

FORENSIC

e-Crime-Studie 2010

Computerkriminalität
in der deutschen Wirtschaft

RISK & COMPLIANCE



Inhalt

Vorwort	3
Eckdaten zur Studiendurchführung	5
Wesentliche Ergebnisse der Studie	6
e-Crime – Verständnis, handelnde Personen und betroffene Unternehmensbereiche	8
Fokus: Moderne Wirtschaftsspionage	20
Prävention, Entdeckung, Reaktion	24
Fazit	34
Forensic Technology von KPMG. Umfangreiche Erfahrungen in der e-Crime-Bekämpfung	35

Vorwort

Computerkriminalität beziehungsweise e-Crime ist auf dem Vormarsch. Viele Studien und Untersuchungen, wie unter anderem auch die KPMG-Studie „Wirtschaftskriminalität in Deutschland 2010“, belegen diesen Trend. Die treibenden Kräfte sind schnell identifiziert: Im Verlauf der letzten Jahre haben sich Unternehmen intern wie auch extern zunehmend vernetzt. Egal ob Smartphones, USB-Sticks oder virtualisierte Netzwerklösungen: Die Systeme der Informations- und Kommunikationstechnologie (IKT) sind aus dem Unternehmensalltag nicht mehr wegzudenken. Dabei werden die Grenzen zwischen den Unternehmen und den mit ihnen kommunizierenden externen und internen Mitarbeitern immer durchlässiger. Auf dem Weg zu fortwährend neu eingeführten Funktionalitäten und noch mehr Effizienz der IKT-Systeme entzieht sich das dahinter stehende technische Konstrukt immer weiter dem Verständnis der Mitarbeiterinnen und Mitarbeiter.

Doch so groß die mit diesen neuen Technologien einhergehenden Effizienzgewinne auch sind, die Risiken sind exponentiell mitgewachsen. Umfassende Sicherheitsmaßnahmen sind nur begrenzt realisierbar und die Kontrolle der Dateneigentümer und -verantwortlichen über ihre Daten lässt sich immer schwerer gewährleisten. Konstruktionsunterlagen können mit dem Handy unauffällig abfotografiert, Millionen von Kundeninformationen bequem auf einem Stick in der Hosentasche transportiert und ausgelagerte Mitarbeiterdaten unbemerkt ausgespäht werden. Für alles gibt es zahlungskräftige Abnehmer.

Um den Gefahren zu begegnen, wurde viel investiert: Technische Schutzmaßnahmen und Sicherheitstechnologien sind inzwischen Standard, wenn auch auf unterschiedlichem Niveau. Trotzdem scheint sich die Gefahrenlage nicht zu verbessern – im Gegenteil. Die Angreifer lernen mit, sodass technische Sicherungsmaßnahmen stets durch neue Systemlücken umgangen werden können. Da die Angreifer die Schwachstellen neuer Technologien aufgrund eines höheren Fachwissens meist schneller kennen als die Unternehmensleitung oder die Mitarbeiter, fühlen sich Unternehmen in diesem „Wettrüsten“ unterlegen.

Aus unserer Sicht ist dies jedoch kein Grund zur Resignation: Lange wurde e-Crime aus einer zu technischen Perspektive betrachtet. Oder – um das Gleiche etwas provokanter auszudrücken – die Unternehmensleitung wälzte die Verantwortung auf die IT-Abteilung ab. Sinnvoll ist dies nicht. Denn natürlich hat die IT-Abteilung zwar das beste Verständnis für Software und Daten, das „e“ im e-Crime ist aber letztendlich nicht mehr als das Medium für alle möglichen wirtschaftskriminellen Handlungen. Und hinter virtuellen Handlungen stecken immer tatsächliche Menschen. Mindestens genau so wichtig wie das Wissen um Bits und Bytes ist daher ein Verständnis für die Motive der Täter, für die Art der Delikte und für die Schadenshöhe. All dies hilft den kaufmännischen Bereichen wie der Geschäftsführung, der Internen Revision und Compliance, die Informationssicherheitsstrukturen kritisch zu hinterfragen, sie zu kontrollieren und zu verbessern. Diesen Prozess möchten wir mit unserer Studie unterstützen.



Alexander Geschonneck
Partner
Forensic Technology

Aus diesem Grund haben wir in der vorliegenden Studie bewusst nicht die IT-Abteilungen befragt. Unsere Gesprächspartner waren in erster Linie Geschäftsführer und Vorstände, Leiter Controlling, Rechnungswesen, Finanzen oder Recht, interne Revisoren und Compliance Officer. Dabei zeigen die Ergebnisse klar: Das Wissen um die mit e-Crime verbundenen Risiken ist in den Führungsetagen angekommen. Als wesentliche Gefahren werden dabei insbesondere der Diebstahl von Kunden- und Arbeitnehmerdaten eingeschätzt. Die von betroffenen Unternehmen genannten Schadenshöhen sind dabei zum Teil beachtlich. Gleichzeitig gibt es in der Prävention, Aufklärung und Reaktion deutliche Defizite. Dies liegt unter anderem auch daran, dass als typischer e-Crime-Täter – nicht zuletzt von den Medien – bisher gerne der ausländische Spion oder der böse Hacker in den Vordergrund gestellt wurde und die Informationssicherheit sich hierauf konzentrierte. Unsere Studie kommt dagegen zu einem anderen Ergebnis: Mindestens genauso gefährlich wie unbekannte, „dunkle Mächte“ sind wohl vertraute Menschen wie (ehemalige) Mitarbeiter, Geschäftspartner oder gar die eigenen Kunden.

Trotz zahlreicher Studien und Umfragen haftet e-Crime immer noch etwas Nebulöses, schwer Greifbares an. Es hat sich noch nicht überall durchgesetzt, dass IT auch für klassische wirtschaftskriminelle Handlungen zum Einsatz kommt und unter e-Crime dann nicht nur das Hacken von Webservern zu verstehen ist. Wenn es uns mit dieser Studie gelingt, das Bewusstsein und Verständnis der nichttechnischen Unternehmensbereiche für e-Crime zu schärfen und so etwas Licht in dieses Dunkelfeld zu bringen, haben wir unser Ziel erreicht.

In diesem Sinne wünsche ich Ihnen eine interessante Lektüre.

Ihr

Alexander Geschonneck

Partner

Forensic Technology

Eckdaten zur Studiendurchführung

Analog zu unserer Studie „Wirtschaftskriminalität in Deutschland 2010“ haben wir auch bei der vorliegenden Umfrage ein international renommiertes Sozialforschungsinstitut, die TNS Emnid in Bielefeld, mit der Durchführung der Befragung beauftragt. Der Fragebogen wurde von dem Bereich Forensic von KPMG mit Unterstützung des Bundeskriminalamts (BKA) und des Bundesministeriums des Innern (BMI) konzipiert. Die Mitarbeiter von TNS Emnid wurden im Vorfeld umfassend geschult. Die persönliche Befragung hat sich dabei bewährt, da viele Umfrageteilnehmer insbesondere aufgrund der Komplexität des Themas einen direkten Gesprächspartner wünschen. Insgesamt wurden im Zeitraum April bis Juni 2010 branchenübergreifend 500 Führungskräfte befragt.

Die Struktur des für die Umfrage konzipierten standardisierten Fragebogens orientierte sich an den für die e-Crime-Bekämpfung besonders zentralen Themenbereichen. Aus diesem Grund haben wir mit dem Aufbau des Fragebogens einen 80/20-Ansatz verfolgt: Die von uns vorgegebenen Auswahlmöglichkeiten zu einer Antwort decken die erfahrungsgemäß wichtigsten beziehungsweise häufigsten 80 Prozent der möglichen Antworten ab. Für die verbleibenden 20 Prozent blieb die Möglichkeit, individuelle Antworten zu geben.

Um insbesondere auch Unterschiede abhängig von der Unternehmensgröße festzustellen, wurden Unternehmen unterschiedlicher Größenklassen befragt. Es wurde hier eine repräsentative und nach Branchen und Umsatzzahlen stratifizierte Stichprobe ausgewählt.

Für die von uns durchgeführte Auswertung wurden die Unternehmen auf der Basis ihres Umsatzes in drei Cluster geteilt. Als „groß“ werden Unternehmen mit einem Jahresumsatz von mehr als 3 Milliarden Euro, als „mittelgroß“ Unternehmen mit einem Jahresumsatz zwischen 250 Millionen und 3 Milliarden Euro und als „klein“ Unternehmen mit einem Jahresumsatz zwischen 50 Millionen und 249 Millionen Euro klassifiziert. Diese Cluster entsprechen denen in unseren Studien zur Wirtschaftskriminalität.

Die Auswertungen wurden immer dort, wo signifikante Unterschiede zwischen den Größenklassen bestehen, ausdifferenziert. Aus Gründen der Übersichtlichkeit wurde darauf bei hoher Ergebnishomogenität verzichtet.

Für eine Analyse des Mittelstands war, wie auch schon in unserer Studie zur Wirtschaftskriminalität, eine besondere Abgrenzung dieser Unternehmensgruppe nach den vorhandenen Eigentümer- und Führungsstrukturen wichtig. Als Mittelstand wurden die Unternehmen definiert, die inhaber- oder familiengeführt sind. Von den 500 befragten Unternehmen traf das auf etwa ein Drittel zu (179 Unternehmen).

Bewusst haben wir bei der aktuellen Umfrage darauf verzichtet, die IT-Abteilungen direkt zu befragen. Grund ist, dass wir das Thema e-Crime stärker aus strategischer und betriebswirtschaftlicher Perspektive analysieren wollten. Unsere Gesprächspartner waren in erster Linie Leiter Controlling/Rechnungswesen, Geschäftsführung/Vorstand, Leiter Recht, Leiter Finanzen sowie Revisoren und Compliance Officer.

Abbildung 1
Welche Position nehmen Sie in Ihrem Unternehmen ein?
(familien- / inhabergeführte Unternehmen)

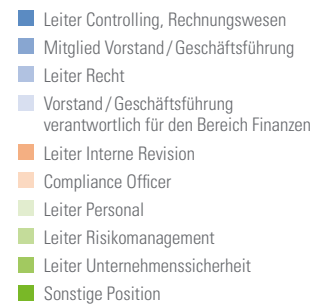
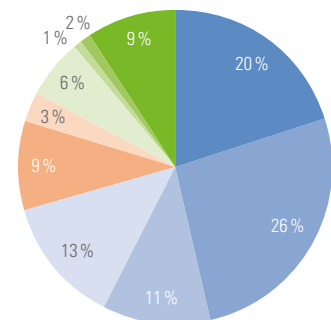
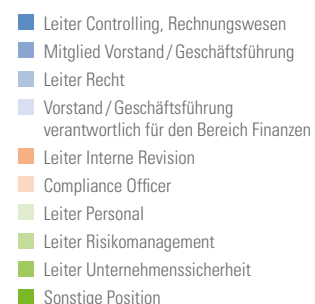
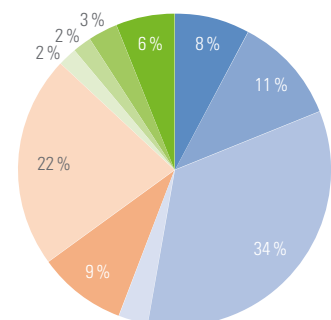


Abbildung 2
Welche Position nehmen Sie in Ihrem Unternehmen ein?
(Großunternehmen)



Quelle: KPMG

Quelle: KPMG

Wesentliche Ergebnisse der Studie

- » Ein Viertel der befragten Unternehmen war in den letzten drei Jahren von e-Crime betroffen. Dabei werden der Diebstahl von Kunden- oder Arbeitnehmerdaten als größtes Risiko eingeschätzt.
- » Die Schadenshöhen rangieren zwischen 100.000 Euro und Millionenbeträgen pro Einzelfall. Vor allem Datendiebstahl und das Ausspähen von geschäftskritischen Unternehmensinformationen verursachen Schäden von über einer Million Euro pro Vorfall.
- » Als Hauptgefahrenquelle identifizieren die Umfrageteilnehmer Mitarbeiter, ehemalige Mitarbeiter und sonstige Insider wie zum Beispiel Geschäftspartner oder Dienstleister. Die Erfahrung der von e-Crime betroffenen Unternehmen bestätigt diese Einschätzung.
- » Je vielfältiger und diffiziler die in Unternehmen eingesetzten Technologien sind, desto komplexer werden die e-Crime-Delikte. Dabei werden Schwachstellen in neuen Technologien ausgenutzt, für die es bisher nur unzureichende Schutzmechanismen gibt. Die Umfrageteilnehmer fühlen sich im „Wettrüsten“ mit den Angreifern unterlegen.
- » Die IT-Abteilung trägt in den meisten Unternehmen, trotz der zunehmend nicht technisch bedingten Schwachstellen, die Hauptverantwortung für die e-Crime-Bekämpfung. Je größer allerdings das Unternehmen ist, desto stärker übernehmen zentrale Bereiche wie zum Beispiel die Interne Revision, das Risikomanagement oder das Compliance Management die Verantwortung für die e-Crime-Bekämpfung.
- » Trotz Krise haben die Umfrageteilnehmer die Ressourcen zur e-Crime-Bekämpfung in den letzten zwei Jahren erhöht und sie planen, dies in Zukunft fortzuführen – wenn auch weniger stark.
- » Zwar wird viel für die Mitarbeitersensibilisierung getan, die Kontrolle wird aber vernachlässigt.
- » Vor allem bei großen Unternehmen spielt „Kommissar Zufall“ in der Aufklärung von e-Crime-Delikten – trotz umfangreicher technischer Monitoringsysteme – eine immer noch allzu gewichtige Rolle.
- » Die Mehrheit der betroffenen Unternehmen hat e-Crime-Delikte gegen ihr Unternehmen zur Anzeige gebracht. Zumeist blieben Anzeigen aus, wenn Angriffe durch bestehende Sicherheitsmaßnahmen erfolgreich abgewehrt wurden beziehungsweise kein finanzieller Schaden entstanden ist. Dennoch besteht eine gewisse Skepsis bei der Zusammenarbeit mit den Strafverfolgungsbehörden.
- » Ein Drittel der von e-Crime betroffenen Unternehmen halten ihre Erstreaktion für nur teilweise angemessen.



e-Crime – Verständnis, handelnde Personen und betroffene Unternehmensbereiche

Ein Viertel der befragten Unternehmen war in den letzten drei Jahren von e-Crime betroffen, 86 Prozent der Umfrageteilnehmer sehen reale Gefahren.

Form vorliegen, wie beispielsweise als Konstruktionspläne, Prozess- und Verfahrensdokumentationen, Softwarequellcode, Produktspezifikationen, Kundendaten oder geistiges Eigentum in Form von Text, Bild und Ton.

e-Crime durchzieht inzwischen weite Teile der Unternehmenslandschaft: Ein Viertel der befragten Unternehmen gab an, in den letzten drei Jahren von e-Crime betroffen gewesen zu sein. Dabei sind große Unternehmen tendenziell mehr im Visier der Kriminellen (31%) als mittelgroße (26%) und kleine Unternehmen (22%). Branchenschwerpunkte sind die Automobilindustrie (35%), Elektronik und Software (32%), Medien und Verlage (32%) und der Maschinenbau (29%). Dies lässt sich mit den in diesen Branchen besonders wertvollen immateriellen Vermögensgegenständen erklären, die in den meisten Fällen in elektronischer

Insgesamt sehen 86 Prozent der Umfrageteilnehmer e-Crime als tatsächliches Risiko für ihre Unternehmen an. Insbesondere die Stützen der deutschen Industrie, der Maschinenbau und die Automobilindustrie, sind hier zu nennen. Auch erwarten 81 Prozent der Umfrageteilnehmer, dass die Risiken in nächster Zeit steigen werden. Gleichzeitig ist die Bedeutung von IT und den damit verarbeiteten Informationen im Unternehmensalltag inzwischen sehr groß: So schätzten 87 Prozent der Umfrageteilnehmer die Abhängigkeit von IKT-Systemen und den durch sie verarbeiteten Daten als hoch oder sehr hoch ein.

Abbildung 3
War Ihr Unternehmen in den vergangenen drei Jahren von e-Crime-Handlungen betroffen?

