KPMG

cutting through complexity

FORENSIC

e-Crime

Computerkriminalität in der deutschen Wirtschaft 2015

INHALT

VORWORT

Liebe Leserinnen und Leser,

seit der Veröffentlichung der letzten e-Crime-Studie von KPMG Anfang 2013 hat sich in der Wahrnehmung des Themas e-Crime in Politik, Wirtschaft, Medien und Bevölkerung sowie in Sachen Datensicherheit und Datenschutz sehr viel getan.

Durch die Veröffentlichungen des Whistleblowers Edward Snowden hat nun eine breite Öffentlichkeit einen Einblick in die technischen Möglichkeiten staatlich gelenkter Cyberspionage und Cybersabotage bekommen – und damit eine Vorstellung, welchen Risiken jeder IT- und Mobiltelefon-Nutzer ausgesetzt ist. Die letzten beiden Jahre waren ebenfalls geprägt von spektakulären Datendiebstählen und Cyberangriffen, die ihren Ursprung bei den klassischen Cyberkriminellen haben. Die Öffentlichkeit scheint abgestumpft ob der Millionen von User-Accounts, die jedes Mal gestohlen werden – selbst von vermeintlich gut geschützten Unternehmen: 1 oder 10 oder 100 Millionen gestohlene Datensätze – wer zählt da noch mit?

Unsere tägliche Ermittlungsarbeit und auch die Ergebnisse der nun vorliegenden, repräsentativ durchgeführten Studie zeigen, dass man zwei Klassen von Unternehmen unterscheiden kann: die, die bereits von e-Crime betroffen sind, und die, die es sein werden oder dies nur noch nicht erkannt haben. Mit diesem Bewusstsein im Hinterkopf lassen sich möglicherweise Maßnahmen zur Prävention, Erkennung und Reaktion auf Cyberangriffe besser planen, ohne zu selbstsicher die bestehende Gefahr zu ignorieren.

Zu guter Letzt haben wir in dieser Studie einen Schwerpunkt auf das Ende 2014 vom Bundeskabinett verabschiedete IT-Sicherheitsgesetz gelegt, um herauszufinden, ob sich die Unternehmen bereits damit beschäftigt haben und welche Kosten ihnen dadurch entstehen. Dies ist zwar nur eine Momentaufnahme, zeigt aber, dass mit der nun zeitnah zu veröffentlichenden Rechtsverordnung mehr Klarheit zu schaffen ist. Wir werden diese Entwicklung weiter beobachten.

Ich wünsche Ihnen viele Erkenntnisse beim Lesen dieser Studie,

Ihr
Alexander Geschonneck

Alexander Geschonneck
Leiter Forensic KPMG
in Deutschland

1 EXECUTIVE SUMMARY

E-CRIME IN UNTERNEHMEN NIMMT DEUTLICH ZU. OPFER SIND INSBESONDERE FINANZDIENSTLEISTER.

Gegenüber der Vorstudie aus dem Jahr 2013 wurden die Befragten **wesentlich häufiger Opfer von e-Crime**. In den vergangenen zwei Jahren waren 40 Prozent der Unternehmen betroffen, 2013 lediglich 27 Prozent. Das entspricht einem **Zuwachs von 50 Prozent**.

Besonders oft müssen sich **Finanzdienstleister** mit e-Crime auseinandersetzen. Von den Vertretern dieser Branche gaben 55 Prozent an, angegriffen worden zu sein. Bei Dienstleistern außerhalb des Finanzsegments waren es lediglich 33 Prozent. Finanzdienstleister erweisen sich damit als **besonders attraktiv für potenzielle Täter**.

DIE BEFRAGTEN ZEIGEN EINE VERSTÄRKTE RISIKOWAHRNEHMUNG.

Entsprechend der gestiegenen Betroffenheit zeigen die Befragten eine **ausgeprägtere Risikowahrnehmung** im Vergleich zur Vorstudie. Ein hohes beziehungsweise sehr hohes Risiko, dass deutsche Unternehmen im Allgemeinen Opfer von e-Crime werden, empfinden 89 Prozent; 70 Prozent rechnen damit, dass dieses Risiko auch in den kommenden zwei Jahren steigen wird. Jedoch zeigt sich **nach wie vor das Phänomen der Risikoverdrängung**. So sehen lediglich 39 Prozent ein hohes beziehungsweise sehr hohes Risiko, künftig selbst betroffen zu sein.

Hinsichtlich **potenzieller Täter** rücken die organisierte Kriminalität, Insider (vor allem im Zusammenhang mit Zugangsberechtigungen und systemadministrativen Tätigkeiten) sowie Geheimdienste in den Fokus.

POTENZIELLE E-CRIME-TÄTER WERDEN PROFESSIONELLER UND AGIEREN VERMEHRT INTERNATIONAL.

Unternehmen empfinden zunehmend weniger Schwierigkeiten bei der Detektion von e-Crime-Vorfällen. Dafür gestalten sich die **Vermeidung und anschließende Verfolgung von Angriffen problematisch**. So sind über 90 Prozent der Befragten der Ansicht, dass e-Crime-Handlungen komplexer werden und somit schwerer auf die Täter zurückzuverfolgen sind. Diese Entwicklung steht in direktem Zusammenhang mit einer **höheren Professionalisierung der Täter** und erklärt auch die Wahrnehmung von organisierter Kriminalität. Schließlich lässt sich beobachten, dass **potenzielle e-Crime-Täter immer häufiger international agieren**, was die Verfolgung zusätzlich erschwert.

DEFINITION E-CRIME

e-Crime bezeichnet die Ausführung von wirtschaftskriminellen Handlungen unter Einsatz von Informations- und Kommunikationstechnologien zum Schaden einer Einzelperson, eines Unternehmens oder einer Behörde. Diese Form der Kriminalität kann sowohl zu einer Schädigung von Sachwerten, zum Beispiel durch Sabotage an Computersystemen, als auch zur Verletzung von Verfügungsrechten an immateriellen Gütern, etwa durch Diebstahl von Quellcodes, Kundendaten oder anderen Informationen, führen. Außerdem können die auf den Systemen basierenden Geschäftsprozesse eines Unternehmens emp-

DAS SELBSTBEWUSSTSEIN DER UNTERNEHMEN HINSICHTLICH IHRER REAKTIONSFÄHIGKEIT BRÖCKELT.

In der Studie des Jahres 2013 waren 99 Prozent der betroffenen Unternehmen der Ansicht, dass sie korrekt auf e-Crime-Vorfälle reagiert haben und es dementsprechend keine Versäumnisse gab. Doch dieses **Vertrauen in die eigene Reaktionsfähigkeit schwindet**. In der diesjährigen Studie gesteht ein Viertel der Betroffenen Schwächen in der Reaktion ein. Allerdings zeigen sich **starke branchenspezifische Unterschiede**. Finanzdienstleister und Industrie empfinden lediglich zu 18 Prozent, dass es Versäumnisse in der Reaktionsphase gibt, bei sonstigen Dienstleistern beispielsweise sind es 44 Prozent. **Schwächen werden dabei vor allem im Rahmen des Incident Management** festgestellt. Unklare Verantwortlichkeiten, eine unklare Informationslage sowie unzureichende und mangelhaft umgesetzte Sofortmaßnahmen zählen zu den meistgenannten Versäumnissen.

UNTERNEHMEN INVESTIEREN MEHR UND TREFFEN VERMEHRT VORBEREITENDE MASSNAHMEN. DENNOCH LÄSST SICH E-CRIME (NOCH) NICHT BEHERRSCHEN.

Obwohl Unternehmen offenbar verstärkt in die Bekämpfung von e-Crime investieren und entsprechende Maßnahmen ergreifen, **beherrschen sie die Risiken von e-Crime nicht**.

Hierfür lassen sich hauptsächlich zwei Ursachen ausmachen. Einerseits beklagen die Befragten nach wie vor **Unachtsamkeit** (88 Prozent) **und mangelndes Risikoverständnis** (77 Prozent) **der Mitarbeiter** – obwohl 86 Prozent der Befragten angeben, dass sie Sensibilisierungs- und Schulungsmaßnahmen für ihre Beschäftigten anbieten.

Andererseits nutzen Angreifer Schwachstellen neuer Technologien. In dieser Hinsicht empfindet ein Großteil der Unternehmen, dass es **noch keine ausreichenden Schutzmaßnahmen** gibt.

DAS IT-SICHERHEITSGESETZ DROHT, DIE INVESTITIONSBUDGETS ZU VEREINNAHMEN.

91 Prozent der Gesetzeskenner erwarten **für die Umsetzung der Anforderungen einen hohen bürokratischen Aufwand**. Diejenigen, die den Aufwand bereits kalkuliert haben, rechnen mit Mehrkosten von 10.000 bis 100.000 Euro. Damit sind die Unternehmen möglicherweise zu zusätzlichen Investitionen gezwungen.

Im Gegenzug für die erwarteten Kosten stellen die Gesetzeskenner **hohe Erwartungen an die Wirksamkeit des IT-Sicherheitsgesetzes (ITSiG)**: 84 Prozent stimmen der Aussage zu, dass Unternehmen durch eine zentrale Sammlung von Angriffsmustern effektiver vor Bedrohungen gewarnt werden können.

findlich beeinträchtigt werden. Informations- und Kommunikationssysteme können hierbei Ziel der Tathandlung, aber auch Tatwerkzeug an sich sein. e-Crime umfasst damit nicht nur Angriffe von außen, die mithilfe von Schadsoftware und unter Ausnutzung von Systemlücken über das Internet erfolgen (landläufig auch als Cybercrime bezeichnet). Vielmehr umfasst e-Crime, im Gegensatz zur landläufigen Definition, Cybercrime sowie das breite Spektrum weiterer Straftaten, die Informations- und Kommunikationstechnologie als Werkzeug einsetzen.

Ebenfalls zu beachten sind klassische wirtschaftskriminelle Handlungen, die durch den Einsatz von Informations- und Kommunikationstechnologie erst möglich beziehungsweise erleichtert werden oder bei denen IT-Werkzeuge zur Verschleierung dienen. Ein Beispiel dafür ist das sogenannte Rogue Trading: Hier nutzen Händler Kontrollschwächen von Handelssystemen im Finanzsektor aus beziehungsweise hebeln Kontrollmechanismen aus, um Genehmigungsgrenzen zu überschreiten und unzulässige Transaktionen auszuführen.

2 RISIKOPROFIL UND KOSTEN VON E-CRIME

2.1 RISIKOWAHRNEHMUNG UND BETROFFENHEIT

Knapp 90 Prozent der Befragten schätzen das generelle Risiko eines deutschen Unternehmens, Opfer von e-Crime zu werden, als hoch beziehungsweise sehr hoch ein. Von einem sehr hohen Risiko gehen sogar 25 Prozent der Befragten aus (Abbildung 01). Damit ist dieser Anteil noch höher als bei der Studie zur Wirtschaftskriminalität in Deutschland, die KPMG im vergangenen Jahr veröffentlichte. Gerade bereits von e-Crime betroffene Unternehmen zeichnen sich durch eine besonders ausgeprägte Risikowahrnehmung aus (64 Prozent hoch beziehungsweise 33 Prozent sehr hoch). Dies stellt eine Steigerung im Vergleich zur Vorgängerstudie dar. In dieser Studie bewerteten 82 Prozent der Unternehmen das Risiko als hoch beziehungsweise sehr hoch (13 Prozent). Die mit e-Crime verbundenen Gefahren rücken demnach vermehrt in den Fokus der deutschen Wirtschaft.

Ein Grund hierfür dürfte darin liegen, dass in den vergangenen zwei Jahren 40 Prozent der Befragten tatsächlich von Computerkriminalität betroffen waren. Im Jahr 2013 war es nur ungefähr ein Viertel der Unternehmen. Daraus ergibt sich ein Zuwachs von über 50 Prozent.

Vor dem Hintergrund der stark gestiegenen Betroffenheit fällt auf, dass sich bei der Wahrnehmung des Risikos für das eigene Unternehmen lediglich ein leichter Rückgang zeigt. Von den Studienteilnehmern schätzen 60 Prozent dieses Risiko als niedrig oder sehr niedrig ein (2013: 65 Prozent). Gerade bisher nicht von e-Crime betroffene Unternehmen wiegen sich in einer trügerischen Sicherheit: Drei Viertel dieser Gruppe gehen von einem niedrigen oder sehr niedrigen Risiko aus.

Immerhin wird das eigene Risiko in Verbindung mit der gestiegenen Betroffenheit ausgeprägter wahrgenommen als noch 2013.

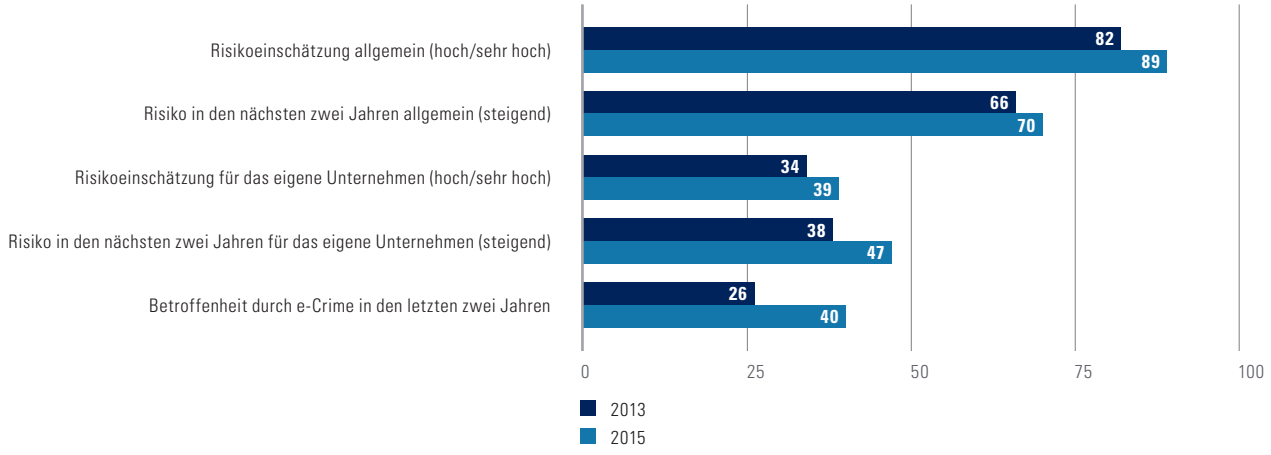
KATEGORIEN

Im Folgenden werden die befragten Unternehmen nach ihrem Umsatz in die Kategorien groß, mittel und klein eingeteilt. Unternehmen mit einem Umsatz von mehr als 3 Milliarden Euro werden der Kategorie „groß" zugeordnet, Unternehmen mit einem Umsatz zwischen 250 Millionen und 3 Milliarden Euro der Kategorie „mittel" und Unternehmen mit einem Umsatz unter 250 Millionen Euro der Kategorie „klein".

01 VERGLEICH ZWISCHEN RISIKOWAHRNEHMUNG UND BETROFFENHEIT

Angaben in Prozent

Quelle: KPMG, 2015



1 Vergleiche KPMG-Studie „Wirtschaftskriminalität in Deutschland 2014“

Vor zwei Jahren ging lediglich etwas mehr als ein Drittel der Befragten von steigenden Risiken für das eigene Unternehmen aus. Inzwischen rechnen 47 Prozent der Befragten damit, dass die mit e-Crime verbundenen Risiken für das eigene Unternehmen steigen werden, was einem Zuwachs von 30 Prozent entspricht. In Bezug auf die deutsche Wirtschaft insgesamt nehmen 70 Prozent der Studienteilnehmer eine Zunahme des Risikos an.

Trotz dieses leicht gestiegenen Risikobewusstseins tritt nach wie vor das schon 2013 festgestellte Phänomen der Risikoverdrängung auf. Das zeigt sich nicht nur hinsichtlich der Risiken von e-Crime, sondern auch von Wirtschaftskriminalität im Allgemeinen.[1]

2.2 DELIKTSPEZIFISCHE RISIKOWAHRNEHMUNG UND BETROFFENHEIT

Gegenüber den Ergebnissen der Studie des Jahres 2013 hat sich die deliktspezifische Risikowahrnehmung geringfügig verschoben (Abbidung 02). Datendiebstahl und Computerbetrug sind nun die meistgefürchteten Deliktstypen und in der Einschätzung der Befragten an der Verletzung von Geschäfts- und Betriebsgeheimnissen sowie der Verletzung von Urheberrechten vorbeigezogen. Jeweils 83 Prozent der Befragten schätzen das Risiko, Opfer der erstgenannten Delikte zu werden, als hoch beziehungsweise sehr hoch ein. Das ent-

KURZDEFINITIONEN DER IN DER STUDIE ABGEFRAGTEN DELIKTSTYPEN*

* Die Kurzdefinitionen sind an Straftatbestände angelehnt.

COMPUTERBETRUG

Betrügerische Handlungen unter Ausnutzung von Kommunikations- und Informationstechnologien und anhand der Manipulation von Datenverarbeitungssystemen beziehungsweise -prozessen

AUSSPÄHEN ODER ABFANGEN VON DATEN

Unberechtigtes Aufzeichnen, Mithören oder Mitlesen von Daten (zum Beispiel E-Mail-Versand, Instant Messaging, Netzwerkverkehr, IP-Telefonie), die sich gerade in der Übermittlung befinden, aber auch von „natürlichen“ Gesprächen über technische Hilfsmittel

MANIPULATION VON KONTO- UND FINANZDATEN

Unberechtigte Veränderung von Konto- und Finanzdaten in Buchhaltungs- oder Zahlungssystemen

DATENDIEBSTAHL

Unberechtigte Aneignung von Daten

VERLETZUNG VON URHEBERRECHTEN

Verstoß gegen die Verwertungsrechte von urheberrechtlich geschützten elektronischen Daten (zum Beispiel Erstellung einer rechtswidrigen Kopie und Verwendung von Softwareprogrammen oder Inhalten audiovisueller Medien)

VERLETZUNG VON GESCHÄFTS- ODER BETRIEBSGEHEIMNISSEN

Unbefugte Aneignung und Weitergabe von vertraulichen oder geheimen Informationen des Unternehmens oder auch von Geschäftspartnern unter Nutzung von Kommunikations- und Informationstechnologien

SYSTEMBESCHÄDIGUNGEN ODER COMPUTERSABOTAGE

Störung von Datenverarbeitungsprozessen, beispielsweise durch Beschädigung oder Manipulation von Computern, Netzwerken oder Datenträgern

ERPRESSUNG

Erpressung unter Androhung von e-Crime-Handlungen

spricht einem Anstieg um 11 Prozent für den Deliktstyp Computerbetrug sowie um 7 Prozent für Datendiebstahl.

Hinsichtlich der Verletzung von Geschäfts- und Betriebsgeheimnissen, der Verletzung von Urheberrechten sowie dem Ausspähen beziehungsweise dem Abfangen von Daten nehmen jeweils rund drei Viertel der Befragten ein hohes beziehungsweise sehr hohes Risiko wahr. Die übrigen Deliktstypen bereiten den Unternehmen deutlich weniger Sorgen.

