspartner.

TaylorWessing

25) Produktpiraterie Das Geschäft mit Nachahmer-Waren, die mit dem Ziel hergestellt werden, einer Original-Ware zum Verwechseln ähnlich zu sein. Dabei werden Markenrechte oder wettbewerbsrechtliche Vorschriften verletzt. Häufig geht Produktpiraterie mit Verletzungen von Urheberrechten, Geschmacksmustern, Patenten und sonstigen Rechten des geistigen Eigentums und gewerblichen Rechtsschutzes einher.

26) Organisierte Kriminalität Von Gewinn- und/oder Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind. Von „organisiert" spricht man, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer zusammenwirken - unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen, unter Anwendung von Gewalt oder anderer einschüchternder Mittel oder unter Einflussnahme auf Politik, Massenmedien, öffentliche Verwaltung, Justiz oder Wirtschaft.

27) Pandemie Länder- und kontinentübergreifende Ausbreitung einer Krankheit, im engeren Sinn einer Infektionskrankheit. Im Gegensatz zur Epidemie ist eine Pandemie somit nicht örtlich beschränkt.

28) Background-Check Überprüfung von Mitarbeitern oder Geschäftspartnern bezüglich der Seriosität, Zuverlässigkeit, finanziellen Verhältnisse, etwaiger Firmenbeteiligungen oder sonstiger verdächtiger Lebensumstände.

29) Compliance Ein Verhaltenskodex für gesetzmäßiges, rechtskonformes und verantwortungsbewusstes Handeln im Unternehmen.

Risiken für den deutschen Mittelstand

Risiken im Einzelnen

Nur jedes zehnte Unternehmen trifft für die Mitarbeiter ausreichende Sicherheitsvorkehrungen für Geschäftsreisen ins Ausland.

Nach einer aktuellen Studie des Verbands Deutsches Reisemanagement e.V. (VDR-Geschäftsreiseanalyse 2008) fanden im Jahr 2007 insgesamt 166,6 Millionen Geschäftsreisen deutscher Unternehmen statt. Davon entfielen rund 14,8 Millionen auf Reisen ins Ausland mit Übernachtung. Im Schnitt sind das 40.660 Auslandsreisen täglich - in unterschiedlichste Länder, teilweise mit erhöhten Risiken oder ungewohnten Bedrohungen. Wer sich darauf nicht vorbereitet, läuft Gefahr, Opfer eines Überfalls, einer Entführung oder eines ungewollten Informationsabflusses zu werden.

56,6 Prozent der befragten Unternehmen gaben an, gar keine Sicherheitsvorkehrungen für Auslandsreisen zu treffen. Am häufigsten, in 15,0 Prozent aller Fälle, findet vor Reiseantritt wenigstens eine Bewertung der Sicherheitslage statt. Zur Vermeidung von Risiken sollten jedoch standardisierte Erreichbarkeiten im Notfall bekannt sein, ein Briefing der Geschäftsreisenden zum sicherheitsgerechten Verhalten durchgeführt oder ein Merkblatt mit Informationen zur Sicherheitslage im jeweiligen Land ausgehändigt werden. Leider werden diese wichtigen Sicherheitsstandards nicht einmal von jedem zehnten mittelständischen Unternehmen berücksichtigt.

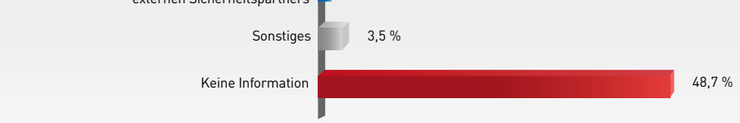
Gibt es in Ihrem Unternehmen einen standardisierten Prozess für Auslandsreisen, um die Sicherheit der Geschäftsreisenden zu erhöhen? (Mehrfachnennungen möglich)

GRAFIK 15 Quelle: Corporate Trust 2009

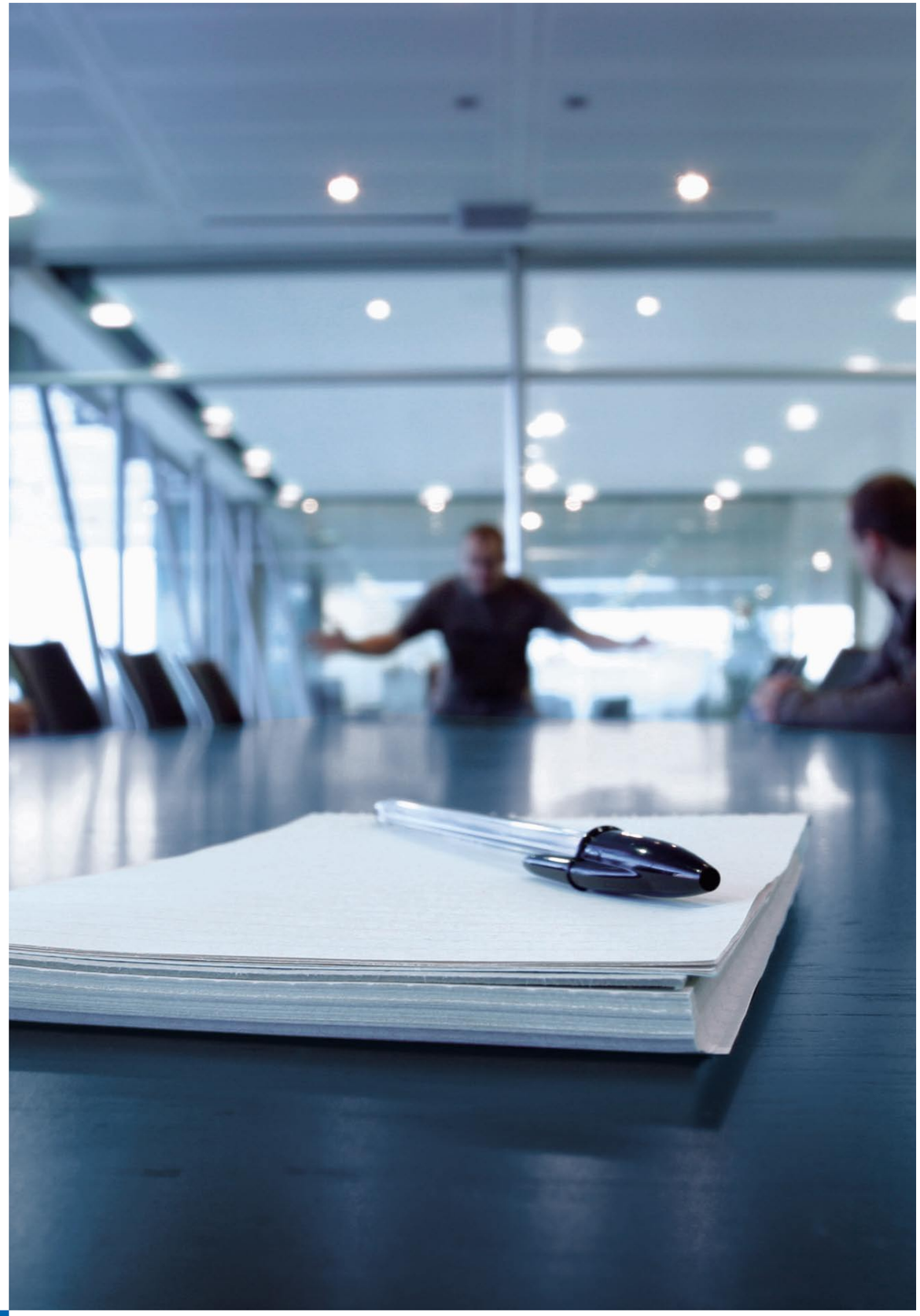
Für die Geschäftsreisenden gibt es meist keine qualifizierten Länderinformationen zur Sicherheitslage.

Die Sicherheitslage in einem Land kann sich jederzeit ändern. Auch bei häufig besuchten Regionen ist es deshalb ratsam, sich jeweils vor Reisebeginn über die aktuelle Situation zu informieren. Hinweise auf aktuelle Feiertage, politische Entwicklungen, geplante Demonstrationen oder Großveranstaltungen vor Ort sind ebenfalls wichtig, um das Verhalten entsprechend anzupassen und gegebenenfalls bestimmte Örtlichkeiten oder Transportmittel zu meiden. Die meisten Unternehmen versehen Ihre Mitarbeiter - wenn überhaupt - nur mit den Sicherheitsinformationen des Auswärtigen Amtes. Diese sind zwar sinnvoll, spiegeln das tatsächliche Risiko aber nur bedingt wider. Insbesondere enthalten sie keine detaillierten Angaben zu bestimmten Regionen, den Business-Metropolen bzw. bestimmten Transportmitteln oder Hotels vor Ort. Diesen Service liefern in der Regel nur Spezialanbieter. Mittelständische Unternehmen greifen jedoch nur erschreckend selten - nämlich in 1,8 Prozent der Fälle - auf diese Informationen zurück.

Welche Informationen erhalten Ihre Mitarbeiter vor Reiseantritt zur entsprechenden Sicherheitslage des jeweiligen Landes?



GRAFIK 16 Quelle: Corporate Trust 2009



Risiken für den deutschen Mittelstand

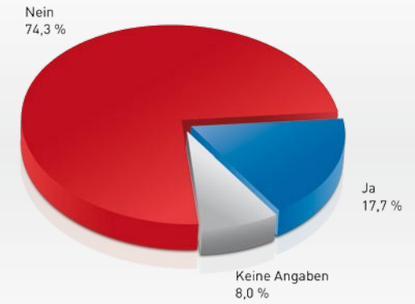
Risiken im Einzelnen

Im Mittelstand gibt es nur selten ein professionelles Krisenmanagement, externe Krisenberater oder eine vorbereitete Krisenkommunikation.

Krisenmanagement bedeutet den systematischen Umgang mit Krisensituationen. Dazu gehören neben der Identifikation und Analyse der jeweiligen Risiken auch ein Notfallplan, die Benennung der Mitglieder im Krisenstab sowie präventive Vorkehrungen. Diese präventiven Maßnahmen sollten zum Beispiel ein regelmäßiges Krisenstabstraining, eine Notfall-Hotline oder eine Strategie für die Krisenkommunikation umfassen.

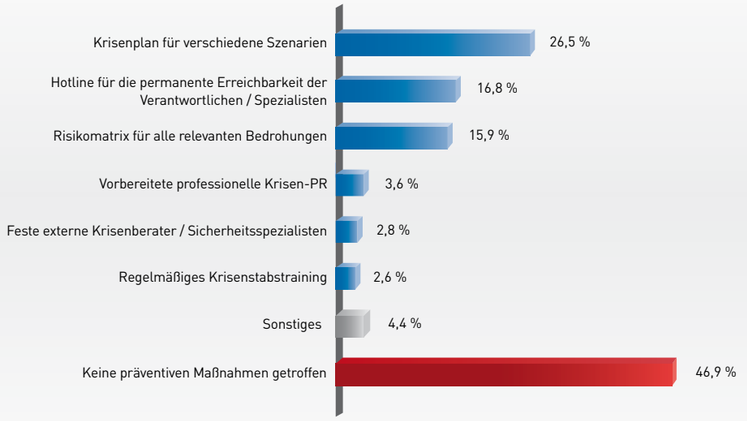
Nur 17,7 Prozent der befragten Mittelständler gaben an, über ein professionelles Krisenmanagement zu verfügen. Fast die Hälfte aller Unternehmen - exakt 46,9 Prozent - hat keinerlei präventive Vorkehrungen getroffen. Immerhin ein gutes Viertel verfügt zumindest über einen Krisenplan für verschiedene Szenarien.

Haben Sie professionelles Krisenmanagement?



GRAFIK 17 Quelle: Corporate Trust 2009

Welche präventiven Maßnahmen haben Sie sonst getroffen, um auf Krisenfälle vorbereitet zu sein?
(Mehrfachnennungen möglich)



GRAFIK 18 Quelle: Corporate Trust 2009

Risiken für den deutschen Mittelstand

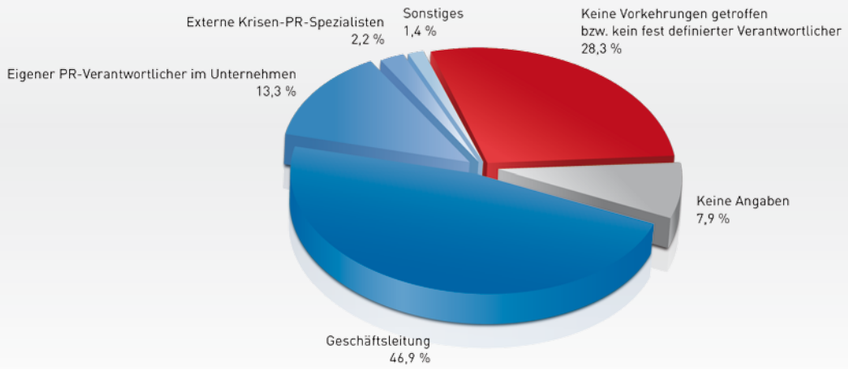
Risiken im Einzelnen

Unbedachte Aussagen in Krisensituationen können zu Imageschäden führen.