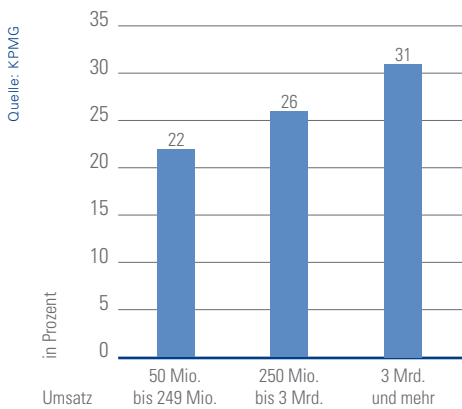
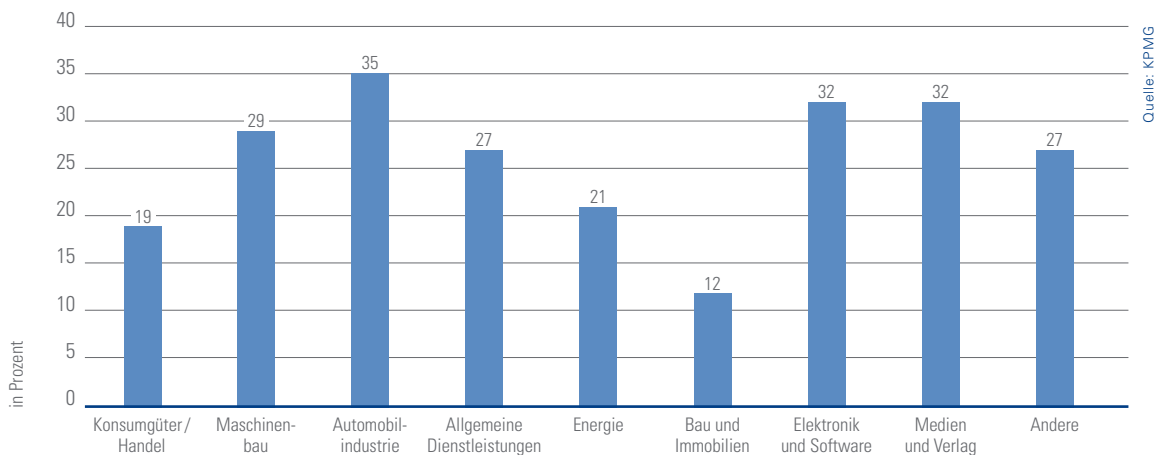


Abbildung 4
War Ihr Unternehmen in den vergangenen drei Jahren von e-Crime-Handlungen betroffen? (nach Branchen)



Der Diebstahl von Kunden- oder Arbeitnehmerdaten wird von den meisten Unternehmen als eines der größten Risiken eingeschätzt.

e-Crime hat viele Gesichter: Das Mithören oder Aufzeichnen von vertraulichen Gesprächen über Mobiltelefone, das Abzapfen von Daten über drahtlose Netzwerke oder das Eindringen in Datenbanksysteme mittels Hackerattacken – bekannte Delikte, die es zu verhindern gilt. Es ist nicht erstaunlich, dass es diese große Vielfalt von e-Crime-Delikten gibt. Schließlich handelt es sich bei e-Crime um nichts anderes als die Nutzung von IKT-Systemen für alle möglichen kriminellen Delikte. Vor allem waren die meisten dieser Handlungen auch schon vor der IT-Durchdringung der Unternehmenswelt möglich, geändert hat sich in erster Linie der damit verbundene Aufwand. Es gilt eine schon lang bekannte Tatsache: Das Verbrechen folgt den Möglichkeiten.

Als besonders bedrohlich schätzen die meisten Unternehmen den Diebstahl von Kunden- oder Arbeitnehmerdaten ein. So nannten 54 Prozent der Befragten den Datendiebstahl durch Interne und 41 Prozent durch Dritte beziehungsweise Externe als großes, also mit einem hohen Schadenspotenzial verbundenes Risiko. Sicherlich ist in diesem Bereich durch zahlreiche öffentlichkeitswirksame Fälle, wie zum Beispiel dem Handel mit Kundendaten von Banken, das Bewusstsein stark geschärft. Außerdem mussten viele der Befragten bereits selbst Erfahrung mit dem Datendiebstahl machen: 62 Prozent der von e-Crime betroffenen Unternehmen wurden in den letzten drei Jahren Opfer von

Datendiebstahldelikten (siehe Abbildung 16).

Ein weiteres wesentliches Risiko ist der Diebstahl von geschäftskritischem Know-how, 51 Prozent der Umfrageteilnehmer fühlen sich hiervon bedroht (siehe Abbildung 5). Auch diese Einschätzung deckt sich mit den tatsächlichen Erfahrungen: 51 Prozent der von e-Crime betroffenen Unternehmen wurden Opfer der Verletzung von Betriebs- und Geschäftsgeheimnissen. Während die Einschätzung dieses Risikos fast unabhängig von der Unternehmensgröße ist, zeigen sich zwischen den Branchen deutliche Unterschiede: Mit einer Nennungshäufigkeit von jeweils über 70 Prozent stechen hier insbesondere die Branchen Maschinenbau (78%), Automobilindustrie (75%) und Elektronik und Software (73%) hervor.

Mobile Datenträger sind die am leichtesten angreifbare Informations- und Kommunikationstechnologie.

Der Laptop im Trolley, der Stick in der Westentasche – noch nie konnten große Informationsmengen so leicht transportiert werden. Das bringt viele Vorteile: So kann der Verkäufer gleich beim Kunden aktuelle Lagerbestände und das Zahlungsverhalten des Gegenübers überprüfen, der Geschäftsführer kann an der Präsentation für einen Großauftrag im Flugzeug arbeiten, sämtliche Ausschreibungsunterlagen hat er auf einem Stick jederzeit griffbereit.

Dass diese Vorteile aber auch mit großen Risiken verbunden sind, zeigen die Ergebnisse unserer Umfrage: Mobile Datenträger werden mit Abstand als das am stärksten gefährdete IKT-System angesehen.

Definitionen

IT-Sicherheit

IT-Sicherheit bezeichnet technische und nicht technische Maßnahmen zur Verringerung des Gefährdungspotenzials für Systeme der Informations- und Kommunikationstechnologie (IKT). Die Bewertung des Gefährdungspotenzials und die Maßnahmenableitung erfolgen unter wirtschaftlichen Gesichtspunkten. Da die IKT-Systeme Medium der Informationsspeicherung und -verarbeitung sind, ist die IT-Sicherheit eng mit der Informationssicherheit verknüpft.

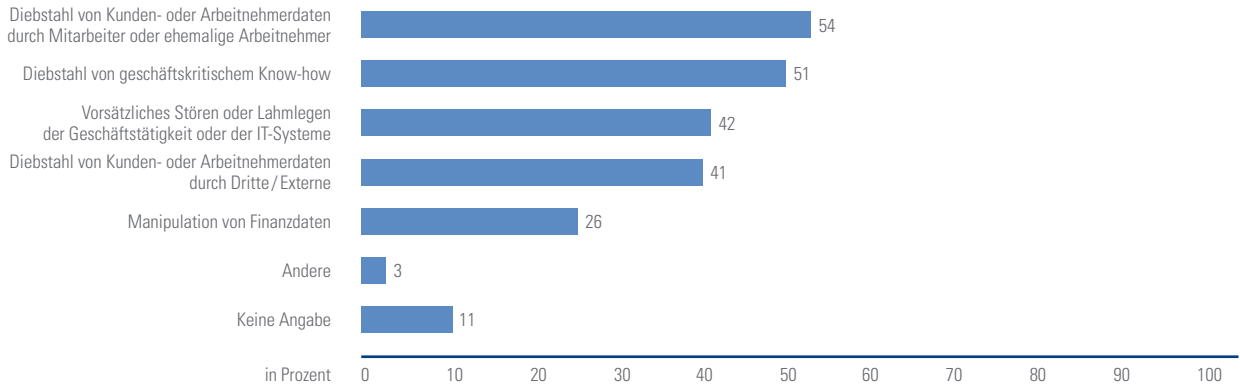
Informationssicherheit

Informationssicherheit schließt IT-Sicherheit mit ein, geht aber weit über die IT-relevanten Fragestellungen hinaus. Die Informationssicherheit bezieht sich ganzheitlich auf den Schutz aller schutzbedürftigen Informationswerte. Daher betrachtet die Informationssicherheit neben der IT auch den Schutz schützenswerter Unternehmensprozesse, den Zugang zu sensiblen Unternehmensbereichen oder den Schutz von Know-how der Mitarbeiter.

e-Crime

e-Crime im Unternehmenskontext bezeichnet die Ausführung von wirtschaftskriminellen Handlungen unter Einsatz von IKT-Systemen zum Schaden eines Unternehmens. Dies kann zur Verletzung von Sachwerten sowie von Verfügungsrechten an immateriellen Gütern führen und/oder die auf IKT-Systemen basierenden Prozesse eines Unternehmens beeinträchtigen. IKT-Systeme können hierbei Ziel der Tathandlung, aber auch Tatwerkzeug an sich sein.

Quelle: KPMG, Jörg Asma, Partner, IT Advisory, Information Protection & Business Resilience



Quelle: KPMG

Abbildung 5

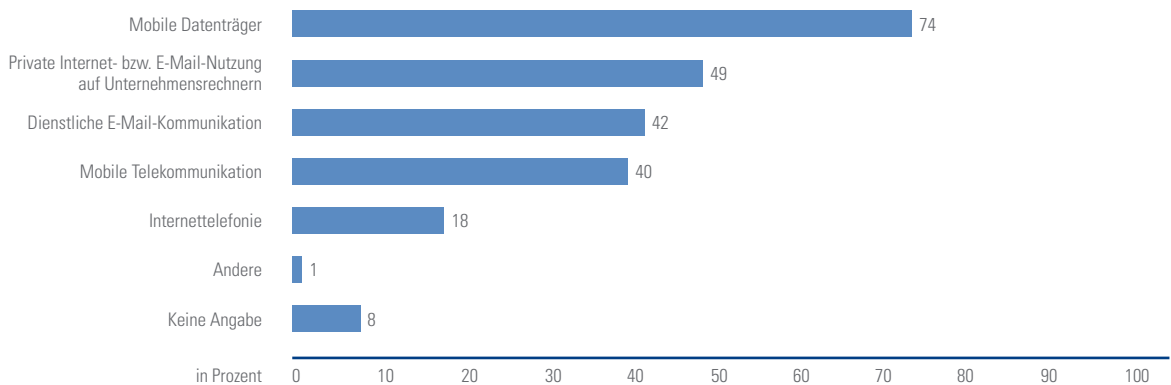
Welche der folgenden e-Crime-Risiken schätzen Sie für Ihr Unternehmen als besonders bedrohlich, das heißt mit hohem Schadenspotenzial ein?

Insbesondere die Automobilindustrie (100%) und der Maschinenbau (83%) stechen hier hervor. Dies lässt sich damit begründen, dass in diesen Branchen das Risiko, das mit einem Diebstahl beispielsweise von Produktinformationen oder Konstruktionsplänen verbunden ist, besonders groß ist. Viele Unternehmen mussten erleben, dass ihre Produkte nach einer Geschäftsreise oder nach der internationalen Expansion plötzlich von der lokalen Konkurrenz originalgetreu nachgebaut wurden. Mobile Datenträger, verlorengegangene Laptops oder das ungesicherte Surfen im öffentlichen Raum spielen dabei eine große Rolle.

vor allem die private Nutzung von Internet und E-Mail auf Dienstrechnern als sehr riskant ein. Eine Erklärung ist, dass insbesondere in der Elektronik- und Software-Industrie ein großes Wissen um gefährliche Angriffsmethoden wie zum Beispiel das Einschleusen von Schadprogrammen, sogenannter Malware, das Ausführen von Phishing-Methoden oder das Durchführen von Man-in-the-Middle-Attacken vorhanden ist. Außerdem basiert die Wertschöpfung aller drei Branchen sehr stark auf immateriellen Werten, die aber im Vergleich zu einer Entwicklungsabteilung in der Automobilindustrie weniger durch einen professionalisierten Know-how-Schutz abgesichert sind. Die geduldete private IT-Nutzung erhöht dabei aufgrund der geringeren Kontrollmöglichkeiten durch Datenschutzbeschränkungen das Risiko zusätzlich.

Abbildung 6

Welche der folgenden Informationstechnologien sehen Sie für Ihr Unternehmen als besonders risikobehaftet an, durch e-Crime Schaden zu nehmen?



Quelle: KPMG

Als Hauptgefahr identifizieren die Umfrageteilnehmer Mitarbeiter, ehemalige Mitarbeiter und sonstige Insider. Die Erfahrung der von e-Crime betroffenen Unternehmen bestätigt diese Einschätzung.



Undurchsichtige Mächte, Geheimdienste, Hacker und Spione? Immer wieder ist in den Medien zu lesen, dass das größte Risiko für die Geschäftsgeheimnisse deutscher Unternehmen von unbekanntem Dritten ausgeht. Viele Unternehmen haben deshalb ihre Informationssicherheitsstrukturen hierauf ausgerichtet und in aufwendige Intrusion-Detection- und Monitoringsysteme investiert.

Unsere Studie kommt zu einem anderen Ergebnis. Wer bereits von e-Crime betroffen war, weiß: Viel gefährlicher als unbekannte Mächte sind oft wohl vertraute Gesichter. So sehen 70 Prozent der von e-Crime betroffenen Unternehmen ehemalige Mitarbeiter oder Insider, die vorsätzlich das vorhandene Wissen missbrauchen, als besonders risikobehaftete Personengruppe an. 46 Prozent

der Betroffenen nennen außerdem Teilzeit- oder Leiharbeitskräfte als hochriskante Gruppe. Diese Personengruppen eint, dass sie gleichzeitig Zugang zu den Systemen haben, oft über detaillierte Prozesskenntnisse verfügen, disziplinarisch aber nur schwer einzubinden sind. Die Branchenverteilung zeigt dabei, dass sich Maschinenbauer – unabhängig von der Betroffenheit – der Gefahr

Fallbeispiel A

Die Gefahr in der Westentasche

USB-Sticks werden immer kleiner, die Gefahren des Datendiebstahls immer größer.

Die Maschinen GmbH A, ein mittelständisches Unternehmen, existiert seit über 100 Jahren und beschäftigt über 1.000 Mitarbeiter. In der Automobil- und Flugzeugbauindustrie ist sie mit technologischen Innovationen seriengefertigter Maschinenbauteile aus Stahl und Kunststoff zum weltweiten Marktführer avanciert.

Um dem Risiko der Wirtschaftsspionage vorzubeugen, hat die Geschäftsführung anlässlich einer verstärkten Konkurrenz aus Fernost eine umfassende Verfahrensrichtlinie an alle Mitarbeiter herausgegeben, die unter anderem dazu auffordert, alle Gefahren und Vorkommnisse

eines potenziellen Informationsabflusses an unautorisierte Dritte sofort zu melden.

Die Vertriebsmitarbeiter des Unternehmens sind durch den immensen Erfolg der innovativen Produkte vor allem im Ausland unterwegs und auf den Einsatz mobiler IT-Geräte angewiesen. Zur Mindestausstattung gehören ein Laptop mit WLAN-Anbindung und Zugangsmöglichkeiten zu gesicherten, internen Datenbereichen, ein Blackberry zur E-Mail-Kommunikation und Telefonie und ein USB-Stick zur einfachen und schnellen Übertragung größerer Datenmengen zwischen einzelnen PCs.

Der zunächst nicht bemerkte Verlust eines USB-Sticks während einer Messeveranstaltung führte dazu, dass einem der größten Konkurrenten des Unternehmens die wichtigsten Produkt- und Kundeninformatio-

nen in die Hände fielen. Die Daten auf dem USB-Stick waren nicht verschlüsselt und obwohl die neueste Verfahrensrichtlinie vorsieht, keine sensiblen Daten auf mobilen Datenträgern zu speichern, hatte es das Unternehmen versäumt, ein durchgängiges Sicherheits- und Verschlüsselungskonzept für mobile IT-Geräte einzuführen, die im Einsatz befindlichen USB-Sticks mit Verschlüsselungssoftware auszustatten und die Mitarbeiter entsprechend zu sensibilisieren. Nach Überprüfung der gesamten mobilen Datenträger im Unternehmen wurde deutlich, dass über 50 Prozent der Speichermedien hochsensible Produkt- und Kundendaten enthielten, die nicht verschlüsselt waren.

Hinweis: Die hier dargestellten Fallbeispiele sind fiktive Fallbeschreibungen und beziehen sich nicht auf tatsächlich existierende Unternehmen. Ähnlichkeiten mit existierenden Unternehmen sind rein zufällig.