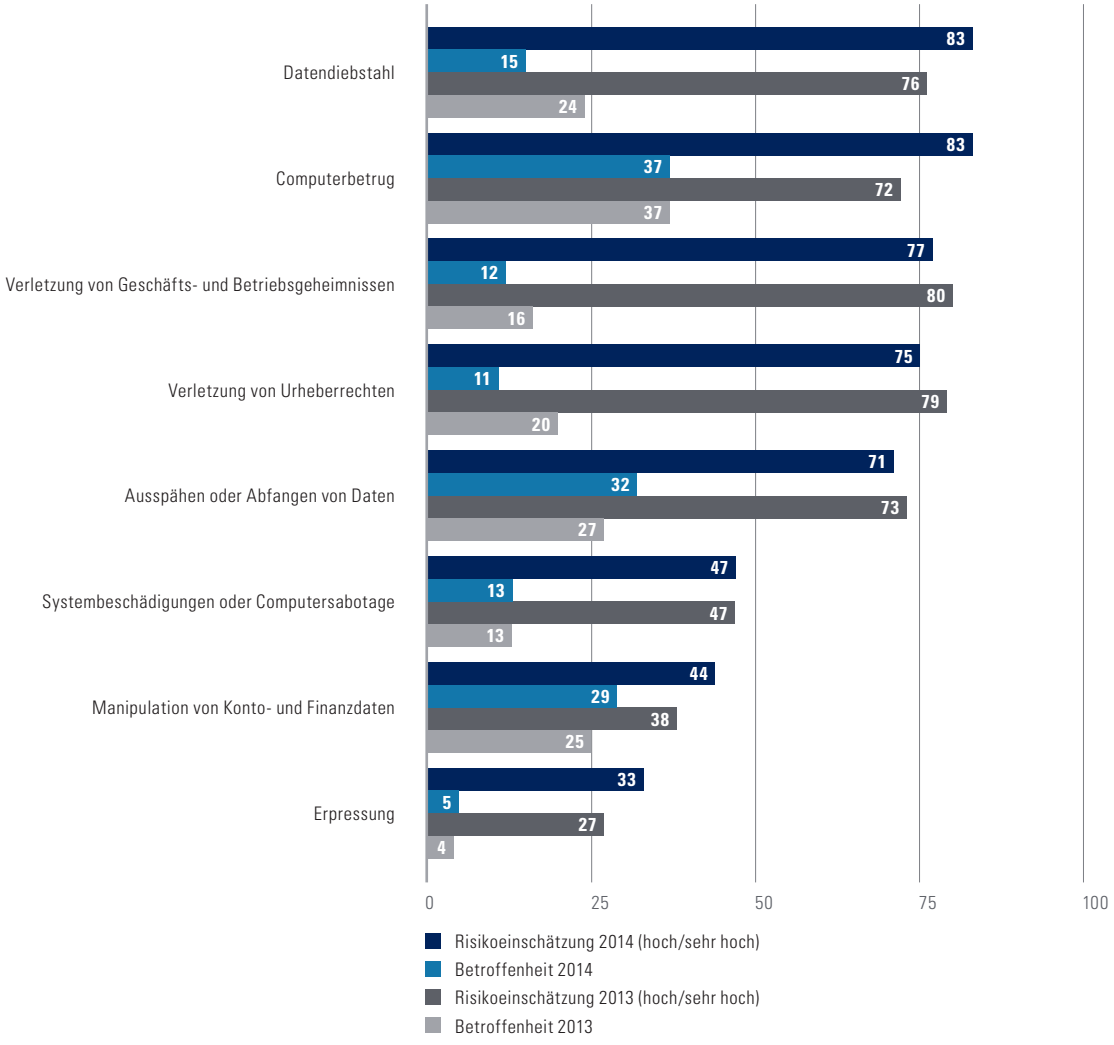
Der Anstieg in der Risikowahrnehmung von Computerbetrug beruht möglicherweise darauf, dass es sich hierbei nach wie vor um den am häufigsten festgestellten Deliktstyp bei den betroffenen Unternehmen handelt. Insgesamt sind 37 Prozent der Befragten bereits Opfer von Computerbetrug geworden. Maßgebenden Einfluss auf diese Zahl haben insbesondere Vertreter der Handelsbranche, in der sich 54 Prozent der Betroffenen mit Computerbetrug auseinandersetzen mussten.

Weitere Deliktstypen, die von Opfern von e-Crime ähnlich häufig angegeben wurden, sind das Ausspähen oder Abfangen von Daten (32 Prozent) sowie die Manipulation von Konto- und Finanzdaten (29 Prozent). Beide sind im Vergleich zu 2013 geringfügig häufiger vorgefallen.

02 VERGLEICH ZWISCHEN DELIKTSPEZIFISCHER RISIKOWAHRNEHMUNG UND BETROFFENHEIT

Angaben in Prozent

Quelle: KPMG, 2015



2 Der Gesamtschaden beinhaltet den eingetretenen Verlust, den entgangenen Gewinn, Ermittlungs- und Folgekosten, Bußgelder, Geldstrafen und eventuelle Gewinnabschöpfungen.

3 Die Betroffenheit gibt unabhängig von der tatsächlichen Anzahl der e-Crime-Vorfälle an, ob ein Unternehmen Opfer eines bestimmten Deliktstyps geworden ist. Die Häufigkeit gibt den Unternehmen die Möglichkeit, die tatsächliche Anzahl der Delikte zu beziffern, beispielsweise 11 bis 50 Mal.

4 Für diese Studie wurden Unternehmen der Branchen Handel, Industrie, Finanzdienstleister und sonstige Dienstleister befragt. Unter dem Begriff der „sonstigen Dienstleister" werden unter anderem Transport- und Logistik-, Informations- und Kommunikationsdienstleister, die Erbringung von wirtschaftlichen oder technologischen Dienstleistungen sowie Dienstleistungen im Gesundheits- oder Sozialbereich und sonstige Dienstleistungen zusammengefasst (siehe auch Seite 30 ff.).

Insgesamt kann man feststellen, dass es nicht die eine typische e-Crime-Handlung gibt, sondern Unternehmen sich gegen eine Vielzahl verschiedener Delikte wappnen müssen. Folglich müssen Unternehmen einerseits im Blick behalten, welche Delikte sie häufig und kostenintensiv betreffen und sich dementsprechend vorbereiten, andererseits dürfen sie aber die Gesamtheit aller Delikte nicht außer Acht lassen.

Bei der Manipulation von Konto- und Finanzdaten fällt auf, dass im Vergleich zu anderen Deliktstypen keine große Diskrepanz zwischen Wahrnehmung und tatsächlicher Betroffenheit herrscht. Das Risiko, Opfer dieses Delikts zu werden, schätzen 44 Prozent der Befragten als hoch beziehungsweise sehr hoch ein. Dieser Wert übersteigt die Betroffenheit lediglich um 15 Prozent. Bezogen auf andere Delikte liegt die Differenz teilweise bei bis zu 68 Prozent.

Das mag an den im Vergleich geringen durchschnittlichen Gesamtschäden[2] bei diesem Deliktstyp von „nur" 128.000 Euro liegen. Dennoch stellt sich die Frage, ob die Befragten den Angriff auf Konto- und Finanzdaten, immerhin der Deliktstyp mit der drittgrößten Betroffenheitsrate, unterschätzen.

Gegenüber den Ergebnissen der Studie von 2013 bestätigt sich der Trend, dass die Verletzung von Geschäfts- und Betriebsgeheimnissen sowie die Verletzung von Urheberrechten an Bedeutung verlieren und seltener auftreten.

Etwas überraschend, gerade angesichts der sehr hohen Risikowahrnehmung, gilt das auch für den Deliktstyp Datendiebstahl, von dem lediglich 15 Prozent der Opfer von e-Crime betroffen waren (2013: 24 Prozent). Diese Entwicklung könnte allerdings auch durch eine bessere Fähigkeit der Unternehmen zur Differenzierung zwischen den Delikten erklärt werden.

Bei den Delikten Datendiebstahl und Verletzung von Urheberrechten besteht eine besonders große Differenz zwischen Risikowahrnehmung und Betroffenheit. Dieser Umstand spiegelt sich nicht nur bei der Untersuchung von e-Crime, sondern auch in Studien zur Wirtschaftskriminalität im Allgemeinen wider. Daher gilt es zu hinterfragen, wie ein solches Missverhältnis zwischen Wahrnehmung und Realität entsteht. Unsere Erfahrung zeigt, dass die tatsächliche Dunkelziffer daten- und technikbezogener Delikte vielfach nicht mit den Angaben der betroffenen Unternehmen übereinstimmt. Häufig mangelt es an einem Überblick über die komplexen technischen Prozesse und an Kontrollmechanismen, die es ermöglichen, diese Deliktstypen zu entdecken und derartige Vorfälle aufzuklären. Außerdem ergeben sich Schwierigkeiten daraus, dass Daten zumeist nicht verschwinden, wie beim Diebstahl materieller Güter, sondern unzulässigerweise kopiert und andernorts verwendet werden. Folglich fallen solche Vorfälle – wenn überhaupt – meist erst später und dann auf, wenn Daten tatsächlich missbraucht werden.

Ein weiterer Grund könnte die mediale Präsenz solcher Delikte sein. Allein in den letzten Monaten wurden e-Crime-Angriffe gegen verschiedenste bekannte Unternehmen in den Medien thematisiert. Folglich haben die Befragten ein besonders ausgeprägtes Risikobewusstsein in Bezug auf solche Vorfälle.

Betrachtet man nach der Betroffenheit nun die tatsächliche Häufigkeit[3] bestätigt sich, dass Computerbetrug und das Ausspähen beziehungsweise das Abfangen von Daten die am häufigsten verwirklichten Delikte sind. Nach Angabe der befragten Unternehmen traten diese Delikte zwischen 11 und 50 Mal im Betrachtungszeitraum auf. Die übrigen Deliktstypen wurden in der Regel hingegen nur mit einem Fall genannt.

Im Vergleich zu anderen Branchen[4] sind insbesondere Finanzdienstleister und Handel häufiger betroffen. Hier zeigt sich die im Durchschnitt hohe Attraktivität dieser Branchen für Angreifer, die wiederum auf den direkt umsetzbaren Marktwert der Daten und Informationen zurückgeführt werden kann. Möglicherweise zeigt dies aber auch, dass diese Branchen bessere Maßnahmen zu Detektion implementiert haben. Schließlich setzen sich Banken und Onlinehandel schon seit Jahren mit Informations- und Kommunikationstechnologien auseinander.

2.3 RISIKOBEHAFTETE TECHNIK UND INFORMATIONEN

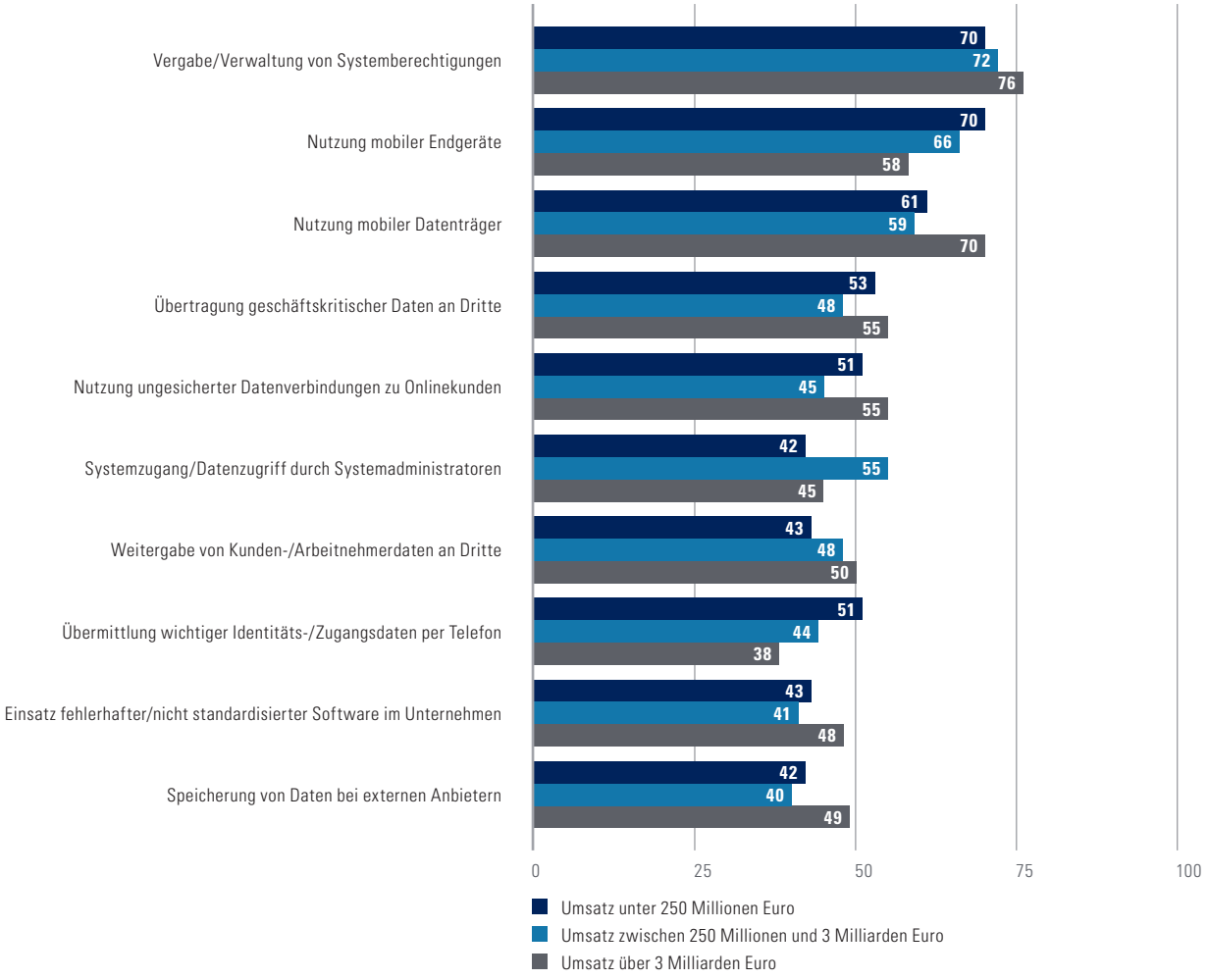
Bei der Betrachtung der für e-Crime typischen Gefahrenquellen entsteht der Eindruck, dass bei der Ausnutzung von Prozesslücken im Unternehmen Insider in den Mittelpunkt rücken (Abbildung 03). Dafür spricht zum einen, dass inzwischen knapp drei Viertel der Befragten die Vergabe und Verwaltung von Systemberechtigungen als besondere Gefahrenquelle betrachten. Damit ist diese Ursache zur meistgenannten avanciert und hat die Verwendung mobiler Datenträger verdrängt, die nur noch von 62 Prozent der Befragten angeführt wird (2013: 70 Prozent). Zum anderen wird dies dadurch bekräftigt, dass Systemzugang und Datenzugriff durch Systemadministratoren von knapp der Hälfte der Unternehmen mit Sorge betrachtet werden (2013: 41 Prozent). Betroffen sind hier insbesondere Finanzdienstleister, möglicherweise da der Zugang zu Kundendaten und Kernbankensystemen eine besondere „Attraktivität" ausübt.

Dass ein mangelhaftes Berechtigungsmanagement eine andauernde, bislang aber häufig unterschätzte Gefahrenquelle darstellt, stellen wir vielfach im Rahmen forensischer Untersuchungen fest. Insofern ist zu begrüßen, dass das Risikobewusstsein größer wird und einen Impuls zur Implementierung angemessener Maßnahmen gibt.

03 RISIKOBEHAFTETE UNTERNEHMENSABLÄUFE

Angaben in Prozent

Quelle: KPMG, 2015



Die Verwendung mobiler Datenträger wird um rund 10 Prozent seltener genannt als noch 2013. Offenbar sehen sich Unternehmen inzwischen besser auf die Verwendung von USB-Sticks, externen Festplatten und so fort vorbereitet als noch vor zwei Jahren. Der Fakt, dass dennoch über die Hälfte der Befragten mobile Datenträger mit besonderer Sorge betrachtet, belegt jedoch, dass die Risiken noch nicht vollständig beherrscht werden. Somit bleiben auch sie ein Thema, mit dem Unternehmen sich zukünftig auseinandersetzen müssen.

Abgesehen davon zeigt sich die Hälfte der Befragten hinsichtlich der Verwendung ungesicherter Datenverbindungen zu Onlinekunden besorgt. In der Studie des Jahres 2013 waren es lediglich 41 Prozent. Da immer mehr Geschäftsverkehr online abgewickelt wird, ist es nicht überraschend, dass Unternehmen hier besondere Vorsicht walten lassen. Sichere, verschlüsselte Verbindungen sollten heutzutage Standard sein, um sensible Informationen zu schützen. Nicht zuletzt der Fall Snowden hat gezeigt, dass der Mangel an entsprechenden Schutzmaßnahmen immense Risiken bei der Sicherheit von Daten bedeutet.

Bei der Betrachtung von IT-Anwendungen sind es insbesondere die Herausforderungen der mobilen Telekommunikation und mobiler Endgeräte, welche die Befragten besonders beschäftigen (Abbildung 04).

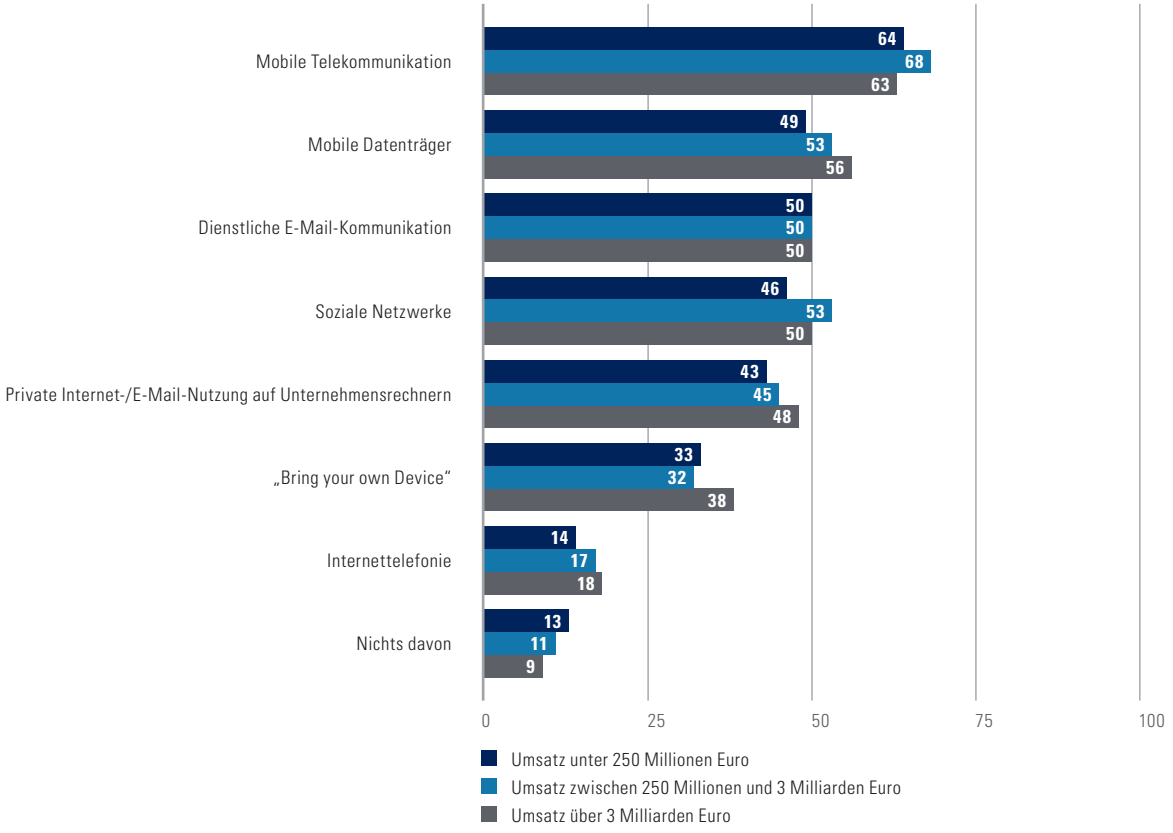
So schätzen, wie schon 2013, knapp zwei Drittel der Befragten mobile Telekommunikation als eine besonders risikobehaftete IT-Anwendung ein.

Die Hälfte der Befragten schätzt zudem die dienstliche E-Mail-Kommunikation sowie die Verwendung sozialer Netzwerke als besonders risikobehaftet ein. Auch wenn die technischen

04 RISIKOBEHAFTETE IT-ANWENDUNGEN

Angaben in Prozent

Quelle: KPMG, 2015



Möglichkeiten für konkrete e-Crime-Delikte bei den genannten Technologien nicht jedem Anwender im Detail bekannt sein werden, bieten sie durch die Fülle an dort gesammelten und auch zum Teil öffentlichen Informationen eine breite Angriffsfläche, die für weitere Delikte genutzt werden kann.

Überraschenderweise wird die geschäftliche (Mit-)Nutzung von Privatgeräten (sogenanntes „Bring your own Device", BYOD), vergleichbar zur vergangenen Studie, lediglich von einem Drittel der Befragten mit Sorge betrachtet.