Es fällt auf, dass im Gegensatz zu den meisten Konzernen nur 2,8 Prozent aller mittelständischen Unternehmen frühzeitig über eine unternehmensbedrohende Sicherheitskrise nachdenken und daher feste Strukturen zu einem externen Krisenberater oder Sicherheitsspezialisten aufbauen. Sich erst im Notfall entsprechende Gedanken zu machen, reicht nicht aus: Die Krise kann sich dann sehr schnell ausweiten, häufig auch aufgrund fehlender professioneller Kommunikation. Die Befragung zeigte, dass nur 3,6 Prozent aller Mittelständler über eine vorbereitete professionelle Krisen-PR[30] verfügen. Wo solche Vorkehrungen fehlen, können unbedachte Aussagen schnell den Eindruck von Überforderung, schlechtem Management oder sogar Hilflosigkeit wecken und damit das Image des Unternehmens beschädigen.

Auf die Frage nach Vorkehrungen und Zuständigkeiten für die Krisenkommunikation wurde zu 46,9 Prozent die Geschäftsleitung als verantwortliche Stelle benannt. Anscheinend wird dem Geschäftsführer oder Vorstand per se zugetraut, die Mechanismen der öffentlichen Berichterstattung bei Krisenszenarien ausreichend zu beherrschen, um einen Reputationsschaden abzuwehren. Nur 13,3 Prozent haben einen eigenen PR-Verantwortlichen im Unternehmen, lediglich 2,2 Prozent haben einen externen Spezialisten für die Krisenkommunikation verpflichtet. 28,3 Prozent sind völlig unvorbereitet und wären bei einem überraschend auftretenden Vorfall wahrscheinlich überfordert.

Welche Vorkehrungen haben Sie getroffen, um bei einem Großschadensereignis oder Krisenfall möglichst professionell Öffentlichkeitsarbeit zu betreiben, bzw. wer übernimmt bei einem Krisenfall die Kommunikation mit den Medien?



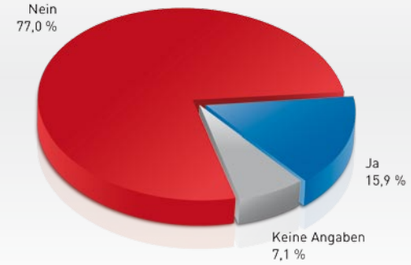
GRAFIK 19 Quelle: Corporate Trust 2009

Nur die wenigsten Unternehmen verfügen über eine Struktur zur professionellen Bekämpfung von Wirtschaftskriminalität.

Die Vorsorge gegen Wirtschaftskriminalität wird nicht nur im Ausland vernachlässigt - es gibt generell zu wenig Schutzvorkehrungen und standardisierte Mechanismen, um dolose Handlungen zu vermeiden oder frühzeitig zu erkennen. Nur 15,9 Prozent aller Unternehmen verfügen über eine Compliance-Abteilung oder eine eigene Struktur zur Bekämpfung von Wirtschaftskriminalität. Hinweise auf kriminelle Handlungen von Mitarbeitern, Kunden oder Geschäftspartnern gehen wahrscheinlich in den meisten Fällen unter - oder es gibt niemanden im Unternehmen, der die „Red flags"[31] oder Verdachtsmomente professionell verfolgen kann.

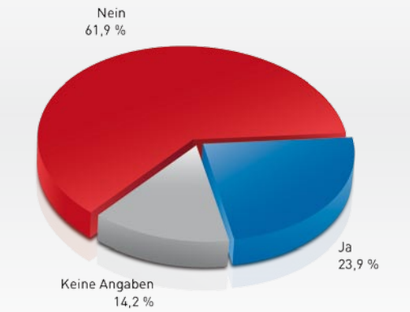
In der Regel ist auch das Management nicht in der Lage, die „Red flags" für Wirtschaftskriminalität zu erkennen. Lediglich 23,9 Prozent der Unternehmen glauben, dass ihre Führungsverantwortlichen genügend sensibilisiert sind, um kriminelle Handlungen von Mitarbeitern frühzeitig zu erkennen. Genau dies würde aber helfen, Delikte zu verhindern oder zumindest die finanziellen Schäden in Grenzen zu halten.

Gibt es im Unternehmen eine Compliance-Abteilung bzw. eine eigene Struktur zur Bekämpfung von Wirtschaftskriminalität, um Hinweise auf dolose Handlungen von Mitarbeitern, Kunden oder Geschäftspartnern professionell zu verfolgen?



GRAFIK 20 Quelle: Corporate Trust 2009

Sind Ihre Führungsverantwortlichen zum Erkennen von „Red flags" für Wirtschaftskriminalität sensibilisiert, um kriminelle Mitarbeiter möglichst früh zu erkennen?



GRAFIK 21 Quelle: Corporate Trust 2009

30) Krisen-PR Unter Krisen-PR oder Krisenkommunikation versteht man jenes Teilgebiet der Öffentlichkeitsarbeit, das sich mit der Information und Kommunikation in Krisensituationen beschäftigt.

31) Red flags Auffälligkeiten im Verhalten von Mitarbeitern oder Vorgesetzten, die auf kriminelle Machenschaften hindeuten könnten.

Risiken für den deutschen Mittelstand

Risiken im Einzelnen

Auch Compliance-Richtlinien, Whistle-Blowing-Systeme oder Fachseminare für die Revision gibt es nur selten.

Obwohl Wirtschaftskriminalität jedes Jahr finanzielle Schäden in Milliardenhöhe in der deutschen Wirtschaft anrichtet, sind die Vorkehrungen gerade im Mittelstand sehr unzureichend. Am häufigsten - nämlich bei 34,5 Prozent der Unternehmen - gibt es noch spezielle Regelungen in den Geschäfts- oder Arbeitsverträgen, um das Risiko zu vermeiden. 19,5 Prozent vertrauen zumindest auf eine ganzheitliche Compliance-Richtlinie im Unternehmen, und bei 18,6 Prozent aller Firmen gibt es standardisierte Prüfungen nach Auffälligkeiten im Rahmen des Internen Kontrollsystems (IKS).

Leider verfügen lediglich 1,8 Prozent aller antwortenden Unternehmen über eine eigene Fraud-Management-Struktur und nur 5,3 Prozent über ein Whistle-Blowing-System[32], das es Mitarbeitern, Geschäftspartnern oder Kunden ermöglichen würde, anonyme Hinweise auf kriminelles Verhalten zu geben.

Welche Maßnahmen wurden konkret im Unternehmen getroffen, um Wirtschaftskriminalität zu verhindern?
(Mehrfachnennungen möglich)

GRAFIK 22 Quelle: Corporate Trust 2009

Praxishinweis MAZARS Hemmelrath: Installieren Sie unternehmensweit ein effektives Enterprise Risk Management (ERM), um Risiken zu minimieren. Dabei sollten Leitlinien entwickelt werden, welche den Mitarbeitern in alltäglichen Situationen Hilfestellung und klare Handlungsprämissen geben. Durch einen eindeutig formulierten und durchgesetzten Verhaltenskodex muss den Mitarbeitern bewusst werden, dass wirtschaftskriminelle Handlungen im Unternehmen konsequent verfolgt und geahndet werden.

Wir empfehlen Unternehmen, ein praktikables Hinweisgebersystem sowie eine monatliche „Sprechstunde" auf oberster Managementebene einzurichten. Unserer Erfahrung nach hat sich diese Vorgehensweise bewährt, denn über 60 Prozent aller erkannten Delikte werden aufgrund von internen Hinweisen aufgedeckt.

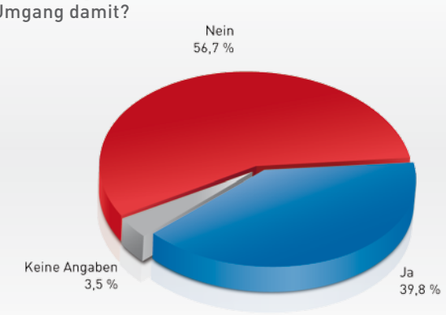
MAZARS

Mehr als die Hälfte aller Unternehmen macht ihren Mitarbeitern oder Geschäftspartnern keine klaren Vorgaben für den Umgang mit vertraulichen Informationen, Daten oder Dokumenten.

Nur wer weiß, wie Informationen zu klassifizieren sind, damit sie vertraulich behandelt werden, kann entsprechend sensibel damit umgehen. In jedem Unternehmen sollte es daher eine Anweisung geben, welche Informationen, Daten oder Dokumente vertraulich, geheim oder offen verwendet werden können und wie sie jeweils zu kennzeichnen sind. Leider erfüllt weniger als die Hälfte aller befragten Unternehmen - genau 39,8 Prozent - diese wichtige Voraussetzung für Informationsschutz.

Die höchste Klassifizierung „Geheim" sollte dabei nur für Daten oder Informationen vergeben werden, bei denen es sich um die „Kronjuwelen" des Unternehmens handelt. Je häufiger ein solches Prädikat leichtfertig, überflüssig oder bei nicht wirklich sensiblen Informationen verwendet wird, um so höher ist die Gefahr, dass Mitarbeiter die Schutzmaßnahmen als unwichtig empfinden und daher nicht einhalten. Für sie ist der Sinn nicht mehr nachvollziehbar. Daher sollte auf eine strikte Beschränkung von „Geheim"- oder „Vertraulich"-Vermerken geachtet werden und diese sollten nur, wenn es tatsächlich erforderlich ist, vergeben werden.

Gibt es genau definierte Vorgaben im Unternehmen für die Klassifizierung der Geheimhaltungsstufe von Informationen, Daten und Dokumenten sowie für den Umgang damit?

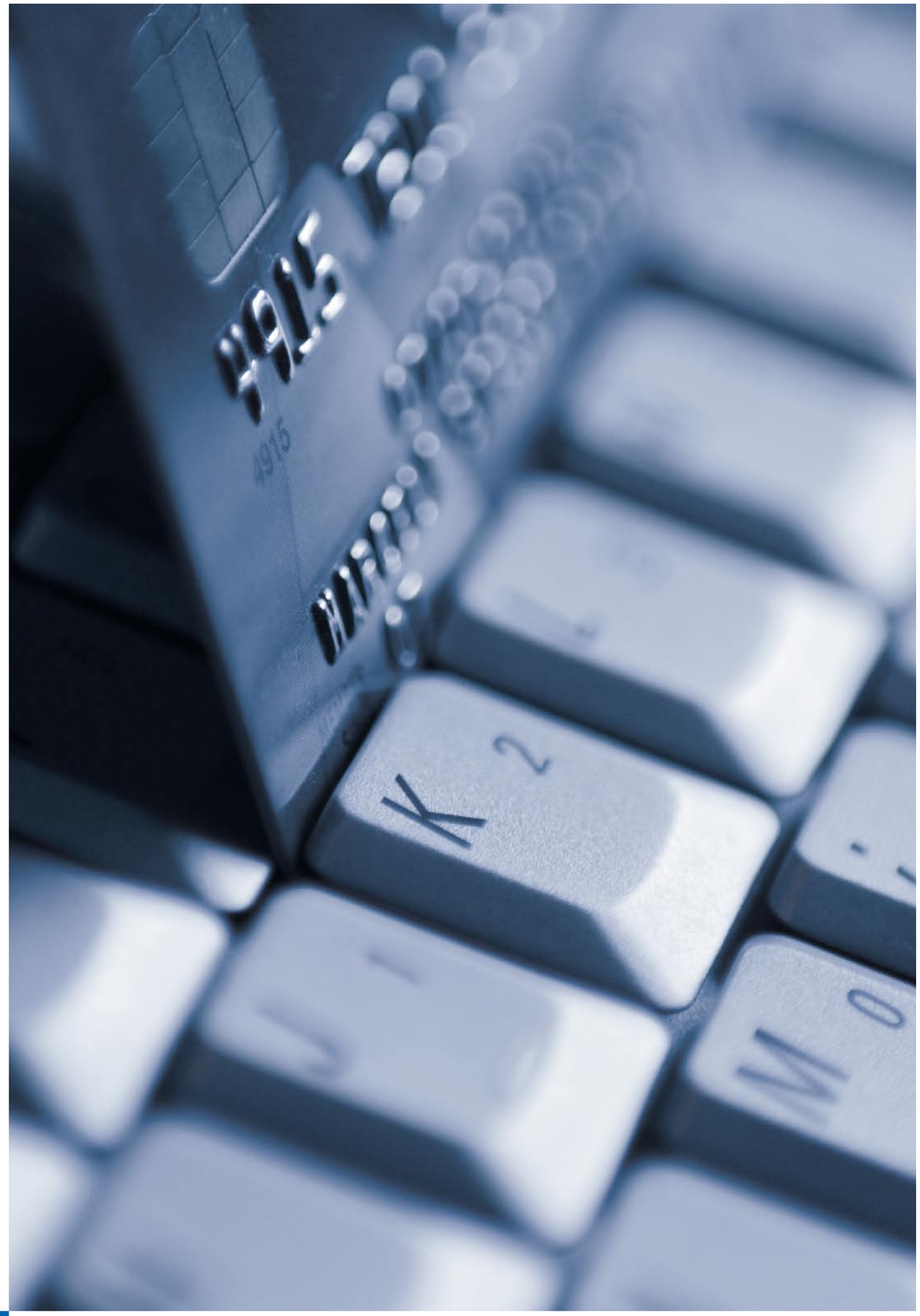


GRAFIK 23 Quelle: Corporate Trust 2009

Praxishinweis RSA: Informationen sind das wichtigste Kapital eines Unternehmens und müssen entsprechend geschützt werden. Dabei sind natürlich nicht alle Informationen gleich wichtig. Die im Unternehmen vorhandenen Informationen sollten deshalb erfasst und nach Geschäftsrelevanz klassifiziert werden. Diese Analyse ist die Basis für die Definition einer neuen Sicherheitsleitlinie und Policies, welche auch die zu ergreifenden Maßnahmen enthalten. Um stets auf dem höchsten Sicherheitsstandard zu sein, müssen sowohl die Policies als auch die Schutzmaßnahmen laufend kontrolliert und den sich ändernden Gegebenheiten angepasst werden.

