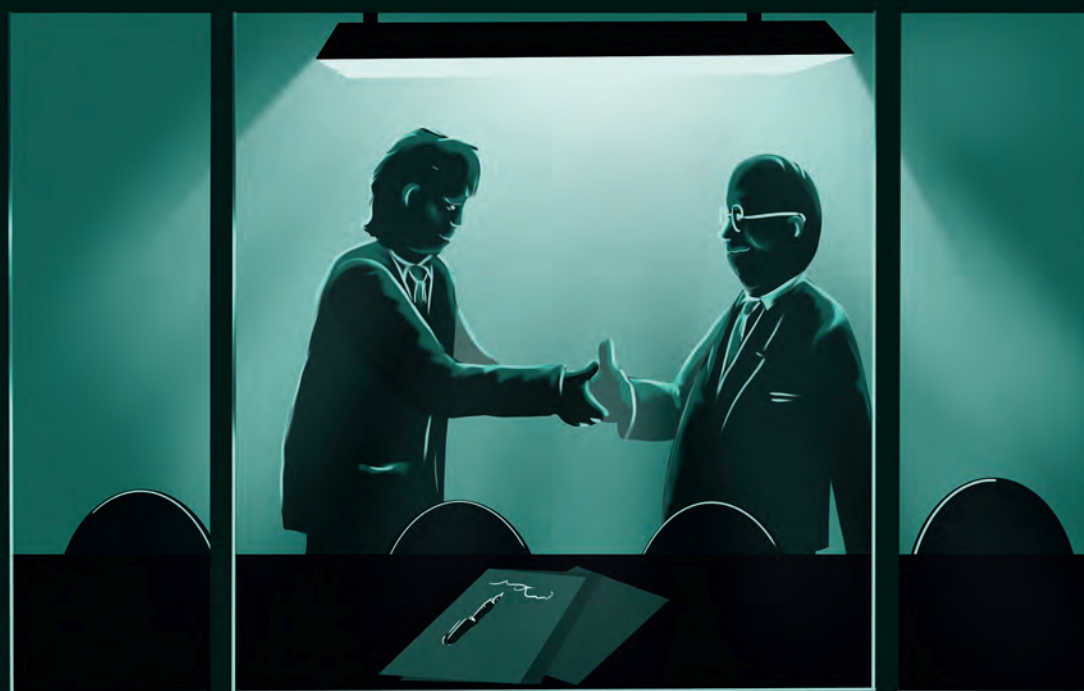


Studie

FORENSIC

Wirtschaftskriminalität in Deutschland 2014



Inhalt

Vorwort	3
Geleitwort	5
Executive Summary	6
1 Risikowahrnehmung entspricht nicht tatsächlicher Betroffenheit	9
2 Prävention – nach wie vor unterschätzt?	18
3 Menschliche Faktoren begünstigen wirtschaftskriminelle Handlungen	28
4 Wirtschaftskriminalität in einzelnen Sektoren – eine branchenspezifische Betrachtung	32
Über diese Studie	37
Über uns	38

Vorwort

Vor 15 Jahren erschien die erste Ausgabe unserer Studie zur Wirtschaftskriminalität in Deutschland. Dies ist Anlass für ein wenig Stolz, denn es gibt kaum Unternehmen, die sich über einen vergleichbar langen Zeitraum systematisch mit dem Thema Wirtschaftskriminalität in Deutschland beschäftigt haben. Wir konnten in dieser Zeit viele Trends einbeziehen, die für die deutsche Compliance-Landschaft prägend waren. Die lange Beobachtungsphase ermöglicht es uns, auch Antwortmuster zu erkennen.

Nehmen wir das Beispiel der Kartellrisiken: Wir sehen hier derzeit, dass die Unternehmen zurückhaltend in die Prävention investieren und kein hohes Risiko bei sich sehen. Wir hatten ein ähnliches Bild in der Zeit vor großen Korruptionsdelikten. Wir hoffen dennoch, dass die Unternehmen daraus Lehren ziehen konnten.