Den Antworten der Befragten zufolge stellen diese sicher, dass Smartphones, Tablets und Ähnliches von Unternehmen gestellt werden und Richtlinien implementiert sind, die den korrekten Gebrauch dieser Geräte festlegen oder es besteht ein grundsätzliches Verbot der Verwendung von Privatgeräten. In diesem Zusammenhang lässt sich insbesondere feststellen, dass Finanzdienstleister BYOD eine sehr geringe Bedeutung beimessen. Im Gegensatz dazu empfinden rund 40 Prozent der sonstigen Dienstleister und der Industrie BYOD als besonders risikobehaftet.

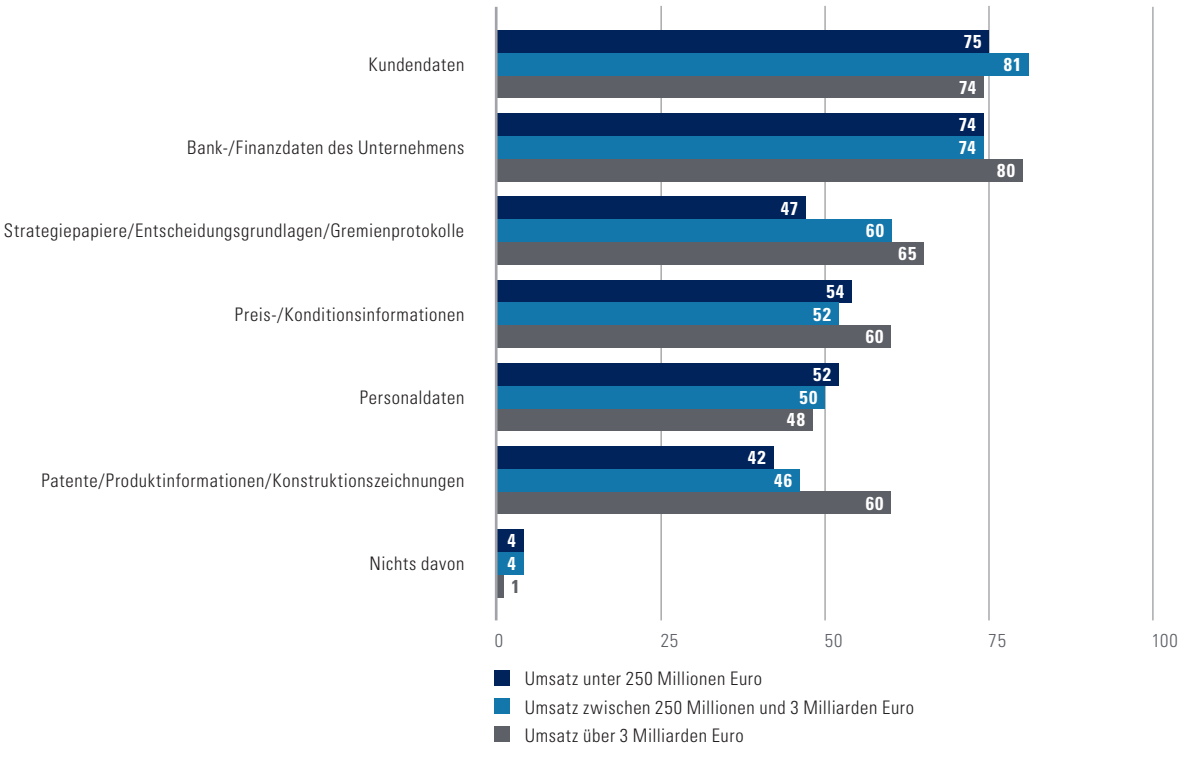
Nach Ansicht von rund drei Vierteln der Befragten bestehen für Kunden- sowie Bank- und Finanzdaten des Unternehmens die größten Risiken im Rahmen eines e-Crime-Vorfalls (Abbildung 05). Dies gilt bei Kundendaten vor allem für Finanzdienstleister und Handel, bei denen diesen Daten die größte Attraktivität aufgrund ihres direkt umsetzbaren Marktwerts innewohnt.

Patente werden, wie zu erwarten, insbesondere von der Industrie besonders häufig als potenzielles Ziel ausgemacht. Insgesamt zeigt sich eine branchentypische Einschätzung der gefährdeten Datenarten.

05 RISIKOBEHAFTETE INFORMATIONEN

Angaben in Prozent

Quelle: KPMG, 2015



5 Das Zukunftsprojekt Industrie 4.0 zielt darauf ab, die deutsche Industrie in die Lage zu versetzen, für die Zukunft der Produktion gerüstet zu sein. Industrieproduktion wird gekennzeichnet sein durch starke Individualisierung der Produkte unter den Bedingungen einer hoch flexibilisierten (Großserien-)Produktion, die weitgehende Integration von Kunden und Geschäftspartnern in Geschäfts- und Wertschöpfungsprozesse und die Verkopplung von Produktion und hochwertigen Dienstleistungen.

Innerhalb der Gruppe der betroffenen Unternehmen nehmen zudem 64 Prozent der Befragten Strategiepapiere, Entscheidungsvorlagen und Gremienprotokolle als besonders risikobehaftet wahr, nicht betroffene Unternehmen nur zu 50 Prozent. Das deutet darauf hin, dass Letztere die entsprechenden Gefahren unterschätzen oder den tatsächlichen Schaden bei Verlust nicht richtig einschätzen.

Vergleicht man die Einschätzung der Unternehmen hinsichtlich der risikobehafteten Daten mit den tatsächlichen betroffenen, handelt es sich vor allem um Kunden- sowie Bank- und Finanzdaten des Unternehmens (Abbildung 06). Risikowahrnehmung und Betroffenheit stimmen hier also überein. Die Unternehmen kennen die potenziellen e-Crime-Ziele innerhalb ihres Unternehmens. Eigene Personaldaten sind über alle Branchen hinweg ein für Täter weniger attraktives Ziel. Diese Aussage gilt entgegen den Befürchtungen der Befragten auch für Strategiepapiere.

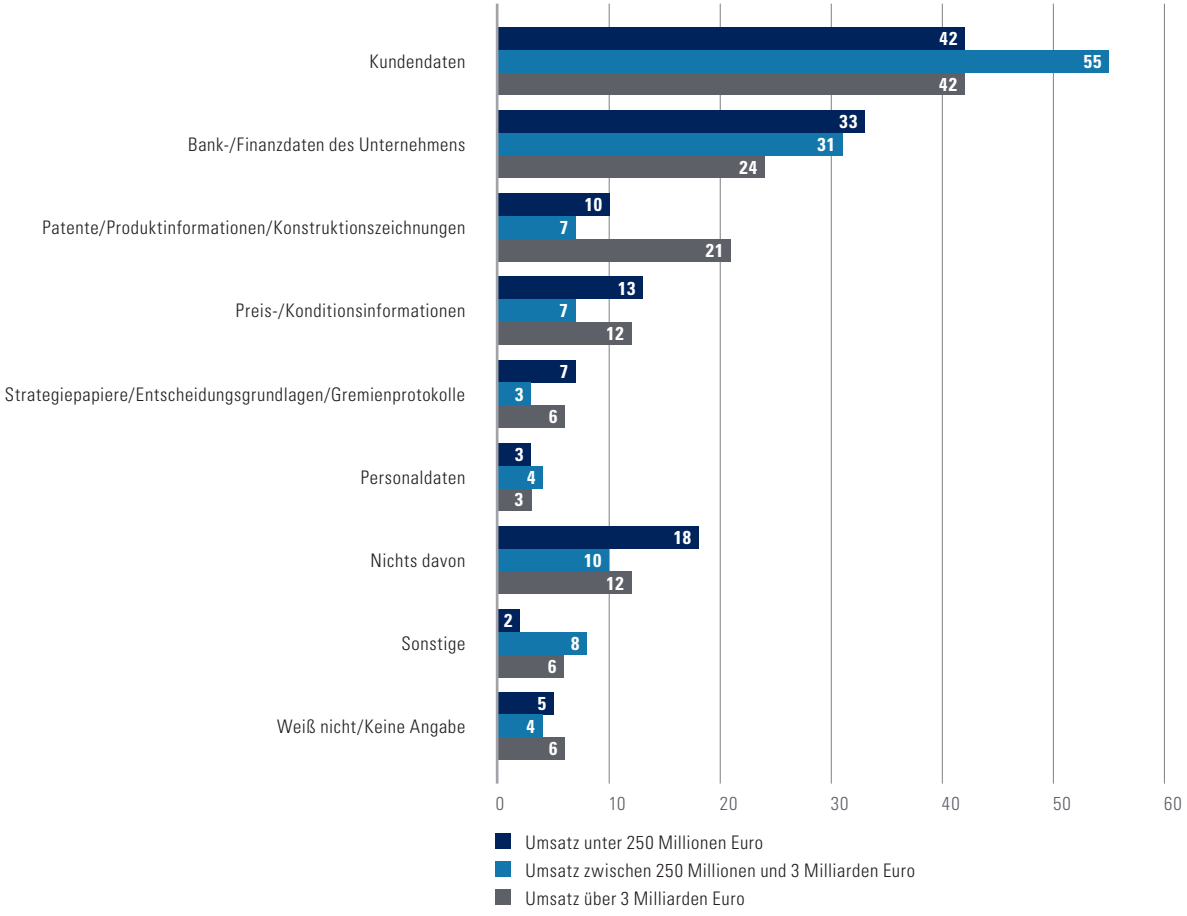
Die Kenntnis der risikobehafteten Daten und Informationen sollte Grundlage der Einführung risikoorientierter Maßnahmen hinsichtlich e-Crime-Prävention, -Detektion und -Reaktion sein.

Abschließend fällt auf, dass der Begriff Industrie 4.0[5] und die damit verbundenen Chancen und Risiken den Befragten bisher branchenübergreifend kaum geläufig ist. Lediglich ein Viertel gibt an, den Begriff „Industrie 4.0“ zu kennen. Davon ist wiederum nur ein Viertel der Ansicht, dass Industrie 4.0 bereits von Bedeutung für die deutsche Industrie ist. Immerhin 44 Prozent denken, dass sich das innerhalb der nächsten fünf Jahre ändern wird.

06 ZIELE VON E-CRIME-INFORMATIONEN

Angaben in Prozent

Quelle: KPMG, 2015



10 Prozent dieser Gruppe verwenden aktuell schon Industrie 4.0-Anlagen oder -Maschinen, bei weiteren 19 Prozent ist ihr Einsatz in Planung.

Im Vergleich zu den generellen Risiken sehen die Befragten bei diesen Anlagen allerdings ein höheres Risiko, Opfer des Ausspähens oder Abfangens von Daten zu werden. Das Risiko des Computerbetrugs oder von Urheberrechtsverletzungen wird dagegen in geringerem Maße wahrgenommen.

Die Komplexität beziehungsweise Offenheit der Systeme wird von 81 Prozent der Befragten als größte Herausforderung wahrgenommen.

2.4 ANGRIFFSZIELE DER TÄTER

Entgegen den Aussagen zu risikobehafteten Unternehmensabläufen, nach denen sich Unternehmen insbesondere um mobile Datenträger und mobile Endgeräte sorgen, sind tatsächlich bargeldlose Zahlungssysteme das häufigste Ziel von e-Crime. Auf diese Kategorie entfallen 30 Prozent der Delikte. Insbesondere Finanzdienstleister und Vertreter des Handels sind hiervon betroffen. Das deckt sich mit der Beobachtung, dass sich e-Crime vor allem dort verwirklicht, wo sich Gewinne am unmittelbarsten erzielen lassen.

Dennoch lässt sich feststellen, dass eine breite Palette von verschiedenen Systemen betroffen ist. Das unterstreicht ein weiteres Mal, dass es nicht nur ein typisches e-Crime-Angriffsmuster gibt und Unternehmen sich folglich nur mithilfe eines umfassenden Präventionsansatzes ausreichend gegen e-Crime wappnen können. Beispielsweise wurden auch Clients und Workstations, externe sowie interne Mailserver und externe Webserver von mindestens 20 Prozent der Befragten als mögliche Ziele eines e-Crime-Delikts genannt.

Neue Technologien, wie beispielsweise Cloud-Services, sind bisher vergleichsweise seltener betroffen. Dieses Ergebnis könnte allerdings auch darauf zurückzuführen sein, dass es noch keine ausreichenden technischen Möglichkeiten zur eigenständigen Detektion von e-Crime-Delikten bei diesen Technologien gibt.

2.5 KOSTEN VON E-CRIME

Angesichts der höheren Betroffenheit gegenüber der vorausgehenden Studie ist der Gesamtschaden durch e-Crime für die deutsche Wirtschaft gestiegen. Die Zunahme der Fallzahlen und Schäden überkompensiert die Effekte der bisher getätigten Investitionen. Klare Zielsetzung der kommenden Jahre muss es sein, ein akzeptables Verhältnis zwischen Investitionen in die Prävention und Detektion sowie Reaktion auf e-Crime einerseits und nicht vermeidbaren Schäden andererseits herzustellen. Unternehmen sind daher auf eine vertiefte Kenntnis ihrer jeweils spezifischen Risikodisposition und der Möglichkeiten und Zusammenhänge einer Maßnahmenstrategie angewiesen.

Die durchschnittliche Gesamtschadenssumme pro befragtes Unternehmen beträgt über alle Delikte hinweg rund 371.000 Euro. Den Unternehmen fällt es jedoch immer noch schwer, konkrete Häufigkeiten für die unterschiedlichen Deliktstypen unternehmensweit zentral zu erfassen.

Bei der Betrachtung deliktspezifischer Schäden ist grundsätzlich zu beachten, dass sie stark durch das Verhältnis von Häufigkeit, Ausmaß und unmittelbarem Schaden sowie Ermittlungs- und Folgekosten geprägt sind. Bei jedem Deliktstyp können im Einzelfall Schäden von über einer Million Euro entstehen. Allerdings weisen, wie schon 2013, die am häufigsten aufgetretenen Deliktstypen die geringsten durchschnittlichen Schadenshöhen pro Deliktstyp-Fall auf (Abbildung 07). Umgekehrt liegen die höchsten durchschnittlichen Schadenssummen bei den Delikten mit der geringsten Betroffenheit vor. Hier ragen insbesondere die Verletzung von Geschäfts- und Betriebsgeheimnissen sowie die Verletzung von Urheberrechten heraus. Für diese Deliktstypen belaufen sich die durchschnittlichen Gesamtschäden pro Unternehmen auf rund 600.000 Euro. Im Gegensatz dazu schätzen die Betroffenen die durchschnittlichen Schadenshöhen für Computerbetrug, das Ausspähen oder das Abfangen von Daten sowie die Manipulation von Konto- und Finanzdaten, den Delikten mit der höchsten Betroffenheit, auf 128.000 bis 253.000 Euro.

Offensichtlich beeinträchtigen die tatsächlich entstandenen Kosten die Risikowahrnehmung der Befragten in erheblichem Maße. Kostenintensive und häufiger auftretende Delikte begründen eine größere Besorgnis der Befragten, was auf ein aktives Risikomanagement hindeuten könnte. Die reine, im Vergleich geringe Betroffenheit von 12 Prozent durch die Verletzung von Geschäfts- und Betriebsgeheimnissen beispielsweise erklärt die entsprechende Risikowahrnehmung nicht. Wie schon dargestellt gilt das exakte Gegenteil für die Manipulation von Konto- und Finanzdaten. Sie verzeichnet zwar eine im Vergleich hohe Betroffenheit von 29 Prozent, jedoch eine geringe Risikowahrnehmung von 44 Prozent.

Insgesamt zeigt sich eine große Spannweite durchschnittlicher Gesamtschäden pro Deliktstyp. Nimmt man dazu noch die einzelnen Branchen in den Fokus, zeigen sich zusätzliche Schwankungen.

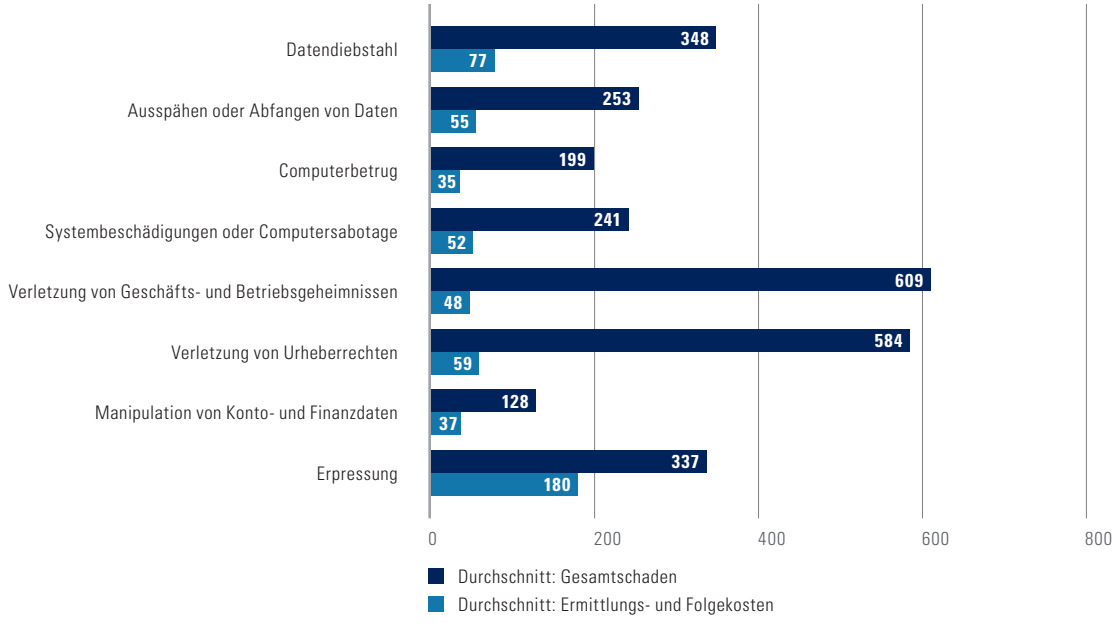
Das Ziel, Schadenssummen soweit wie möglich zu reduzieren, kann nur durch routinierten Umgang in den Phasen der Prävention, Detektion und Reaktion betreffend der genannten Delikte erreicht werden. Unternehmen sollten sich daher durch gezielte präventive und detektive Maßnahmen und vor allem durch konkrete, eingeübte Handlungsanweisungen auf den Ernstfall vorbereiten. Dabei sollten sie sich insbesondere auf ihre häufigen und/oder schadensintensiven Deliktstypen konzentrieren, wobei selbstverständlich auch andere Deliktstypen zumindest im Hinblick auf die Delikts-Awareness nicht zu vernachlässigen sind. Sie müssen dabei jedoch auch beachten, dass jeder Fall – ungeachtet der durchschnittlichen Gesamtschadenshöhe – individuell ist.

Entsprechendes trifft auch auf die Ermittlungs- und Folgekosten zu. In dieser Hinsicht zeigen die Investitionen in Prävention, Detektion und Reaktion jedoch erste Resultate. Die durchschnittlichen Ermittlungs- und Folgekosten sind von 100.000 auf rund 68.000 Euro gesunken. Sie machen damit lediglich 18 Prozent der durchschnittlichen Gesamtschäden aus. In der vergangenen Studie waren es

07 DURCHSCHNITTLICHE GESAMTSCHÄDEN UND DURCHSCHNITTLICHE ERMITTLUNGS- UND FOLGEKOSTEN

Angaben in Tausend Euro

Quelle: KPMG, 2015



noch etwa 25 Prozent. Entscheidend dürfte dabei einerseits die gezieltere Reaktion auf bekannte und mehrfach auftretende Delikte sein, andererseits aber auch die verbesserte Fähigkeit vieler Unternehmen, erkannte Vorfälle zu klassifizieren und eine risikoorientierte Entscheidung über Art und Tiefe der internen und externen Weiterverfolgung zu treffen. In nicht wenigen Fällen wird mittlerweile eine Bestandsaufnahme mit dem Ziel durchgeführt, Aufklärungsmöglichkeiten, Kosten und Nutzen zu beurteilen. Nach Abwägung aller Faktoren ist dann auch eine Entscheidung gegen eine weitere Aufklärung möglich.