RSA
The Security Division of EMC

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



Risiken für den deutschen Mittelstand

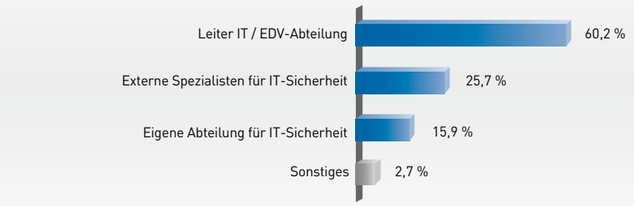
Risiken im Einzelnen

Für die EDV, als elektronische Nabelschnur der Geschäftsprozesse, gibt es häufig keine ausreichend strukturierten Sicherheitsvorkehrungen.

Der Informationsschutz in mittelständischen Unternehmen wird oft ausschließlich als EDV-Aufgabe verstanden und liegt deshalb in der Zuständigkeit der IT-Verantwortlichen. Viele Unternehmen legen jedoch ihr Hauptaugenmerk bei der IT auf die Verfügbarkeit von Daten, weniger auf die bestmögliche Absicherung gegen unberechtigte Zugriffe. Es hat sich daher schon mehrfach gezeigt, dass nicht jeder IT-Verantwortliche automatisch auch ein guter IT-Sicherheitsspezialist ist.

Ein illegaler Zugriff und damit der Abfluss von Informationen kann ebenso von innen erfolgen wie von außen. Das eigene Know-how und die Sicherheit der Daten und Informationen sind dadurch in Gefahr. Trotzdem verfügen nur 15,9 Prozent der Unternehmen über eine eigene Abteilung für IT-Sicherheit. Bei 60,2 Prozent gibt es ausschließlich einen Leiter der IT- bzw. EDV-Abteilung.

Wer ist in Ihrem Unternehmen für die IT-Sicherheit verantwortlich?
(Mehrfachnennungen möglich)



GRAFIK 24 Quelle: Corporate Trust 2009

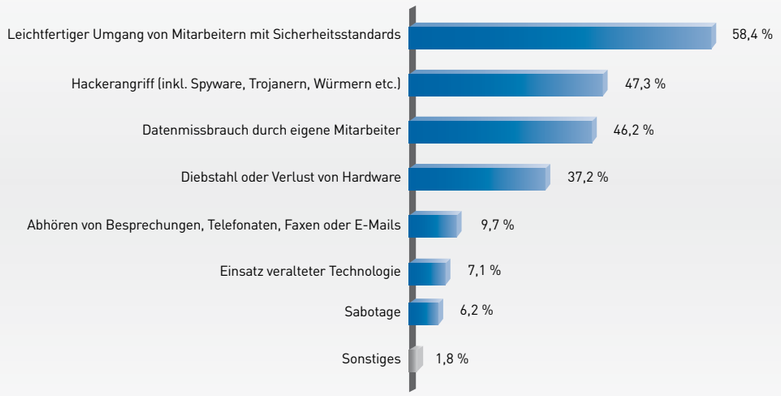
Risiken für den deutschen Mittelstand

Risiken im Einzelnen

Eigene Mitarbeiter stellen das größte Risiko für die IT-Sicherheit und den Informationsabfluss dar.

58,4 Prozent der befragten Unternehmen gaben an, dass der leichtfertige Umgang ihrer Mitarbeiter mit Sicherheitsstandards die größte Bedrohung für die Sicherheit der IT oder Telekommunikation ist. Auf Platz zwei folgen Hackerangriffe mit 47,3 Prozent und an dritter Stelle der böswillige Datenmissbrauch durch eigene Mitarbeiter mit 46,2 Prozent. Da Diebstahl und Verlust von Hardware - mit 37,2 Prozent an vierter Stelle genannt - ebenfalls durch das Personal verursacht werden können, ergibt sich als Fazit, dass die eigenen Mitarbeiter insgesamt das größte Risiko für die Sicherheit von IT und Telekommunikation darstellen.

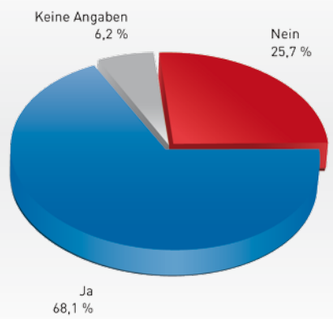
Wo sehen Sie die größten Bedrohungen für die Sicherheit Ihrer IT und Telekommunikation?
(Mehrfachnennungen möglich)



GRAFIK 25 Quelle: Corporate Trust 2009

Gerade weil die Mitarbeiter eine so große Bedrohung für die Sicherheit von Informationen darstellen, sei es vorsätzlich oder aus Leichtsinn, muss es standardisierte Prozesse im Unternehmen geben, die Datenmissbrauch verhindern oder zumindest sofort aufzeigen. Dazu gehört, dass Datenzugriffe protokolliert und stichpunktartig nach Auffälligkeiten gescreent werden. Mittelständische Unternehmen scheinen sich dessen in hohem Maße bewusst zu sein: Beachtliche 68,1 Prozent der Unternehmen gaben an, sämtliche Datenzugriffe aufzuzeichnen.

Werden sämtliche Datenzugriffe im Unternehmen protokolliert?

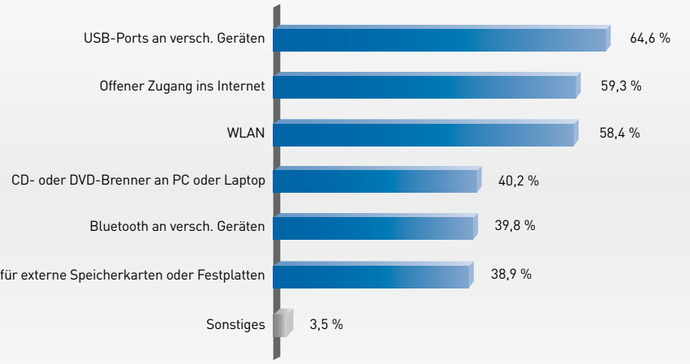


GRAFIK 26 Quelle: Corporate Trust 2009

Offene Zugänge ins Internet bzw. ungehinderte Möglichkeiten der Datenspeicherung eröffnen viele Gelegenheiten für Datenmissbrauch.

Ein schneller Datenaustausch und allzeit verfügbare Informationen gelten heute als wesentliche Voraussetzungen für erfolgreiche Geschäftsprozesse. Die Möglichkeiten der modernen IT lassen sich aber auch für kriminelle Zwecke missbrauchen. Je leichter Mitarbeiter die Daten, auf die sie ungehinderten Zugriff haben, auf eine CD, DVD oder einen USB-Stick kopieren bzw. über den freien Zugang ins Internet nach außen transferieren können, desto höher ist das Risiko. 64,6 Prozent der mittelständischen Unternehmen verfügen an verschiedenen Geräten über einen USB-Port, an den Mitarbeiter problemlos einen Stick anschließen können. Immer noch fast 60 Prozent ermöglichen ihren Mitarbeitern den freien Zugang ins Internet, und genau 58,4 Prozent haben WLAN im Unternehmen.

Welche Möglichkeiten der Datenspeicherung bzw. des Datenaustausches gibt es für Ihre Mitarbeiter durch die Hard- und Software? (Mehrfachnennungen möglich)



GRAFIK 27 Quelle: Corporate Trust 2009

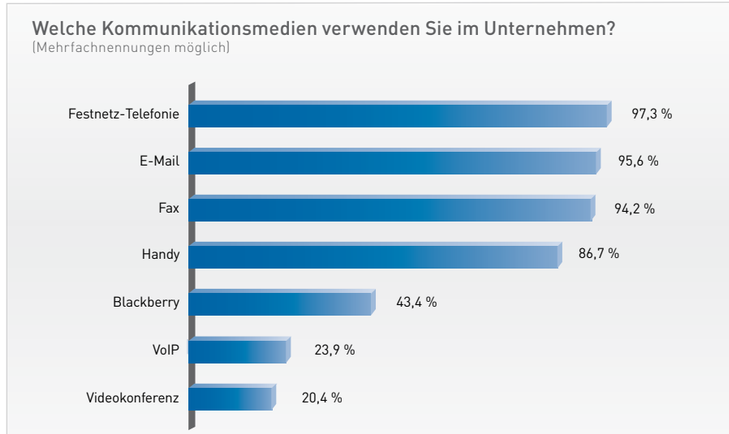
Risiken für den deutschen Mittelstand

Risiken im Einzelnen

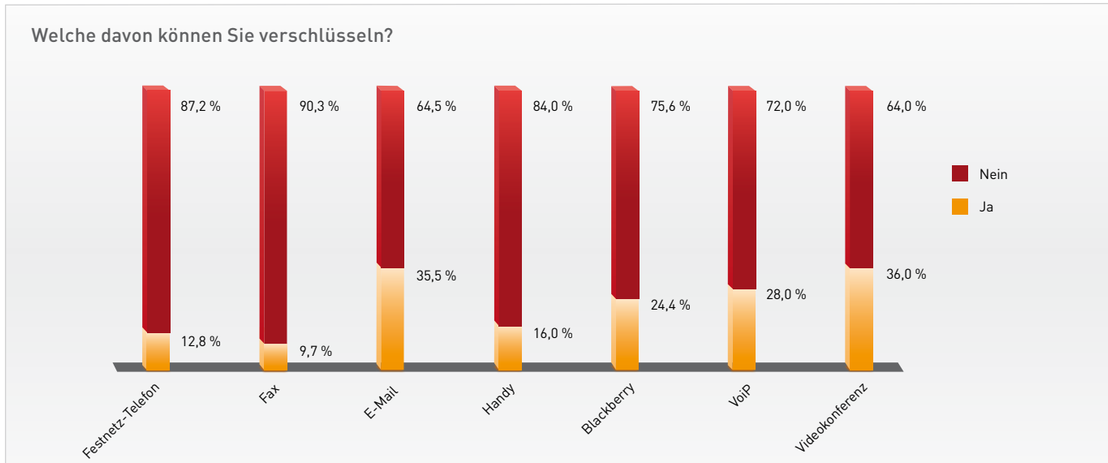
Kommunikation wird in den wenigsten Fällen verschlüsselt. Dadurch können vertrauliche Daten oder Gespräche leicht in falsche Hände geraten.

Die Kommunikation eines Unternehmens findet heute über unterschiedlichste Medien statt: E-Mails werden von einem PC zum anderen, auf einen Laptop oder mobil auf einen Blackberry versandt. Bei der Telekommunikation kommen herkömmliche Festnetz-Telefone und Faxgeräte noch genauso zum Einsatz wie Mobiltelefone, Blackberrys oder Voice over IP (VoIP), also Gespräche über Datenleitungen oder das Internet. Auch Videokonferenzen werden in Zeiten der Finanz- und Wirtschaftskrise immer häufiger geführt, weil die mittelständischen Unternehmen bei den Geschäftsreisen sparen. Obwohl fast alle Unternehmen auf eine Vielzahl von Kommunikationsmöglichkeiten zurückgreifen, werden nur die wenigsten Wege sicher verschlüsselt, um einen Informationsabfluss auszuschließen.

Mit 97,3 Prozent ist die Festnetz-Telefonie der am meisten genutzte Kommunikationsweg. Trotzdem verfügen nur 12,9 Prozent der Unternehmen über eine Verschlüsselungsmöglichkeit. Beim E-Mail-Verkehr - mit 95,6 Prozent das zweitwichtigste Kommunikationsmedium - haben immerhin 35,5 Prozent die Möglichkeit der Verschlüsselung.



GRAFIK 28 Quelle: Corporate Trust 2009



GRAFIK 29 Quelle: Corporate Trust 2009

Risiken für den deutschen Mittelstand

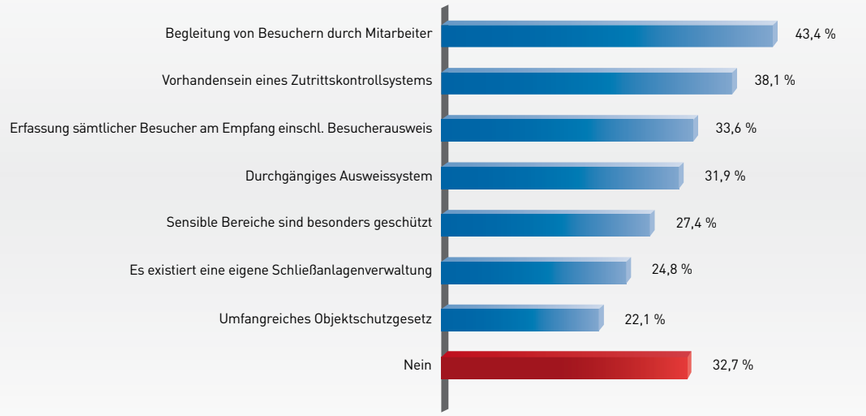
Risiken im Einzelnen

Die Objektsicherheit bzw. der Schutz vor ungehindertem Zugang ins Unternehmen scheint auch im Mittelstand einen relativ hohen Stellenwert zu genießen.