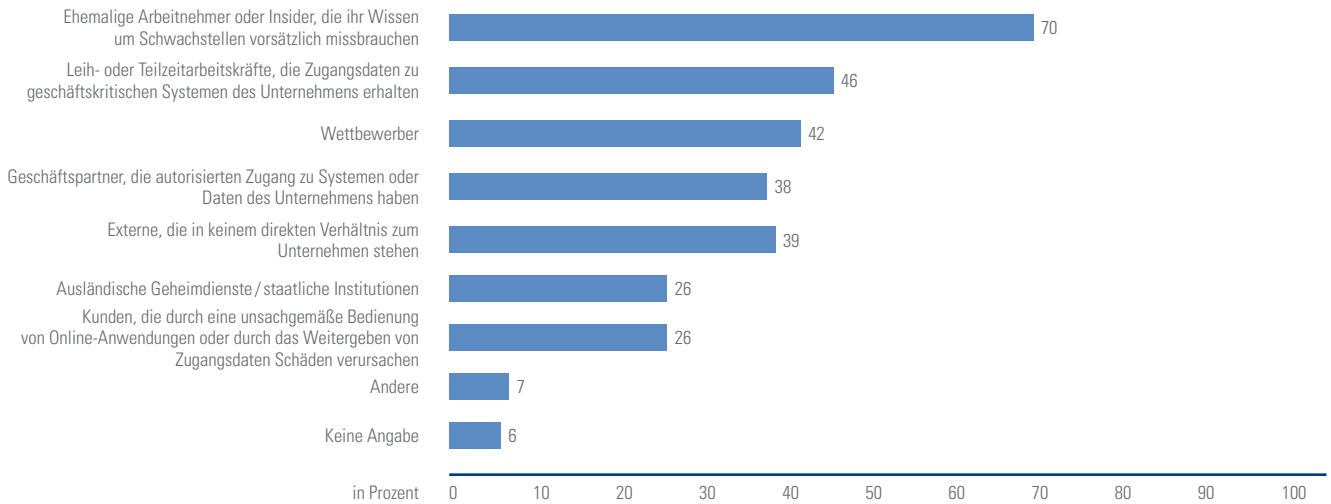


Abbildung 7
 Welche der folgenden Personengruppen schätzen Sie persönlich als bedeutsame Gefahrenquelle für Ihr Unternehmen ein?
 (nur betroffene Unternehmen)

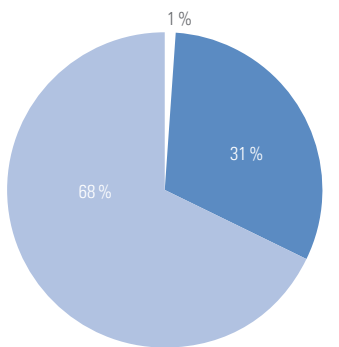
am stärksten bewusst sind, die von den ehemaligen Arbeitnehmern und Insidern ausgeht.

hindern, dass Ex-Mitarbeiter mit vielleicht nicht mehr hundertprozentiger Loyalität weiterhin Zugang zu Systemen haben.

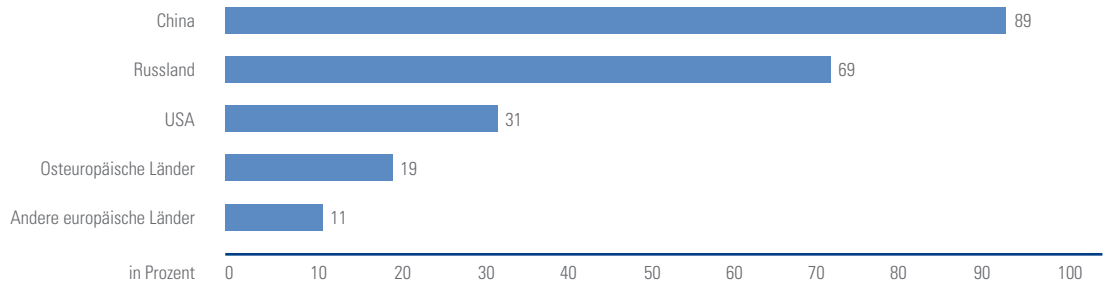
Tatsächlich hat die Gefahr, dass aus ehemaligen Mitarbeitern Täter werden, mit der Krise stark zugenommen. Insbesondere langjährige und loyale Mitarbeiter fühlen sich durch eine krisenbedingte Entlassung oft unfair behandelt. Gleichzeitig steht so manch einer aufgrund des Arbeitsplatzverlustes unter starkem finanziellem Druck. Wer in einer derartigen Situation auch noch leichten Zugriff auf sensible und potenziell wertvolle Daten hat, erfüllt alle drei Voraussetzungen des sogenannten Fraud Triangles – Rechtfertigung, Motivation und Gelegenheit (siehe Abbildung 11). Das Risiko krimineller Handlungen steigt signifikant an. Dies trifft insbesondere für nur sehr kurzfristig angestellte und oft wechselnde Teilzeitarbeitskräfte und Leiharbeiter zu.

Dieses Ergebnis spiegelt sich auch darin wider, dass fast 70 Prozent der Umfrageteilnehmer keine länderspezifischen Risiken sehen. Der ausländische Spion ist damit von nicht so großer Bedeutung, wie dies bei der Zeitungslektüre erscheinen mag. Von den Befragten, die e-Crime doch in einen Zusammenhang mit bestimmten Ländern stellen, wurden die aufstrebenden Wirtschaftsmächte China (89%) und Russland (69%) als besonders bedrohlich eingestuft. Der Branchenvergleich zeigt, dass sich insbesondere Maschinenbau, Automobilindustrie sowie Elektronik und Software länderspezifischen Risiken ausgesetzt sehen. Aufgrund der vergleichsweise hohen Exportquoten und vor allem der Anfälligkeit für Produkt- oder Raubkopien dieser Branchen erstaunt dieses Ergebnis nicht.

Abbildung 8
 Sehen Sie die Gefahrenquellen von e-Crime-Handlungen im Wesentlichen in Verbindung mit konkreten Ländern?



- Nein, e-Crime sehe ich nicht länderspezifisch.
- Ja, e-Crime steht in Verbindung mit bestimmten Ländern.
- Keine Angabe



Quelle: KPMG

Abbildung 9

Befragte Unternehmen, die e-Crime-Handlungen mit bestimmten Ländern verbinden, nennen die folgenden Länder an erster Stelle.

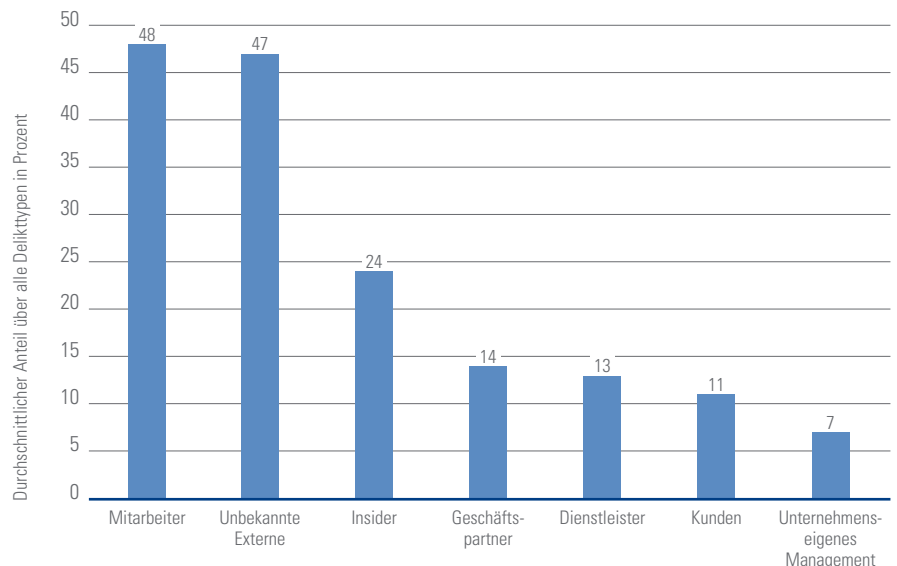
Die dargestellte Risikoeinschätzung in Bezug auf das Risiko „Interne“ wird durch die tatsächliche Erfahrung betroffener Unternehmen bestätigt. So nannten 48 Prozent der Unternehmen, die über die bei ihnen vorgefallenen e-Crime-Vorkommnisse berichteten, ihre eignen Mitarbeiter als Täter, 24 Prozent nannten sonstige Insider und 7 Prozent das Management. Dabei werden Mitarbeiter insbesondere im Rahmen von Daten-diebstahl (62%), Verletzung von Geschäfts- oder Betriebsgeheimnissen (62%), Erpressung (60%), Manipulation von Finanzdaten (58%) und Betrug (55%) zum Täter. Bei der Verletzung von Betriebs- und Geschäftsgeheimnissen sind Insider (38%) als insgesamt zweitwichtigster Täterkreis in Erscheinung getreten. Das

Management ist zwar mit durchschnittlich 7 Prozent über alle Delikttypen die am seltensten genannte Gruppe, tritt aber bei einzelnen Typen wie insbesondere der Manipulation von Finanzdaten (25%) verstärkt in Erscheinung.

Dicht gefolgt werden die Mitarbeiter als am häufigsten genannte Gruppe von unbekanntem Externen, die an 47 Prozent der Delikte beteiligt waren. Sie spielen vor allem im Rahmen von geheimer Überwachung, Wirtschaftsspionage (70%), Verletzung von Schutz- und Urheberrechten (56%), Systembeschädigung oder Computersabotage (56%) und dem Ausspähen und Abfangen von Daten (55%) eine große Rolle.

Abbildung 10

Welcher Täterkreis war bei den begangenen e-Crime-Handlungen beteiligt?



Quelle: KPMG

Die Gruppen Geschäftspartner (14%) und Dienstleister (13%) eint das ihnen oft entgegengebrachte Vertrauen. So sind ein Austausch von sensiblen Daten sowie der Zugang zu Teilen des IT-Systems im Rahmen von integrierten Lieferketten inzwischen Standard. Da diese beiden „Externen“ jedoch oft bei bestimmten Delikttypen wie dem Datendiebstahl, der Verletzung von Geschäfts- oder Betriebsgeheimnissen und der Verletzung von Schutz- und Urheberrechten auftreten, sollte das Vertrauen zumindest kritisch hinterfragt

werden. Denn im Endeffekt gilt das alte Sprichwort: Eine Kette ist nur so stark wie ihr schwächstes Glied. Wichtig ist deshalb ein umfängliches internes Kontrollsystem, das alle potenziellen Schwachstellen und Gefahrenquellen abdeckt. Das Gleiche gilt auch für Kunden, die mit 11 Prozent zwar nur vergleichsweise selten als Täter genannt wurden, jedoch bei einzelnen Deliktarten – insbesondere der Verletzung von Schutz- und Urheberrechten (25%) – eine recht große Rolle spielen.

Fallbeispiel B

Eine Kette ist nur so stark wie ihr schwächstes Glied

Die Maßnahmen zur Gefahrenabwehr gegen e-Crime-Delikte müssen auch Geschäftspartner und Dienstleister des Unternehmens umfassen.

Die Medien-Gruppe B gehört zu den führenden Medien- und Verlagsgesellschaften in Europa mit mehr als 3.000 Mitarbeitern in fast allen EU-Ländern und einem Umsatz von knapp 400 Millionen Euro. Das Produkt- und Serviceangebot der Mediengruppe umfasst neben den klassischen Verlagswerken wie Bücher, Fachmagazine, Zeitschriften und CD-ROMs auch Serviceangebote, wie zum Beispiel Direktmarketing, Telemarketing und Vertrieb von Online-News-Produkten.

Anlässlich eines von seiner US-amerikanischen Muttergesellschaft im letzten Geschäftsjahr gestarte-

ten unternehmensweiten Compliance-Programms entwickelte das Unternehmen ein umfangreiches Regelwerk zur IT- und Informationssicherheit und ließ sich die Kenntnisnahme von Verhaltensrichtlinien von jedem Mitarbeiter schriftlich bestätigen.

Vor einigen Monaten wurden Anschuldigungen in der Tagespresse bekannt, nach denen bei der Medien-Gruppe B ein intensiver Handel mit Kundendaten betrieben wird. Die Geschäftsführung des Unternehmens war sich zunächst unsicher, wie hier zu reagieren ist und ließ durch die Presseabteilung alle Verdachtsmomente gegen das eigene Unternehmen zurückweisen. Die interne Revision hatte die Sicherheitsmaßnahmen zum Schutz von Kundendaten im Haus erst kürzlich überprüft und für gut befunden.

Durch die Einschaltung eines unabhängigen Prüfers wurden die Datenverarbeitungsprozesse noch einmal eingehend geprüft und es wurde festgestellt, dass eine Vielzahl von

Geschäftspartnern und Dienstleistern der Mediengruppe nicht in gleicher Weise wie die Mitarbeiter auf die Einhaltung der Regelwerke und Verhaltensrichtlinien verpflichtet wurden. Es gab einige kleinere Dienstleister wie zum Beispiel Werbe- und Onlineagenturen, die umfangreiche Zugangsrechte zu Kundendaten erhalten hatten, ohne die notwendigen Schutzmechanismen einzuführen. Bei einem dieser Dienstleister wurde ein unrechtmäßiger Abzug von Kundendaten entdeckt. Der Täter konnte jedoch nicht ermittelt werden, da die Agenturen keine Zugriffslogs führten und da keine vertraglichen Verpflichtungen über Sicherheitsmechanismen vereinbart waren.

Hinweis: Die hier dargestellten Fallbeispiele sind fiktive Fallbeschreibungen und beziehen sich nicht auf tatsächlich existierende Unternehmen. Ähnlichkeiten mit existierenden Unternehmen sind rein zufällig.

IT-Abteilungen sind häufig die Achillesferse der e-Crime-Prävention. Die von Systemadministratoren ausgehenden Gefahren werden von den betriebswirtschaftlichen Abteilungen trotz einiger spektakulärer Fälle weiterhin unterschätzt.

Während die Umfrageteilnehmer Insider zu Recht als größte Gefahrenquelle sehen, werden die von Systemadministratoren ausgehenden Gefahren oft unterschätzt. Obwohl sie mit ihren umfassenden Zugangsberechtigungen per Definition Insider sind und vielfältige Gelegenheiten (vergleiche Fraud Triangle) zu e-Crime-Delikten haben, nannten nur 37 Prozent der Umfrageteilnehmer Systemadministratoren als bedeutende Gefahrenquelle. Erfahrungsgemäß übersteigen die Möglichkeiten der Systemadministratoren für

potenzielle e-Crime-Delikte die Vorstellungskraft der Unternehmensleitung. Scheinbar gehen die Unternehmen davon aus, dass Systemadministratoren ihren Zugang zu sensiblen Daten nicht kriminell nutzen.

Aktuelle Fälle beweisen das Gegenteil. So war es ein Mitarbeiter der IT-Abteilung einer Bank, der im Rahmen einer großen Datenmigration sensible Daten kopierte und verkaufte. Auch unsere Beratungserfahrung zeigt: Die IT-Abteilungen sind aufgrund der umfangreichen Administratorenrechte ihrer Mitarbeiter, teilweise wenig formalisierter Prozesse und des fachlichen Know-hows im Rahmen der e-Crime-Prävention häufig die Achillesferse. Hinzu kommen Zeit- und Kostendruck sowie zunehmender Einsatz von externen Kräften. Die internen Kontrollsysteme müssten hier einen Schwerpunkt setzen.