Ein weiterer interessanter, aber kaum überraschender Punkt ist: Die Bereitschaft, Geld auszugeben, ist in der Krise nach wirtschaftskriminellen Handlungen am größten. Sollen wir dieses allzu menschliche Vorgehen wirklich akzeptieren? Ich denke, nein!

Vielmehr möchten wir verdeutlichen, dass ein derartiges Vorgehen den Grundsätzen des ökonomischen Prinzips widerspricht. Bei einem Vergleich der Eintrittswahrscheinlichkeit einer wirtschaftskriminellen Handlung mit dem daraus entstehenden Gesamtschaden dürften die Auswirkungen letzten Endes für betroffene Unternehmen schwer abzuschätzen, aber immens sein. Darüber hinaus gilt es, die Schwächung der Marktposition des betroffenen Unternehmens durch mögliche Reputationsschäden zu berücksichtigen. Demgegenüber stehen vergleichsweise geringe Ausgaben in präventive Maßnahmen. Mit der Implementierung effektiver präventiver Maßnahmen können jedoch sowohl Eintrittswahrscheinlichkeit als auch Schäden deutlich reduziert werden. Folglich sind höhere Ausgaben in Prävention ein Muss im Sinne des ökonomischen Prinzips, da der Vorteil der verminderten Gesamtschäden gegenüber den (im Vergleich geringen) Implementierungs- und Instandhaltungskosten einzelner Präventionsmaßnahmen überwiegt.

Wir hoffen, erneut veranschaulichen zu können, dass die für Compliance verantwortlichen Stellen in Unternehmen bei ihrer Tätigkeit jede Unterstützung benötigen. Dies betrifft nicht nur die Reaktion und Detektion, sondern insbesondere die Prävention, damit so selten wie möglich ein Vorfall eintritt.

Was wir feststellen können: Das Thema Wirtschaftskriminalität steht im täglichen Fokus der Geschäftsführung und Vorstände. Dass es dort in angemessener Weise bleibt und nicht aus den Augen verloren wird, ist das Anliegen dieser Studie.



Alexander Geschonneck

Partner, Leiter Forensic,
KPMG in Deutschland



Geleitwort

Die deutsche Wirtschaft kann nur dort erfolgreich sein, wo sie sicher vor Bedrohungen und Angriffen Dritter ist. Sicherheitsrisiken werden im Kontext von Globalisierung und technischem Fortschritt zunehmend komplexer und vielschichtiger. Der Schutz zentraler Unternehmenswerte in Form von Mitarbeitern, Know-how, Vermögen und Eigentum ist daher für jedes Unternehmen unabdingbar – vom international aufgestellten Konzern bis hin zum kleinen und mittelständischen Zulieferer.

Wirtschaftskriminalität ist eines dieser steigenden Sicherheitsrisiken. Durch die Begrifflichkeit entsteht leicht der falsche Eindruck, dass es sich hier ausschließlich um kriminelle Handlungen der Wirtschaft selbst handele. Tatsächlich sind jedoch die Unternehmen im Regelfall die Opfer: So entstehen der deutschen Wirtschaft jedes Jahr Schäden in Milliardenhöhe durch Wettbewerbsverstöße und strafbare Handlungen wie Betrug, Veruntreuung, Unterschlagung, Erpressung, Korruption, Spionage oder Produktpiraterie. Die Täter und Tätergruppen sind dabei ebenso vielfältig wie ihre Motive. Sie bedienen sich dabei eines weiten, oftmals kombinierten Spektrums an Vorgehensweisen – von der Cyberattacke über den elektronischen Angriff bis hin zum Innentäter.