Rund ein Drittel der Mittelständler kann nicht sagen, wer sich gerade in ihrem Unternehmen aufhält. Die große Mehrzahl hat jedoch Schutzvorkehrungen getroffen, um Mitarbeiter, Maschinen, Produkte, Daten und Informationen vor unberechtigten Dritten zu schützen. 43,4 Prozent lassen jeden Besucher von einem Mitarbeiter begleiten, immerhin 38,1 Prozent verfügen über ein Zutrittskontrollsystem, und 33,6 Prozent erfassen jeden Besucher am Empfang.

Dies zeigt, dass die Sicherheit der Gebäude, der darin arbeitenden Mitarbeiter sowie der Sachwerte und Informationen von den Unternehmen als sehr wichtig eingestuft wird. Ein Zaun, eine Absperrung oder ein Drehkreuz demonstrieren unübersehbar Sicherheit, weil solche Barrieren den Zugang wirkungsvoll begrenzen. Das vermittelt subjektiv ein gutes Gefühl, aber davon sollte man sich nicht täuschen lassen: Im Konzept einer umfassenden Unternehmenssicherheit stellt die Objekt- oder Gebäudesicherheit nur einen Teilbereich dar.

Wissen Sie zu jeder Zeit, wer sich im Unternehmen aufhält, um die personelle und organisatorische Sicherheit gewährleisten zu können? (Mehrfachnennungen möglich)



GRAFIK 30 Quelle: Corporate Trust 2009

Praxishinweis RSA: Die physikalische Authentifizierung von Personen im Unternehmen ist wichtig und richtig. Umfassende Sicherheit genießt jedoch nur das Unternehmen, das auch den Zugang zu seinen IT-Systemen durch eine Authentifizierung schützt und den Zugriff auf die Daten durch ein Rechte-Management regelt. Das individuelle Anforderungsprofil des Benutzers entscheidet welche Authentifizierungsmöglichkeiten zum Einsatz kommen. Dies können Einmal-Passwort (OTP) über Token, zertifikatsbasierte oder auch eine wissensbasierte Authentifizierung sein. Durch ein Log-Management-System wird protokolliert und ausgewertet wer, wann auf was zugreift, um Sicherheitsvorfällen in Echtzeit schnell entgegenwirken zu können.

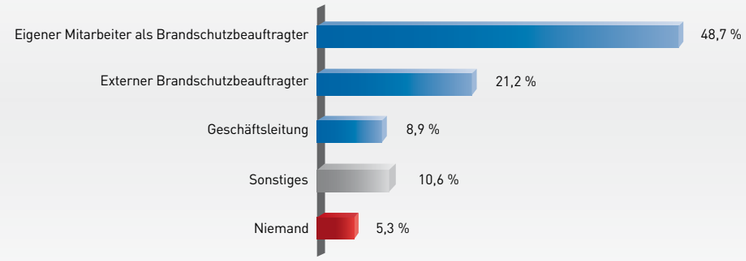
RSA
The Security Division of EMC

In aller Regel gibt es Verantwortlichkeiten und ausreichende Vorkehrungen im Unternehmen, um bei einem Brand oder sonstigen Gefahren möglichst schnell Alarm auszulösen und größeren Schaden abzuwenden.

Nur 5,3 Prozent der Unternehmen verzichten auf regelmäßige Brandschutzbegehungen und die erforderliche Dokumentation. Alle anderen mittelständischen Unternehmen haben Verantwortlichkeiten definiert und erfüllen ihre gesetzlich vorgeschriebenen Pflichten. Am häufigsten - mit 48,7 Prozent - ist ein eigener Mitarbeiter für den Brandschutz zuständig. Externe Brandschutzbeauftragte kommen bei 21,2 Prozent der Firmen zum Einsatz. Die Geschäftsleitung wurde nur von 8,9 Prozent als verantwortlich für die Brandschutzbegehungen genannt.

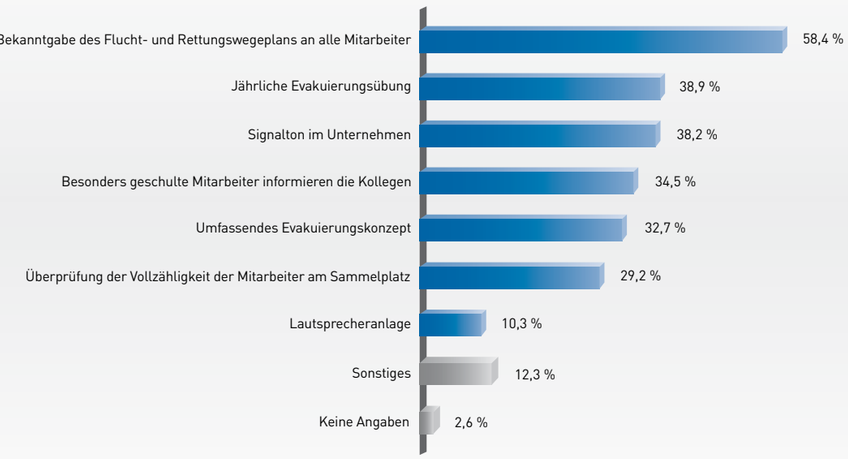
Auch die Evakuierung[33] des Unternehmens bei einem Feuer, einer Bombendrohung oder einem sonstigen Großschadensfall wird - im Gegensatz zu anderen Risiken - meist überproportional gut gemeistert. 58,4 Prozent haben den Flucht- und Rettungswegeplan allen Mitarbeiter bekannt gemacht, erfreuliche 38,9 Prozent führen eine jährliche Evakuierungsübung durch. Weitere 38,2 Prozent verfügen über ein akustisches Warnsignal im Unternehmen.

Wer führt die gesetzlich vorgeschriebenen Brandschutzbegehungen sowie die erforderliche Dokumentation durch?



GRAFIK 31 Quelle: Corporate Trust 2009

Wie evakuieren Sie Ihr Unternehmen im Gefahrenfall bzw. welche Sicherheitsvorkehrungen gibt es?
(Mehrfachnennungen möglich)



GRAFIK 32 Quelle: Corporate Trust 2009

33) Evakuierung Die Räumung eines Gebäudes oder Gebiets von Menschen.

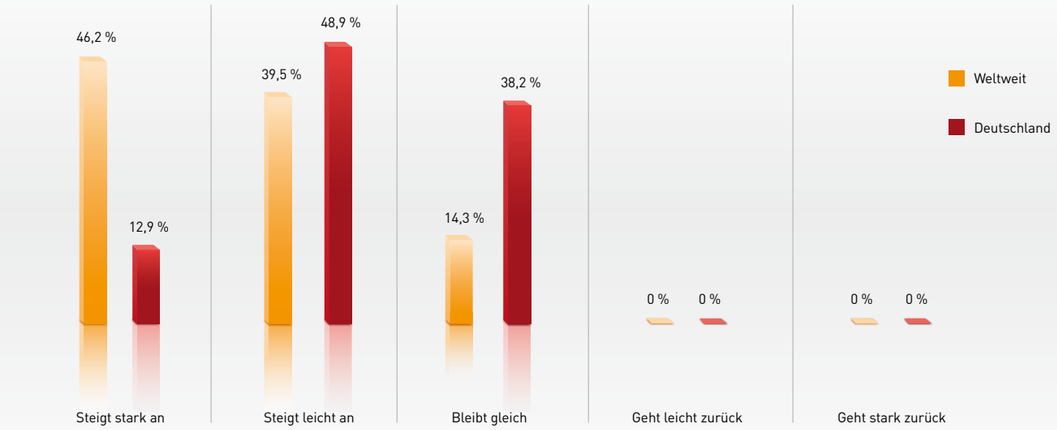
Risiken für den deutschen Mittelstand

Einschätzung der zukünftigen Bedrohung

Das weltweite Risiko durch Kriminalität wird steigen.

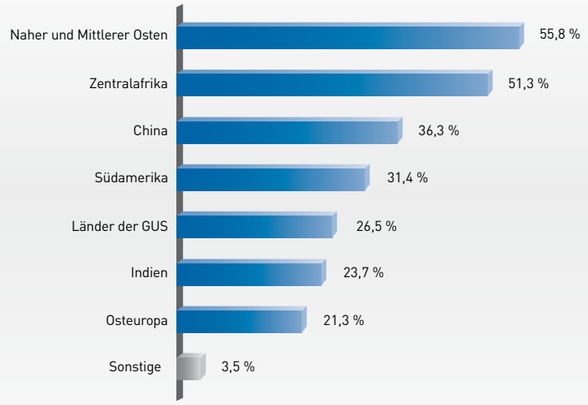
Die überwiegende Mehrzahl der mittelständischen Unternehmen unterhält Geschäftsbeziehungen im Ausland. In vielen Regionen existiert ein erhöhtes Risiko für die unterschiedlichsten Bedrohungen. Die zukünftige Bedrohung durch Kriminalität, Naturkatastrophen, Pandemien oder Großschadensereignisse wird daher von den meisten Mittelständlern für das Ausland deutlich höher eingeschätzt als für Deutschland selbst.

Wie ist Ihre Einschätzung für die zukünftige Entwicklung von Sicherheitsrisiken in Deutschland und weltweit ?



GRAFIK 33 Quelle: Corporate Trust 2009

In welchen Regionen drohen aus Ihrer Sicht zukünftig die größten Risiken durch politische Unruhen, Bürgerkriege oder Instabilität der Länder?
(Mehrfachnennungen möglich)



GRAFIK 34 Quelle: Corporate Trust 2009

Ziemlich genau ein Drittel der befragten Unternehmen - 33,6 Prozent - ist auch in Krisenregionen oder sicherheitskritischen Ländern unterwegs (vgl. Seite 23, Grafik 12). Diese Mittelständler haben in der Regel bereits Erfahrungen mit den unterschiedlichen Kriminalitätsformen und länderspezifischen Bedrohungen gemacht. Befragt nach ihrer Einschätzung, in welchen Regionen künftig die größten Risiken durch politische Unruhen, Bürgerkriege oder Instabilität der Länder bestehen, gaben die meisten Unternehmen - exakt 55,8 Prozent - den Nahen und Mittleren Osten als wahrscheinlichen Hauptbrennpunkt an. Auch von Zentralafrika (51,3 Prozent) und China (36,3 Prozent) nimmt man an, dass sie in Zukunft sicherheitskritisch sein werden.

Risiken für den deutschen Mittelstand

Einschätzung der zukünftigen Bedrohung

Die zukünftige Bedrohung durch Kriminalität, Natur- bzw. Umweltkatastrophen, Pandemien, Brände oder Explosionen wird für das eigene Unternehmen in Deutschland überwiegend höher eingeschätzt als im Ausland.

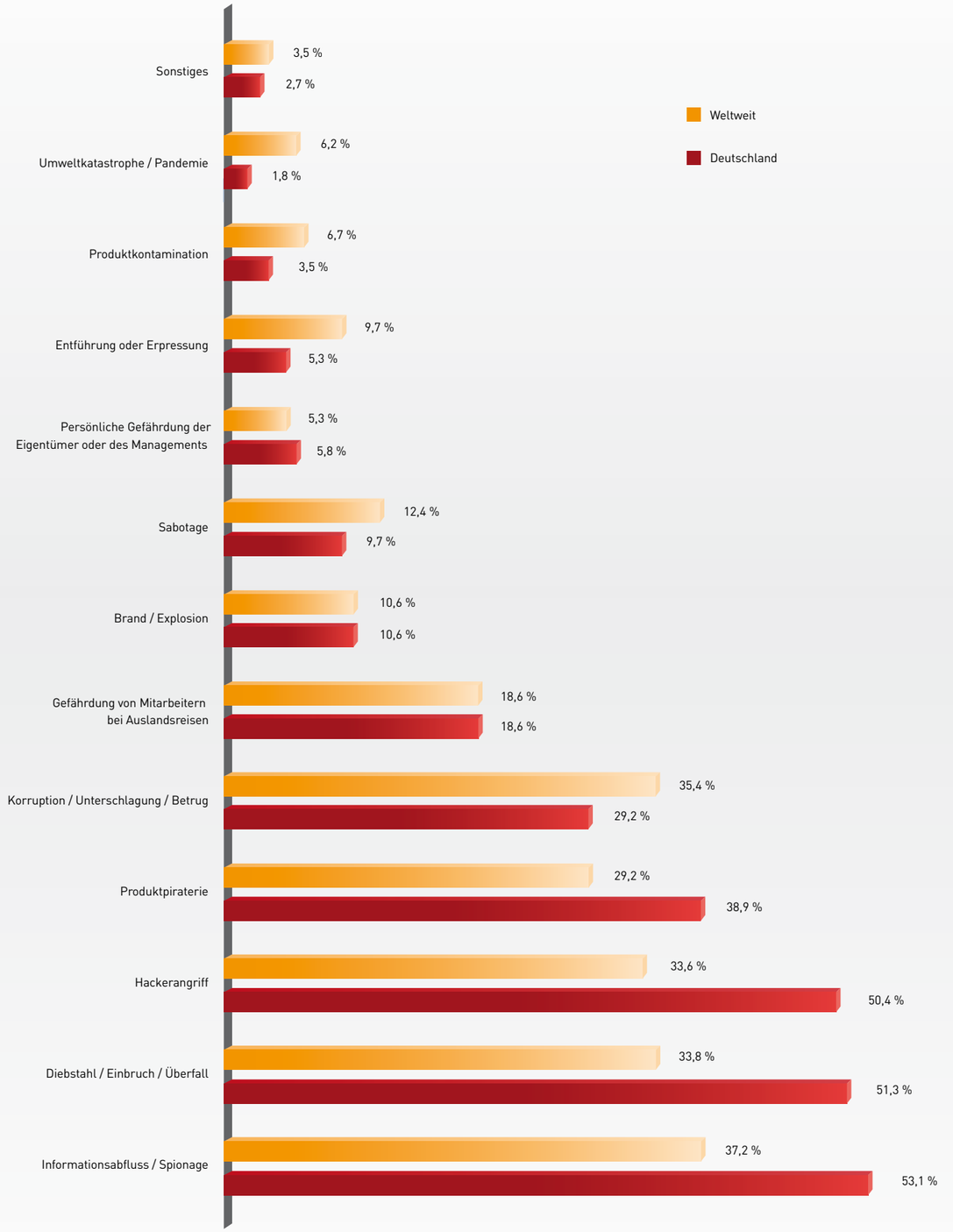
Das Gefahrenbarometer 2010 soll Auskunft über die zukünftige Bedrohung für den deutschen Mittelstand geben. Daher wurden Unternehmen befragt, welche klassischen Sicherheitsrisiken bzw. Gefahren sie in den nächsten Jahren für ihr eigenes Unternehmen erwarten. Die Bedrohung durch verschiedene Risiken wird sehr unterschiedlich gesehen. Überraschend war, dass für die meisten Risiken das Bedrohungspotenzial in Deutschland höher eingestuft wird als im Ausland. Bedenkt man, dass die Mehrheit aller mittelständischen Unternehmen im Ausland präsent ist (siehe Seite 15, Grafik 6), so glauben anscheinend viele Firmen, eher an ihrem deutschen Stammsitz angegriffen zu werden als bei der ausländischen Tochter, Niederlassung oder dem Joint-Venture.