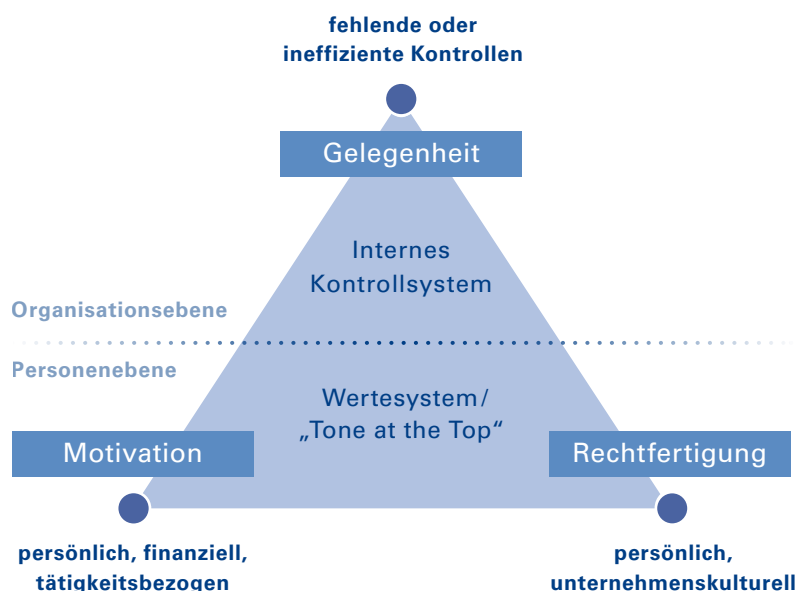


Abbildung 11

Das Fraud Triangle zeigt Faktoren, die Fraud begünstigen
(nach Donald R. Cressey,
US-amerikanischer Soziologe und Kriminologe)

Quelle: KPMG

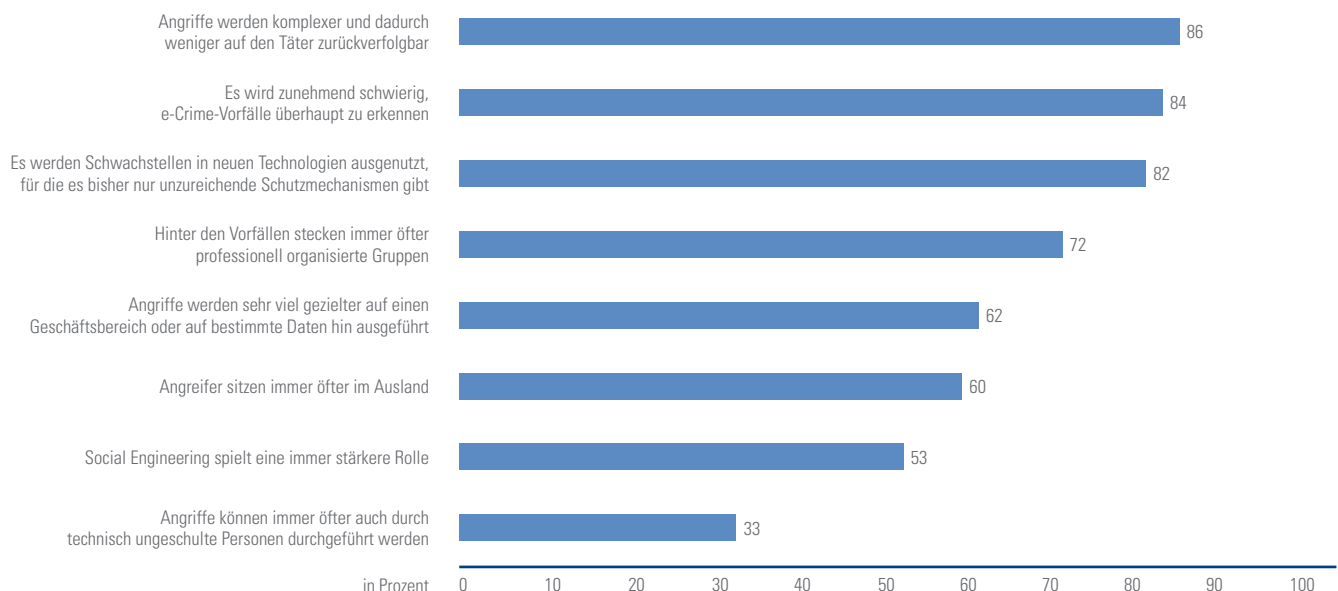
Die Komplexität der Angriffe nimmt proportional zu den in Unternehmen verwendeten Technologien zu. Viele Unternehmensverantwortliche fühlen sich den Angreifern im „Wettrüsten“ unterlegen.

Bis vor ein paar Jahren noch konnten sich Unternehmen mit vergleichsweise einfachen Sicherheitsmaßnahmen vor e-Crime schützen. Firewalls und Antivirusprogramme wurden zum Standardschutz. Doch mit der immer stärker vernetzten Unternehmenslandschaft sowie der Miniaturisierung der Geräte ist es zu einem regelrechten „Wettrüsten“ gekommen. Ein weiterer Faktor ist in der steigenden Komplexität und Fehleranfälligkeit von Softwareprodukten zu sehen. Entwicklungsfehler durch den Hersteller und Konfigurationsfehler durch das Unternehmen bieten verstärkt Angriffsflächen. So inves-

tieren Unternehmen zwar zunehmend in die Informationssicherheit, potenzielle Angreifer entwickeln aber laufend neue Angriffsstrategien und -methoden.

Diesen Trend belegt unsere Studie: So gaben 86 Prozent der Umfrageteilnehmer an, dass die Angriffe immer komplexer werden. 82 Prozent stimmten außerdem der Aussage zu, dass Schwachstellen in neuen Technologien ausgenutzt würden, für die es bisher keine ausreichenden Sicherheitsmaßnahmen gibt. Unternehmen fühlen sich in diesem Wettlauf also unterlegen. Parallel beobachten 63 Prozent der Umfrageteilnehmer, dass die Täter immer gefährlicher werden und relevante Geschäftsbereiche und sensible Daten gezielt angreifen. In der Automobilbranche stimmten sogar 80 Prozent dieser These zu.

Abbildung 12
Wie haben sich e-Crime-Vorfälle in den letzten Jahre verändert?



Quelle: KPMG

Auch spielt das sogenannte Social Engineering nach Aussage von gut der Hälfte (53%) der Befragten eine immer größere Rolle. Hierbei überspringen die Kriminellen die virtuellen Mauern mit Hilfe allzu einfach preisgegebener oder sogar öffentlich publizierter Informationen von interessanten Wissensträgern im Unternehmen. So finden sich in sozialen Netzwerken persönliche und oft auch firmeninterne Details, die bei der Formulierung von individualisierten E-Mails oder fingierten Anrufen bei IT-Support oder Sekretariat helfen. Klickt der angeschriebene Mitarbeiter dann zum Beispiel auf den E-Mail-Anhang, installiert sich unbemerkt eine Schadsoftware, die dann zum Beispiel im Hintergrund Nutzernamen und Passwörter protokolliert. Durch das Social Engineering werden die Angriffe gezielter und damit gefährlicher.

In diesem Zusammenhang ist darauf hinzuweisen, dass derartige Angriffe heutzutage auch von technisch ungeschulten Personen durchgeführt werden können. Einfache, aber hochgefährliche Hackertools werden inzwischen sogar seriösen Computerzeitschriften als CD beigelegt. So hat sich eine Art „Sandkasten“-e-Crime entwickelt: Wo einst eine fundierte Ausbildung nötig war, reicht heute schon ein mit etwas Spieltrieb gepaartes PC-Wissen sowie die notwendige kriminelle Energie.

Fallbeispiel C „Sandkasten“-e-Crime wird zum Problem

Für immer komplexere Angriffe ist immer weniger Know-how notwendig.

Hacker haben die Angewohnheit, ihre Software-Tools im Internet zur Verfügung zu stellen. Obwohl in vielen Fällen strafbewährt, kann sich praktisch jeder solche Tools herunterladen. Auch die Anleitungen sind über das Internet erhältlich. Ein Praktikant der Media Group C beschaffte sich die Software. Er lud sich ein Tool herunter, mit dem sich das Passwort des Betriebssystems verändern oder löschen lässt. Damit

verschaffte er sich Zugriff auf den Computer einer Kollegin und kopierte mehrere zur Veröffentlichung anstehende E-Books. Vor ihrer geplanten Publizierung kursierten die E-Books im Internet.

Das heißt, anstatt der aufwendigen Berechnung des aktuellen Passworts lässt sich einfach durch Veränderung des Passworts ein unautorisierter Zugriff auf einen Computer erlangen. Man startet schlicht ein solches Tool auf einer bootfähigen CD auf dem fremden Computer. Mit ein paar Eingaben, die auch für den Laien möglich sind, ist das ursprüngliche Passwort auf ein Passwort der Wahl veränderbar. Mit Hilfe des neuen Passworts kann man sich auf dem fremden Computer einloggen.

Dies zeigt wie einfach komplexe Angriffe möglich sind. Es zeigt aber auch, dass die Tat durch eine durchgängige Betreuung des Praktikanten zur verhindern gewesen wäre. Auch ein Rechner mit deaktivierter Bootmöglichkeit von CD-ROM, USB etc. hätte diesen Angriff verhindern können.

Hinweis: Die hier dargestellten Fallbeispiele sind fiktive Fallbeschreibungen und beziehen sich nicht auf tatsächlich existierende Unternehmen. Ähnlichkeiten mit existierenden Unternehmen sind rein zufällig.

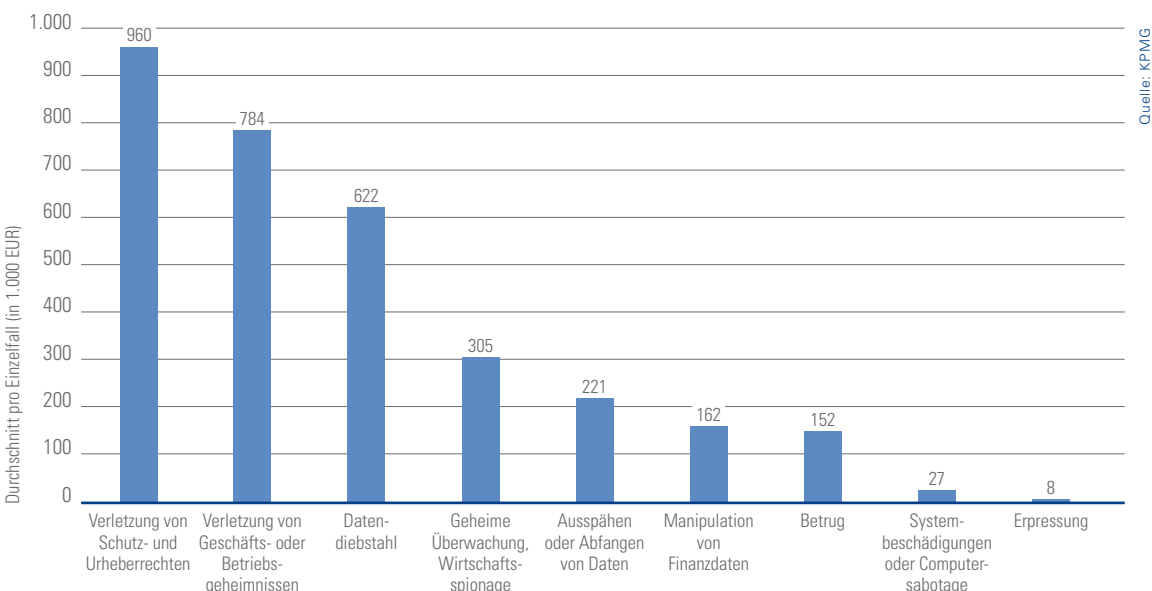
Die Schadenshöhe bei e-Crime-Delikten bewegt sich pro Einzelfall zwischen wenigen 1.000 Euro bis zu Millionenbeträgen. Vor allem die Verletzung von Schutz- und Urheberrechten verursacht Schäden von über einer Million Euro pro Vorfall.

Aufgrund der hohen Variabilität und uneinheitlichen Berechnungsmethoden ist eine exakte Analyse der Schadenshöhen je Delikttyp nur schwer möglich. So nennt die Energie- und Maschinenbaubranche den Kundenverlust als wichtigstes Kriterium zur Schadensbestimmung, wobei im Maschinenbau außerdem die Verschlechterung der Wettbewerbs- und Innovationssituation eine erhebliche Rolle spielt. In der Automobil-, Software- und Medienbranche bestimmen die mit e-Crime verbundenen Reputationsschäden we-

sentlich die Schadenshöhe. Auch wenn viele der genannten Schadentypen nur schwer auf den Euro genau zu beziffern sind, lassen sich auf der Basis der vorliegenden Ergebnisse einige interessante Schlüsse ziehen.

Zunächst einmal ist festzuhalten, dass die genannten Schadenshöhen in dieser Studie auf deutlich höhere wirtschaftliche Verluste für die deutsche Wirtschaft hindeuten als bisher angenommen. In diversen Studien und Schätzungen ist die Rede von einstelligen Milliardenbeträgen. Würde man nun die in dieser Studie angegebenen Schadenshöhen von durchschnittlich etwa 300.000 Euro pro Delikt mit den in der Polizeilichen Kriminalstatistik genannten Fällen der Computerkriminalität multiplizieren, käme man zumindest auf zweistellige Milliardenbeträge. Die Polizeiliche Kriminalstatistik erfasst natürlich nur die tatsächlich gemeldeten Fälle, wie groß die Dunkelziffer ist, lässt sich dagegen nicht genau sagen.

Abbildung 13
Welche Schadenshöhen würden Sie für die einzelnen e-Crime-Vorfälle ansetzen? (von e-Crime betroffene Unternehmen)



Mit der Spezifizierung der Schadenshöhen nach Delikttypen in dieser Studie und weiteren Forschungsergebnissen in der Zukunft kann aber ein deutlich höherer Schaden angenommen werden.

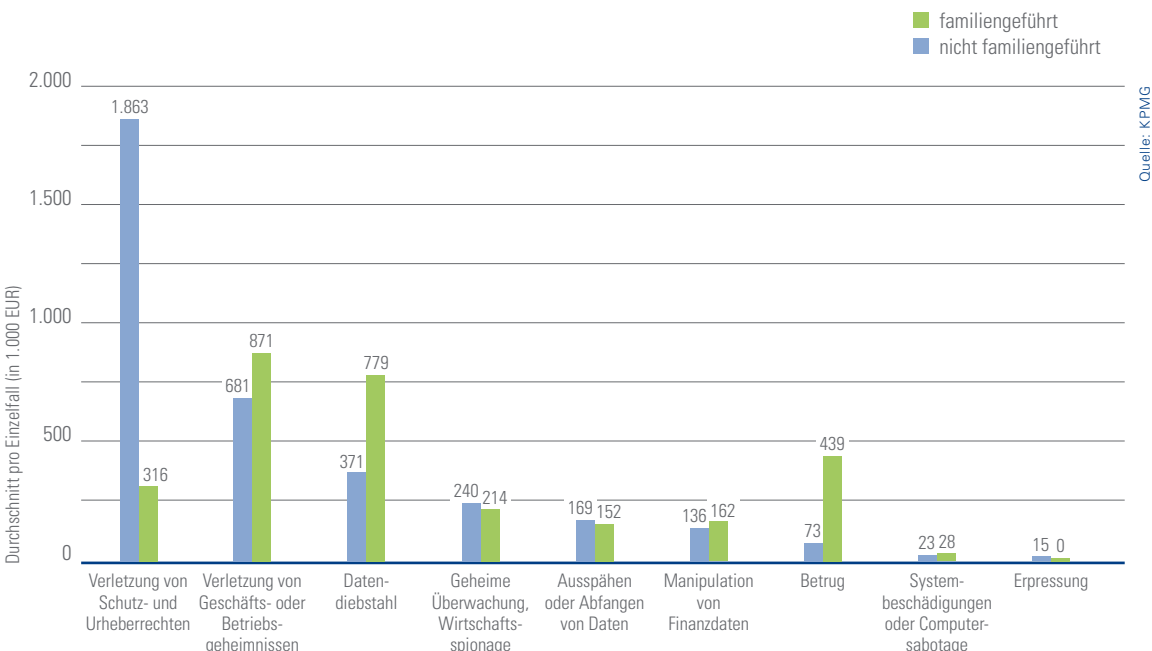
Dabei verursachen die Verletzung von Schutz- und Urheberrechten, die Verletzung von Geschäfts- und Betriebsgeheimnissen und der Datendiebstahl mit Abstand die größten Schäden pro Einzelfall: Bei jedem dieser Delikttypen nannten die Umfrageteilnehmer im Schnitt Beträge von zum Teil deutlich über einer halben Million Euro pro Einzelfall.

Interessant ist auch, dass der Datendiebstahl insbesondere bei mittelständischen Unternehmen enorme Schäden verursacht. Während sowohl kleinere als auch große Unternehmen eine durchschnittliche Schadenshöhe von etwa 160.000 Euro angaben, schätzen mittelständische Unternehmen den Schaden pro Einzelfall auf über 1,2 Millionen Euro.

Für diese Unternehmen bedeutet das: e-Crime kann zu bestandsgefährdenden Schäden führen. Auch wenn die genannten Beträge für Großunternehmen zum Teil noch „aus der Portokasse“ zu zahlen sein mögen, sind mittelständische Betriebe in ihrer Existenz bedroht.