Nicht nur in Bezug auf die Meldepflicht des IT-Sicherheitsgesetzes wird es für Unternehmen zunehmend wichtig, die risikoorientierte Beurteilung eines e-Crime-Vorfalls und die Entscheidung über abgeleitete Maßnahmen für Dritte nachvollziehbar zu dokumentieren. Was recht simpel klingt, erweist sich im Alltag aber oft als Herausforderung, da technisch-organisatorische, rechtliche und kaufmännische Aspekte durch eine klare Verantwortlichkeit schlüssig miteinander in Bezug gesetzt werden müssen. Oft fehlt es an Informationen und gegenseitigem thematischen Verständnis aller Beteiligten. Symptomatisch hierfür ist die von den befragten Unternehmen nach wie vor geäußerte Schwäche, im Ernstfall schnell Verantwortlichkeiten zu klären und für einen reibungslosen Informations- und Kommunikationsfluss zu sorgen.

Bei der deliktspezifischen Betrachtung der Ermittlungs- und Folgekosten weist der Deliktstyp Erpressung mit 180.000 Euro mit Abstand die höchsten Kosten dieser Art auf. Diese Zahl dürfte jedoch aufgrund der geringen Fallzahlen wenig aussagekräftig sein. Aussagekräftiger ist hier schon der zweite Rang, den Datendiebstahl mit 77.000 Euro einnimmt. Es fällt auf, dass die Ermittlungs- und Folgekosten bei diesem Deliktstyp in Relation zum Gesamtschaden höher ausfallen als bei den meisten anderen Delikten. Möglicherweise entstehen hier höhere Ermittlungskosten, da die Detektion der Tat und die Verfolgung der Täter größere Schwierigkeiten bereiten.

2.6 PERSONENGRUPPEN UND LÄNDER IN VERBINDUNG MIT E-CRIME UND TATSÄCHLICHE TÄTER

Die Befragten messen unterschiedlichen Personengruppen ein im Vergleich zur Vorgängerstudie breiteres Risikopotenzial bei (Abbildung 08).

Die organisierte Kriminalität wird als die potenziell gefährlichste Personengruppe empfunden. Fast zwei Drittel der Befragten und sogar rund drei Viertel der Betroffenen sowie der Finanzdienstleister sehen sie als bedeutsame Gefahrenquelle. Daran ist sehr gut zu erkennen, dass e-Crime zu einer lukrativen Einnahmequelle für Kriminelle geworden ist. Es ist zu erwarten, dass es teilweise den „klassischen" Delikten wie Diebstahl oder Betrug den Rang ablaufen wird.

Zudem sehen sich 51 Prozent der Befragten besonders durch ehemalige Arbeitnehmer beziehungsweise Insider bedroht (59 Prozent bei betroffenen Unternehmen). Ursache hierfür ist häufig ein mangelhaftes Berechtigungsmanagement, da die Zugriffsrechte ausscheidender Mitarbeiter vielfach nicht rechtzeitig – wenn überhaupt – entzogen werden. Gegenüber 2013 nehmen sie durch die Zunahme der organisierten Kriminalität zwar nicht mehr die Spitzenposition im Ranking ein, verzeichnen aber dennoch einen Anstieg um 8 Prozent.

Geheimdienste und andere staatliche Institutionen, sowohl aus dem Aus- als auch dem Inland, werden inzwischen verstärkt als potenzielle Gefahrenquelle ausgemacht (41 Prozent Ausland, 33 Prozent Inland). Das bedeutet einen Sprung um 15 beziehungsweise 18 Prozent. Es ist davon auszugehen, dass der Fall Snowden und die entsprechenden Erkenntnisse über das Handeln von Geheimdiensten einen erheblichen Anteil an diesem Anstieg haben.

Insbesondere Finanzdienstleister (60 Prozent, bei insgesamt 38 Prozent) betrachten darüber hinaus Kunden von Onlineanwendungen, die durch eine unsachgemäße Bedienung Risiken verursachen, als potenziell gefährliche Personengruppe. Angesichts der

fortdauernden Verbreitung von Onlinebanking und weiteren Onlineanwendungen ist das wenig überraschend. Potenzielle Täter haben zahlreiche Möglichkeiten – über Privat-PCs mit mangelhaften Schutzmechanismen – die mögliche Unkenntnis von Kunden oder die unsachgemäße Bedienung von Anwendungen auszunutzen.

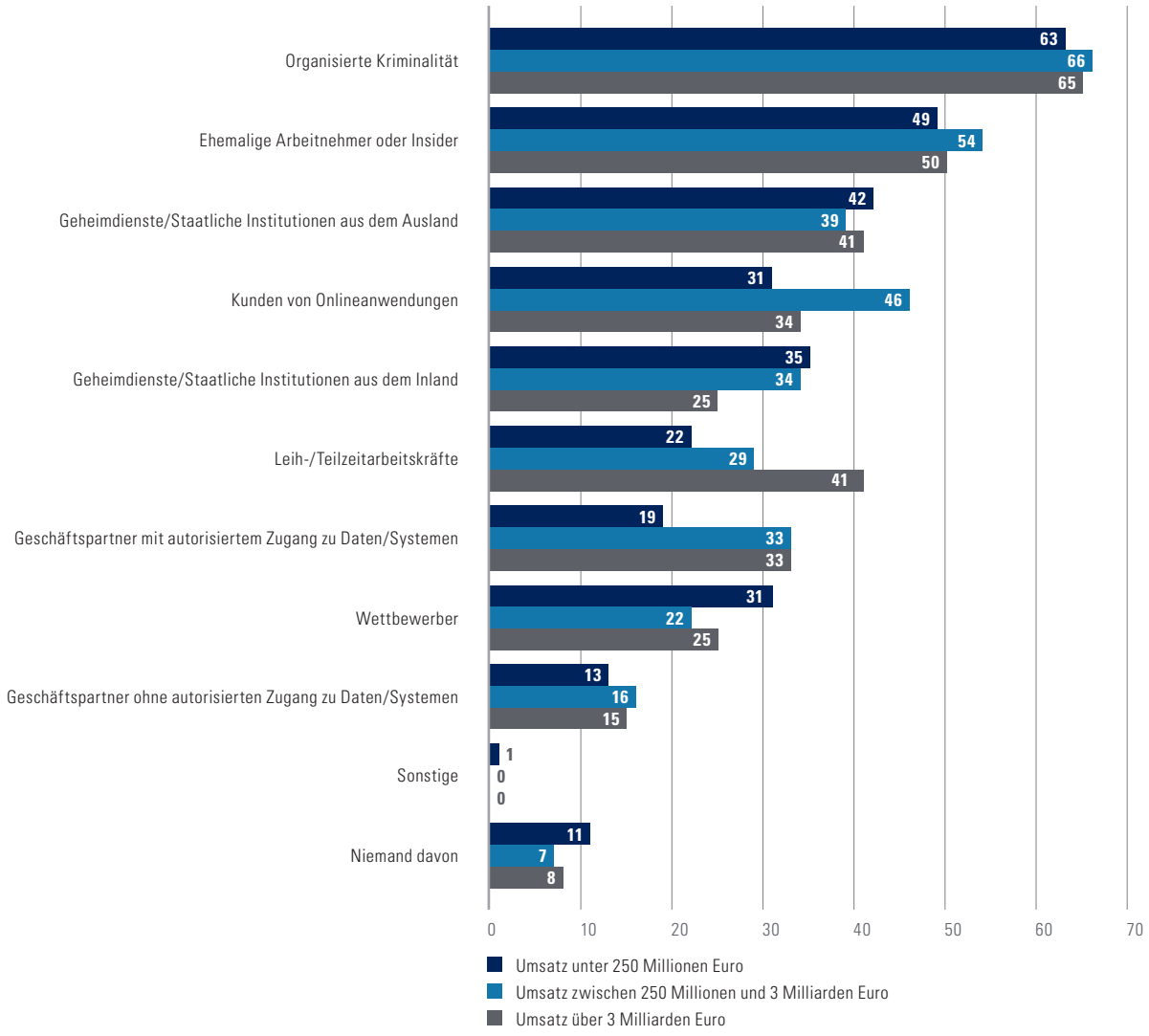
Hinsichtlich der tatsächlichen Täter bestätigt sich die Tendenz, dass unbekannte Externe den Großteil dieser Gruppe ausmachen (Abbildung 09). Insofern sind die Bedenken der Befragten bezüglich der organisierten Kriminalität begründet, die ja in der Regel in diese Kategorie fällt.

Allerdings scheint auch das zunehmende Misstrauen gegenüber Mitarbeitern gerechtfertigt zu sein. Gerade bei kleineren und mittleren Unternehmen nimmt der Anteil dieser Tätergruppe bei den Delikten Computerbetrug, Systembeschädigungen oder Computersabotage sowie Manipulation von Konto- und Finanzdaten zu. Das könnte allerdings auch auf größere Erfolge bei der Ermittlung der Täter hindeuten, sodass sie nun klar identifiziert werden können. Bei Erpressung und Verletzung von Geschäfts- und Betriebsgeheimnissen fällt es Unternehmen jedoch nach wie vor schwer, die Täter zu ermitteln.

08 POTENZIELL GEFÄHRLICHE PERSONENGRUPPEN

Angaben in Prozent

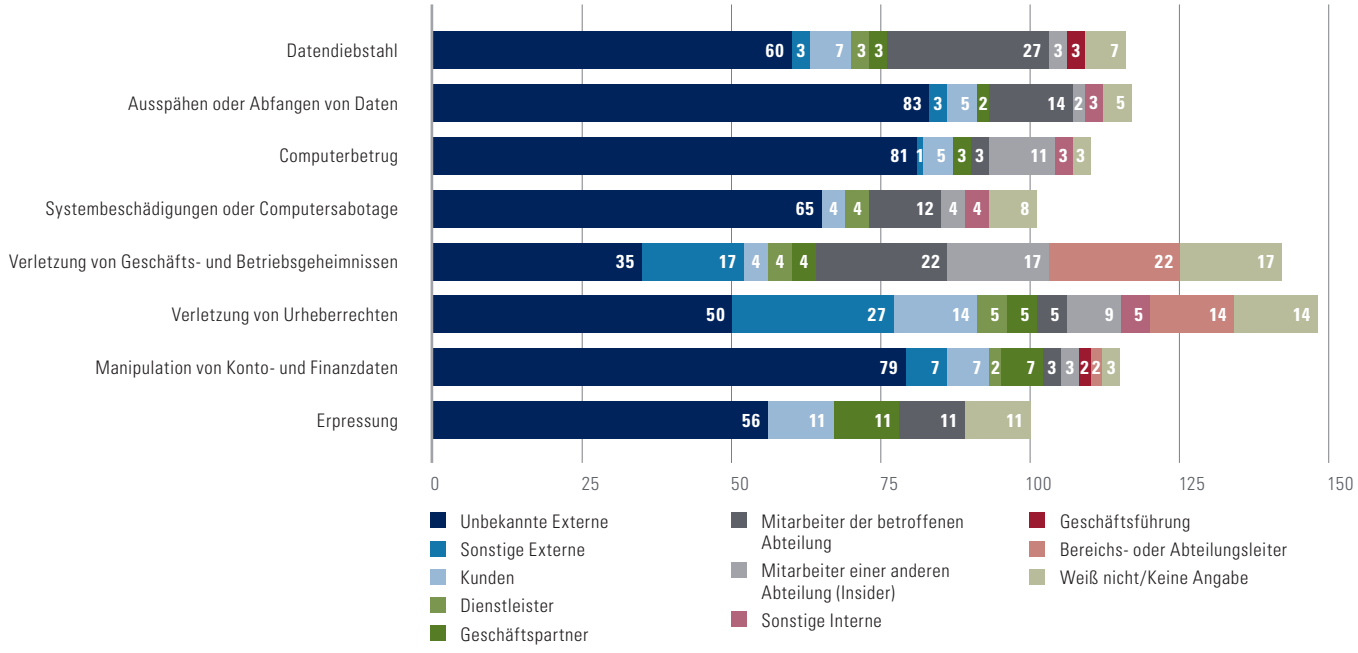
Quelle: KPMG, 2015



09 HERKUNFT DER TÄTER

Angaben in Prozent

Quelle: KPMG, 2015



Etwa die Hälfte der Befragten verbindet e-Crime mit bestimmten Ländern (2013: 42 Prozent). Wie schon in der vergangenen Studie werden zunächst China und Russland von etwa einem Viertel der Befragten genannt. Dahinter folgen nun, nach einem Anstieg um 7 Prozent auf 19 Prozent, die USA. Angesichts der Enthüllungen um NSA, PRISM und Co. erscheint dieser Sprung fast schon gering. Das lässt darauf schließen, dass Unternehmen möglicherweise schon immer entsprechende Aktivitäten aus den Vereinigten Staaten heraus vermutet haben.

Von den USA verdrängt folgt der osteuropäische Raum, den 17 Prozent der Befragten in Verbindung mit e-Crime bringen.

Es fällt auf, dass Finanzdienstleister China, Russland und die USA deutlich seltener mit e-Crime verbinden als andere Branchen. Dafür nennen 27 Prozent der Unternehmen dieser Branche den osteuropäischen Raum als Gefahrenquelle. Hier wird offenbar eine Verbindung zur organisierten Kriminalität hergestellt, die vielfach aus dieser Region tätig wird.

Es bleibt festzuhalten, dass e-Crime nach wie vor eine globale Herausforderung darstellt.

3 PRÄVENTION, DETEKTION UND REAKTION

3.1 PRÄVENTION

3.1.1 Verfügbarkeit von Personal

Basis einer guten Prävention ist immer auch die Personalakquise beziehungsweise die entsprechende Weiterbildung des bestehenden Personals. Grundsätzlich mangelt es den Unternehmen zumeist nicht an der Verfügbarkeit von Personal im IT-Bereich. Insbesondere die Finanzdienstleister verlassen sich auf eine vergleichsweise dicke Personaldecke. Es stellt sich jedoch die Frage, ob die Qualifikation des Personals das tatsächlich erforderliche Aufgabenprofil abdeckt. Der Markt für Fachkräfte mit notwendiger Qualifikation in Bezug auf e-Crime kann aktuell als angespannt bezeichnet werden. Ob sich die vermeintlich entspannte Personalsituation, die 42 Prozent der Befragten sehen, und die damit verbundenen Erwartungen im Ernstfall als beständig erweisen, bleibt abzuwarten. Immerhin erkennt auch ein Viertel der Unternehmen Herausforderungen bei der internen Rekrutierung und Weiterbildung von Personen für die Prävention und Detektion von sowie die Reaktion auf e-Crime. Auch extern finden diese Unternehmen kaum geeignete Bewerber.

3.1.2 Begünstigende Faktoren

Unternehmen haben im Vergleich zu 2013 stärker in die Prävention von e-Crime investiert. Nur noch 39 Prozent der Befragten beklagen ein limitiertes Budget für Sicherheitsmaßnahmen, lediglich 44 Prozent empfinden fehlende Ad-hoc-Kontrollen als begünstigenden Faktor für e-Crime. In der Studie 2013 traf dies noch auf mehr als die Hälfte der Unternehmen zu. Auch in der Aus- und Fortbildung des Personals durch Schulungs- und Sensibilisierungsmaßnahmen hat sich nach Einschätzung der Studienteilnehmer etwas getan. Knapp zwei Drittel der Befragten sahen hier 2013 noch Defizite bei der Schulung und Sensibilisierung des Personals. Inzwischen ist ihr Anteil auf 60 Prozent gesunken.

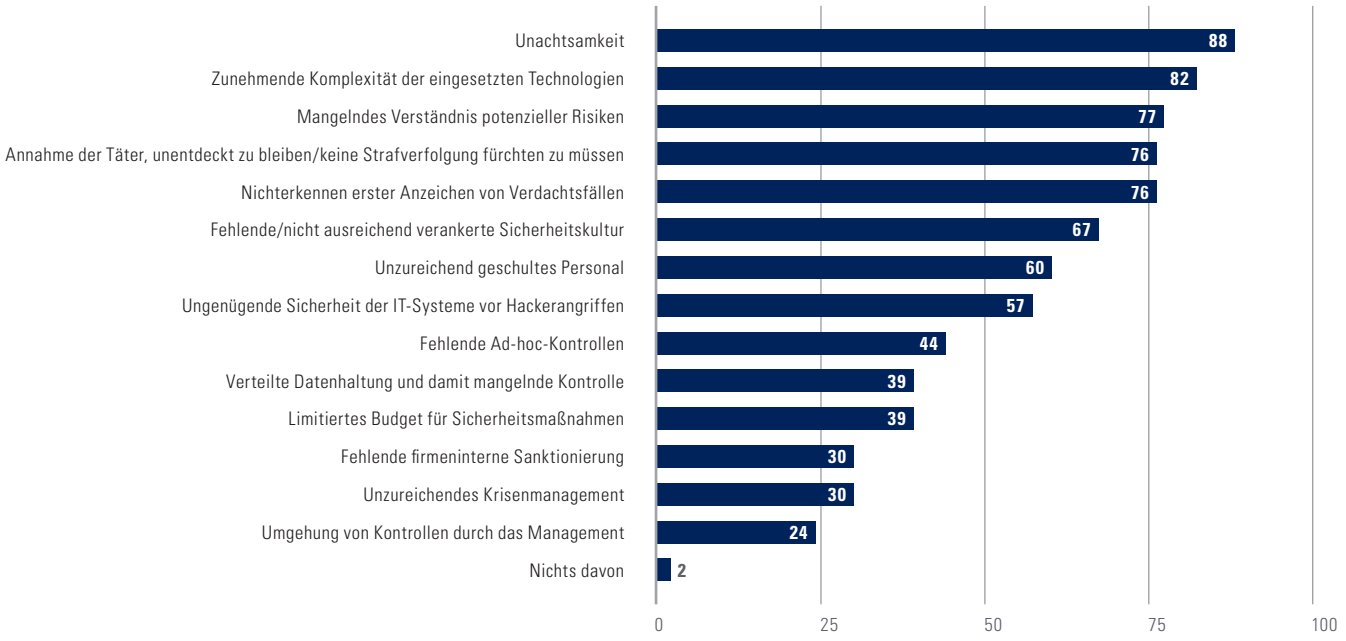
Trotz dieser positiven Entwicklungen besteht nicht der Eindruck, dem Problem e-Crime Herr zu werden.

Gerade in technischer Hinsicht nehmen Unternehmen zunehmend große Herausforderungen durch neue Technologien wahr. Von den Studienteilnehmern geben 76 Prozent an, dass vor allem Schwachstellen in neuen Technologien ausgenutzt werden.

10 E-CRIME BEGÜNSTIGENDE FAKTOREN

Angaben in Prozent

Quelle: KPMG, 2015



Hier gebe es bisher noch keine ausreichenden Schutzmechanismen. Bezeichnend dafür empfinden 66 Prozent der Befragten, dass insbesondere durch Cloud-Computing neue Angriffsmöglichkeiten entstehen.

Hinsichtlich begünstigender Faktoren für e-Crime erweisen sich die komplexe Technik sowie die mangelnde Achtsamkeit und das eingegrenzte Verständnis potenzieller Risiken durch Mitarbeiter weiter als nicht beherrschbar. Mindestens 77 Prozent der Befragten betrachten diese Kategorien mit besonderer Sorge (Abbildung 10).

Insbesondere Unachtsamkeit nimmt gegenüber der Vorgängerstudie und auch der Studie zur Wirtschaftskriminalität eine noch prominentere Position ein. Diesen Faktor nennen 88 Prozent der Unternehmen als begünstigend. Das zeigt, dass die von den Befragten wahrgenommene Verbesserung bei der Schulung und Sensibilisierung ihrer Beschäftigten nur bedingt die Realität widerspiegelt. Dieses Ergebnis betont noch einmal, wie wichtig sensibilisierende Maßnahmen für die Beschäftigten sind, damit sie die nötige Umsicht im Umgang mit Systemen, Daten, Prozessen sowie potenziellen Tätern entwickeln.

Solche Maßnahmen sind umso wichtiger, als der Faktor zunehmende Komplexität von Technik in der Wahrnehmung der Unternehmen an Bedeutung gewonnen hat. Mit 82 Prozent ist er nun der am zweithäufigsten genannte Faktor. Gerade die umsatzstärksten Unternehmen scheinen mit ihrer Technik zunehmend Schwierigkeiten zu bekommen, 91 Prozent unter ihnen empfinden diesen Faktor als begünstigend für e-Crime.