Praxishinweis Taylor Wessing: Unsere anwaltliche Beratungspraxis zeigt, dass die Fälle von Geheimnisverrat und Spionage deutlich zunehmen und die meisten Rechtsverletzungen aus dem Unternehmen selbst heraus geschehen. Dieses Risiko sollten Unternehmer und Führungskräfte stets im Blick haben. Die betrieblichen Sensoren für Industriespionage sind in der Regel die Mitarbeiter. Daher sollten Meldepflichten und auch Melderechte für Mitarbeiter bei Verdachtsmomenten als präventive Regelungen Gegenstand der Arbeitsverhältnisse sein. Das so genannte „Whistleblowing" von Verstößen an eine zuständige Stelle sollte Teil der Corporate-Compliance-Regelungen sein und eingeführt werden.

Es eignen sich sogenannte „Codes of Conduct", die auch Sanktionen für Verstöße vorsehen sollten. Soweit ein Betriebsrat besteht, sind die Mitbestimmungsrechte bei der Einführung derartiger Regelungen zu beachten. Auch der Hinweis auf die Strafbarkeit von Industriespionage (§ 17 UWG, Verrat von Geschäfts- und Betriebsgeheimnissen) in Arbeitsverträgen, Verhaltensrichtlinien oder Betriebsvereinbarungen hat regelmäßig erheblich abschreckende Wirkung, verbunden mit der Androhung entsprechender Schadensersatzansprüche.

TW TaylorWessing

Welche dieser klassischen Sicherheitsrisiken bzw. Gefahren sehen Sie in den nächsten Jahren für Ihr Unternehmen in Deutschland und weltweit? (Mehrfachnennungen möglich)



GRAFIK 35 Quelle: Corporate Trust 2009

PRÄVENTION

GEPLANTE MASSNAHMEN DER UNTERNEHMEN

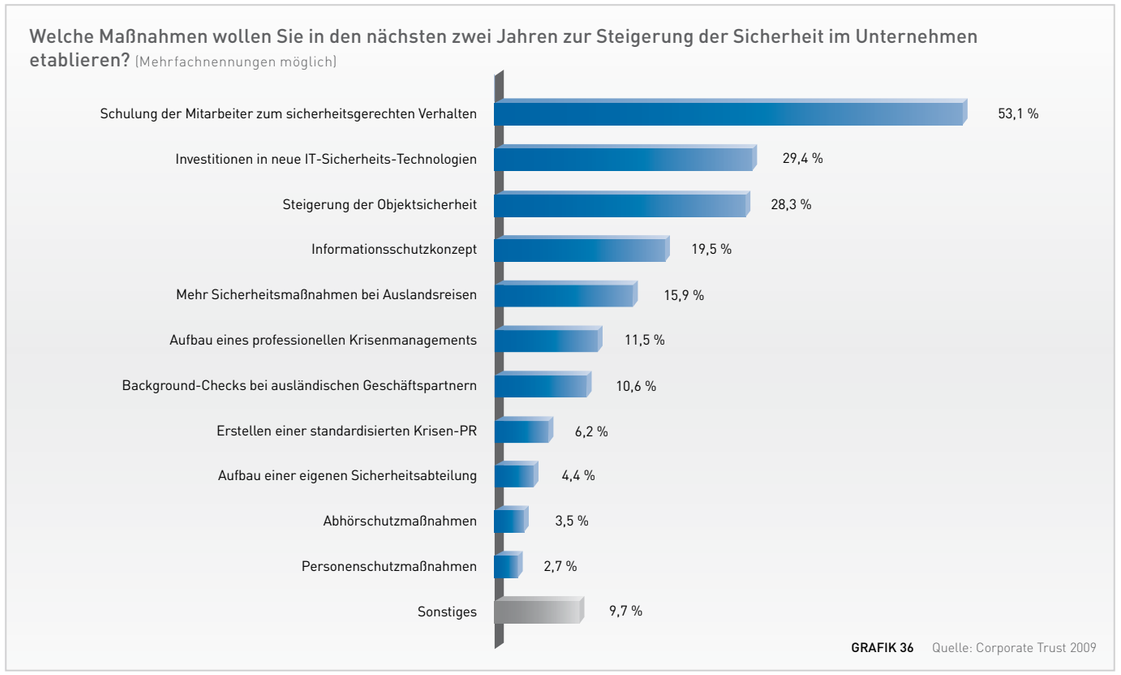
Der deutsche Mittelstand hat erkannt, dass Investitionen in das Sicherheitsverhalten ihrer eigenen Mitarbeiter den größten Schutz bieten. Eigene Strukturen gegen Korruption oder ein professionelles Krisenmanagement wird es aber leider auch künftig zu selten geben.

Aus den gemeldeten Schäden, der Bewertung des jeweiligen Risikos für verschiedene Bedrohungsszenarien und dem von den Unternehmen erwarteten Anstieg der Kriminalität lässt sich folgern, dass die eigenen Mitarbeiter die größte Bedrohung für das Unternehmen darstellen. Daher wollen die meisten Mittelständler in puncto Sicherheit zukünftig mehr in ihre Beschäftigten investieren.

Über die Hälfte aller Unternehmen - genau 53,1 Prozent - plant für ihre Mitarbeiter Schulungen zum sicherheitsgerechten Verhalten. Die Bedrohung eines Hackerangriffs auf die IT - bei den Schäden mit 14,1 Prozent an dritter Stelle (siehe Seite 17, Grafik 8) und desgleichen mit 50,4 Prozent bei der Einschätzung der künftigen Risiken in Deutschland (siehe Seite 45, Grafik 35) - veranlasst die Unternehmen, auch mehr in neue IT-Technologien zu investieren. Mit 29,4 Prozent stehen diese geplanten Investitionen auf Platz zwei beim Mittelstand.

Obwohl Korruption, Betrug oder Untreue mit 15,1 Prozent bei den Schäden die zweithäufigste Ursache war (vgl. Seite 17, Grafik 8), will nur jedes zehnte Unternehmen in Zukunft Background-Checks[34] bei ausländischen Geschäftspartnern durchführen. Ähnlich verhält es sich beim Krisenmanagement[35] oder der professionellen Krisenkommunikation[36].

Bei der Schadenshäufigkeit (vgl. Seite 17, Grafik 8) wurden im Schnitt zwar weniger Einzelfälle von Brand, Explosion, Produktkontamination, Entführung, Erpressung oder Gefährdung eines Mitarbeiters im Ausland genannt, sie kommen aber dennoch bei vielen Mittelständlern vor. Wenn ein Unternehmen dann nicht die richtigen Strukturen hat, um mit der Situation souverän umzugehen, ist die Reputation nach außen und nach innen gefährdet. Zu einem professionellen Risiko- oder Notfallmanagement gehören zum Beispiel ein definierter Krisenstab sowie eine gut vorbereitete Strategie zur Krisenkommunikation. Leider wollen nur 11,5 Prozent ein professionelles Krisenmanagement im Unternehmen etablieren und nur 6,2 Prozent eine standardisierte Krisen-PR aufbauen.



GRAFIK 36 Quelle: Corporate Trust 2009

34) Background-Check Überprüfung von Mitarbeitern oder Geschäftspartnern bezüglich der Seriosität, Zuverlässigkeit, finanziellen Verhältnisse, etwaiger Firmenbeteiligungen oder sonstiger verdächtiger Lebensumstände.

35) Krisenmanagement Der systematische Umgang mit Krisensituationen. Dazu gehören die Identifikation und Analyse der jeweiligen Risiken, ein Notfallplan, die Benennung der Mitglieder im Krisenstab sowie präventive Vorkehrungen.

ANGEPASSTE SICHERHEITSSTRUKTUREN FÜR DEN MITTELSTAND

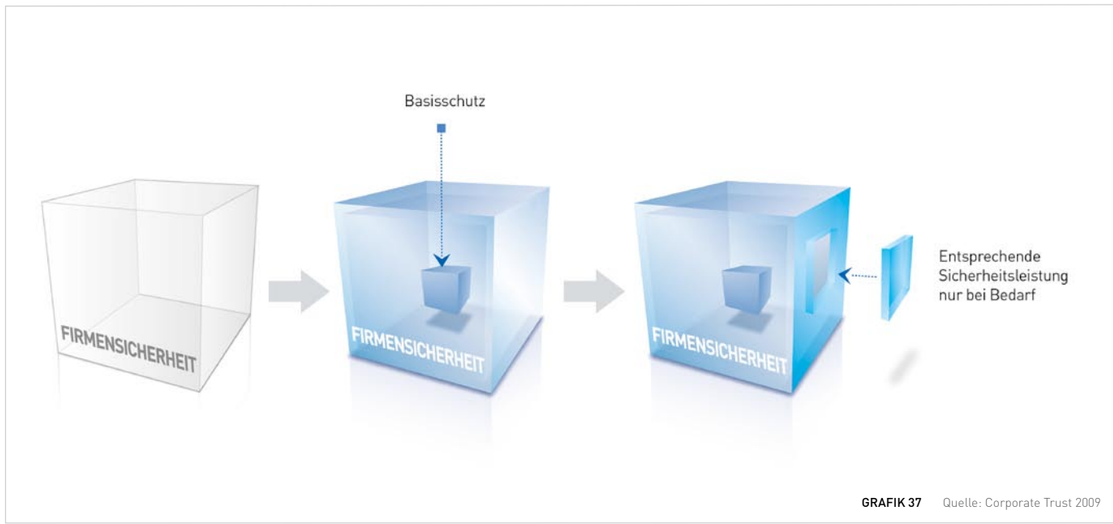
Mittelständische Unternehmen können einen Großteil ihrer Sicherheitsaufgaben auslagern. Ein professionelles externes Sicherheitsmanagement bedeutet schlanke Strukturen und eine permanente Verfügbarkeit von Spezialisten - Kosten entstehen nur bei entsprechendem Bedarf.

Viele mittelständische Unternehmen haben die gleichen Sicherheitsanforderungen wie große Konzerne, sie wollen sich aber keine eigene Corporate Security[37] mit großem Personalaufwand leisten. Um trotzdem gegen kriminelle Angriffe, Großschadensereignisse oder unvorhersehbare Schäden mit Krisenpotenzial gerüstet zu sein, sollten sie sich entsprechend vorbereiten. Einen Großteil der Sicherheitsstrukturen kann man heute an Spezialanbieter auslagern. Solche Dienstleister konzentrieren sich nicht nur voll auf ihr Thema, sondern verfügen auch über Sicherheitsspezialisten für alle Bereiche sowie ein internationales Netzwerk. Wichtigste Voraussetzung sollte es sein, dass eine permanente Erreichbarkeit gewährleistet ist.

Das Outsourcing[38] von Sicherheitsdienstleistungen an einen professionellen Partner liegt bei mittelständischen Unternehmen heute im Trend: Es ermöglicht schlanke Strukturen im eigenen Unternehmen, geringe Kosten und ein Höchstmaß an Qualifikation für die einzelnen Anforderungen.

Für ein professionelles Handling aller Sicherheitsanforderungen sollten bei Bedarf folgende Bereiche durch Spezialisten abgedeckt werden können:

- Risiko- und Notfallmanagement
- Krisenkommunikation
- Prävention gegen Wirtschaftskriminalität
- Informationsschutz / Spionageabwehr
- Professionelle Ermittlungen
- IT-Sicherheit
- Reisesicherheit
- Business Continuity Management
- Persönliche Sicherheit der Geschäftsleitung und der Eigentümer
- Eigentumsschutz



GRAFIK 37 Quelle: Corporate Trust 2009

36) Krisenkommunikation Unter Krisenkommunikation oder Krisen-PR versteht man jenes Teilgebiet der Öffentlichkeitsarbeit, das sich mit der Information und Kommunikation in Krisensituationen beschäftigt.

37) Corporate Security Bezeichnung für die Sicherheitsabteilung eines großen Konzerns, in der alle sicherheitsrelevanten Themen bearbeitet werden.