Die Differenzierung nach Eigentümerstruktur zeigt: Im Schnitt ist die Schadenshöhe bei familiengeführten Unternehmen um 20 Prozent höher als bei nicht familiengeführten Unternehmen. Dieses Ergebnis ist auf die mit extrem großen Schäden behaftete Deliktart Verletzung von Schutz- und Urheberrechten zurückzuführen: Die Schadenshöhe bei Familienunternehmen übertraf die anderer Unternehmen hier fast um den Faktor fünf. Im Durchschnitt über alle Deliktarten stehen dem niedrigere Schadenshöhen insbesondere in den Bereichen geheime Überwachung, Wirtschaftsspionage und Datendiebstahl gegenüber.

Abbildung 14
Welche Schadenshöhen würden Sie für die einzelnen e-Crime-Vorfälle ansetzen?



Fokus: Moderne Wirtschaftsspionage*

* *Wirtschaftsspionage wird in der Öffentlichkeit meistens als Begriff für alle Formen der Spionage in der Wirtschaft verwendet. Wir haben uns deshalb entschieden, diesen Begriff für unsere Studie übergreifend zu verwenden. Richtigerweise müsste aber zwischen Industrie- und Wirtschaftsspionage unterschieden werden. Während unter Industrie-spionage die illegale Beschaffung von Know-how durch konkurrierende Unternehmen verstanden wird, meint Wirtschaftsspionage eher die staatlich gelenkte oder gestützte Ausforschung von Informationen in der Wirtschaftswelt.*

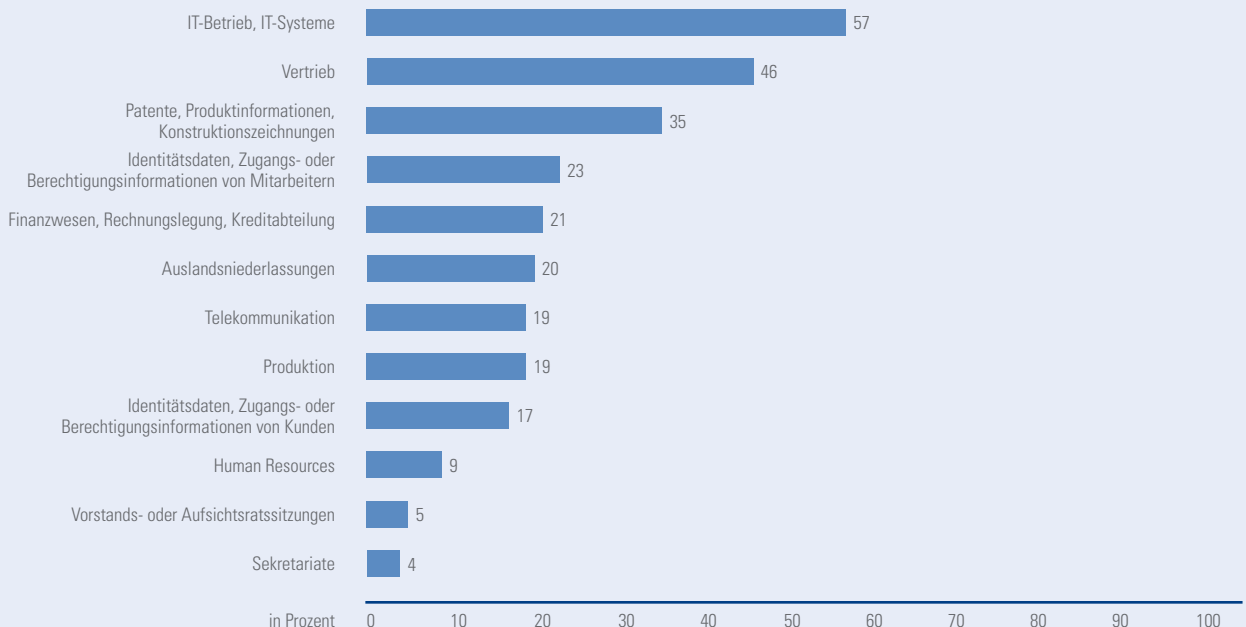
„Fleißig, unauffällig und zuvorkommend“ – der Austauschstudent aus Fernost war als Praktikant sehr beliebt. Über mehrere Sommerferien hinweg unterstützte der Konstruktionstechniker die F&E-Abteilung eines süddeutschen Maschinenbauers, oft machte er abends Überstunden. Was niemand ahnte: Zu später Stunde kopierte er sensible Firmenunterlagen und schickte sie an seine staatlichen Auftraggeber in der Heimat. Nur durch einen Zufall wurde der Informationsabfluss bemerkt. Der sympathische Praktikant entsprach nicht den gängigen Klischees und doch war er ein Spion.

Spionage hat sich verändert, seit ein paar Jahren sind immaterielle Vermögensgegenstände nicht nur verstärkt im Visier, der Abzug relevanter Informationen ist dank moderner Technologien auch deutlich einfacher geworden. Der Anfang Juni 2010 vom Bundesministeriums des Innern veröffentlichte Verfassungsschutzbericht 2009 kommt zum gleichen

Ergebnis: „Deutschland als technologie- und exportorientierte Nation lebt von den ‚Rohstoffen‘ Wissen, Wissensvorsprung und Innovation. Sie sind zentrale Objekte der Wertschöpfungskette und zugleich ihre entscheidenden Wettbewerbsvorteile. Dies weckt Begehrlichkeiten von Konkurrenzunternehmen und fremden Staaten. (...) Staaten wie Russland und China betreiben mit ihren Nachrichtendiensten aktiv Spionage in den Bereichen Wirtschaft, Wissenschaft und Forschung. (...) Die größte Bedrohung stellen derzeit internetbasierte Angriffe auf Computersysteme und mobile Kommunikation deutscher Wirtschaftsunternehmen und Behörden dar.“

Insbesondere Großunternehmen haben die Gefahrenlage – nicht zuletzt dank ausführlicher Medienberichterstattung – erkannt. Und auch wenn sich so manch ein mittelständischer Unternehmer weiterhin fragen mag: „Wer will mich schon ausspähen?“, verbreitet sich die Erkenntnis, dass

Abbildung 15
Welche Bereiche Ihres Unternehmens waren Ziel der e-Crime-Delikte?
Selektion: Befragte, deren Unternehmen in den vergangenen drei Jahren von e-Crime betroffen waren



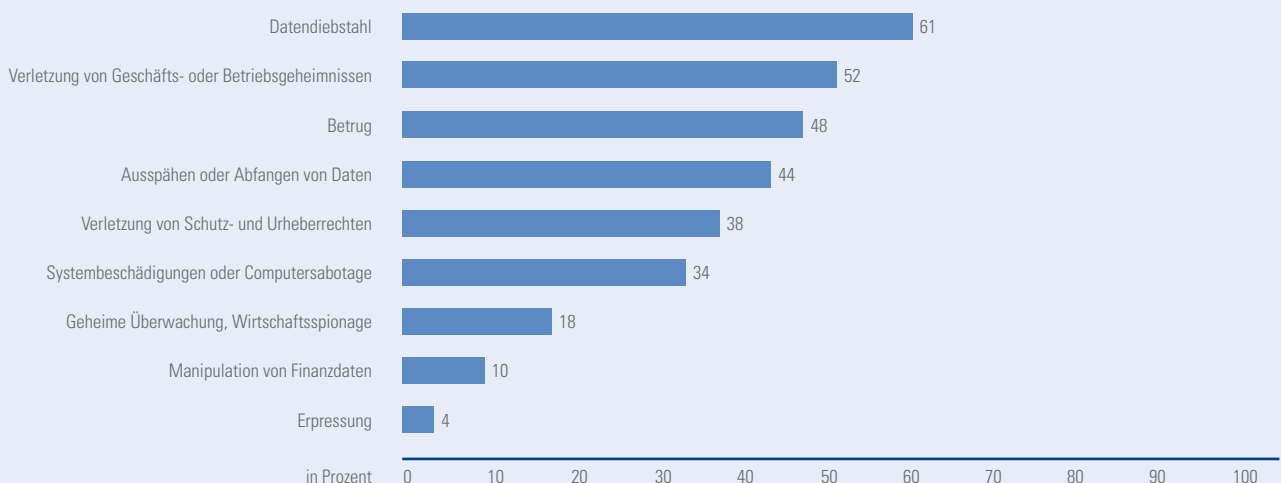
das Wirtschaftsspionagerisiko mit der Unternehmensgröße nichts zu tun hat. Im Gegenteil: Insbesondere der Erfolg kleiner und mittelgroßer Unternehmen basiert nicht selten auf sehr innovativen und einzigartigen Patenten oder einer werthaltigen, zentralen Kundendatenbank. Werden diese Informationen ausgespäht, kann die Existenz bedroht sein. Zudem besteht natürlich auch das Risiko, dass über den Umweg eines mittelständischen (Dienstleistungs-)Unternehmens ein Großkunde ausgespäht werden kann. Hier liegen für das Dienstleistungsunternehmen gegebenenfalls hohe Haftungsrisiken.

Analysiert man die angegriffenen Unternehmensbereiche von betroffenen Unternehmen, wird schnell klar, dass in den meisten Fällen eine Form der Wirtschaftsspionage – sei es aus dem Ausland oder aus Deutschland – zumindest eine nahe liegende Erklärung liefert. Ob IT, Vertrieb, Patente oder Auslandsniederlassung: All dies sind Bereiche, die gern im Visier

der modernen Spione stehen. Auch nennen 73 Prozent der Umfrageteilnehmer die Gewinnung von Wettbewerbsvorteilen als Motivation für e-Crime-Delikte.

Auf die Frage der betroffenen Unternehmen nach verschiedenen e-Crime-Handlungen nennen zwar nur 18 Prozent der Befragten die geheime Überwachung und Wirtschaftsspionage. Bedenkt man allerdings die Nennungshäufigkeit von eigentlich klassischen Spionagehandlungen wie Datendiebstahl und Verletzung von Betriebs- und Geschäftsgeheimnissen, lässt sich dies vor allem damit erklären, dass viele Unternehmen ein veraltetes Bild von Wirtschaftsspionage haben. An den internen Täter, wie den Konstruktionsmitarbeiter in unserem Eingangsbeispiel, scheinen viele in diesem Zusammenhang nicht zu denken. Insbesondere Großunternehmen scheinen hier schon einen Schritt weiter: Mit 30 Prozent ist die Nennungshäufigkeit in dieser Gruppe überproportional hoch. Nach unserer

Abbildung 16
 Von welchen der genannten e-Crime-Handlungen war Ihr Unternehmen in den letzten drei Jahren betroffen?
 Selektion: Befragte, deren Unternehmen in den vergangenen drei Jahren von e-Crime betroffen waren



Erfahrung lässt sich dies nicht damit erklären, dass Großunternehmen öfter angegriffen werden. Tatsächlich befinden sich mittelständische Unternehmen – nicht zuletzt aufgrund der unzureichenden technischen und organisatorischen Präventionsmaßnahmen – mindestens ebenso sehr im Visier der Angreifer.

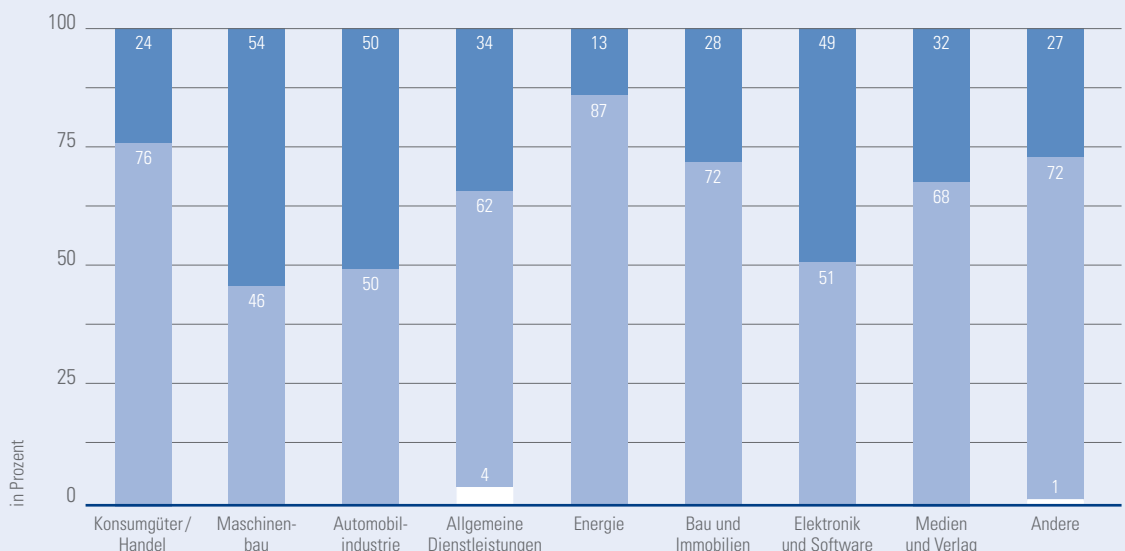
Länderspezifische Risiken sehen vor allem Vertreter der Branchen Maschinenbau, Automobilbau sowie Elektronik und Software. Grund ist zum einen die hohe Exportquote dieser Branchen und zum anderen die große Bedeutung immaterieller Vermögensgegenstände wie Patente und Wissen. Als riskante Länder werden dabei vor allem China und Russland empfunden, die Einschätzungen des Bundesministeriums des Innern werden hier also bestätigt.

Als Fazit lässt sich sagen: Den meisten e-Crime-Delikten liegt eine Form des Ausspähens von Daten zugrunde. Nicht immer müssen dabei aber ausländische Konkurrenzunternehmen

im Spiel sein, auch wenn die von aufstrebenden und um technologischen Anschluss kämpfenden Nationen ausgehenden Gefahren zunehmen. Dabei werden die Unternehmen aber seltener direkt aus dem Ausland ausgespäht. Die in vielen Köpfen immer noch vorherrschenden – und durch die Presse gern gepflegten – Bilder vom Spion, der mit hochgekrempeltem Kragen monatelang vor dem Eingangstor lauert, sind veraltet. Moderne Spionage bedient sich häufig Unternehmensinterner wie (ehemaliger) Mitarbeiter oder Dienstleister. Auch die fortschreitende Integration entlang der Lieferkette erhöht die Spionagerisiken. Neben der Beseitigung technischer Schwachstellen muss daher bei der e-Crime-Bekämpfung vor allem auch die menschliche Motivation und Rechtfertigung (zum Beispiel von entlassenen Mitarbeitern), aber auch die Integrität neuer Mitarbeiter (zum Beispiel schon bei der Rekrutierung) im Auge behalten werden.

Abbildung 17
Sehen Sie die Gefahrenquellen von e-Crime-Handlungen im Wesentlichen in Verbindung mit konkreten Ländern?
(nach Branchen)

- Ja, e-Crime steht in Verbindung mit bestimmten Ländern.
- Nein, e-Crime sehe ich nicht länderspezifisch.
- Keine Angabe



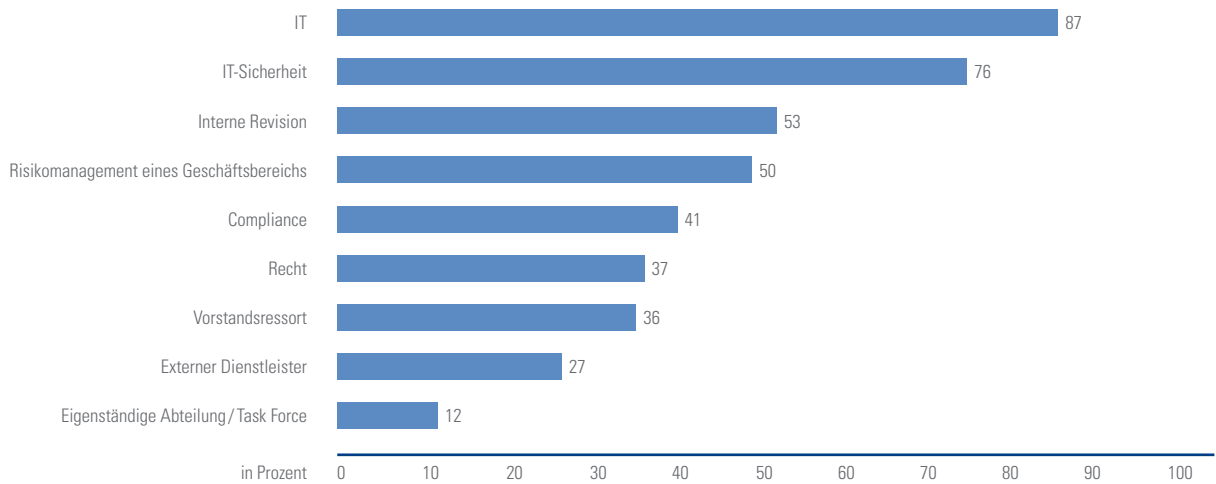
Quelle: KPMG



© 2010 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Konzerngesellschaft der KPMG Europe LL, und Mitglied des KPMG Netzwerks. KPMG ist ein Markenname der KPMG International Cooperative („KPMG International“), einer juristisch in Panama registrierten, aber in den USA steuerlich ansässigen, Personengesellschaft. Alle Rechte vorbehalten. Printed in Germany. KPMG und das KPMG-Logo sind eingetragene Warenzeichen von PwC LLP, New York, NY, USA.