Grundsätzlich gelten dieselben Bedenken sogar für die insgesamt sehr gut auf e-Crime vorbereiteten Finanzdienstleister, wobei Vertreter dieser Branche häufiger das Gefühl haben, ihre Risiken zu kennen. Sonstige Dienstleister kämpfen nach wie vor mit grundlegenden Aspekten, wie unzureichend geschultem Personal, limitiertem Budget, unzureichendem Krisenmanagement und der Umgehung von Kontrollen durch das Management, die die übrigen Branchen inzwischen besser beherrschen.

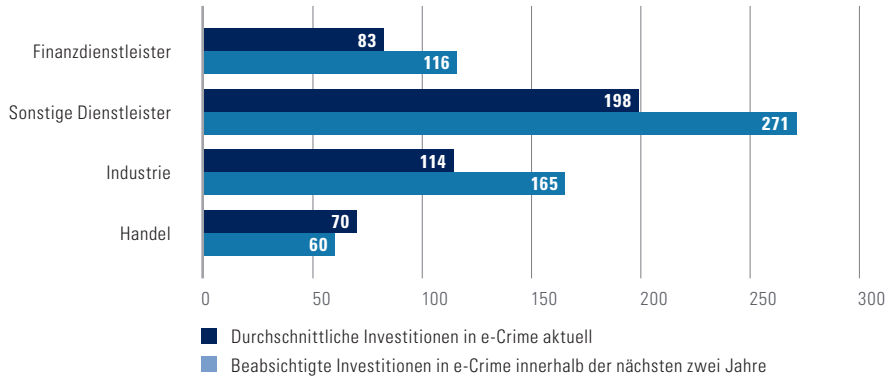
3.1.3 Aktuelle und geplante Investitionen

Wie schon in der Vorgängerstudie sah sich nahezu die Hälfte der Befragten nicht dazu in der Lage, ein genaues Investitionsvolumen für die Bekämpfung von e-Crime anzugeben. Anhand der Angaben wird klar ersichtlich, dass betroffene Unternehmen den jeweiligen Fall zum Anlass nehmen, verstärkt in die Bekämpfung von e-Crime zu investieren. Investitionen sind dadurch vorfallsgetrieben und nicht strategisch. Durchschnittlich investieren die betroffenen Unternehmen 115.000 Euro mehr als nicht betroffene Unternehmen. Diese Tendenz ist erfreulich, aber auch notwendig und konnte 2013 nicht in dieser Deutlichkeit festgestellt werden.

11 AKTUELLE UND GEPLANTE INVESTITIONEN IN DIE BEKÄMPFUNG VON E-CRIME

Angaben in Tausend Euro

Quelle: KPMG, 2015



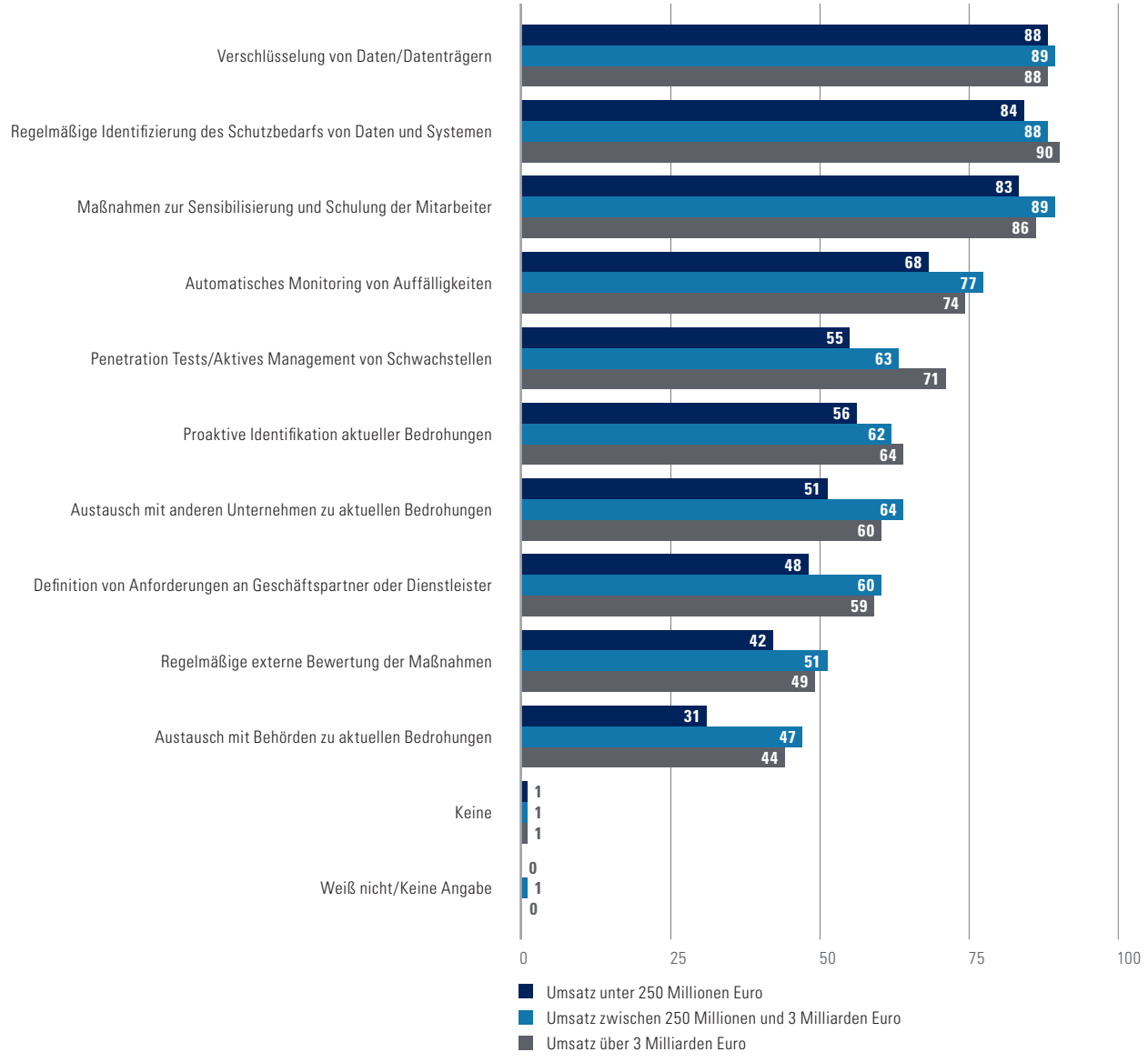
Die aktuelle Gefährdungslage zeigt Wirkung: Die Investitionen in die Prävention, Detektion und Reaktion werden weiterhin deutlich erhöht. Die Verteilung nach Branche und Unternehmensgröße entspricht dabei überwiegend der aktuellen Investitionsstruktur. Das deutet zudem darauf hin, dass die Unternehmen den Kreislauf aus kontinuierlicher Veränderung der Angriffsmuster und notwendiger Anpassung des eigenen Maßnahmenkanons zunehmend akzeptieren.

Die Hälfte der Unternehmen plant, in alle drei Bereiche zu investieren. Dabei zeigt sich die Tendenz, dass vermehrt in Prävention und Detektion investiert werden soll. Unsere Erfahrung zeigt, dass das im Vergleich zu fallbedingten Investitionen ein zu bevorzugender Ansatz ist: Frühzeitige Investitionen in Prävention und Detektion kompensieren die Implementierungs- und Instandhaltungskosten der entsprechenden Maßnahmen dadurch, dass sie e-Crime-Vorfälle verhindern oder die Schäden zumindest im Zuge einer rechtzeitigen Eindämmung und effektiven Aufklärung mindern. Investitionen, die erst in der Phase der Reaktion greifen, erzielen nicht denselben Effekt und sind oft höher. Damit widersprechen sie dem ökonomischen Prin-

12 PRÄVENTIONSMASSNAHMEN

Angaben in Prozent

Quelle: KPMG, 2015



zip. Dennoch sehen wir vielfach, dass vorsorgliche Ausgaben gemieden werden. Insofern ist der Trend dieser Studie zu begrüßen.

3.1.4 Maßnahmen zur Prävention

Nach wie vor ist ein Mix aus Präventionsmaßnahmen notwendig. Den Unternehmen gelingt es weiterhin nicht, die Sensibilisierungsmaßnahmen auf ein Niveau zu heben, das die Unachtsamkeit – den e-Crime nach ihrer Wahrnehmung begünstigenden Hauptfaktor – von ihrer Spitzenposition verdrängt.

Diese Tatsache überrascht, da 86 Prozent der Befragten angeben, dass sie Sensibilisierungs- und Schulungsmaßnahmen für die Mitarbeiter durchführen. Dies gilt sogar unabhängig von der Größe der Unternehmen. Möglicherweise sind die Maßnahmen daher nicht ausreichend, sei es auf qualitativer oder quantitativer Ebene. Ein anderer Grund könnte darin liegen, dass die Personalsituation doch kritischer ist als angegeben.

Neben Schulungsmaßnahmen gehören die Verschlüsselung von Daten und Datenträgern (89 Prozent) sowie die regelmäßige Überprüfung des Schutzbedarfs von Daten und Systemen (87 Prozent) zu den standardmäßig implementierten präventiven Maßnahmen (Abbildung 12).

Knapp drei Viertel der Unternehmen (80 Prozent der Betroffenen) führen eine automatische Anomalieerkennung durch. Abgesehen davon zeigt sich zwischen betroffenen und nicht betroffenen Unternehmen lediglich der Unterschied, dass bereits betroffene Unternehmen häufiger die Möglichkeit ergreifen, sich mit anderen Unternehmen über aktuelle Bedrohungen auszutauschen.

Auf Umsatz basierende Unterschiede können erstaunlich selten festgestellt werden. Dies gilt mit Ausnahme der Durchführung von Penetration Tests. Große Unternehmen nehmen sie zu 71 Prozent vor, kleine Unternehmen nur zu 55 Prozent.

Die größten Unterschiede treten zwischen den einzelnen Branchen auf. Es bestätigt sich ein weiteres Mal, dass Finanzdienstleister umfangreicher gegen e-Crime gewappnet sind als andere Branchen und die sonstigen Dienstleister im Vergleich am schlechtesten vorbereitet sind (siehe hierzu Kapitel 5).

13 ENTDECKUNG DER E-CRIME-HANDLUNG

Angaben in Prozent

Quelle: KPMG, 2015

3.2 DETEKTION UND AUFKLÄRUNG

3.2.1 Detektion der Handlung

Weiterhin ist ein breites Spektrum von Detektionsmöglichkeiten zu berücksichtigen (Abbildung 13). Die strukturierte und sichere Zusammenführung von Informationen aus unterschiedlichen Detektionskanälen stellt eine Herausforderung dar. Nach wie vor werden e-Crime-Vorfälle vor allem durch offene Hinweise Unternehmensexterner entdeckt (58 Prozent). Es zeichnet sich aber auch eine zunehmende Bedeutung von Hinweisen aus internen Routineprüfungen und Monitoringsystemen ab. Ein Teil der Vorfälle lässt sich also durch standardisierte technische Maßnahmen besser erkennen.

Unverändert bleibt der Zufall in nahezu der Hälfte der Vorfälle Ursache der Entdeckung. Ein Grund dafür ist die Stagnation der Hinweise durch Unternehmensinterne, sei es hinsichtlich von Auffälligkeiten an Computersystemen (51 Prozent) oder hinsichtlich anderer Personen (33 Prozent). Auch hier deutet sich wieder an, dass Mitarbeiter möglicherweise nicht wirksam sensibilisiert werden. Unachtsamkeit ist nach wie vor der am häufigsten genannte risikoerhöhende Faktor im Zusammenhang mit e-Crime.

Die Bedeutung von Hinweisen durch Strafverfolgungs- und Aufsichtsbehörden hat, außer bei den Finanzdienstleistungsunternehmen, abgenommen. Die möglichen Konsequenzen sollten vor dem Hintergrund des ITSiG durchdacht werden (siehe hierzu Kapitel 5).

Auch anonyme Hinweise, Ombudsmann oder Whistleblowing spielen eine geringe und abnehmende Rolle. Insgesamt zeigt sich, dass vor allem offene und nicht standardisierte Meldungen im Vordergrund stehen. Hier sollten die Unternehmen auf eine Professionalisierung auf meldender und annehmender Seite hinwirken, um verwertbare Informationen als Entscheidungsgrundlage für weitere Schritte zur Verfügung zu haben.

3.2.2 Operative Aufklärung

e-Crime-Vorfälle werden zu etwa 80 Prozent durch unternehmenseigene Ressourcen der IT und IT-Sicherheit behandelt, eine nochmalige Steigerung gegenüber 2013 (Abbildung 14).

Interne Revision und Compliance bilden einen nachgelagerten Reaktionsbereich und werden von etwa zwei Dritteln der Befragten mit der Aufklärung betraut. Externe IT-Sicherheitsdienstleister sind noch deutlich vor externen Forensic-Dienstleistern involviert. Das breite Verantwortungsspektrum zeigt die unterschiedlichen Charaktere von e-Crime-Delikten. Damit besteht aber auch die Gefahr, dass bei der Aufklärung nicht abgestimmte Aufklärungsmethoden zum Einsatz kommen. Das kann möglicherweise Auswirkungen auf Qualität, Kosten, Angemessenheit und Gerichtsverwertbarkeit der Ergebnisse haben.

Zudem fällt auf, dass große und auch mittelgroße Unternehmen einen umfassenden Aufklärungsansatz wählen und mehreren Organen gleichzeitig diese Aufgabe übertragen. So waren bei Unternehmen mit einem mittleren Umsatz die IT-Abteilung, die IT-Sicherheits-Abteilung, die Interne Revision sowie die Compliance-Abteilung jeweils in mehr als 70 Prozent der Vorfälle gemeinsam für die operative Aufklärung zuständig. Das kann aber auch ein Indiz dafür sein, dass die Prozesse und Verantwortlichkeiten für unterschiedliche Arten von e-Crime-Delikten in den Unternehmen noch nicht deutlich herausgearbeitet und definiert sind. Das Gleiche gilt für Finanzdienstleister und in eingeschränktem Maße für den Handel.

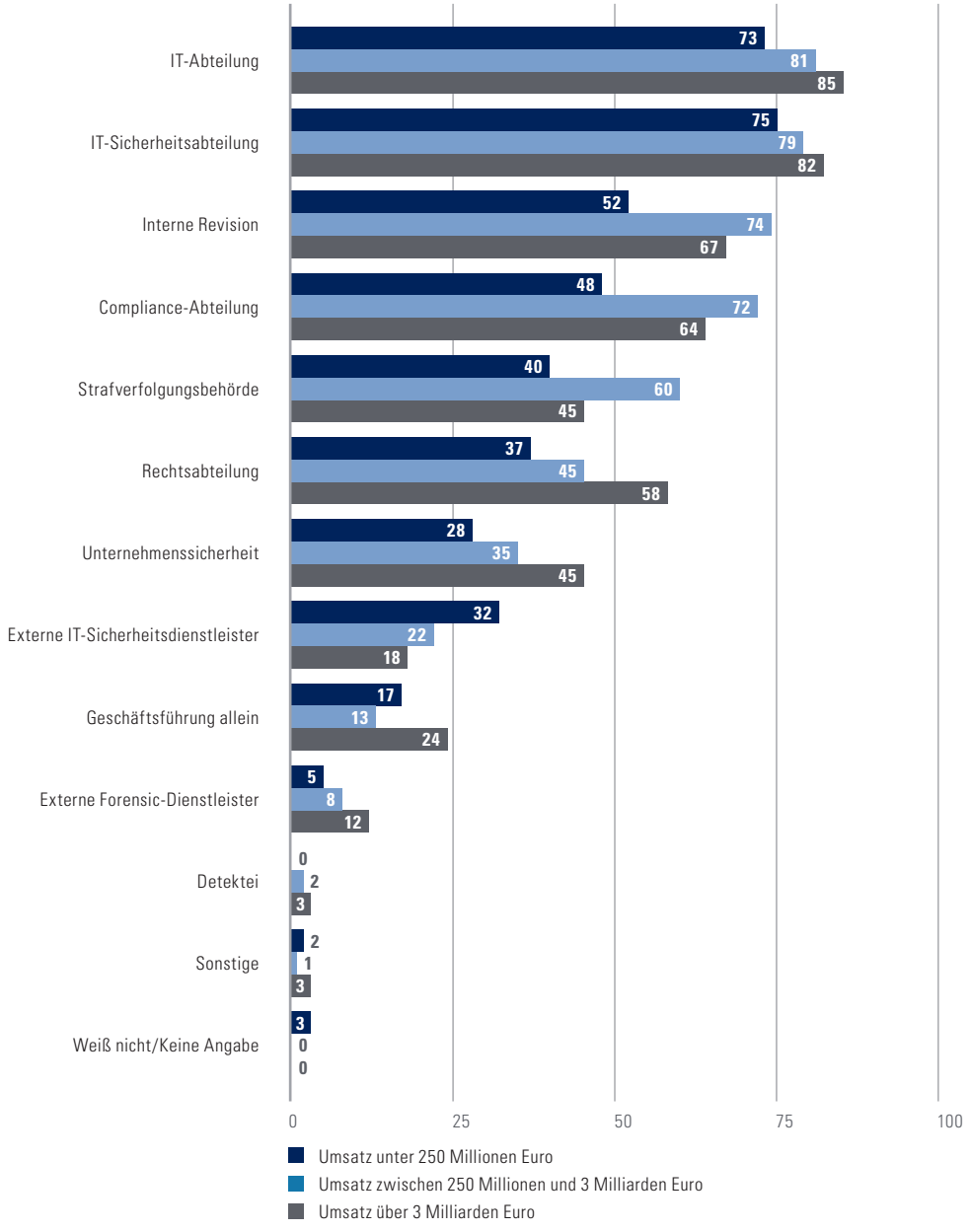
3.2.3 Maßnahmen zur Aufklärung

Daten und Menschen sind nach wie vor der Schlüssel zur Aufklärung. Der grundsätzliche Maßnahmenkanon und seine Strukturierung sind im Wesentlichen konstant geblieben (Abbildung 15). Die Häufigkeit, mit der Aufklärungsmaßnahmen durchgeführt wurden, ist jedoch mehrheitlich gesunken. So wurde nur noch in 66 Prozent der Fälle eine elektronische Datenanalyse vorgenommen (2013: 77 Prozent). Hintergrundrecherchen kamen nur in 43 Prozent der Vorfälle zum Einsatz, ein Rückgang um 29 Prozent gegenüber 2013. Die dritte klassische Maßnahme der operativen Aufklärung, die Mitarbeiterbefragung, wurde in 46 Prozent der Fälle vorgenommen (2013: 56 Prozent). Zutrittsprotokoll- und Buchhaltungsdaten wertet jeweils etwa ein Drittel der Unternehmen aus. Andere Maßnahmen wie beispielsweise die Analyse von E-Mail-Konten

14 ORGANE DER OPERATIVEN AUFKLÄRUNG

Angaben in Prozent

Quelle: KPMG, 2015



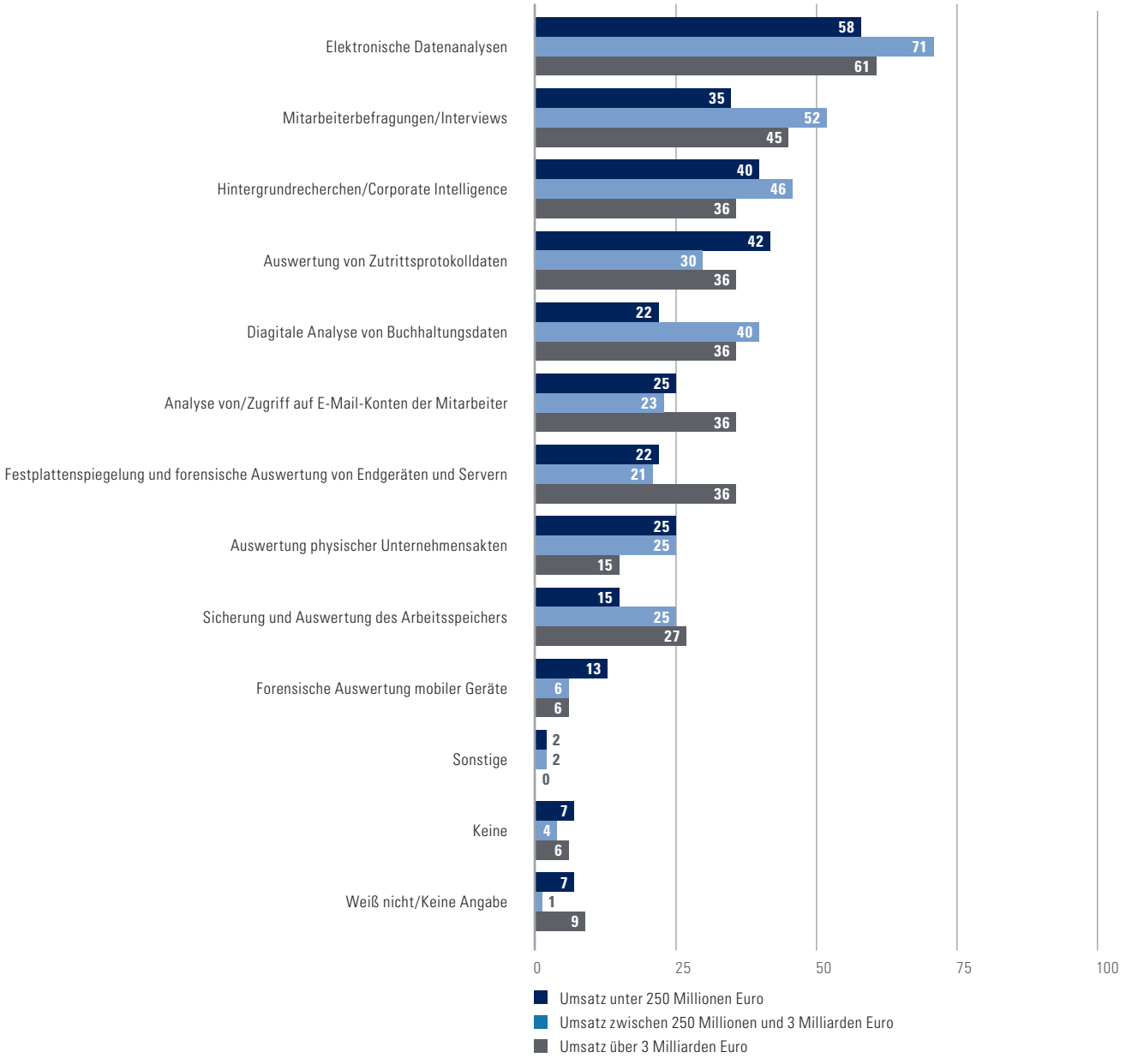
oder die Spiegelung von Festplatten führen lediglich rund 25 Prozent der Befragten durch.