38) Basic Trust Outsourcing von Sicherheitsdienstleistungen, www.basic-trust.de

Prävention

Risikomanagement aus Sicht von Experten

Alexander Haudan
Rechtsanwalt
TAYLOR WESSING
Deutschland

„Steigenden Risiken für sensitive Informationen durch Investitionen in die Prävention begegnen“

TaylorWessing

Der Schutz von Know-how wird als Thema zunehmend auch von mittelständischen Unternehmen wahrgenommen. Die vorliegenden Studienergebnisse decken sich mit unserer Beratungspraxis. Das Bewusstsein für die Risiken steigt, die Verletzungsfälle nehmen zu, und Prävention gewinnt an Bedeutung. Mehr als die Hälfte der befragten Unternehmen, immerhin beachtliche 53,1 Prozent, sehen in Informationsabfluss/Spionage das bedeutendste unternehmerische Risiko der kommenden Jahre und betrachten die Mitarbeiterschulung als mit Abstand wichtigste Präventivmaßnahme, um sicherheitsgerechtes Verhalten im Unternehmen zu trainieren.

Die Bedeutung der Prävention unterstreicht Taylor Wessing aus anwaltlicher Sicht nachdrücklich. Betriebliches Know-how stellt für Unternehmen aller Branchen einen erheblichen, oft sogar den einzigen Unternehmenswert dar und kann sowohl technische als auch wissenschaftliche (Forschung & Entwicklung) und betriebswirtschaftliche Aspekte betreffen. Internet und globalisierte Märkte gefährden geheimes Know-how durch interne wie externe Angriffe.

Die Risiken für den Abfluss geheimen Know-hows sind vielfältig und werden in oftmals betroffenen kleineren und mittelständischen Unternehmen häufig nicht oder zu spät erkannt oder nicht ernst genommen.

1. Betriebs- und Geschäftsgeheimnisse sind über die Strafnorm § 17 UWG geschützt. Unter Strafe gestellt ist die Weitergabe von Geheimnissen an Dritte während der Dauer des Arbeitsvertrages (Abs. 1) und das Sichverschaffen oder Sichern eines Geschäftsgeheimnisses durch die Herstellung einer Verkörperung und die Verwertung oder Mitteilung eines so gesicherten Geheimnisses (Abs. 2).

- Dreh- und Angelpunkt der Norm ist das Vorliegen eines Geschäftsgeheimnisses: die nicht offenkundige, von einem Geheimhaltungswillen getragene Tatsache, an der ein betriebliches Geheimhaltungsinteresse besteht. Kurz gesagt: der Wissensvorsprung des Unternehmens vor Wettbewerbern.

- Daher muss zunächst sichergestellt werden, dass ein Geheimnis auch ein Geheimnis bleibt. Neben der Beschränkung des Zugangs zu geheimem Know-how muss auch der Wille des Unternehmers zur Geheimhaltung erkennbar sein.

2. Risiken für den Know-how-Abfluss

- Das größte Risiko stellen Mitarbeiter dar, die Geheimnisse an Dritte verraten oder zu eigenen Wettbewerbszwecken nutzen. Häufig geht dem Rechtsbruch eine innere Distanzierung zum Arbeitgeber voraus, die durch Übergehen bei Beförderungen, Unzufriedenheit mit dem Gehalt oder dem Inhalt der Arbeit oder Auseinandersetzungen mit Kollegen ausgelöst werden kann.

- Ein regelmäßig unerkanntes Risiko schlummert in Behördenakten. Insbesondere produzierende Unternehmen, die immissionsschutzrechtliche oder andere behördliche Genehmigungen benötigen, müssen regelmäßig Unterlagen zu betrieblichen Abläufen oder Konstruktionszeichnungen vorlegen. Die Informationsfreiheitsgesetze sowie das Umweltinformationsgesetz gewähren Jedermann(!)-Rechte auf Einsicht in Behördenakten, die von Wettbewerbern zur Ausforschung genutzt werden. Ebenso sind Geheimnisse in öffentlichen Auslegungsverfahren gefährdet.

- In der Zusammenarbeit mit Zulieferern oder Abnehmern sowie in Projekt- und Forschungsgemeinschaften wird häufig betriebliches Know-how offenbart, um aus dem Wissen der Beteiligten neue Produkte und innovative Prozesse zu entwickeln.

- Gesellschaftsrechtliche Informations- und Berichtspflichten können insbesondere bei Joint-Venture-Verträgen zu einem nicht beabsichtigten Know-how-Transfer führen.

- Einbruchstellen sind in der Regel Datennetze. Angriffe von innen durch unrechtmäßiges Kopieren von Dateien stellen dabei eine wesentlich größere und relevantere Gefahr dar als Hacker-Angriffe von außen.

3. Prävention ist möglich, auch wenn bei krimineller Energie kein absoluter Schutz besteht.

- Im Vordergrund stehen tatsächliche Maßnahmen, die auch den Geheimhaltungswillen dokumentieren. In Datennetzen sollten Zugriffsberechtigungen auf geheime Informationen restriktiv vergeben werden. Der persönliche Zugang zu Bereichen, in denen mit Geheimnissen umgegangen wird, sollte nur den damit befassten Mitarbeitern offenstehen (F&E-Abteilung, Labore). Mitarbeiter von Fremdfirmen sollten auf dem Betriebsgelände konsequent kontrolliert werden, insbesondere wenn diese in geheimnisrelevanten Bereichen arbeiten. Bei der Überwachung am Arbeitsplatz (Kameras, Kontrolle von Telefon und Internet) sind datenschutz- und betriebsverfassungsrechtliche Fragen zu berücksichtigen und ggf. vorab der Betriebsrat einzubinden.

- Bei der Begründung von Arbeitsverhältnissen kann der neue Arbeitgeber von seinem Recht auf Fragen mit Arbeitsplatzbezug Gebrauch machen oder ein polizeiliches Führungszeugnis anfordern. In Arbeitsverträgen kann Trägern von Geschäftsgeheimnissen ein nachvertragliches Wettbewerbsverbot auferlegt werden, üblich sind außerdem Geheimhaltungs- und Kundenschutzvereinbarungen, die durch eine Vertragsstrafe unterlegt werden sollten. Die bei einer Kündigung anfallende Karenzentschädigung ist zwar kostspielig; die nachträgliche Sicherung bereits abgeflossenen und zu Wettbewerbszwecken durch den Geheimnisträger genutzten Know-hows ist jedoch bedeutend teurer. Bei Beendigung des Arbeitsverhältnisses hat sich ein „Exit-Gespräch“ bewährt, in dem der vertragsgemäße Umgang mit sensiblen Kontaktdaten sichergestellt wird.

- Behörden sollten Unterlagen, die Geheimnisse enthalten, in einem verschlossenen und versiegelten Umschlag erhalten, wobei jedes Blatt mit einem Stempel „Geheim“ sowie der Firma gekennzeichnet werden sollte. Auf diese Weise werden die Sachbearbeiter vor einer Aushändigung an Dritte gewarnt und zur Rücksprache mit dem betroffenen Unternehmen aufgefordert.

- Verträge mit Zulieferern und Abnehmern sowie F&E-Verträge sollten eine vertragsstrafebewehrte Geheimhaltungsklausel enthalten. Die Vertragsstrafe sollte eine empfindliche Sanktion darstellen und den erwartbaren Mindestschaden abdecken.

- Schließlich sollte die Schutzrechtsstrategie ständig überprüft werden. Patente und Gebrauchsmuster helfen bei dem Schutz technischen Know-hows. Da die Offenlegung im patentamtlichen Verfahren zu einer Verbreitung des Know-hows führen kann, ist ein Patentschutz jedoch nicht in jedem Fall das Mittel der Wahl.

4. Im Fall des Falles gilt: Ruhe bewahren!

- Jede voreilige arbeits- oder zivilrechtliche Maßnahme warnt den Täter und führt zur Beseitigung von Beweismitteln. § 17 UWG ist Strafnorm und ermöglicht eine Strafanzeige sowie Durchsuchungen und Beschlagnahmen durch die Staatsanwaltschaft. In aller Regel können für die Geltendmachung zivilrechtlicher Ansprüche erforderliche Beweismittel nur auf diesem Wege erlangt werden.

Zum Abschluss die aus Sicht von Taylor Wessing wesentlichen Hinweise aus der Praxis:

- Prävention ist von zentraler Bedeutung – einmal abgeflossene Geheimnisse können nur unter größten Schwierigkeiten wieder gesichert werden. Wir empfehlen daher eine regelmäßige „Know-how Due Diligence“.

- Und: **Geheimnisschutz ist Chefsache!**

Ihr
Alexander Haudan

Prävention

Risikomanagement aus Sicht von Experten

Hubertus Eichler
Partner, Wirtschaftsprüfer,
Steuerberater, Certified
Internal Auditor (CIA)
MAZARS Hemmelrath GmbH
Wirtschaftsprüfungs- und
Beratungsgesellschaft

„Ein gutes Risikomanagement ermöglicht eine erfolgreiche Unternehmenssteuerung“

MAZARS

Durch das Übergreifen der globalen Finanzkrise auf die Realwirtschaft ergeben sich für Unternehmen zunehmend wirtschaftliche, finanzielle und auch rechtliche Unsicherheiten. Sie betreffen nahezu sämtliche Unternehmensbereiche - insbesondere Finanzen, Produktion, Einkauf und Vertrieb. Hierdurch, aber auch aufgrund der sich abzeichnenden Regulierung im Gefolge der Krise, sehen sich sowohl Vorstände als auch Aufsichtsorgane und Gesellschafter erhöhten Haftungsrisiken ausgesetzt.

Eine vorausschauende und an nachhaltigen Kriterien ausgerichtete Unternehmensstrategie ist unseres Erachtens wichtig, um diese Risiken - die teilweise ohne historisches Vorbild sind - aktiv zu steuern und sie bereits im Vorfeld zu vermeiden. Unsere jahrelange Erfahrung in der Beratung mittelständischer Unternehmen zeigt: Präventive Maßnahmen im Bereich des Risikomanagements sind bessere Garanten für Stabilität und Sicherheit als die nachträgliche Aufdeckung von Schäden mittels aufwändiger Untersuchungsmethoden. Gleichzeitig hilft professionelle Vorsorge, unkalkulierbare Verluste zu vermeiden, indem sie die Transparenz erhöht und Folgekosten senkt. Darüber hinaus werden die an das Unternehmen gestellten rechtlichen Anforderungen abgedeckt.

Fazit: Ein gutes Risikomanagement ermöglicht eine erfolgreiche Unternehmenssteuerung, bei der Unternehmensziele erreicht, gesetzliche Anforderungen sowie freiwillige Kodizes (Compliance) erfüllt und Risiken rechtzeitig vermieden werden.

Wir empfehlen daher ein „Enterprise Risk Management“, das - ausgehend von einer nachhaltigen Unternehmensstrategie - einen ganzheitlichen und konzernübergreifenden Ansatz zum Umgang mit Risiken gewährleistet. Diese Strategie muss nach unserer Erfahrung auf einer gesunden Unternehmenskultur aufsetzen. Idealerweise gründet sich der Rahmen des unternehmerischen Handelns auf ein Gerüst klarer Prozesse und Verhaltensregeln. Diese sollten unternehmensweit installiert, kommuniziert, verstanden und auch akzeptiert werden. Entscheidend ist, dass sich die Regeln pragmatisch umsetzen, mühelos in bestehende Prozesse und Systeme integrieren und vor allem im Tagesgeschäft „leben“ lassen.

Unliebsame Überraschungen und negative Folgewirkungen können sich auch aus einer bis dato erfolgreichen Globalisierungsstrategie ergeben. 69 % der Studienteilnehmer haben Geschäftsbeziehungen im Ausland. Es ist davon auszugehen, dass eine massive Verschlechterung der wirtschaftlichen Rahmenbedingungen - vor allem in weniger entwickelten Ländern - zu einer „Mitnahmementalität“ bei Mitarbeitern und Geschäftspartnern führen wird. Von daher raten wir, insbesondere auch Auslandsstandorte bei der Risikoprävention zu berücksichtigen.

Laut der Studie gehören Diebstahl, Korruption, Betrug und Untreue zu den am häufigsten genannten Schäden der letzten drei Jahre. Nur die wenigsten Unternehmen verfügen offenbar über ein standardisiertes Konzept zum Umgang mit diesen Risiken. Vielmehr wird versucht, sie mittels vertraglicher Regelungen oder Handlungsanweisungen in den Griff zu bekommen.

Ein ethisch und moralisch jederzeit einwandfreies Handeln der Führungskräfte überzeugt die Stakeholder des Unternehmens von der Nachhaltigkeit des Geschäftsmodells und fördert dadurch die Unternehmensstrategie, auch in wirtschaftlich turbulenten Zeiten. Neben klaren Handlungsprämissen - wie zum Beispiel einer Ethik-Richtlinie - haben sich flankierende Kontrollmaßnahmen sowie Ethik-Hotlines als erfolgreich erwiesen, um Wirtschaftskriminalität vorzubeugen.