Prävention, Entdeckung, Reaktion



Quelle: KPMG

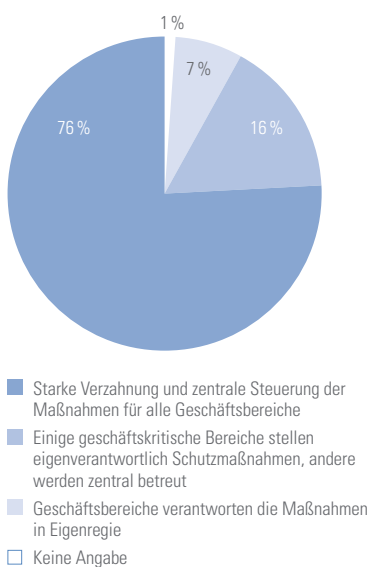
Abbildung 18
Welche Abteilung / Organisationseinheit verantwortet in Ihrem Unternehmen die e-Crime-Bekämpfung?

Die Hauptverantwortung für die e-Crime-Bekämpfung liegt in der IT-Abteilung. Je größer das Unternehmen, desto stärker werden Bereiche wie Interne Revision, Risikomanagement und Compliance involviert.

die Geschäftsbereiche das Thema in Eigenregie verantworten sollten.

Wie zu erwarten war, sind die Hauptverantwortlichen für die e-Crime-Bekämpfung in der IT beziehungsweise der IT-Sicherheit zu finden. Grund ist das in diesen Abteilungen naturgemäß besonders stark vorhandene fachliche Know-how. Je größer das Unternehmen, desto stärker werden andere Bereiche wie insbesondere die Interne Revision, das Risikomanagement und/oder Compliance mit der e-Crime-Bekämpfung betraut. Die Umfrageteilnehmer gaben mit wachsender Unternehmensgröße an, dass die rein fachliche Expertise für die Wahl der organisatorischen Verankerung weniger von Bedeutung ist. Stattdessen stehen hier der potenzielle finanzielle Schaden und seine Auswirkungen auf das gesamte Unternehmen, die Integration in bestehende interne Kontrollsysteme und die befürchteten Reputations- und Imageschäden im Vordergrund. Insbesondere auch vor dem Hintergrund der oben beschriebenen e-Crime-Risiken durch Mitarbeiter der IT-Abteilung erscheint eine Involvierung anderer Bereiche von großer Bedeutung.

Abbildung 19
Wie würden Sie die gegenseitige Verzahnung der einzelnen Geschäftsbereiche in Bezug auf Maßnahmen zur Prävention, Erkennung und Reaktion auf e-Crime-Delikte charakterisieren?



e-Crime ist ein bereichsübergreifendes und dadurch hochkomplexes Thema: Ein Informationsleck kann sich im Vertrieb genauso wie in der Entwicklungs- oder Finanzabteilung befinden, und es können Mitarbeiter ebenso wie Kunden- oder Geschäftspartnerdaten betroffen sein. Diese Komplexität spiegelt sich auch in der organisatorischen Verankerung des Themas bei den Studienergebnissen wider: Über praktisch alle Größenklassen sowie Branchen hinweg nannten die Umfrageteilnehmer im Durchschnitt vier verschiedene Bereiche, die jeweils Verantwortung für die e-Crime-Bekämpfung tragen.

Allerdings befürworten gleichzeitig 76 Prozent der Umfrageteilnehmer eine starke Verzahnung und zentrale Steuerung der Aktivitäten, nur 7 Prozent vertreten die Meinung, dass

Trotz Krise haben die Umfrageteilnehmer die Ressourcen zur e-Crime-Bekämpfung in den letzten zwei Jahren erweitert und planen sie – wenn auch weniger stark – in Zukunft weiter zu erhöhen.

Erwartungsgemäß korreliert die Anzahl der auf die e-Crime-Bekämpfung spezialisierten Mitarbeiter stark mit der Unternehmensgröße: Kleine Unternehmen beschäftigen derzeit durchschnittlich fünf entsprechend spezialisierte Mitarbeiter, in mittelgroßen sind es sechs und in großen Unternehmen zwölf Mitarbeiter.

Während in praktisch allen Unternehmensbereichen der Rotstift ange-setzt wurde, wird in die Bekämpfung von e-Crime weiterhin investiert: Im Durchschnitt haben die befragten Unternehmen ihre personellen Kapazitäten in den vergangenen zwei

Jahren um 50 Prozent gesteigert, in den nächsten zwei Jahren planen die Umfrageteilnehmer die Anzahl der in diesem Bereich tätigen Mitarbeiter um weitere 17 Prozent zu erhöhen. Gerade in großen Unternehmen geht dies – angetrieben von der Forderung nach proaktivem Handeln – mit dem Auf- und Ausbau von Compliance-Abteilungen einher.

Die Investitionen in Sach- und Personalkosten folgen dem gleichen Trend: Auch wenn es zwischen den Unternehmensklassen signifikante Unterschiede gibt, zeigt sich doch über alle Klassen und Branchen hinweg, dass im Durchschnitt die Budgets für die e-Crime-Bekämpfung steigen.

Abbildung 20
Wie viel investiert Ihr Unternehmen pro Jahr in die e-Crime-Bekämpfung?

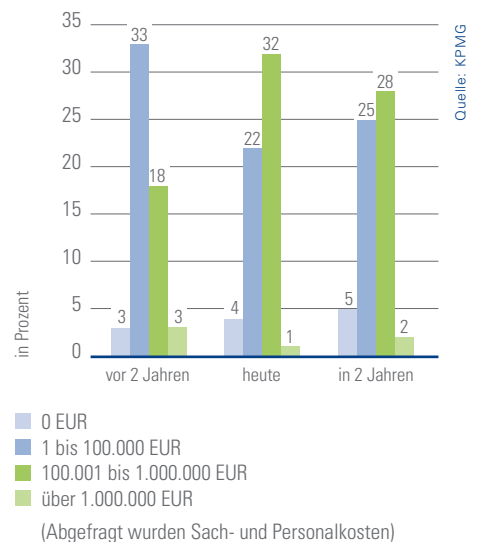
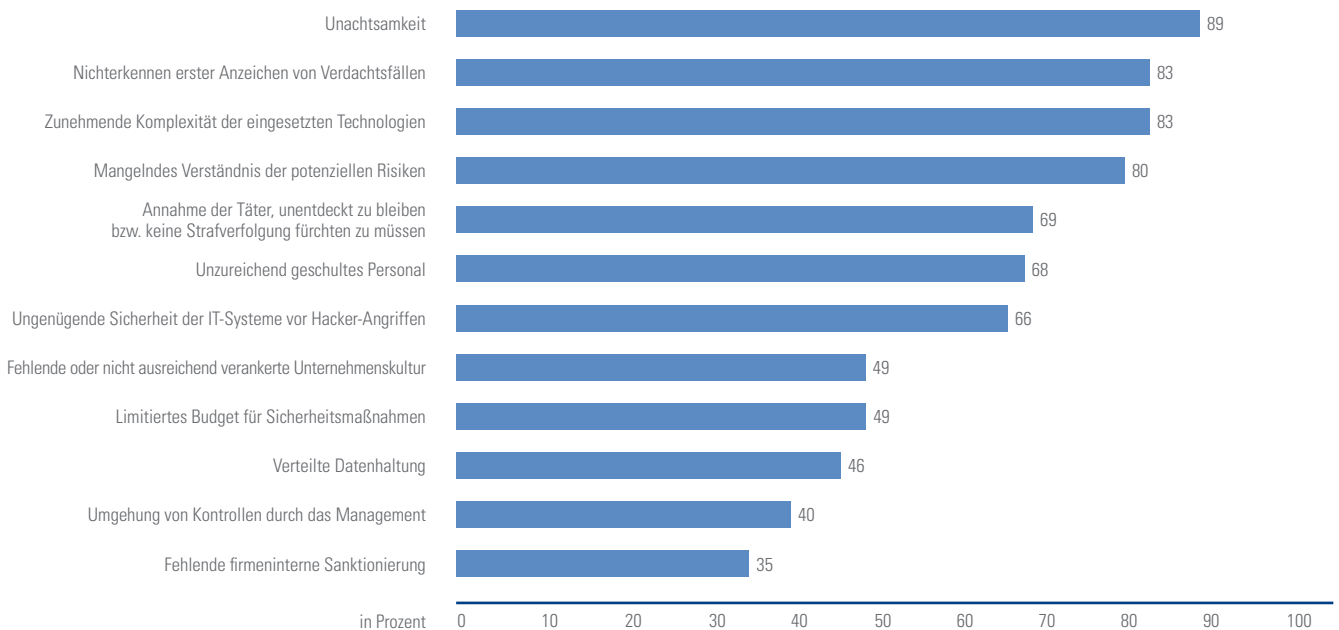
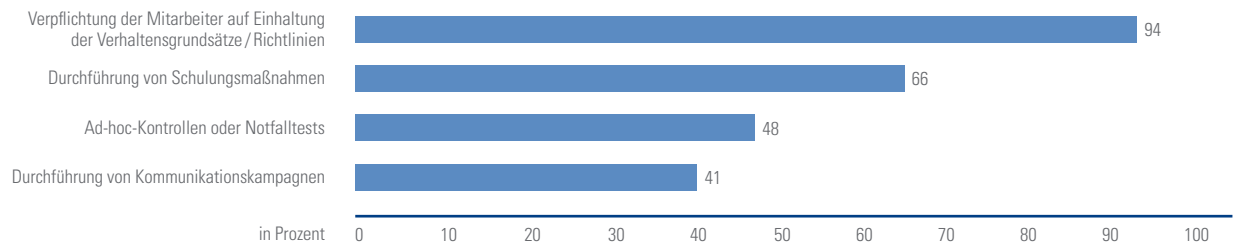


Abbildung 21
Welche Umstände begünstigen Ihrer Meinung nach das Entstehen von e-Crime besonders?





Quelle: KPMG

Abbildung 22

Welche Maßnahmen haben Sie zur Sensibilisierung Ihrer Mitarbeiter bezüglich bestehender e-Crime-Risiken ergriffen?

Präventivmaßnahmen im Rahmen der Mitarbeitersensibilisierung und -verpflichtung sind weitverbreitet. Dem „Tone at the Top“ wird eine große Bedeutung zugemessen. Die regelmäßige Kontrolle, ob die Regelwerke auch eingehalten werden, wird dagegen vernachlässigt.

e-Crime braucht ein Einfallstor und in vielen Fällen ist das – oft unbewusst – der einzelne Mitarbeiter. Eine noch so ausgeklügelte Informationssicherheitsstruktur ist machtlos, wenn Mitarbeiter zum Beispiel fahrlässig mit Zugangsdaten umgehen, mobile Datenträger unverschlüsselt transportieren oder potenziell gefährliche Programme in Eigenregie installieren. Auch arbeiten immer mehr Mitarbeiter im Home Office oder unterwegs. Der verantwortungsbewusste Umgang mit IT sowie der Schutz sensibler Daten entziehen sich dem Arbeitgeber damit weitestgehend.

Die Umfrage zeigt, dass die Unternehmen sich der immensen Bedeutung sensibilisierter und informierter Mitarbeiter bewusst sind. So nannten die Teilnehmer Unachtsamkeit und das Nichterkennen erster Anzeichen von Verdachtsfällen als die wichtigsten Umstände, die e-Crime begünstigen.

Insofern ist es erfreulich, dass Maßnahmen zur Sensibilisierung der Mitarbeiter weitverbreitet sind: So gaben 94 Prozent der Umfrageteilnehmer an, die Mitarbeiter regelmäßig auf die Einhaltung von schriftlich definierten Verhaltensgrundsätzen und Richtlinien zum Umgang mit den IKT-Systemen zu verpflichten.

Nach den mobilen Datenträgern nannten die Studienteilnehmer die private Internet- beziehungsweise E-Mail-Nutzung auf Firmenrechnern als besonders risikobehaftetes IKT-System. Oft kann der private Internetzugriff über Firmensysteme aus unternehmenskulturellen Gründen nicht verboten werden. Umso wichtiger ist zumindest eine klare Regelung und Abgrenzung von zulässiger und nichtzulässiger Nutzung und deren regelmäßige Kontrolle. Erfreulich ist daher, dass fast alle Umfrageteilnehmer (92 %) angaben, eine derartige Regelung schriftlich definiert zu haben. Unterschiede nach Unternehmensgröße, Betroffenheit und Eigentümerstruktur gibt es hierbei kaum.

Auch wenn die Umfrageteilnehmer klar definierten Verhaltensgrundsätzen offenbar Bedeutung zumessen, wird bei gut der Hälfte der Unternehmen darauf verzichtet, die Einhaltung der Verhaltensgrundsätze und Richtlinien zu überprüfen: Nur 48 Prozent der Umfrageteilnehmer gaben an, Ad-hoc-Kontrollen oder Notfalltests durchzuführen. Selbst bei Großunter-

nehmen lag die Quote nur bei knapp über 50 Prozent. Positiv sticht alleine die Bau- und Immobilienbranche hervor, bei der Kontrollen mit 68 Prozent recht weit verbreitet sind. Als Fazit lässt sich an dieser Stelle festhalten: Ein ausgewogenes Verhältnis zwischen „Tone at the Top“, Verpflichtung, regelmäßiger Kommunikation, Schulung und Kontrolle besteht bei den meisten Unternehmen nicht.

Positiv ist dagegen, dass mit 89 Prozent ein hoher Anteil der Umfrageteilnehmer angab, dass das Manage-

ment die Bedeutung der Informationssicherheit und der e-Crime-Prävention eindeutig kommuniziert. Deutlich unterdurchschnittlich schneidet hier die Branche Medien und Verlage ab, in der immerhin 21 Prozent die sonst üblichen Instrumente wie Unternehmenswerte und Grundsätze nicht nutzen. Bedenklich, wenn man berücksichtigt, dass in dieser Branche digitalisierte Inhalte und deren Verfügbarkeit häufig das wichtigste Kapital sind.

Fallbeispiel D

Die Policy als Feigenblatt

Unternehmensrichtlinien sind wichtig, ohne entsprechende Kontrollen können sie aber zu einer trügerischen Sicherheit führen.

Ganzheitliche Konzepte zur Regelung der privaten Nutzung von geschäftlich bereitgestellter IT-Infrastruktur werden in Unternehmen sehr oft vernachlässigt. Dadurch sind die Aufklärungsmöglichkeiten bei einem e-Crime-Vorfall sehr stark eingeschränkt. Warum ist das so?

Die über das Internet verfügbaren privaten E-Mail-Dienste können dazu genutzt werden, sensitive Unternehmensinformationen an unberechtigte Externe zu mailen. Unternehmensinformationen können natürlich auch über den unternehmenseigenen E-Mail-Dienst an unberechtigte Externe versendet werden.

Umfassend eindämmen lassen sich diese Gefahren nicht, sind doch Internet und E-Mail aus vielen Pro-

zessen der Unternehmen nicht mehr wegzudenken. Viele Unternehmen verbieten jedoch bewusst die private Nutzung über entsprechende Unternehmensrichtlinien. Die meisten von ihnen wiegen sich jedoch in einer trügerischen Sicherheit. Wirklich eindämmen lässt sich die private Nutzung – vom Deaktivieren der Möglichkeiten zur E-Mail- und Internetnutzung einmal abgesehen – erst durch Nutzungskontrollen. Erst wenn der einzelne Mitarbeiter wahrnimmt, dass sein Fehlverhalten entdeckt werden kann, wird dies Auswirkungen auf sein Verhalten haben.