Diese vergleichsweise geringen Zahlen könnten durch eine Zunahme der risikoorientierten Vorfallsklassifikation, Bestandsaufnahme und Vorfallsakzeptanz beeinflusst sein. Möglicherweise wurden bestimmte Maßnahmen bisher aber auch nicht zielführend und passend angewandt. Eine zunehmende Professionalisierung in der unternehmensinternen Aufklärung kann hier zu einer Reduktion der eingesetzten Instrumente geführt haben. Bei einem Teil der Vorfälle könnten auch bessere Kenntnisse über die Deliktstypen und mögliche Auswirkungen der Angriffe zu der nüchternen kaufmännischen Entscheidung geführt haben, keine Aufklärungsmaßnahmen in die Wege zu leiten. Das Erklärungsmodell der Überwälzung auf eine Cyberversicherung dürfte durch die übliche Selbstbeteiligung nicht greifen.

15 AUFKLÄRUNGSMASSNAHMEN

Angaben in Prozent

Quelle: KPMG, 2015



3.3 REAKTION UND SANKTIONIERUNG

3.3.1 Versäumnisse bei der Reaktion

Unternehmen zeigen sich nach wie vor selbstbewusst in Bezug auf die eigene Reaktionsfähigkeit. Keine Versäumnisse bei der Reaktion auf e-Crime sehen 75 Prozent. Auf der anderen Seite zeigt das Ergebnis aber auch: Das Selbstbewusstsein bröckelt. In der Studie des Jahres 2013 waren noch 99 Prozent der Unternehmen davon überzeugt, angemessen auf die jeweiligen Vorfälle reagiert zu haben.

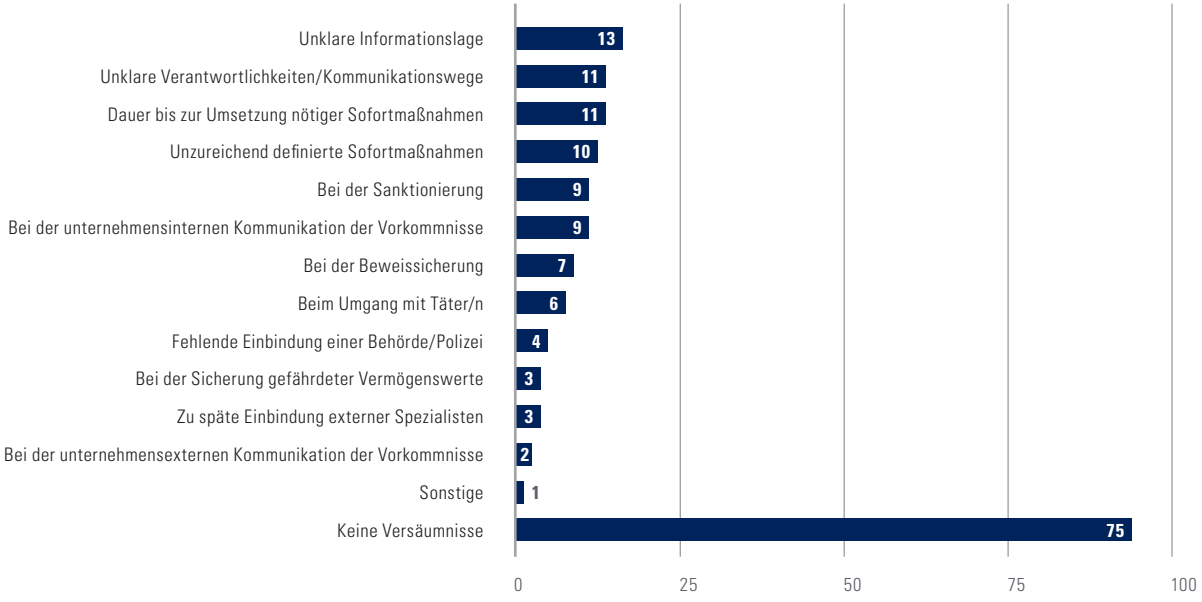
Die Erfahrungen der letzten zwei Jahre haben Schwächen in der Reaktion aufgezeigt. Der entscheidende Erfolgsfaktor wird zukünftig darin liegen, abstrakte Informationen und Ergebnisse aus unterschiedlichen Identifikations- und Aufklärungsmaßnahmen zu komprimieren und zu einer kaufmännischen Entscheidungsgrundlage zusammenzuführen. Dieses vorrangige Ziel kann insbesondere durch klare Verantwortlichkeiten und Informationswege sowie definierte Sofortmaßnahmen erreicht werden. Gerade diese Aspekte des Incident Managements werden von den Betroffenen am häufigsten als Versäumnisse bei der Reaktion festgestellt (Abbildung 16). Grundlage der Umsetzung eines verbesserten Incident Managements ist allerdings skalierbar verfügbares qualifiziertes Personal.

Auffallend ist, dass vor allem Finanzdienstleister und Industrie kaum Versäumnisse in der Phase der Reaktion erkennen. Lediglich 18 Prozent geben diese an. Sonstige Dienstleister sind in dieser Hinsicht gewissermaßen ein Gegenpol. Unter ihnen sind 44 Prozent der Ansicht, dass es in bestimmten Reaktionsbereichen Versäumnisse gab – ein großes Gefälle besteht anscheinend insbesondere bei der Sanktionierung und der Beweissicherung. Einerseits kann man dieses Eingeständnis mit Sorge betrachten, andererseits ist es erfreulich, dass Vertreter dieser Branche ihren Nachholbedarf tatsächlich erkennen und sich damit intensiv auseinandergesetzt haben. Diese Erkenntnis spiegelt sich auch in den von den sonstigen Dienstleistern geplanten Investitionen wider.

Betrachtet man die Unternehmen nach den einzelnen Umsatzklassen, zeigt sich die Tendenz, dass sowohl kleine als auch große Unternehmen vergleichsweise häufig Versäumnisse in der Reaktion einräumen (37 Pro-

16 VERSÄUMNISSE IN DER REAKTION
Angaben in Prozent

Quelle: KPMG, 2015



zent bei kleinen, 30 Prozent bei großen Unternehmen), Befragte der mittleren Umsatzkategorie hingegen sehen lediglich zu 17 Prozent Schwächen in dieser Phase.

Eine besonders große Diskrepanz besteht auch bei der Sanktionierung. Große Unternehmen erkennen hier in 21 Prozent, kleine in 13 Prozent und mittlere in 2 Prozent der Vorfälle Versäumnisse.

3.3.2 Sanktionierung

Die Verfolgung von e-Crime-Vorfällen bereitet den Unternehmen nach wie vor größte Schwierigkeiten. So geben 95 Prozent der Unternehmen an, dass Angriffe immer komplexer werden und dadurch weniger auf den Täter zurückverfolgbar sind. In diesem Zusammenhang muss man auch die von den Unternehmen zunehmend empfundene Professionalisierung und Internationalisierung der Täter beachten. Sie dürfte ihre Verfolgbarkeit einschränken.

Daher fehlt es in vielen Fällen an einer aus Abschreckungserwägungen wünschenswerten Sanktionierung, da der Täter nicht identifiziert werden konnte. Dies war bei 36 Prozent der sonstigen Dienstleister der Fall; bei Finanzdienstleistern und Handel konnte in 16 Prozent der Vorfälle kein Täter ermittelt werden. Hinsichtlich der tatsächlichen Konsequenzen ist der Sanktionierungskanon strukturell gleich geblieben (Abbildung 17). Nach wie vor stehen strafrechtliche Konsequenzen im Vordergrund (59 Prozent), zivil- und arbeitsrechtliche werden anscheinend eher als nachrangig betrachtet (28 beziehungsweise 24 Prozent).

Die umsatzstärksten Unternehmen verlassen sich weniger auf strafrechtliche Konsequenzen als die übrigen Befragten (39 Prozent). Dafür scheuen sie deutlich seltener davor zurück, arbeitsrechtliche Konsequenzen zu ergreifen.

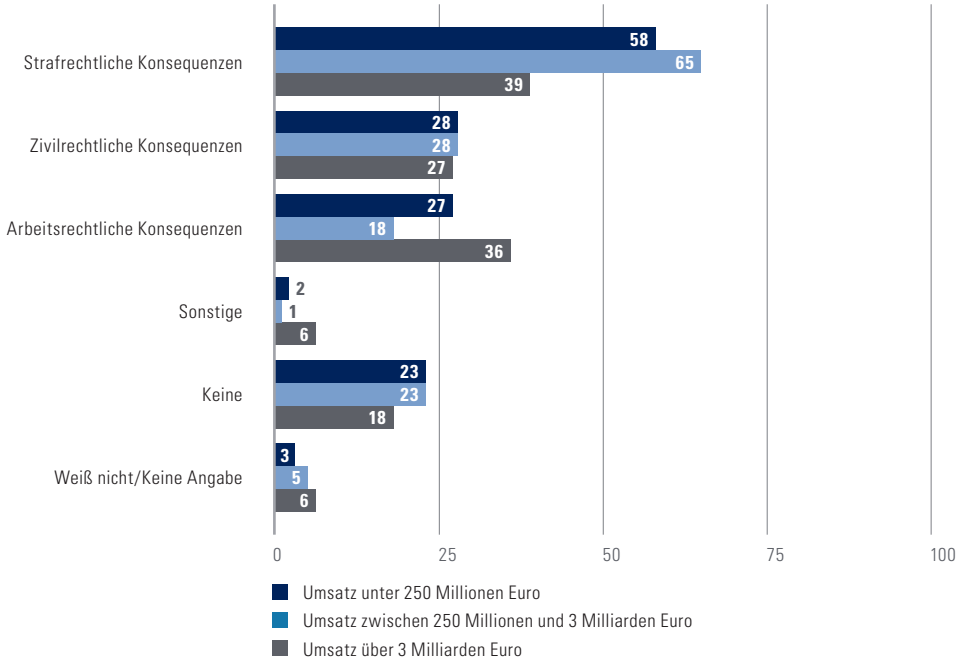
Die Handelsbranche sanktioniert am stringentesten. Lediglich 16 Prozent der Fälle blieben ohne Konsequenzen für die Täter. Tätern drohen in dieser Branche zudem neben strafrechtlicher Verfolgung (73 Prozent) auch häufiger zivilrechtliche Konsequenzen (41 Prozent).

Ein solch umfassender Sanktionierungsansatz übt eine enorm abschreckende Wirkung aus. Zukünftige Fallzahlen können gemindert werden, wenn die Täter entsprechende Strafen fürchten müssen.

17 SANKTIONIERUNG

Angaben in Prozent

Quelle: KPMG, 2015



4 BRANCHENFOKUS

2013 stand die Branche der Finanzdienstleister, darunter vor allem Kreditinstitute und Versicherungen, im besonderen Fokus von e-Crime. Daran hat sich im Wesentlichen nichts geändert. Jedoch zeigen sich in dieser Studie auffällige Unterschiede zwischen der Branche „Sonstige Dienstleister", den übrigen Branchen und insbesondere den Finanzdienstleistern. Unter dem Begriff der sonstigen Dienstleister werden unter anderem Transport- und Logistik-, Informations- und Kommunikationsdienstleister, die Erbringung von wirtschaftlichen oder technologischen Dienstleistungen sowie Dienstleistungen im Gesundheits- oder Sozialbereich und sonstige, nicht in eine der aufgezählten Kategorien fallende Dienstleistungen zusammengefasst.

Im folgenden Abschnitt werden die Ergebnisse im Einzelnen dargestellt und mögliche Interpretationen der Unterschiede präsentiert.

4.1 RISIKOPROFIL UND KOSTEN VON E-CRIME

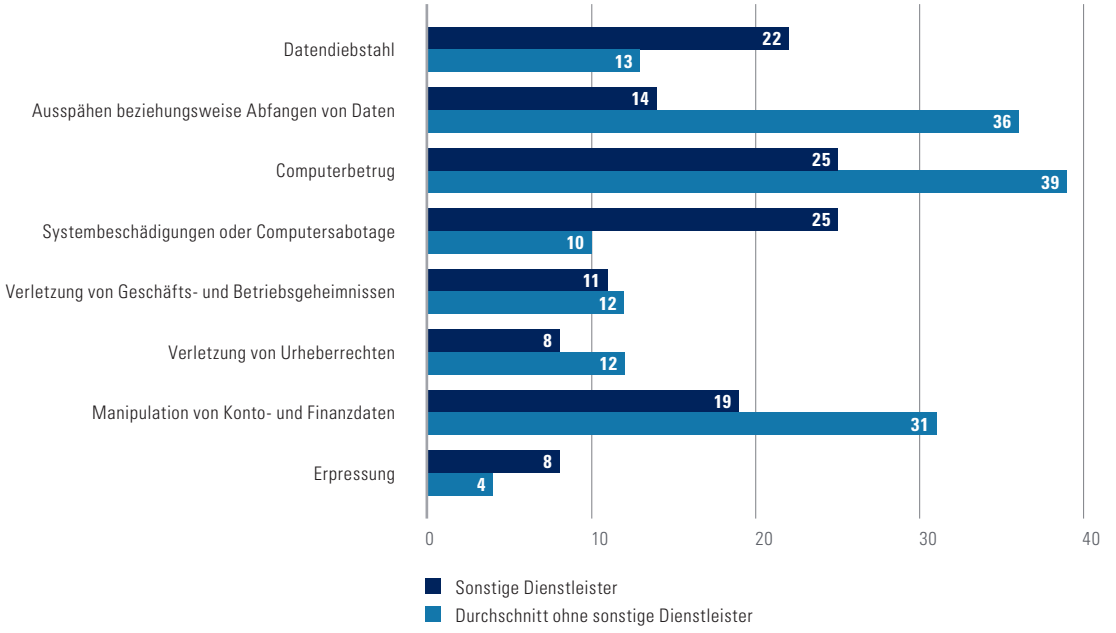
Grundsätzlich zeigt sich die Tendenz, dass die Gruppe der sonstigen Dienstleister gegenüber den restlichen Befragten einen Nachholbedarf aufweist. Dieser Kontrast zeigt sich in der Regel gegenüber den Finanzdienstleistern am deutlichsten.

Das äußert sich unter anderem in der Risikowahrnehmung. So sind die sonstigen Dienstleister das Paradebeispiel für das Phänomen der Risikoverdrängung. Unter den Befragten dieser Branche schätzen 88 Prozent das generelle Risiko, Opfer von e-Crime zu werden, als hoch beziehungsweise sehr hoch ein. Hinsichtlich des eigenen Unternehmens nehmen jedoch nur noch 33 Prozent ein solches Risiko wahr, bei Finanzdienstleistern sind es bei einer ähnlichen generellen Risikoeinschätzung 48 Prozent, beim Handel 47 Prozent.

Möglicherweise steht dieses Ergebnis im Zusammenhang mit der im Vergleich sehr geringen Betroffenheit der sonstigen Dienstleister (33 Prozent). Finanzdienstleister mussten sich wesentlich häufiger mit e-Crime auseinandersetzen (55 Prozent).

18 BRANCHENSPEZIFISCHE BETROFFENHEIT
Angaben in Prozent

Quelle: KPMG, 2015



Deutlich wird das insbesondere bei den drei meistgenannten Deliktstypen, dem Computerbetrug (bei sonstigen Dienstleistern 25 Prozent Betroffenheit), dem Ausspähen oder dem Abfangen von Daten (14 Prozent Betroffenheit) sowie der Manipulation von Konto- und Finanzdaten (19 Prozent Betroffenheit). Gegenüber den durchschnittlichen Ergebnissen der restlichen Befragten liegt der Prozentsatz der Betroffenen pro Delikt um circa 10 bis 20 Prozent niedriger (Abbildung 18).

Derartige Unterschiede werfen die Frage nach den Gründen dieser Diskrepanz auf. Dabei muss in Betracht gezogen werden, dass die sonstigen Dienstleister ihre Betroffenheit nur unzureichend erfasst und daher nicht korrekt angegeben haben und die Dunkelziffer höher liegt. Grund zu dieser Annahme besteht vor allem deshalb, weil es anhand der weiteren Fragestellungen dieser Studie offenkundig wird, dass die übrigen Branchen besser gegenüber e-Crime gewappnet sind und insbesondere in Detektion und Verfolgung der Täter bessere Ergebnisse erzielen. Diese Aussage gilt vor allem für Finanzdienstleister und mit Abstrichen auch für den Handel. Außerdem empfinden 86 Prozent der sonstigen Dienstleister, dass es zunehmend schwierig wird, e-Crime überhaupt zu entdecken.

Entgegen der sonst sehr geringen Betroffenheit fällt jedoch auch auf, dass Datendiebstahl bei sonstigen Dienstleistern wesentlich häufiger aufgetreten ist. Zudem sind Cloud-Dienste wesentlich öfter von e-Crime betroffen. Zusammen mit der mangelnden Vorbereitung ergibt sich hier eine besonders gefährliche Situation, nicht nur für unternehmenseigene, sondern auch für Kundendaten. Sie könnte als Folge der mangelnden Risikowahrnehmung gedeutet werden.

Über die gesamten Ergebnisse der Studie hinweg entsteht der Eindruck, dass sich die Vertreter der sonstigen Dienstleister bewusst sind, dass sie vergleichsweise schlecht gegenüber e-Crime geschützt sind.