Ihr

Hubertus Eichler

Prävention

Risikomanagement aus Sicht von Experten

Michael Frauen
Regional Director
RSA
Security Division of EMC

„IT-Sicherheit ist strategisch und damit Chefsache“

RSA
The Security Division of EMC

Der Mittelstand ist eine wichtige Triebfeder für Innovation in Deutschland. Daher sind mittelständische Unternehmen ein häufiges Ziel von Industriespionage und laufen Gefahr, dass unternehmenskritische Informationen abfließen. Gerade in letzter Zeit haben die Medien umfangreich über Sicherheitsprobleme und -lücken in Unternehmen und öffentlichen Einrichtungen berichtet. Daraus wird ersichtlich, dass die Bedrohung real ist und erhebliche Auswirkungen auf Reputation und Geschäft der betroffenen Firmen haben kann. Unternehmen beklagen Einzelschäden in Höhen von 10.000 Euro bis zu mehreren Millionen Euro. Laut einer aktuellen Studie verursacht ein größerer Datenverlust einen durchschnittlichen Schaden von 2,4 Millionen Euro. Umgerechnet auf die betroffenen Datensätze zahlt jedes Unternehmen durchschnittlich 112 Euro pro Datensatz. Es besteht also Handlungsbedarf.

Die Unternehmen stehen dabei vor der Herausforderung, Informationsangebot und Informationsschutz unter einen Hut zu bringen. In der modernen Arbeitswelt ist es unabdingbar, Informationen einem bestimmten Nutzerkreis ständig und flexibel zugänglich zu machen. Zum Beispiel brauchen die zunehmend mobilen Mitarbeiter auch unterwegs Zugang zu den Unternehmenssystemen. Damit steigt das Risiko eines Datenverlusts, da von unterschiedlichsten Endgeräten auf sensible Unternehmensdaten zugegriffen wird. Auch die Kunden wollen sich überall und jederzeit online über neue Angebote und Lösungen informieren können. In jedem Fall sollen relevante Informationen schnell und flexibel zur Verfügung stehen - sowohl den Mitarbeitern als auch den Kunden, die von verbesserten Services und beschleunigten Abläufen profitieren.

Dem gegenüber steht der Schutz von Informationen, der unerlässlich ist, um die Wettbewerbsposition des Unternehmens zu sichern. Die Verantwortlichen stehen dabei vor der Herausforderung, eine Balance zwischen dem „Security-Level“, den Kosten und der Handhabbarkeit für den Anwender zu finden. Die Einschätzung des Risikos bestimmt letztlich den Level des Informationsschutzes. Dabei spielen gesetzliche Vorgaben und vertragliche Verpflichtungen gegenüber Kunden und Partnern eine Rolle, aber auch das Eigeninteresse. Denn Informationen gehören zum wichtigsten Kapital eines Unternehmens - Grund genug, sie konsequent vor Missbrauch und Verlust zu schützen. Um den Zielkonflikt zwischen Informationsbereitstellung und Informationsschutz zu lösen, ist die Implementierung einer unternehmensweiten Information-Risk-Management-Strategie ein Muss. Dazu gehören technologische und organisatorische Maßnahmen, aber auch die Sensibilisierung und Aufklärung der eigenen Mitarbeiter.

Aufklärung der Mitarbeiter für mehr Sicherheit

Wie wichtig gerade dieser Bereich ist, zeigt die vorliegende Studie. Demnach sind die größten Bedrohungspotenziale im leichtfertigen Umgang mit Sicherheitsstandards sowie im Datenmissbrauch durch eigene Mitarbeiter zu sehen. Um Letzteren einzudämmen, muss eine Sensibilisierung im Umgang mit den Daten stattfinden. In Unternehmen gibt es im Wesentlichen zwei Typen von internen Tätern, die für Informationsabfluss verantwortlich sind: Der eine ist kriminell motiviert und verkauft die Informationen gezielt. Der andere handelt aus Unwissenheit oder Leichtfertigkeit, ohne sich überhaupt über das Risiko im Klaren zu sein. So kann schon ein zu laut geführtes Telefonat im voll besetzten Zug oder eine Vorstandssitzung in einem ungenügend abhörsicheren Konferenzraum ausreichen, um Informationen leichtfertig preiszugeben.

Es gilt also, die Mitarbeiter für den korrekten Umgang mit vertraulichen Informationen zu sensibilisieren. Sie müssen kontinuierlich über Risiken und Folgen eines unbedarften Umgangs mit kritischen Daten aufgeklärt werden. Voraussetzung dafür ist das Bewusstsein, welchen Wert bestimmte Informationen für geschäftskritische Prozesse des jeweiligen Unternehmens haben.

Information Risk Management: der Prozess zum Erfolg

Dem Missbrauch oder Diebstahl vertraulicher Daten lässt sich wirksam begegnen, indem technologische Maßnahmen die Aufklärung der Mitarbeiter unterstützen und ergänzen. Gerade in wirtschaftlich schwierigen Zeiten sollte das Thema Informationssicherheit nicht vernachlässigt werden - denn die Bedrohung des Informationskapitals durch Industriespionage und andere wirtschaftlich motivierte Straftaten wird eher zunehmen als abnehmen. Gegen Angriffe von außen sind IT-Infrastrukturen heute schon gut geschützt. Erheblicher Nachholbedarf besteht dagegen - wie auch die Studienergebnisse zeigen - beim Schutz der Informationen selbst. Diese sind gefährdet, sobald sie den schützenden Rahmen der Infrastruktur verlassen. Dabei sind nicht alle Informationen gleich wichtig. Um auf der sicheren Seite zu sein, sollten Unternehmen einen Prozess installieren, der die fortlaufende Überprüfung und Überwachung von Informationen gewährleistet.

An erster Stelle stehen dabei die Informationsanalyse und die Identifizierung der Risiken: Die im Unternehmen vorhandenen Daten werden erfasst und nach Geschäftsrelevanz klassifiziert. Gleichzeitig werden bereits vorhandene Sicherheitsstrukturen und -lücken identifiziert und bewertet. Diese Analyse ist die Basis für die Definition einer Sicherheitsleitlinie sowie eines Regelwerks, das auch die notwendigen Maßnahmen auf allen Ebenen enthält. Berücksichtigt werden dabei nicht nur die IT-Infrastruktur in Form von Verschlüsselung und Maßnahmen gegen unerwünschten Datenabfluss (Data Loss Prevention), sondern auch die Geschäftsprozesse und die Sensibilisierung der Mitarbeiter. Ist eine Sicherheitsstrategie entwickelt, so werden in der Folge die entsprechenden Maßnahmen umgesetzt. Um stets auf dem höchsten Sicherheitsstandard zu sein, müssen sowohl das Regelwerk als auch die Schutzmaßnahmen laufend überprüft und gegebenenfalls modifiziert werden.

RSA unterstützt Unternehmen bei Aufbau und Implementierung solcher Sicherheitsstrategien durch einen ganzheitlichen Lösungsansatz. Dieser basiert auf den bestehenden Rahmenbedingungen des Unternehmens und setzt direkt bei den geschäftskritischen Informationen und den jeweils gegebenen Risiken an. Berücksichtigt werden organisatorische, prozessuale, personelle und technologische Aspekte - wie Authentifizierung, Verschlüsselung, Log-Management, Compliance Reporting und Data Loss Prevention (DLP). Eine allgemeingültige Standardlösung gibt es dabei nicht. Stattdessen bietet RSA den Unternehmen konkrete Maßnahmen in Form von individuellen Risk Assessments und Audits an, um Risiken zu analysieren. Auf diese Weise lassen sich Schwachstellen und potenzielle Angriffsziele aufdecken, sodass gezielte Gegen- und Schutzmaßnahmen möglich sind. Damit können Mittelständler auch in Zukunft sicherstellen, dass ihr wichtigstes Kapital geschützt ist und zum Nutzen des Unternehmens eingesetzt werden kann.

Ihr

Michael Frauen

AUSBLICK

UNTERNEHMENSSICHERHEIT 2010

Die Risiken werden weltweit steigen. Je loyaler die Mitarbeiter einem Unternehmen gegenüberstehen, desto höher die Sicherheit.

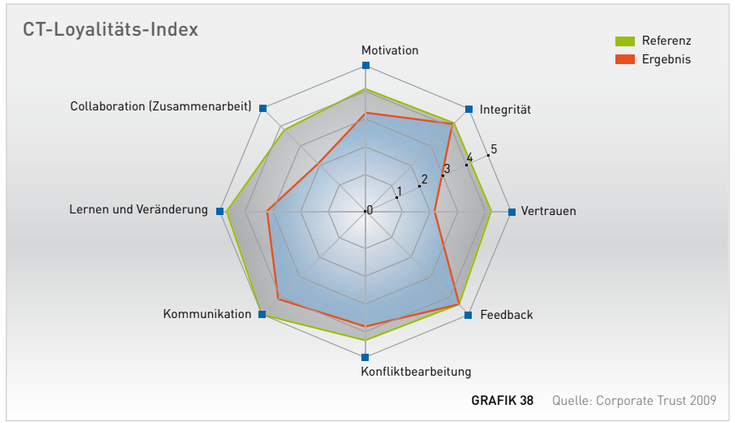
BASIC TRUST®
Die Basis für mehr Sicherheit.

Neben der allgemeinen Bedrohung durch Kriminelle, Terroristen oder die Konkurrenz aus dem In- und Ausland wird auch das Risiko durch die eigenen Mitarbeiter steigen. Die Finanz- und Wirtschaftskrise wird dazu führen, dass mehr Mitarbeiter um ihren Arbeitsplatz fürchten müssen oder sogar entlassen werden. Kurzarbeit oder Sparmaßnahmen bei den Unternehmen können für viele Arbeitnehmer bedeuten, dass sie am Ende des Monats weniger in der Tasche haben. Damit laufen sie Gefahr, selbst in eine finanzielle Schieflage zu geraten. Ist die Loyalität der Mitarbeiter in einem Unternehmen oder einer bestimmten Abteilung gering, steigt das Risiko sprunghaft an.

Je weniger sich ein Unternehmen dessen bewusst ist und die nötigen Vorbereitungen trifft, desto leichter ist es angreifbar. Um Mitarbeiterloyalität zu messen, hat Corporate Trust den „CT-Loyalitäts-Index" entwickelt. Ähnlich wie ein Röntgenbild hilft, Schwachstellen im Körper zu identifizieren, zeigt der „CT-Loyalitäts-Index", welche Störfelder im Unternehmen zu Illoyalität führen. Anhand dieser Analyse kann ein Unternehmen punktgenau gegensteuern. Vergleichbar mit fachmännischen Griffen bei der Akupressur können die Spezialisten von Corporate Trust mit gezielten Maßnahmen die Loyalität im Unternehmen steigern.

Da sich die weltweite Sicherheitslage in einigen Regionen verschärft und auch der islamische Terrorismus noch mehrere Jahre eine Rolle spielen wird, muss jedes Unternehmen zunehmend Maßnahmen treffen, um die Sicherheit ihrer Mitarbeiter zu gewährleisten und Produkte sowie Sachwerte zu schützen. Vor allem bei Auslandsreisen oder -aufenthalten werden mehr Vorkehrungen notwendig sein. Wirtschaftliche Perspektiven liegen häufig in Aufbau- und Entwicklungsländern. Dort gibt es jedoch teilweise eine besonders hohe Kriminalität.

Nach dem KonTraG - dem Gesetz zur Kontrolle und Transparenz im Geschäftsverkehr - ist die Geschäftsleitung verpflichtet, die nötigen Vorkehrungen zu treffen, um Risiken frühzeitig zu erkennen und Gefahren vom Unternehmen abzuwenden. Daher sollte es für jedes Unternehmen auch eine Selbstverständlichkeit sein, eine geeignete Sicherheitsstruktur aufzubauen, um allen zukünftigen Risiken und Gefahren gewachsen zu sein. Outsourcing ist dabei für den Mittelstand oft die sinnvollste und wirtschaftlichste Lösung.



GRAFIK 38 Quelle: Corporate Trust 2009

Ein integriertes Schutzkonzept und ständige Aufmerksamkeit sind die beste Versicherung gegen Industriespionage und Geheimnisverrat.

TaylorWessing

Wirtschaftskrise und Globalisierung erhöhen das unternehmerische Risiko von kriminellen Angriffen auf geheimes Know-how. Wir erwarten eine weitere Zunahme von Verletzungsfällen, die sich bereits in unserer Beratungspraxis zeigt.

Wirksamer und effizienter Schutz vor Geheimnisverrat ist möglich und setzt frühzeitiges und umfassendes Handeln voraus. Im Rahmen eines integrierten Schutz- und Risikomanagementkonzeptes müssen neben den unternehmensinternen Abläufen die rechtlichen Rahmenbedingungen für den Schutz geheimen Know-hows gewährleistet sein. Die ständige Überprüfung der Vertragsbeziehungen zu Mitarbeitern (Wettbewerbsverbote, Geheimhaltungs- und Kundenschutzvereinbarungen, „Exit-Gespräche") und externen Vertragspartnern mit Zugang zu Know-how (insbesondere F&E-Kooperationen und Zulieferer) sowie die Kontrolle der Außenbeziehungen des Unternehmens mit Bezug zu Geschäftsgeheimnissen (insbesondere zu Behörden) sind unverzichtbar. Denn: nur geheimes Wissen ist geschützt.

Mit diesen Maßnahmen wird das Bewusstsein der Mitarbeiter für die Bedeutung von Know-how für den unternehmerischen Erfolg geschärft, das zentraler Bestandteil der Unternehmenskultur und in den Leitlinien oder Compliance Grundsätzen verankert und regelmäßiger Bestandteil von Mitarbeiterschulungen sein sollte. Ein integriertes Schutzkonzept und die ständige Aufmerksamkeit aller am Umgang mit Know-how Beteiligten sind die beste Versicherung gegen Industriespionage und Geheimnisverrat.

Ein gutes Risikomanagement ermöglicht eine erfolgreiche Unternehmenssteuerung.