Auch das ausnahmslose Verbot der privaten Nutzung und entsprechende Kontrollen sind jedoch zu kurz gegriffen, wenn man an den Aspekt der Aufklärung denkt. In der Werbeagentur AG D stand ein Mitarbeiter unter dem Verdacht sensitive Informationen über eine geplante Kampagne per E-Mail an ein Konkurrenzunternehmen verschickt zu haben. Die private E-Mail-Nutzung über das Internet und das unternehmenseigene E-Mail-System waren verboten. Die E-Mails des verdächtigen Mitarbei-

ters konnten ohne dessen Einverständniserklärung im Rahmen einer Sonderuntersuchung jedoch nicht analysiert werden. Der Grund dafür war die faktische Duldung der privaten E-Mail-Kommunikation. Das Verbot der privaten Nutzung in der Unternehmensrichtlinie wurde weder regelmäßig kommuniziert, noch hielt sich das Management selbst daran. Zudem wurde die Einhaltung des Verbots nicht kontrolliert mit der Konsequenz, dass auch entsprechende Sanktionen fehlten. Die Sonderuntersuchung musste einen anderen Weg einschlagen, wurde langwieriger und kostenintensiver. Letztendlich gestand der Mitarbeiter. Mit einem ganzheitlichen Konzept zur Regelung der privaten Nutzung der unternehmenseigenen IT-Infrastrukturen hätte sich der Aufwand für die Sonderuntersuchung drastisch reduzieren lassen. Auf ein Geständnis lässt sich keinesfalls immer zählen.

Hinweis: Die hier dargestellten Fallbeispiele sind fiktive Fallbeschreibungen und beziehen sich nicht auf tatsächlich existierende Unternehmen. Ähnlichkeiten mit existierenden Unternehmen sind rein zufällig.

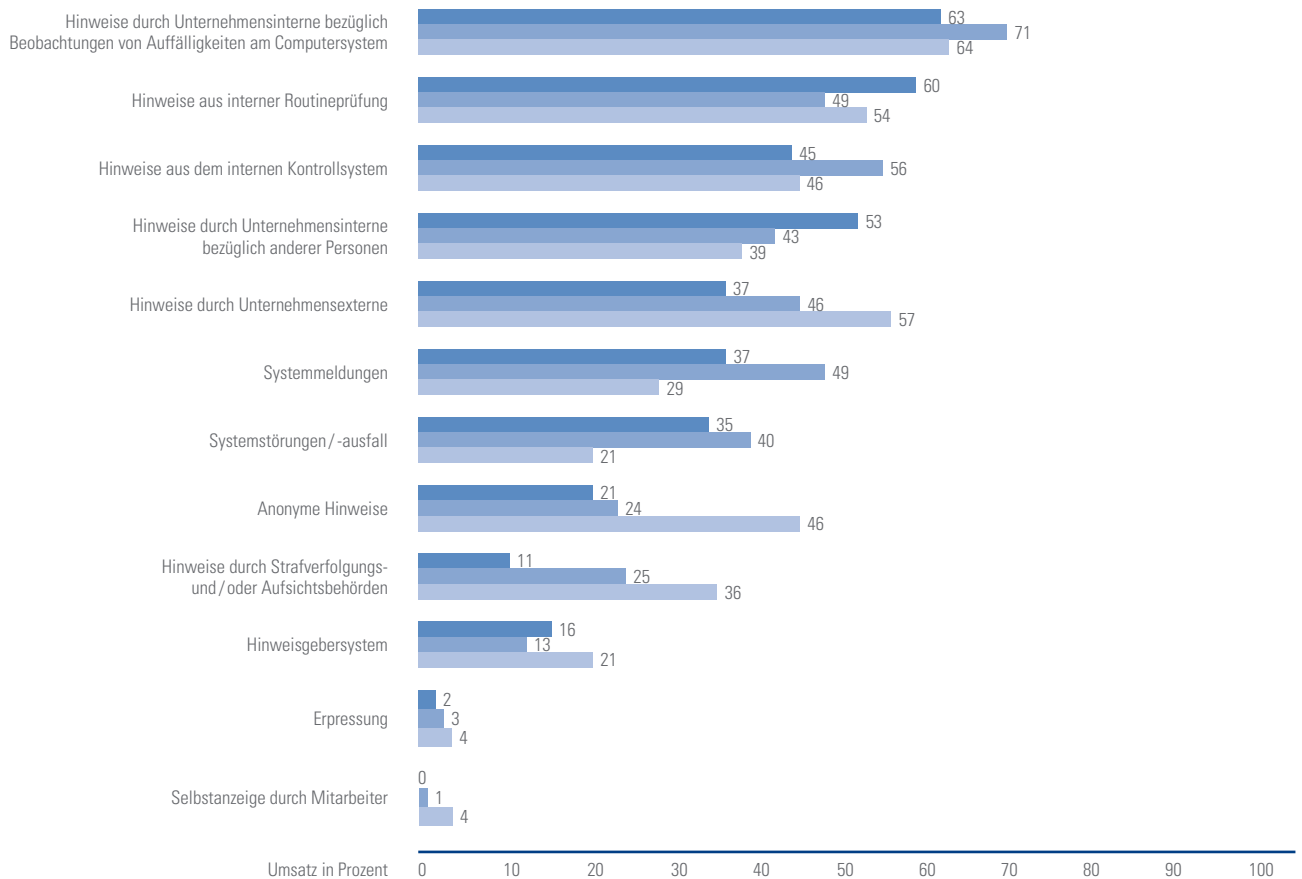
Vor allem bei großen Unternehmen spielen bei der e-Crime-Erkennung neben den etablierten, technischen Monitoringsystemen auch Hinweisgebersysteme und die Zusammenarbeit mit den Strafverfolgungsbehörden eine zunehmend wichtige Rolle.

„Wirtschaftskriminalität in Deutschland 2010“ lautet: Anstatt zuverlässige und kontrollierbare Kanäle für die Aufdeckung von Wirtschaftskriminalität zu etablieren, verlassen sich Unternehmen zu stark auf den „Kommissar Zufall“. Diese Aussage muss in der aktuellen Umfrage für den Bereich e-Crime differenzierter betrachtet werden. Die befragten Unternehmen stützen sich in der Regel auf bestehende Sicherheits- und Überwachungssysteme und geben an, über interne Routineprüfungen, interne Kontrollsysteme und automatisierte Systemmeldungen e-Crime-Vorfälle zu erkennen. Es ist jedoch zu hinterfragen, ob damit ein Großteil der Vorfälle tatsächlich erkannt wird.

Da ein hohes Entdeckungsrisiko und empfindliche Sanktionen eine starke abschreckende Wirkung haben, muss die Aufklärungsarbeit von oberster Priorität sein. Auch ermöglicht die Analyse begangener Straftaten die Verbesserung des Kontrollsystems. Ein Ergebnis der KPMG-Studie

Abbildung 23
Wodurch sind Sie auf Fälle von e-Crime erstmalig aufmerksam geworden?

- 50 Mio. bis 249 Mio. EUR
- 250 Mio. bis 3 Mrd. EUR
- 3 Mrd. EUR und mehr



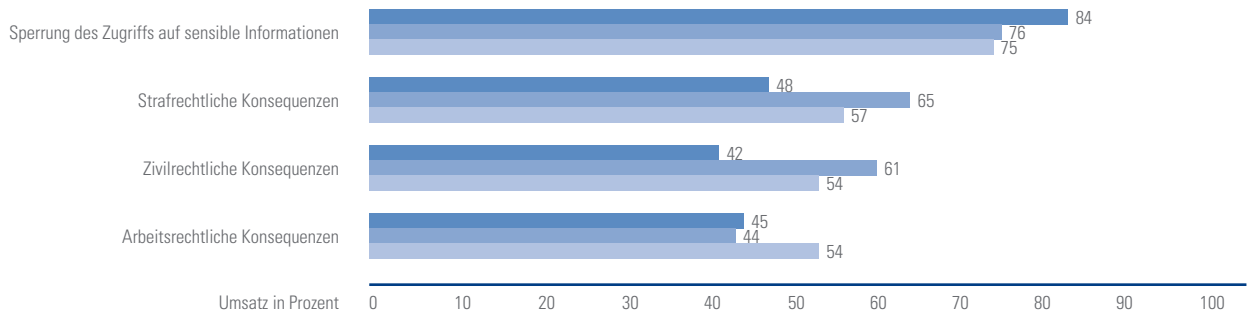


Abbildung 24
Welche Sanktionen hat Ihr Unternehmen gegen die e-Crime-Täter ergriffen?

■ 50 Mio. bis 249 Mio. EUR
 ■ 250 Mio. bis 3 Mrd. EUR
 ■ 3 Mrd. EUR und mehr

Selektion: Unternehmen, bei denen Wirtschaftskriminalität aufgetreten ist, unabhängig vom Zeitpunkt

Mess- und Monitoringsysteme können nur das melden, was auch als e-Crime-Delikt definiert wurde und systemseitig erkannt werden kann. Deshalb spielen auch bei der Erkennung von e-Crime-Delikten die Erkennung durch anonyme Hinweisgebersysteme und das Wissen der Strafverfolgungsbehörden eine zunehmend wichtige Rolle. Hier lassen sich aus der e-Crime-Studie interessante Aussagen erkennen: Es sind vor allem Großunternehmen, die auf e-Crime-Delikte durch anonyme Hinweise und Mitteilungen durch die Strafverfolgungsbehörden aufmerksam werden. Bei kleinen und mittelgroßen Unternehmen spielen diese Kanäle eine deutlich geringere Rolle. Eine Erklärung ist, dass sich Whistleblower bei mittelständischen Unternehmen oft nicht sicher sind, inwieweit ihr Hinweis überhaupt wertgeschätzt wird oder ob sie nicht im Gegenteil als Denunziant behandelt werden. Nach unserer Beratungserfahrung existieren bei kleinen und mittelständischen Unternehmen bisher nur selten sichere, anonyme Hinweisgebersysteme. Der direkte Weg zu den Strafverfolgungsbehörden ist nicht zuletzt aufgrund der im Vergleich zu Großunternehmen größeren persönlichen Bindung zum Unternehmen und zur Geschäftsführung häufig gesperrt. Auch sind die Hinweisgeber bei kleineren und mittelgroßen Unternehmen aufgrund des für den Hin-

weis notwendigen Spezialwissens oft leicht identifizierbar.

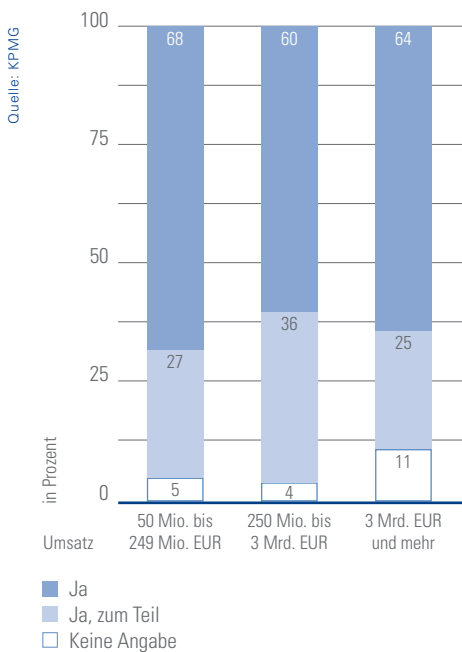
In nur gut der Hälfte der Fälle kann ein Täter ermittelt werden. Die präventive Wirkung eines hohen Aufdeckungs- und Sanktionsrisikos bleibt somit oft ungenutzt. Gleichwohl werden aufgeklärte Delikte konsequent sanktioniert.

Praktisch unabhängig von der Unternehmensgröße und Branche liegt die Ermittlungsquote des Täters im Schnitt bei nur etwa 50 bis 60 Prozent. Bedenkt man, dass damit in knapp der Hälfte der Fälle auf eine Sanktionierung und damit auf die oben dargestellte abschreckende Wirkung verzichtet wird, ist diese Quote relativ niedrig. Sie deckt sich allerdings mit der von den Studienteilnehmern getroffenen Aussage, dass die Angriffe komplexer werden und immer seltener auf einzelne Täter zurückzuführen sind.

Von e-Crime betroffene Unternehmen sanktionieren Delikte meist konsequent. Zwar steht mit der Sperrung sensibler Informationen ein recht stumpfes Schwert an erster Stelle, strafrechtliche, zivilrechtliche und arbeitsrechtliche Konsequenzen sind aber gleichzeitig von vergleichsweise hoher Bedeutung.

Abbildung 25

Hat Ihr Unternehmen in der Rückschau nach Kenntnis des Verdachts beziehungsweise der Taten angemessen und zeitnah gehandelt?



Den Strafverfolgungsbehörden wird ein großes Vertrauen entgegengebracht.

Zu begrüßen sind die scheinbar geringen Berührungspunkte zu den Strafverfolgungsbehörden: So gaben 91 Prozent der von e-Crime betroffenen Unternehmen an, diese nach eingehender Abwägung einzubeziehen. 64 Prozent der von e-Crime betroffenen Unternehmen haben dann auch tatsächlich die Delikte angezeigt, bei Großunternehmen lag die Quote sogar bei 72 Prozent.

Entscheidet sich ein Unternehmen gegen die Strafanzeige, ist nur in wenigen Fällen mangelndes Vertrauen in die Behörden ursächlich. In den meisten Fällen können Angriffe durch bestehende Sicherheitsmaßnahmen abgewehrt werden beziehungsweise es ist kein finanzieller Schaden entstanden, sodass eine Anzeige keine Konsequenzen hätte. Zudem haben viele Unternehmen schon arbeitsrechtliche Maßnahmen ergriffen und sehen somit nicht die Notwendigkeit, Strafanzeige zu erstatten.

Ein Drittel der von e-Crime betroffenen Unternehmen halten ihre Erstreaktion für nur teilweise angemessen. Der Maschinenbau meldet sogar zu fast 50 Prozent rückblickend Versäumnisse.

Wird ein e-Crime-Vorfall bekannt, muss schnell reagiert werden. Um weiteren Datenverlusten vorzubeugen, müssen Vollmachten und Berechtigungen entzogen werden. Damit die Täter ihre Spuren nicht verwischen können, gilt es, Beweise so schnell wie möglich zu sichern. Und nicht zuletzt muss eine koordi-

nierte Kommunikationsstrategie – intern und gegebenenfalls auch extern – entwickelt werden.

Je größer das Unternehmen desto größer ist der Grad der Eigenständigkeit in der Reaktion auf e-Crime-Vorfälle. Größere Unternehmen berufen hierzu zum Beispiel eine Task Force ein, die sich umfassend um die Koordination der Ermittlungen kümmert. Mittlere und kleine Unternehmen gaben in der Studie hingegen an, sofort externe, unabhängige Spezialisten für die Reaktion und Ermittlung von e-Crime-Vorfällen zu Rate zu ziehen.

Zwar beurteilt die Mehrheit der Unternehmen ihre Erstreaktion als angemessen, trotzdem sehen viele einen Verbesserungsbedarf: Immerhin ein Drittel der von e-Crime betroffenen Unternehmen beurteilt ihre Erstreaktion als teilweise nicht angemessen, beim Maschinenbau lag die Quote sogar bei fast 50 Prozent.

Dabei können die Versäumnisse in die zwei Kategorien Prozesse und Technik unterteilt werden. Aus prozessualer Sicht sind die am meisten genannten Versäumnisse eine unklare Informationslage, die Dauer bis zur Umsetzung nötiger Sofortmaßnahmen und unklare Verantwortlichkeiten in der Kommunikationskette. Dabei sind von den ersten zwei Punkten vor allem kleine und mittelgroße Unternehmen betroffen, den dritten Punkt identifizieren dagegen überproportional viele Großunternehmen. Aus technischer Sicht werden in erster Linie Versäumnisse bei der Beweissicherung sowie die zu späte Einbindung externer Fachleute genannt.

Wichtig ist dabei auch die frühzeitige Information der Presseabteilung. Diese sollte – insbesondere wenn

Kunden- oder Mitarbeiterdaten betroffen sind – ausreichend Zeit haben, eine adäquate Kommunikationsstrategie zu erarbeiten. Ein Großteil der Großunternehmen scheint sich dessen bewusst zu sein: 72 Prozent gaben an, die Presse- und Kommunikationsabteilung bei Bekanntwerden der Fälle einzubeziehen. Bei mittleren und kleinen Unternehmen ist dieses Bewusstsein deutlich weniger ausgeprägt. Dies mag zum Teil gerechtfertigt sein, da das Medieninteresse mit einer sinkenden Unternehmensgröße in der Regel abnimmt. Trotzdem müssen Unternehmen unabhängig von der Unternehmensgröße potenziell betroffene Kunden, Mitarbeiter und Geschäftspartner informieren. Eine abgestimmte Kommunikationsstrategie ist dabei in jedem Fall von immenser Bedeutung.