So fällt die Risikowahrnehmung hinsichtlich risikobehafteter IT-Anwendungen oder Unternehmensabläufe bei dieser Branche wesentlich höher aus als bei den restlichen Befragten. Das wird dadurch untermauert, dass 86 Prozent der sonstigen Dienstleister der Ansicht sind, dass gerade neue Technologien für e-Crime ausgenutzt werden, da es für sie noch keine ausreichenden Schutzmaßnahmen gibt.

Auch die Bewertung des Risikos mobiler Datenträger illustriert diesen Mangel an Vorbereitung. Sowohl in der Frage nach IT-Anwendungen als auch der nach Unternehmensabläufen empfinden über zwei Drittel der sonstigen Dienstleister USB-Sticks, externe Festplatten oder Ähnliches als besonders risikobehaftet. Demgegenüber betrachtet deutlich weniger als die Hälfte der Finanzdienstleister diese Anwendungen mit Sorge. Die Häufigkeit, mit der diese Antwortmöglichkeit gewählt wurde, ist auch insgesamt rückläufig. Offenbar haben die übrigen Befragten, insbesondere die Finanzdienstleister, bereits Vorkehrungen getroffen, um die Anfälligkeit mobiler Datenträger zu minimieren.

Auch beim Thema „Bring your own Device“ bleiben sonstige Dienstleister zusammen mit der Industrie in der Vorbereitung hinter den restlichen Befragten zurück. So betrachten lediglich 18 Prozent der Finanzdienstleister diese Anwendung als besonders risikobehaftet, bei den sonstigen Dienstleistern sind es 42 Prozent.

Das deutet darauf hin, dass die geschäftliche (Mit-)Nutzung von privater Technik in der Branche „Sonstige Dienstleister“ nicht ausreichend geregelt ist und insofern Sicherheitsrisiken, wie beispielsweise der Verlust von oder der unrechtmäßige Zugang zu sensiblen Unternehmensdaten, bestehen. Vielfach ist es für Unternehmen nicht zu vermeiden, dass ihre Beschäftigten bei der Arbeit auch auf Privatgeräte zurückgreifen. In solchen Fällen ist es unerlässlich, ein entsprechendes Regelungskonzept zu implementieren, um Unternehmensinterna vor etwaigen Risiken zu schützen.

4.2 PRÄVENTION, DETEKTION UND REAKTION

Bei den e-Crime begünstigenden Faktoren kämpfen sonstige Dienstleister nach wie vor „an der Basis“. Unter anderem trifft man weiterhin auf unzureichend geschultes Personal, limitierte Budgets, unzureichendes Krisenmanagement und die Umgehung von Kontrollen durch das Management (Abbildung 19). Außerdem fehlen Ad-hoc-Kontrollen sowie eine firmeninterne Sanktionierung – Faktoren, die Finanzdienstleister um 40 Prozent weniger als besondere Gefahrenquelle wahrnehmen.

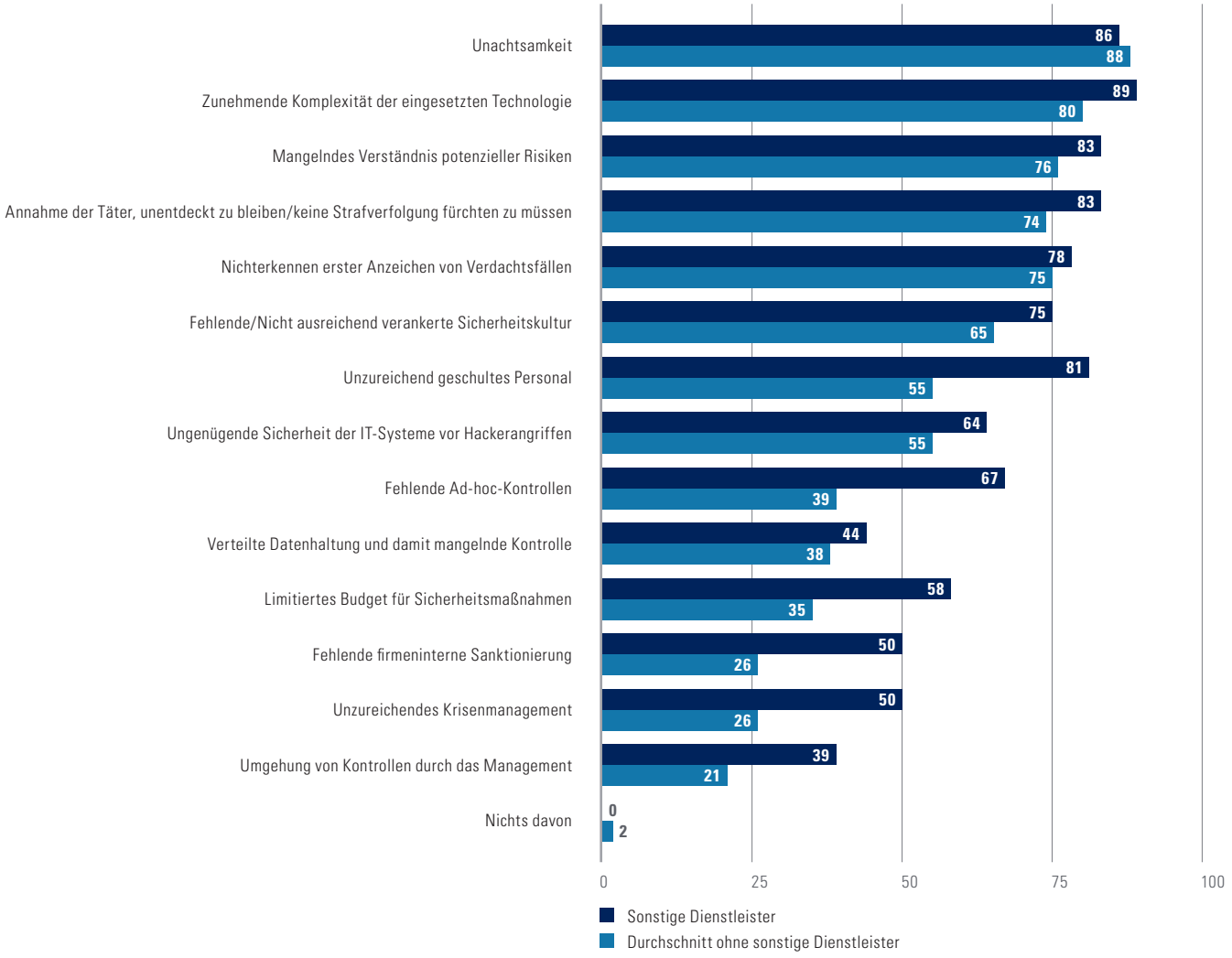
Bei den tatsächlich implementierten Präventionsmaßnahmen sind die Finanzdienstleister allen anderen Branchen voraus. Allerdings sind hier die Unterschiede zwischen den sonstigen Dienstleistern und Handel/Industrie nicht so deutlich wie bei anderen Fragestellungen.

Auffällig ist jedoch, dass weniger als zwei Drittel der sonstigen Dienstleister Monitoringmaßnahmen durchführen. Im Vergleich dazu ergreifen 90 Prozent der Finanzdienstleister sowie knapp drei Viertel der übrigen Befragten derartige Maßnahmen. Fehlendes Monitoring könnte auch zur Erklärung der geringeren Betroffenheit beitragen, da die Detektion von Delikten durch solche Maßnahmen wesentlich effektiver wird. Darüber hinaus suchen sonstige

19 E-CRIME BEGÜNSTIGENDE FAKTOREN NACH BRANCHE

Angaben in Prozent

Quelle: KPMG, 2015



Dienstleister wesentlich seltener den Austausch über aktuelle Bedrohungen mit anderen Konzernen oder Behörden. Die Kommunikation über Bedrohungslagen und mögliche Lösungsansätze wird anscheinend unterschätzt, was die Optimierung des Schutzes vor e-Crime erschwert.

Erfreulicherweise hat die Branche erkannt, dass sie Nachholbedarf hat. Obwohl sich im Branchenvergleich die geringste Betroffenheit zeigt, investieren sonstige Dienstleister aktuell mit durchschnittlich 198.000 Euro am stärksten in die Bekämpfung von e-Crime. Finanzdienstleister geben im Durchschnitt nur 83.000 Euro aus, haben allerdings auch schon ein im Vergleich besseres Schutzniveau erreicht.

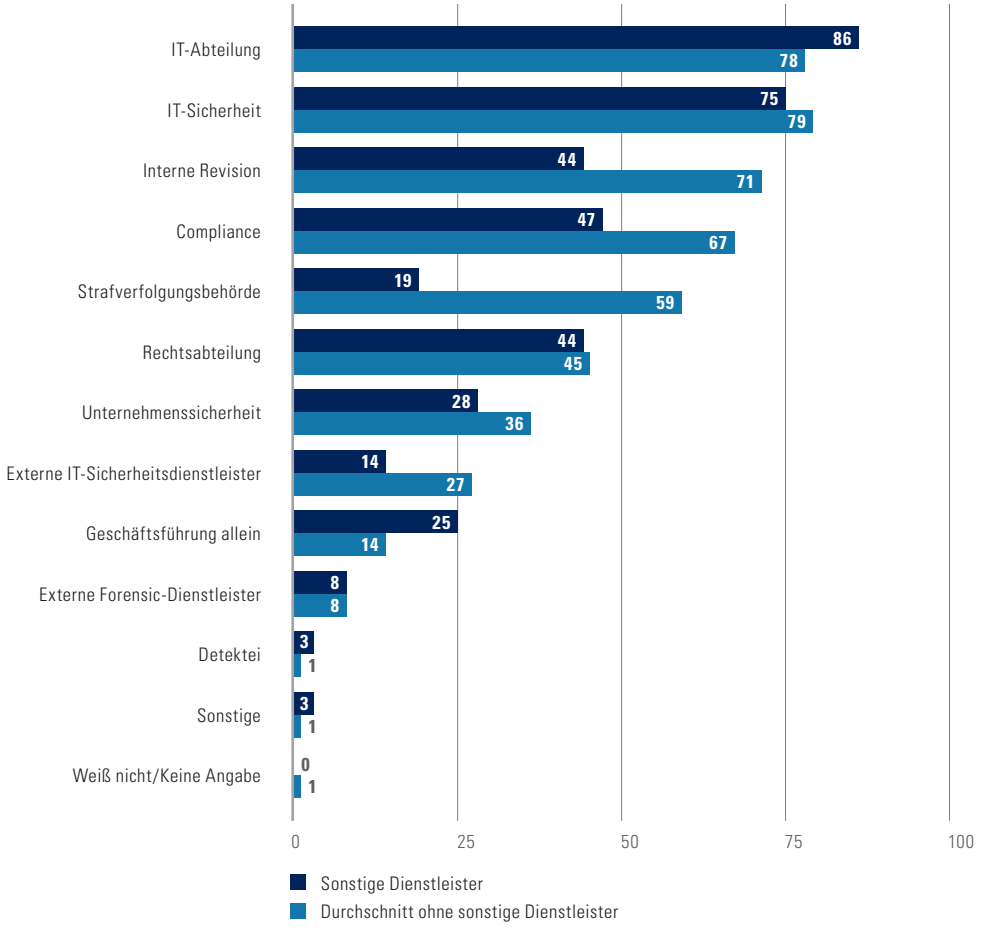
Dieser Trend wird sich entsprechend den Angaben der Befragten auch in den kommenden zwei Jahren bestätigen. Sonstige Dienstleister planen über den betrachteten Zeitraum sogar noch höhere Investitionen von durchschnittlich 271.000 Euro und damit über 100.000 Euro mehr als die übrigen Befragten.

Als problematisch dürfte sich jedoch erweisen, dass zwei Drittel der Befragten dieser Branche bei der internen und externen Rekrutierung und Weiterbildung von Personal mit Schwierigkeiten rechnen. Diese Einschätzung ist unserer Erfahrung nach zutreffend. Gerade aktuell sollte man den Kampf um qualifiziertes Personal nicht unterschätzen.

20 BRANCHESPEZIFISCHE ORGANE DER AUFKLÄRUNG

Angaben in Prozent

Quelle: KPMG, 2015



Bei Detektion und Aufklärung der Taten zeigen sich weitere Unterschiede. So wurden Angriffe auf sonstige Dienstleister wesentlich häufiger durch interne Hinweise entdeckt, sei es durch Routineprüfungen (69 Prozent) oder durch Mitarbeiter (61 Prozent). Hinweise von Unternehmensexternen führten hingegen deutlich seltener zur Aufdeckung von e-Crime.

In der operativen Aufklärung scheinen sich die immer noch begrenzten Ressourcen der sonstigen Dienstleister bemerkbar zu machen. Während die befragten Unternehmen (ohne sonstige Dienstleister) zu mindestens zwei Dritteln angaben, IT-Abteilung, IT-Sicherheit, Interne Revision sowie Compliance-Abteilung mit dieser Aufgabe zu betrauen, waren unter den sonstigen Dienstleistern nur IT-Abteilung und IT-Sicherheit zu einem vergleichbar hohen Prozentsatz involviert (Abbildung 20).

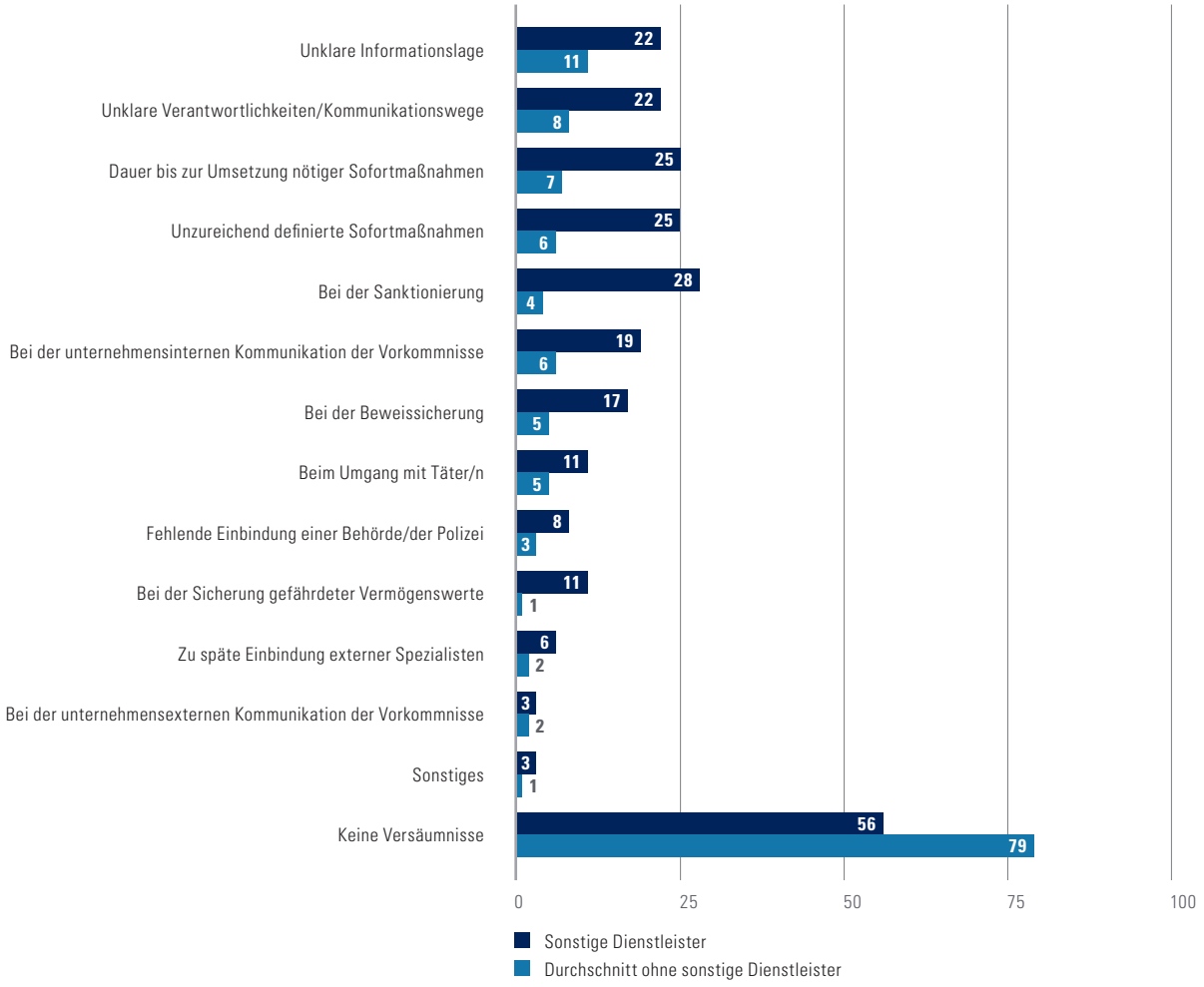
Auch der Mangel an Ressourcen bedeutet größere Schwierigkeiten bei der Verfolgung der Täter. Folglich sieht über ein Viertel der Befragten aus dieser Branche hier Versäumnisse in der Reaktion.

Bei der tatsächlichen Aufklärung greifen sonstige Dienstleister auf eine größere Bandbreite an Maßnahmen zurück. Genannt werden insbesondere technische Maßnahmen wie die Auswertung von Zutrittsprotokolldaten, die bei 44 Prozent der Vorfälle vorgenommen werden. Bei Finanzdienstleistern sind es nur 24 Prozent. Dieser Unter-

21 VERSÄUMNISSE IN DER REAKTION NACH BRANCHE

Angaben in Prozent

Quelle: KPMG, 2015



schied tritt bei Festplattenspiegelungen noch deutlicher zutage. Sonstige Dienstleister setzen dieses Instrument in 39 Prozent der Fälle und damit fast viermal häufiger als Finanzdienstleister ein (11 Prozent).

Diese Zahlen könnten darauf hindeuten, dass sonstige Dienstleister seltener eine entsprechende Vorklassifikation der Angriffe vornehmen und sie daher nicht effektiv und effizient aufklären können.

Der Nachholbedarf, den Vertreter dieser Branche beim Umgang mit e-Crime wahrnehmen, spiegelt sich vor allem in den von ihnen empfundenen Versäumnissen in der Reaktion wider. 44 Prozent geben an, dass es Schwächen in dieser Phase gegeben habe; bei Finanzdienstleistern trifft dies nur auf 18 Prozent der Befragten zu.

Es ist auffallend, dass die Versäumnisse vielfältiger Natur zu sein scheinen, insbesondere gegenüber den anderen Branchen (Abbildung 21). So wurden bei den restlichen Befragten lediglich vier Antwortmöglichkeiten zu mindestens 11 Prozent als Versäumnis wahrgenommen. Dreimal betrifft dies den Handel, der eine unklare Informationslage (16 Prozent), unklare Verantwortlichkeiten (11 Prozent) sowie die Dauer bis zur Umsetzung von Sofortmaßnahmen (11 Prozent) als Versäumnis empfunden hat. Finanzdienstleister geben in den wenigsten Fällen Versäumnisse an. So wurden sieben der 13 gegebenen Antwortmöglichkeiten von ihnen nicht genannt. Sonstige Dienstleister alleine hingegen empfanden, dass neun verschiedene Aspekte nicht korrekt umgesetzt wurden, fünf davon wurden sogar von mindestens 22 Prozent angegeben.

Schwierigkeiten zeigen sich dabei insbesondere im Incident Management. Zu nennen sind zum Beispiel die Implementierung und tatsächliche Umsetzung von Sofortmaßnahmen, die Regelung von Verantwortlichkeiten sowie die Schaffung einer klaren Informationslage. Das lässt wiederum Rückschlüsse auf fehlende Ressourcen oder auch einen Mangel an Personal beziehungsweise nicht entsprechend vorbereitetes und sensibilisiertes Personal zu. Die Investitionsbereitschaft lässt aber darauf schließen, dass die sonstigen Dienstleister aktuell versuchen, diese Schwachpunkte aufzuarbeiten.