MAZARS

Viele Unternehmen sind bereits von den Auswirkungen der identifizierten Risiken aufgrund der globalen Wirtschafts- und Finanzkrise betroffen. Doch die Krise bietet auch Chancen: Sie liegen zum Beispiel in der intensiven Auseinandersetzung mit den Risiken und ihrer Verhinderung durch den Aufbau eines präventiven Risikomanagement-Systems. Die Optimierung dieser Prozesse führt letztlich auch zu einer effizienteren Unternehmenssteuerung.

Effektives Risikomanagement setzt ein gelebtes Integritätsmanagement sowie ein Compliance Management voraus, das auf die wesentlichen Normen und Regeln ausgerichtet ist. Durch eine solche, an nachhaltigen Grundsätzen ausgerichtete Management-Strategie lässt sich der Weg durch die Krise nach unserer Einschätzung erfolgreich bewältigen. Diese Strategie muss auf eine Unternehmenskultur gegründet sein, die sich zur Verantwortung bekennt und damit sämtliche Anspruchsgruppen (Stakeholder) anspricht und überzeugt. Gleichzeitig kann verstärkte Transparenz zu mehr Glaubwürdigkeit gegenüber der Öffentlichkeit und den unterschiedlichen Anspruchsgruppen führen.

Information Risk Management als ganzheitliche IT-Security Strategie.

RSA
The Security Division of EMC

Gerade in wirtschaftlich schwierigen Zeiten sollte das Thema Informationssicherheit nicht vernachlässigt werden. Denn die Bedrohung des Informationskapitals durch Industriespionage und andere wirtschaftlich motivierte Angriffe wird eher zunehmen als abnehmen. Besonders mittelständische Unternehmen sind ein häufiges Ziel von Industriespionage und gefährdet, was den Abfluss unternehmenskritischer Informationen betrifft. Der Schutz der Informationen durch die Implementierung einer unternehmensweiten Information-Risk-Management-Strategie ist daher unerlässlich, um die Wettbewerbsposition des Unternehmens zu sichern.

Gegen Angriffe von außen sind IT-Infrastrukturen heute schon gut geschützt. Erheblichen Nachholbedarf gibt es – wie auch die Studienergebnisse zeigen – beim Schutz der Information selbst. Diese ist gefährdet, sobald sie den schützenden Rahmen der Infrastruktur verlässt. Dabei sind nicht alle Informationen gleich wichtig. Daher müssen die im Unternehmen vorhandenen Daten erfasst und nach Geschäftsrelevanz klassifiziert werden. Um auf der sicheren Seite zu sein, sollten Unternehmen einen Prozess aufsetzen, der die kontinuierliche Überprüfung und Überwachung der Informationen gewährleistet. Eine allgemeingültige Standardlösung gibt es dabei nicht. Stattdessen bietet RSA den Unternehmen konkrete Maßnahmen zur Risikoanalyse in Form von individuellen Risk Assessments und Audits an, um Schwachstellen und potenzielle Angriffsziele zu identifizieren, bevor entsprechende Gegen- und Schutzmaßnahmen ergriffen werden. So können Mittelständler auch in Zukunft sicherstellen, dass ihr wichtigstes Kapital geschützt ist und zum Wohle des Unternehmens eingesetzt werden kann.

Glossar

- **Background-Check**
  Überprüfung von Mitarbeitern oder Geschäftspartnern bezüglich der Seriosität, Zuverlässigkeit, finanziellen Verhältnisse, etwaiger Firmenbeteiligungen oder sonstiger verdächtiger Lebensumstände.

- **Compliance**
  Ein Verhaltenskodex für gesetzmäßiges, rechtskonformes und verantwortungsbewusstes Handeln im Unternehmen.

- **Corporate Security**
  Bezeichnung für die Sicherheitsabteilung eines großen Konzerns, in der alle sicherheitsrelevanten Themen bearbeitet werden.

- **Definition der EU für KMU**
  http://ec.europa.eu/enterprise/entrepreneurship/facts_figures.htm
  Kleine und Mittlere Unternehmen, wenn sie von größeren Unternehmen unabhängig sind, weniger als 250 Mitarbeiter und weniger als 50 Millionen Euro Umsatz bzw. weniger als 43 Millionen Euro Bilanzsumme haben.

- **Dunkelfeld**
  In der Kriminologie bezeichnet das Dunkelfeld die Differenz zwischen den amtlich registrierten Straftaten - dem so genannten Hellfeld - und der vermutlich begangenen Kriminalität.

- **Evakuierung**
  Die Räumung eines Gebäudes oder Gebiets von Menschen.

- **Geheimhaltungsstufe**
  Festlegung einer Schutzstufe oder Schutzklasse für Daten oder Informationen gemäß der jeweiligen Schutzwürdigkeit und individuellen Gefährdung.

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

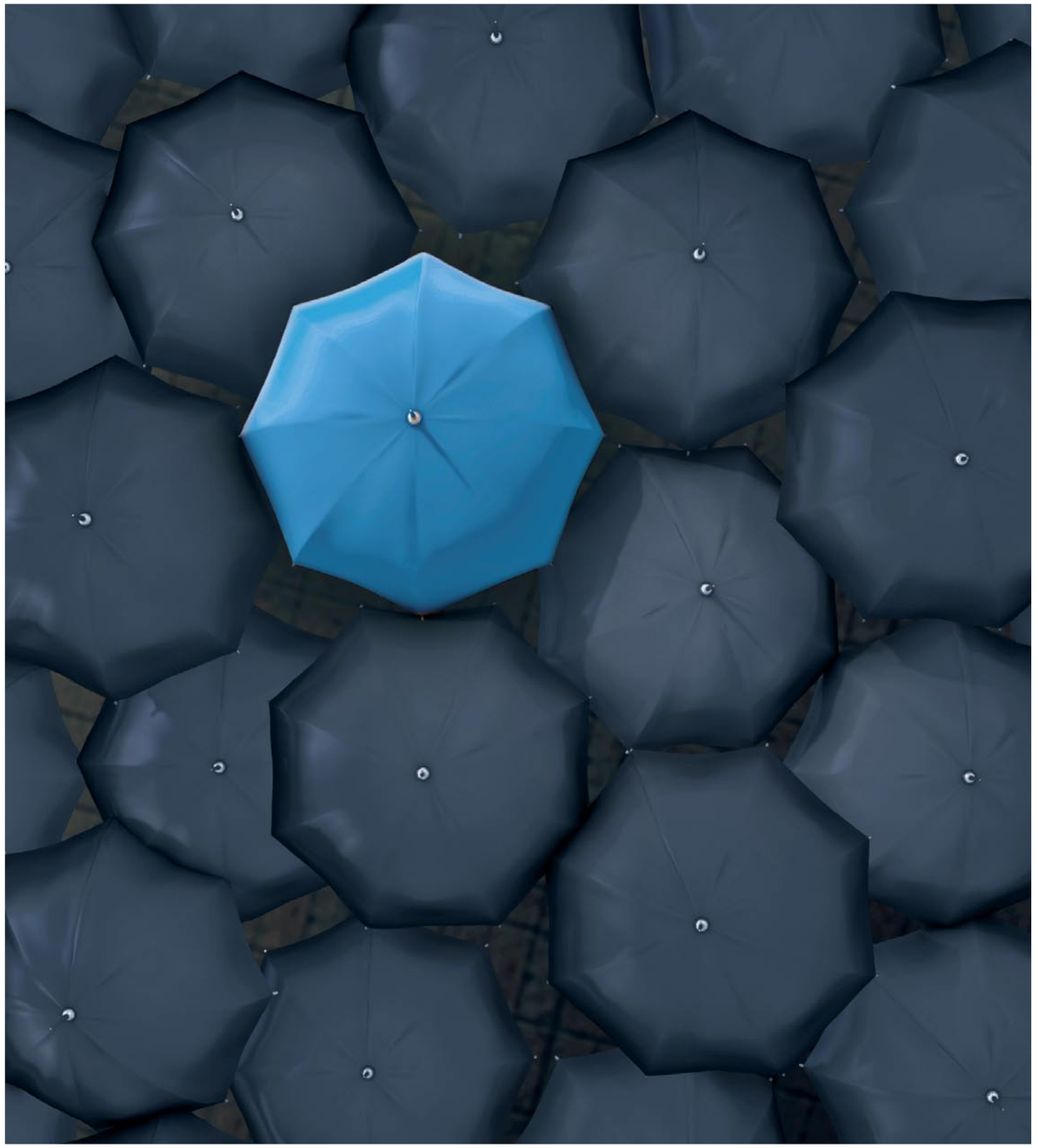
- **Hellfeld**
  Kriminalistischer Ausdruck zur Bezeichnung der angezeigten bzw. den Behörden bekannt gewordenen Delikte.

- **Industriespionage**
  Umgangssprachlich für Konkurrenzausspähung, teilweise auch für Wirtschaftsspionage. Wird häufig als Oberbegriff für Spionage bei Unternehmen verstanden.

- **Korruption**
  Der Missbrauch einer Vertrauensstellung in einer bestimmten Funktion, um einen materiellen oder immateriellen Vorteil zu erlangen, auf den kein rechtlich begründeter Anspruch besteht.

- **Krisenmanagement**
  Der systematische Umgang mit Krisensituationen. Dazu gehören die Identifikation und Analyse der jeweiligen Risiken, ein Notfallplan, die Benennung der Mitglieder im Krisenstab sowie präventive Vorkehrungen.

- **Krisen-PR**
  Unter Krisen-PR oder Krisenkommunikation versteht man jenes Teilgebiet der Öffentlichkeitsarbeit, das sich mit der Information und Kommunikation in Krisensituationen beschäftigt.



- **Krisenregion**
  Als Krisengebiet, Krisenherd oder Krisenregion werden Gegenden bezeichnet, in denen Sicherheitsrisiken ein schwer oder nicht mehr beherrschbares Ausmaß erreicht haben. Dazu gehören politische, ethnische oder wirtschaftliche Konflikte und Probleme oder Schäden durch Umwelt- und Naturkatastrophen.

- **Krisenstab**
  Gruppe von Personen innerhalb einer Organisation zum Notfall- oder Katastrophenmanagement. Der Krisenstab selbst übernimmt nicht die Führung, sondern funktioniert nur unter einem führungserfahrenen und alleinverantwortlichen Leiter. Dies stellt sicher, dass auch unter hohem Druck Entscheidungen schnell getroffen und mit vereinten Kräften umgesetzt werden können.

- **Organisierte Kriminalität (OK)**
  Von Gewinn- und/oder Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind. Von „organisiert" spricht man, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer zusammenwirken – unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen, unter Anwendung von Gewalt oder anderer einschüchternder Mittel oder unter Einflussnahme auf Politik, Massenmedien, öffentliche Verwaltung, Justiz oder Wirtschaft.

- **Pandemie**
  Länder- und kontinentübergreifende Ausbreitung einer Krankheit, im engeren Sinn einer Infektionskrankheit. Im Gegensatz zur Epidemie ist eine Pandemie somit nicht örtlich beschränkt.

- **Produktpiraterie**
  Das Geschäft mit Nachahmer-Waren, die mit dem Ziel hergestellt werden, einer Original-Ware zum Verwechseln ähnlich zu sein. Dabei werden Markenrechte oder wettbewerbsrechtliche Vorschriften verletzt. Häufig geht Produktpiraterie mit Verletzungen von Urheberrechten, Geschmacksmustern, Patenten und sonstigen Rechten des geistigen Eigentums und gewerblichen Rechtsschutzes einher.

- **Red flags**
  Auffälligkeiten im Verhalten von Mitarbeitern oder Vorgesetzten, das auf kriminelle Machenschaften hindeuten könnten.

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

- **Verschlüsselung**
  Vorgang, bei dem klar lesbare Texte oder auch Informationen anderer Art - wie Ton- oder Bildaufzeichnungen - mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine unleserliche, nicht einfach interpretierbare Zeichenfolge umgewandelt werden.

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

Ansprechpartner

Christian Schaaf
Geschäftsführer
CORPORATE TRUST,
Business Risk &
Crisis Management GmbH

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

Claudia Tödtmann
Redakteurin
Verlagsgruppe
Handelsblatt GmbH

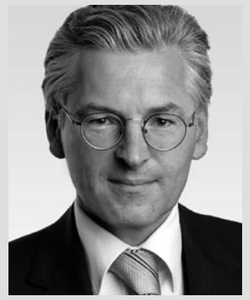
www.vhb.de
c.toedtmann@vhb.de

Die Studie Gefahrenbarometer 2010 wurde durch Corporate Trust, in Zusammenarbeit mit Frau Claudia Tödtmann, Verlagsgruppe Handelsblatt, erstellt. Begleitet und unterstützt wurde die Studie durch die Rechtsanwaltskanzlei TAYLOR WESSING, die Wirtschaftsprüfungs- und Beratungsgesellschaft MAZARS Hemmelrath GmbH und RSA, The Security Division of EMC.

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

Alexander Haudan
Rechtsanwalt
TAYLOR WESSING
Deutschland

www.taylor-wessing.com
a.haudan@taylor-wessing.com



Hubertus Eichler
Partner, Wirtschaftsprüfer,
Steuerberater, Certified
Internal Auditor (CIA)
MAZARS Hemmelrath
GmbH Wirtschaftsprüfungs-
und Beratungsgesellschaft

www.mazars.de
hubertus.eichler@mazars.de

Michael Frauen
Regional Director
RSA
Security Division of EMC

www.rsa.com
michael.frauen@rsa.com

CORPORATE TRUST
Business Risk & Crisis Management GmbH

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

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

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