Noch wichtiger wird die Vorbereitung und Bereitschaft, auf e-Crime-Delikte schnell und angemessen reagieren zu können, wenn personenbezogene

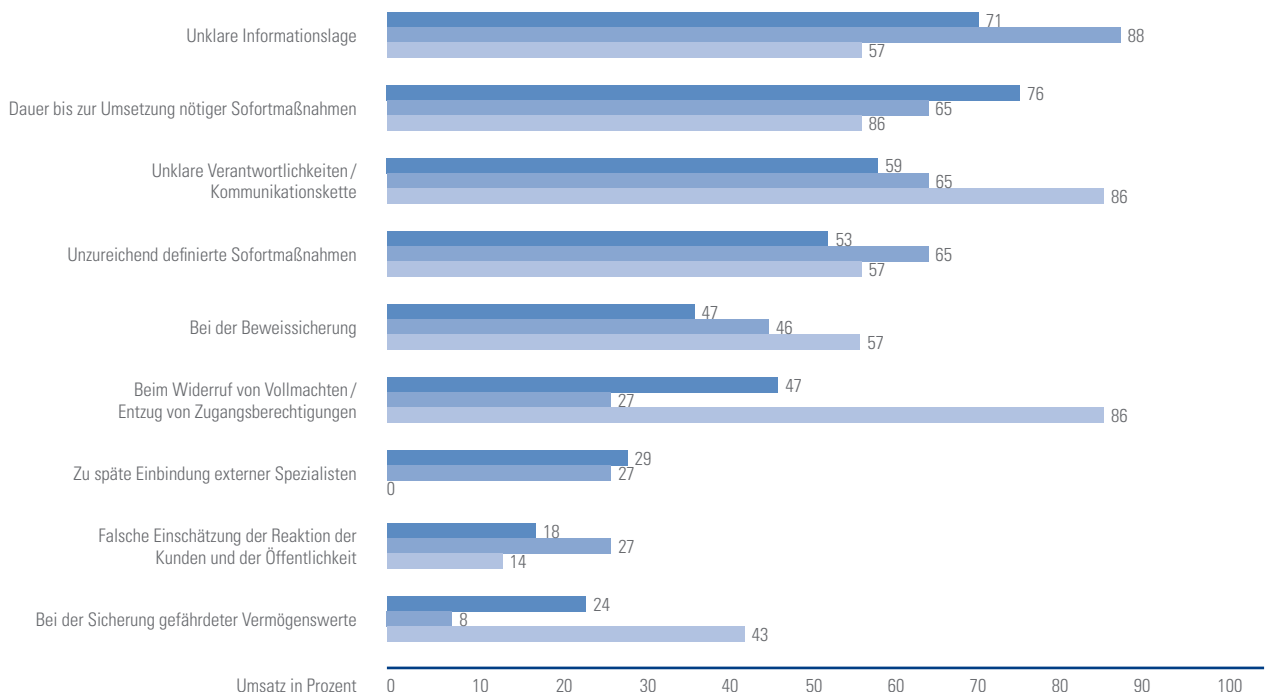
Daten mit im Spiel sind. Die jüngste Novelle des Bundesdatenschutzgesetzes gibt hier eine Informationspflicht vor: Bei Erkennen eines Datenmissbrauchs müssen Aufsichtsbehörden und Betroffene informiert werden. In diesem speziellen Fall wird nun die Frage wichtiger, wie das Unternehmen Datenmissbrauchsfälle erkennt und wie es den Gesetzesanforderungen genügt.

Insgesamt deuten die Umfrageergebnisse auf eine unzureichende Vorbereitung der Unternehmen auf e-Crime-Delikte und auch damit verbundene Krisensituationen hin. Auch wenn das Auftreten von e-Crime-Delikten und den daraus möglicherweise entstehenden Reputationsschäden und Krisensituationen an sich natürlich nicht planbar ist, ist es die Reaktion dagegen schon. Sinnvoll ist es daher, Abläufe, Kommunikationskaskaden und Verantwortlichkeiten ganz klar im Vorfeld zu definieren.

Abbildung 26
In welchen Bereichen gab es in der Erstreaktion aus Ihrer Sicht Versäumnisse?

■ 50 Mio. bis 249 Mio. EUR
■ 250 Mio. bis 3 Mrd. EUR
■ 3 Mrd. EUR und mehr

Selektion: Unternehmen, die nur zum Teil angemessen auf e-Crime-Delikte reagierten



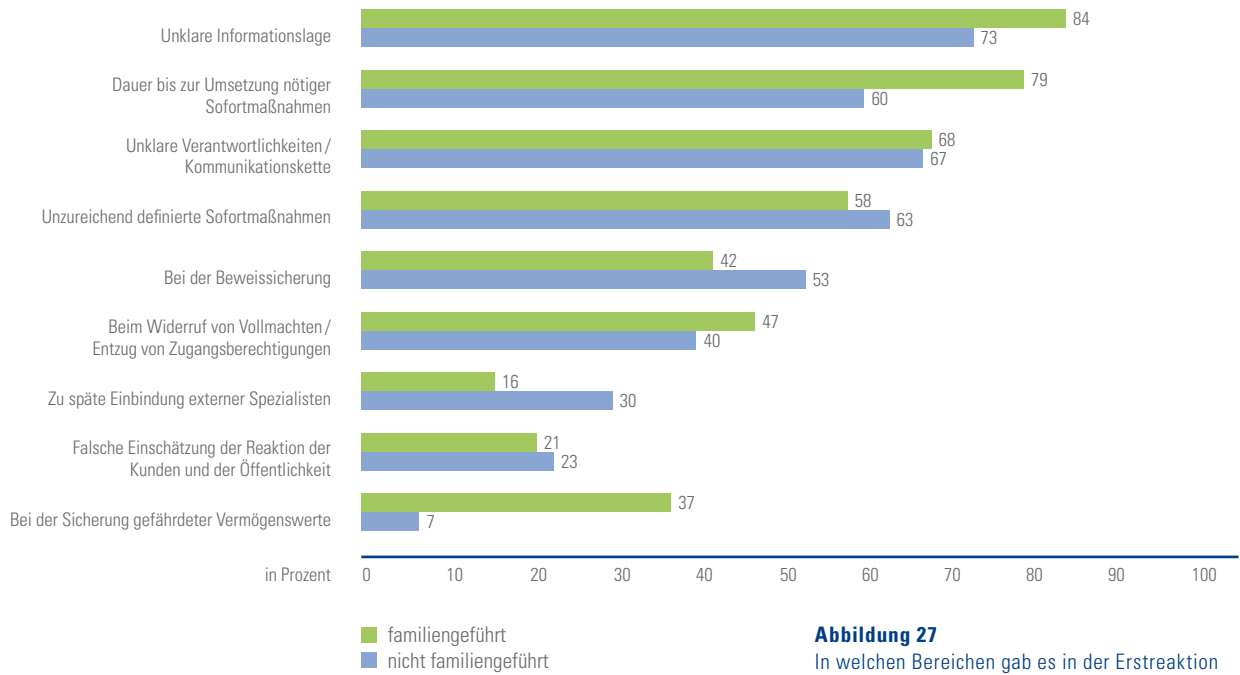


Abbildung 27

In welchen Bereichen gab es in der Erstreaktion aus Ihrer Sicht Versäumnisse?
 Selektion: Unternehmen, die nur zum Teil angemessen auf e-Crime-Delikte reagierten

Fallbeispiel E

Schnell mal selbst ermitteln oder Spezialisten einschalten?

Die professionelle Reaktion auf e-Crime-Vorfälle ist entscheidend bei der Aufklärung und bei der Verwendbarkeit von Beweisen

In der Medical GmbH E sollte ein hinreichend verdächtiger Vertriebsmitarbeiter freigestellt werden. Das einzubeziehende Betriebsratsgremium tagte am Mittag und dem Anliegen der Geschäftsführung wurde zugestimmt. Der betreffende Mitarbeiter wurde mit sofortiger Wirkung freigestellt, seine Zugangskarte wurde ihm entzogen und der Entzug seiner Systemberechtigungen wurde angeordnet. Niemand dachte jedoch an den Laptop des Mitarbeiters.

Dieser wurde erst am Folgetag durch den Mitarbeiter übergeben.

Eine folgende Analyse des Laptops durch externe Spezialisten zeigte, dass die Festplatte des Laptops professionell gelöscht wurde. Auch eine Analyse des Sicherungsstands vom persönlichen Netzlaufwerk des Mitarbeiters vom Tag der Freistellung ergab, dass darauf alle Daten gelöscht waren. Möglich war dies durch einen Fernzugriff des Mitarbeiters auf seine Daten des Netzlaufwerks. Die Zugriffsmöglichkeit wurde schlicht zu spät entzogen.

Das waren vermeidbare Fehler in der Reaktion. Das Unternehmen hatte keine Erfahrung mit Krisensituationen. Eine Notfallvorsorge hatte nicht stattgefunden. Außerdem kann in der Regel nur eine eingehende Beschäftigung mit Szenarien und Täter-

typen von e-Crime-Vorfällen helfen, in einem Ernstfall gut vorbereitet zu sein.

Durch das gezielte Planen solcher Ereignisse, beispielsweise über Workshops mit externen Ermittlungsspezialisten, lassen sich konkrete Verantwortlichkeiten und Prozeduren für klassische Fallszenarien definieren. Die Reaktion der verantwortlichen Personen oder einer professionellen Task Force wird so planbar.

Hinweis: Die hier dargestellten Fallbeispiele sind fiktive Fallbeschreibungen und beziehen sich nicht auf tatsächlich existierende Unternehmen. Ähnlichkeiten mit existierenden Unternehmen sind rein zufällig.



Fazit

Kein Unternehmen kann sich der fortschreitenden IT-Durchdringung aller Geschäftsprozesse entziehen, denn ohne Ausnutzung der damit einhergehenden Effizienzgewinne wären weder Großkonzerne noch mittelständische Unternehmen wettbewerbsfähig. Die Kehrseite: Mit der einhergehenden Vernetzung der Unternehmenslandschaft sind sensible Informationen immer schwerer zu schützen. Unsere Studie zeigt, dass die einhergehenden Gefahren real sind: Ein Viertel der befragten Unternehmen ist in den letzten drei Jahren Opfer von e-Crime-Delikten geworden. Und dies trotz signifikanter Investitionen in Informationssicherheit. Der Grund: Die Angreifer sind im „Wettrüsten“ immer einen Schritt voraus, Schwachstellen neuer Technologien werden ausgenutzt, bevor ein entsprechender Schutz am Markt vorhanden ist.

Hauptgefahrenquelle ist dabei nicht der sich aus fernen Ländern „einhackende“ Spion, sondern bekannte Gesichter: Die Umfrageteilnehmer nennen Mitarbeiter, ehemalige Mitarbeiter und sonstige Insider wie Geschäftspartner oder Dienstleister als häufigste Täter. Hintergrund ist nicht zuletzt die Wirtschaftskrise, die zu zahlreichen – oft als ungerecht empfundenen – Entlassungen

von Know-how-Trägern geführt hat. Unter finanziellem Druck stehend, nutzen diese ehemaligen Mitarbeiter ihr Fach- und Prozesswissen durch den Verkauf sensibler Informationen aus. Hier spielen als Abnehmer dann neben deutschen Konkurrenten häufig ausländische Konkurrenzunternehmen eine zunehmend wichtige Rolle. Dabei sind die durch e-Crime entstehenden Schäden signifikant, insbesondere der Datendiebstahl und das Ausspähen von Informationen führen zu Verlusten in Millionenhöhe.

In Bezug auf Prävention, Entdeckung und Aufklärung weist die Studie auf signifikante Mängel hin. Insbesondere, dass die Hauptverantwortung weiterhin auf die IT-Abteilungen „abgewälzt“ wird, ist kritisch. Wichtig wäre, dass die unternehmerischen Geschäftsbereiche wie Interne Revision, Compliance und nicht zuletzt die Geschäftsführung stärker involviert werden. Zwar verfügt die IT-Abteilung über das notwendige technische Fachwissen, dies allein ist in der e-Crime-Bekämpfung allerdings nicht ausreichend. Denn dank fortschreitender technischer Entwicklung ist für e-Crime-Delikte ein Informatikstudium längst keine Voraussetzung mehr: Die notwendigen Programme kann jeder versierte Laie aus dem Internet herunterladen, oft liegt die

entsprechende Software sogar seriösen Computerzeitschriften bei. Immer wichtiger wird deshalb, dass e-Crime aus strategischer, also betriebswirtschaftlicher Perspektive, angegangen wird. Insbesondere die Sensibilisierung der Mitarbeiter ist dabei von wesentlicher Bedeutung. Hier tun die Umfrageteilnehmer zwar schon viel, gleichzeitig wird aber die Kontrolle vernachlässigt – ein ausgewogenes Verhältnis zwischen „Tone at the Top“, Sensibilisierung, Kontrolle und Sanktionierung besteht bei den meisten Unternehmen noch nicht.

Ohne Frage wurde in den letzten Jahren viel in Informationssicherheit investiert und die befragten Unternehmen planen dies auch weiterhin zu tun. Gleichwohl zeigt unsere Studie deutlich: Egal wie hoch die Investitionen auch sein mögen, ohne einen einhergehenden Kulturwandel ist die präventive Wirkung unzureichend. e-Crime muss weniger technisch gedacht werden. Denn im Endeffekt handelt es sich bei dem „e“ in e-Crime nur um eine Methode: Hinter den Delikten stehen immer tatsächliche Menschen, deren Motive stärker in den Vordergrund der e-Crime-Prävention, -Entdeckung und -Aufklärung rücken müssen.

Forensic Technology von KPMG

Umfangreiche Erfahrungen in der e-Crime-Bekämpfung

Der Bereich Forensic Technology von KPMG bietet technische und organisatorische Maßnahmen zur Prävention, Analyse und Aufklärung forensischer Sachverhalte. Wir führen Sonderuntersuchungen durch, sichern gerichtsverwertbare digitale Beweismittel, untersuchen Sicherheitsvorfälle und analysieren große Datenbestände.

Zu unserem Angebot gehören unter anderem die folgenden Dienstleistungen:

Evidence and Disclosure Management

Erfassung, Speicherung, Abfrage, Analyse, Sichtung und Verteilung großer Volumen von sichergestellten Informationen und der hieraus erzeugten Aufbereitungsergebnisse (E-Discovery) in einem dedizierten und sicherheitszertifizierten Forensic Data Center.

Records Risk Management

Unterstützung der Mandanten bei der Klärung aller Fragen im Zusammenhang mit Risiken und der Verantwortung für Daten und Dokumente (Records) und der Einhaltung der damit verbundenen rechtlichen Anforderungen. Schaffung von Transparenz für die Unternehmensleitung über den Informationsbestand durch Kategorisierung und Klassifizierung der Datenbestände.

Forensic Data Analytics

Fraud-Detection-Routinen und die von KPMG entwickelte Analyseplattform KTrace helfen bei der Untersuchung von großen strukturierten Datenbeständen nach Auffälligkeiten oder schon näher identifizierten Sachverhalten.

In Zusammenarbeit mit der Service Line IT Advisory von KPMG und hier insbesondere dem Bereich Information Protection & Business Resilience betreuen wir den ganzheitlichen Informationsschutz rund um die Kernprozesse und Informationswerte eines Unternehmens und tragen so zur Wertsteigerung im Unternehmen bei.

Unsere Spezialisten verfügen über ein umfassendes Wissen zu Informationssicherheitsmanagementsystemen, Zertifizierungen (zum Beispiel ISO/IEC 27001 und BS 25999), zu einem Datenschutzmanagement und zum Business-Continuity-Management.

Kontakt

KPMG AG

Wirtschaftsprüfungsgesellschaft

Klingelhöferstraße 18

10785 Berlin

Alexander Geschonneck

Partner

Forensic Technology

T +49 30 2068-1520

ageschonneck@kpmg.com

Autorenteam:

Dr. Stefan Weiss, Thomas Fritzsche



Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt Ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

© 2010 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Konzerngesellschaft der KPMG Europe LLP und Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. KPMG und das KPMG-Logo sind eingetragene Markenzeichen von KPMG International.