Die fehlende Sanktionierung der Täter wird als das größte Versäumnis empfunden. Offenbar fehlt es gerade bei der Aufklärung der Vorfälle und der anschließenden Verfolgung der Täter an den notwendigen Ressourcen. In etwas mehr als einem Drittel der Fälle wurden Täter nicht sanktioniert. Mögliche Ursache hierfür könnte die fehlende Identifizierung der Täter sein, da diese immer professioneller und internationaler agieren und die sonstigen Dienstleister nicht über entsprechende Maßnahmen zur Identifikation verfügen. Im Vergleich dazu kamen die Täter bei den besser vorbereiteten Finanzdienstleistern und dem Handel lediglich in 16 Prozent der Delikte ohne Konsequenzen davon.

An diesem Punkt müssen die sonstigen Dienstleister unbedingt ansetzen. Solange die Täter sich nicht vor möglichen Konsequenzen fürchten müssen, dürfte die Branche ein attraktives Ziel für e-Crime-Delikte bleiben.

Insgesamt liegen die sonstigen Dienstleister in der Bekämpfung von e-Crime hinter den übrigen Branchen zurück. Allerdings ist das Problem in der Branche bekannt und viele Unternehmen bekunden inzwischen ihren Willen zu investieren, um die vorhandenen Schwächen zu überwinden.

5 IT-SICHERHEITSGESETZ

Das erklärte Ziel des IT-Sicherheitsgesetzes (ITSiG) ist es, Deutschlands digitale Infrastrukturen zu den sichersten weltweit zu machen. In Kürze soll es in den Bundestag eingebracht und voraussichtlich noch im Jahr 2015 verabschiedet werden.

Kernpunkte des IT-Sicherheitsgesetzes

Das ITSiG betrifft vor allem die Betreiber Kritischer Infrastrukturen (KRITIS) und indirekt ihre Dienstleister. Im Kern enthält das Gesetz zwei neue Anforderungen: KRITIS-Betreiber werden verpflichtet, Störungen ihrer Informationstechnik, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit dieser kritischen Strukturen führen oder führen können, an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Ihnen wird auferlegt, konkrete allgemeine und branchenspezifische Mindeststandards in der IT-Sicherheit umzusetzen. Zudem kann das BSI alle zwei Jahre einen geeigneten Nachweis einfordern, um die Umsetzung dieser Anforderungen zu überprüfen. Als Beispiele werden im Entwurf ein Informationssicherheits-Managementsystem (ISMS), Maßnahmen zur Prävention und Detektion, ein Inventar kritischer Assets und Business Continuity Management (BCM) genannt.

Nach Inkrafttreten soll eine konkretisierende Rechtsverordnung folgen. Die wichtigsten offenen Fragen sind:

- Wer oder was genau zählt zu den Kritischen Infrastrukturen?
- Welche Sicherheitsvorfälle sind zu melden und in welchem Detailgrad?
- Welcher zusätzliche Aufwand entsteht durch die Mindestanforderungen?

Ergebnisse der e-Crime-Studie

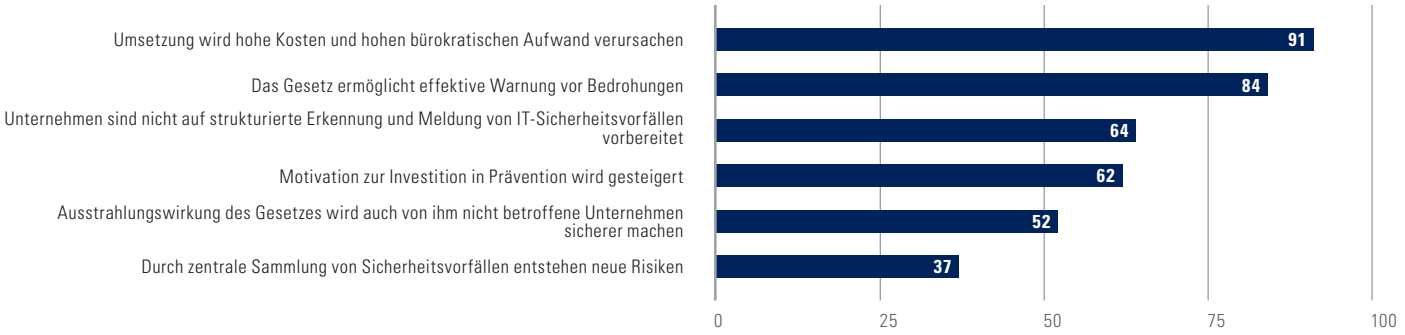
Der bereits jetzt absehbare Umfang der Anforderungen sollte deutschen Unternehmen Anlass dazu geben, sich ausführlich mit dem ITSiG zu befassen. Viele Befragte der e-Crime-Studie haben sich jedoch noch nicht tiefer gehend mit dem Thema auseinandergesetzt und offenbaren große Unsicherheiten im Hinblick auf die Auswirkungen des Gesetzes auf ihr Unternehmen. Von den Teilnehmern geben 61 Prozent an, noch nicht mit dem IT-Sicherheitsgesetz vertraut zu sein. Dabei geht die Mehrheit der Befragten, die das Gesetz bereits kennen, davon aus, dass sie davon auch betroffen sein werden.

Die Umsetzung der Anforderungen wird mit hohem bürokratischem Aufwand verbunden sein – dieser Aus-

22 ERWARTUNGEN AN DAS IT-SICHERHEITSGESETZ

Angaben in Prozent

Quelle: KPMG, 2015



sage stimmen 91 Prozent der Informierten zu. Von ihnen haben sich zum Zeitpunkt der Befragung jedoch erst 18 Prozent mit den möglichen Kosten für ihr Unternehmen auseinandergesetzt. Sie erwarten Mehrkosten von 10.000 bis 100.000 Euro. Damit droht das ITSiG, die Investitionsbudgets der Unternehmen zu vereinnahmen und zwingt sie möglicherweise zu zusätzlichen Investitionen.

Im Gegenzug für die erwarteten Kosten stellen die Gesetzeskenner hohe Erwartungen an die Wirksamkeit des ITSiG: 84 Prozent stimmen der Aussage zu, dass Unternehmen durch eine zentrale Sammlung von Angriffsmustern effektiver vor Bedrohungen gewarnt werden können. Zudem erhoffen sich 62 Prozent eine höhere Motivation der Unternehmen für Investitionen in die Prävention von e-Crime, und immerhin die Hälfte erwartet, dass das ITSiG durch seine Ausstrahlungswirkung auch nicht unmittelbar vom Gesetz betroffene Unternehmen sicherer machen wird.

Umgang mit dem ITSiG

Trotz der noch offenen konkretisierenden Rechtsverordnung sollten potenziell betroffene Unternehmen bereits jetzt ihren Vorbereitungsstand im Hinblick auf die Umsetzung der Anforderungen prüfen und bei erkennbaren Lücken Nacharbeiten vorbereiten. Leitfragen der Vorbereitung sind:

- Welche Anlagen, Einrichtungen oder Teile davon sind im Unternehmen kritisch und damit potenziell vom Gesetz betroffen?
- Sind die bestehenden Meldewege bei Vorfällen und die bisher erfassten Informationen ausreichend?
- Welche Herausforderungen entstehen bei einer multinationalen Aufstellung des Unternehmens und gegebenenfalls international unterschiedlichen Anforderungen an die IT-Sicherheit?
- Entsprechen die Sicherheitsstandards im Unternehmen dem im Gesetz skizzierten Sollzustand oder kann er andernfalls innerhalb von zwei Jahren erreicht werden?

Diese Fragen sollten bereits jetzt bearbeitet werden. Denn mit dem IT-Sicherheitsgesetz wird zukünftig von den Betreibern Kritischer Infrastrukturen mehr Aktivität in der IT-Sicherheit gefordert.

Bei der Ausgestaltung der Details besteht die Möglichkeit einer kooperativen Zusammenarbeit mit dem Gesetzgeber. Den entsprechenden Arbeitskreisen wird im Entwurf – beispielsweise bei der Festlegung der branchenspezifischen Mindeststandards – ein hoher Stellenwert zuteil. Neben unterstützenden Tätigkeiten erhält insbesondere das BSI durch das ITSiG eine Informationsfülle und Handlungsmacht, die international ihresgleichen sucht. Mit dem geplanten Ressourcenaufbau steigen die Überwachungs- und Prüfmöglichkeiten und somit auch der Druck auf die Unternehmen, die Vorgaben zeitnah umzusetzen.

FINANZDIENSTLEISTER SIND BESSER INFORMIERT

Die Unternehmen der Finanzbranche ragen unter den Befragten als bisher am besten informierte Teilnehmer heraus und gehen damit mit gutem Beispiel voran. Nur 39 Prozent der Unternehmen der Branche sind noch nicht mit dem ITSiG vertraut und nur 45 Prozent der Informierten trauen sich noch keine Kostenschätzung zu. Das ist deutlich weniger als in den Bereichen Industrie, Handel und andere Dienstleister, in denen sich teils mehr als zwei Drittel der Befragten noch nicht mit dem Gesetz auseinandergesetzt haben. Ein Grund für diesen Unterschied liegt wahrscheinlich darin, dass unter den Finanzdienstleistern bereits fast die Hälfte der Befragten davon ausgeht, die Anforderungen des Gesetzes auch umsetzen zu müssen. Erstaunlicherweise tut dies der Akzeptanz des ITSiG aber keinen Abbruch: Im Vergleich mit den anderen Branchen werden die Potenziale des Gesetzes deutlich positiver bewertet.

Wilhelm Dolle
Partner, Security Consulting
+49 30 2068-2323
wdolle@kpmg.com

6 ÜBER DIESE STUDIE

In der diesjährigen Studie wurden 505 repräsentativ nach Branche und Umsatz ausgewählte Unternehmen zu ihren Erfahrungen im Feld der Computerkriminalität befragt (Abbildung 23).

Wie in den vorherigen e-Crime-Studien zur Computerkriminalität in Deutschland wurde das Sozialforschungsinstitut TNS Emnid in Bielefeld mit der Durchführung der Interviews beauftragt. Die Interviews wurden telefonisch von im Vorfeld speziell von TNS Emnid geschulten Mitarbeitern durchgeführt. Die Antworten sowie die konkreten Gesprächspartner wurden KPMG nicht bekannt gemacht. Wir haben in der aktuellen Umfrage bewusst darauf verzichtet, gezielt IT-Abteilungen anzusprechen. Grund hierfür war, dass wir das Thema e-Crime stärker aus strategischer und betriebswirtschaftlicher Perspektive heraus analysieren wollten. Die Gesprächspartner waren in erster Linie Leiter der Internen Revision, Leiter des Rechnungswesens oder auch Leiter der Rechtsabteilung (Abbildung 24).

Die Erfahrung hat gezeigt, dass die Teilnehmer der Studie aufgrund der Komplexität des Themas eine persönliche Befragung bevorzugen. Die Interviews wurden im November/Dezember 2014 durchgeführt.

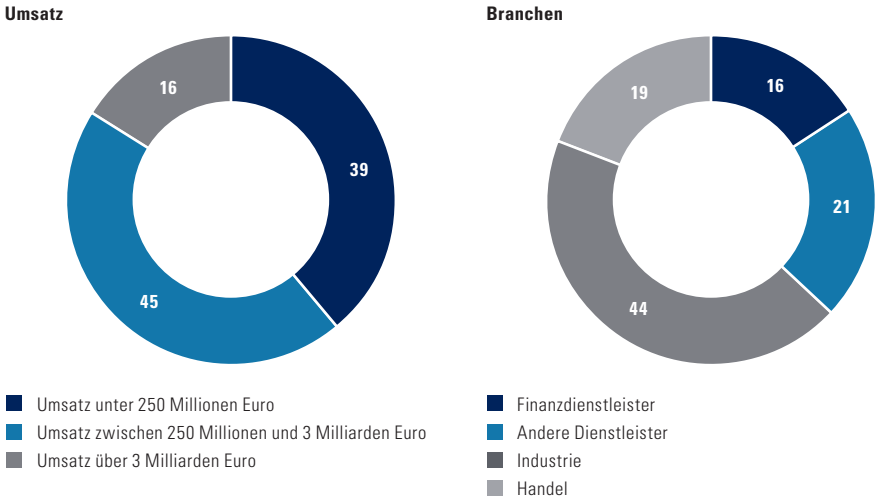
Der standardisierte Fragebogen orientiert sich an der Struktur der Vorgängerstudie, wobei mit Bezug auf die diesjährigen Schwerpunkte Anpassungen vorgenommen wurden.

Der Fragebogen wurde durch den Bereich Forensic der KPMG AG Wirtschaftsprüfungsgesellschaft konzipiert.

23 STUDIENTEILNEHMER NACH UMSATZ UND BRANCHE

Angaben in Prozent

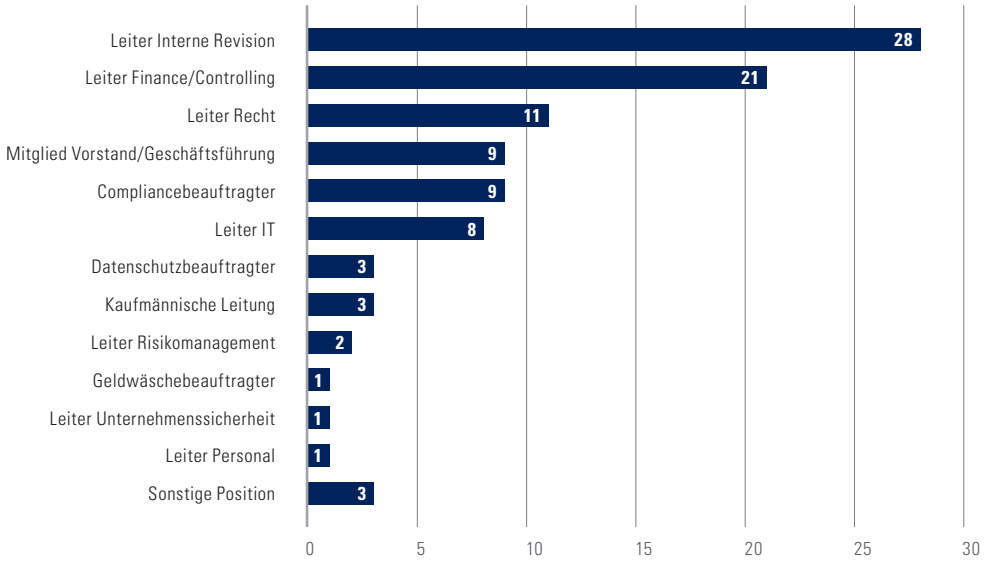
Quelle: KPMG, 2015



24 POSITION DER ANSPRECHPARTNER

Angaben in Prozent

Quelle: KPMG, 2015



ÜBER KPMG FORENSIC

Der Bereich Forensic von KPMG erbringt Leistungen rund um die Prävention, Aufdeckung und Aufklärung von Wirtschaftskriminalität und anderen Bedrohungslagen. Unser Servicespektrum umfasst die folgenden Dienstleistungen:

FORENSIC INVESTIGATIONS

Bei Verdacht auf wirtschaftskriminelle Sachverhalte führen unsere Experten unabhängige unternehmensinterne Untersuchungen auf Basis erprobter Methoden und umfangreicher Kenntnis von Fraud-Mustern durch. Dabei geben wir Hilfestellung bei der Täterermittlung, der Schadensbezifferung, der Feststellung von Verantwortlichkeiten sowie beim Umgang mit Aufsichts- und Strafverfolgungsbehörden. Anhand der Untersuchungsergebnisse erstellen wir eine beweiskräftige Dokumentation für gerichtliche wie außergerichtliche Auseinandersetzungen. Zudem unterstützen wir die rechtlichen Berater unserer Mandanten bei der Aufklärung von Einzelsachverhalten.

FORENSIC TECHNOLOGY

Wir unterstützen bei der Erstreaktion und -beurteilung, der Eindämmung, der Beweissicherung, der Analyse sowie der gerichtsfesten Aufbereitung (inklusive der Wiederherstellung nicht mehr ansprechbarer Daten) von informations- beziehungsweise datenbezogenen Sicherheitsvorfällen.

Des Weiteren geben wir Hilfestellung bei der Optimierung des Zusammenspiels technologischer, organisatorischer und datenschutzrechtlicher Herausforderungen im Zusammenhang mit Cyber Security-Vorfällen und bei der Beweisführung anhand großer Datenmengen.

Zur Entdeckung von Schwachstellen in Kontrollsystemen sowie zur Aufdeckung von unternehmensschädigenden Handlungen nehmen wir die Analyse umfangreicher Unternehmensdaten vor.

FORENSIC DUE DILIGENCE

Im Rahmen von Transaktionen unterstützen unsere Spezialisten bei der Identifizierung von Fraud-Risiken, Compliance-Schwachstellen und der Aufarbeitung konkreter Vorfälle beim Kaufobjekt. Dabei werden wir sowohl auf Käufer- als auch auf Verkäuferseite tätig.

Auf Basis der Erkenntnisse aus Forensic Due Diligence sowie der gezielten Analyse des vorhandenen Compliance-Systems leisten wir zudem Unterstützung bei der Umgestaltung von Compliance-Mechanismen und der Entwicklung konkreter Maßnahmen- und Reaktionspläne.

DATENSCHUTZ

Wir unterstützen bei der Aufklärung von und der Reaktion auf Datenschutzverstöße und Datenabflüsse und beraten bei der Einrichtung und Optimierung der Datenschutzorganisation. Dazu zählen unter anderem Status-Checks zur Erstanalyse des Datenschutz-Managementsystems, Datenklassifizierungsprojekte, aber auch die Erstellung von Verfahrensverzeichnissen, geeigneten Lösch- und Sperrkonzepten sowie die Gestaltung von Datenverarbeitungen über Unternehmens- und Landesgrenzen hinweg.

Außerdem geben wir Hilfestellung bei der datenschutzkonformen Implementierung von Monitoringmaßnahmen.

FRAUD RISK MANAGEMENT

Unsere Spezialisten unterstützen bei der Implementierung von Maßnahmen zur Prävention, Aufdeckung und angemessenen Adressierung von Wirtschaftskriminalität. Dabei nehmen wir eine strukturierte Erfassung und Bewertung von Fraud-Risiken zur Entwicklung individueller Maßnahmen vor. Außerdem begleiten wir bei der Analyse und Optimierung unternehmensinterner Richtlinien, Prozesse und Kontrollen zur Vermeidung und Aufdeckung von Fehlverhalten. Zur Sensibilisierung der Mitarbeiter der Mandanten und Führungskräfte bieten wir auf das jeweilige Unternehmen zugeschnittene Schulungen und Fortbildungsmaßnahmen an.

CORPORATE INTELLIGENCE

Um Integritätsrisiken frühzeitig erkennen zu können, führen unsere Experten Integrity Due Diligences (IDD) mittels Bereitstellung von Hintergrundinformationen durch und unterstützen bei der datenschutzkonformen Einrichtung risikoorientierter IDD-Prozesse und -Systeme. Im Hinblick auf den ungewollten Abfluss von Vermögenswerten unterstützen wir mit Asset Tracing Services, um die Rückgewinnung zu ermöglichen und zu erleichtern.

FORENSIC DATA CENTER

Um Unternehmen oder Behörden bestmöglich unterstützen und Untersuchungshandlungen unabhängig durchführen zu können, betreibt Forensic Technology ein hochgesichertes Forensic Data Center (FDC). Hier ermöglichen über 50 Server mit skalierbarem Speicherplatz die passgenaue Bereitstellung von E-Rooms und den weltweiten, sicheren Zugriff unter Wahrung datenschutzrechtlicher Anforderungen. Das Forensic Data Center ist ISO 27001-informationssicherheitszertifiziert.

Durch den übergreifenden Ansatz werden Unternehmensrisiken jeglicher Art erfasst, gemeinsam mit den Mandanten bewertet und entsprechend nachverfolgt.

Mit über 80 forensischen Spezialisten an den Standorten Berlin, Frankfurt am Main, Hamburg, Köln und München steht KPMG seinen Mandanten bundesweit zur Verfügung.

KONTAKT

KPMG AG
Wirtschaftsprüfungsgesellschaft
Klingelhöferstraße 18
10785 Berlin

Alexander Geschonneck
Leiter Forensic
T +49 30 2068-1520
ageschonneck@kpmg.com

www.kpmg.de/forensic

An dieser Studie haben mitgewirkt:
Thomas Fritzsche
Dr. Klara Weiand
Marc Oliver Scheben

Follow us!
www.kpmg.de/twitter_forensic