Der Schutz vor Wirtschaftskriminalität ist seit jeher die primäre Verantwortung der Wirtschaft selbst. Dies geschieht im besten Fall präventiv. Allerdings ist es aufgrund der Vielzahl und Komplexität möglicher Szenarien unmöglich, eine 100-prozentige Sicherheit zu erreichen. Vor diesem Hintergrund wird die Fähigkeit immer entscheidender, im Ernstfall möglichst frühzeitig Vorfälle zu erkennen und Schäden zu begrenzen. Unternehmensprozesse sind so zu gestalten, dass sie die Balance zwischen notwendiger Sicherheit und praxisgerechter Beherrschbarkeit erhalten. In Bürokratismus und übermäßigen Kontrollen zu erstarren, hieße den wirtschaftlichen Erfolg zu gefährden. Das gilt auch für den rechtlichen Rahmen bei der Bekämpfung von Wirtschaftskriminalität. Wir benötigen keine zusätzlichen Regularien wie etwa ein gesondertes Unternehmensstrafrecht – sie bieten gegenüber bestehenden Vorschriften keinen Mehrwert. Vielmehr müssen bestehende Gesetze konsequenter angewendet und durchgesetzt werden.

Global Player und größere Mittelstandsunternehmen verfügen über professionelle Sicherheitsabteilungen. Diese bilden mit ihrem Know-how und ihren Netzwerken den Grundpfeiler für die Sicherheit in der deutschen Wirtschaft. Handlungsbedarf besteht jedoch bei kleinen und mittelständischen Unternehmen (KMU). Diese sind für einen erfolgreichen Eigenschutz auf die Unterstützung von Experten angewiesen. Staat und Wirtschaft sind hier gemeinsam gefordert, geeignete Angebote weiterzuentwickeln und kohärent umzusetzen. Zu diesem Zweck haben die deutsche Wirtschaft und die Bundesregierung im August 2013 vereinbart, erstmals ein ganzheitliches Schutzkonzept – eine nationale Wirtschaftsschutzstrategie – bis Ende 2015 zu erarbeiten.

Die vorliegende Studie „Wirtschaftskriminalität in Deutschland 2014“ bietet allen Interessierten die Möglichkeit, sich einen Überblick zur aktuellen Entwicklung der Wirtschaftskriminalität in Deutschland zu verschaffen – ein Überblick, der für eine sachgerechte Diskussion über geeignete Schutz- und Bekämpfungsmaßnahmen erforderlich ist.



Dr. Markus Kerber
BDI-Hauptgeschäftsführer

Markus Kerber ist seit 2011 Hauptgeschäftsführer und Mitglied des Präsidiums des Bundesverbands der Deutschen Industrie e. V. (BDI). Der studierte Wirtschafts- und promovierte Sozialwissenschaftler startete seine Karriere bei S. G. Warburg und der Deutschen Bank in London. Anschließend wurde er Finanzvorstand bei GFT Technologies AG. 2006 wechselte er in die Politik: zuerst als Abteilungsleiter im Bundesinnenministerium und ab 2009 im Bundesfinanzministerium.

Executive Summary

1

Die Risikowahrnehmung datenbezogener Delikte ist deutlich höher als die anderer Deliktsarten; die Dunkelziffer liegt möglicherweise höher als gedacht.

Das Risiko aktuell **im Fokus der Medien** stehender Deliktsarten wie Datendiebstahl/Datenmissbrauch wird als wesentlich höher empfunden als jenes anderer Delikte, die deutlich häufiger auftreten.

87 Prozent der Befragten stufen das **Risiko** an sich als hoch bzw. sehr hoch ein. Daher ist davon auszugehen, dass die Dunkelziffer hoch ist und **die tatsächliche Betroffenheit höher** ausfällt als von den Befragten angegeben.

Dies ist gegebenenfalls darin begründet, dass die Unternehmen **keinen ausreichenden Überblick** und **nicht genügend Kontrolle** über die betroffene Technik haben und so datenbezogene Vorfälle gar nicht entdecken können.

2

Gefühlte Sicherheit trotz objektiv fehlender Prävention

85 Prozent der befragten Unternehmen schätzen ihren **Schutz** vor wirtschaftskriminellen Handlungen als gut bzw. sehr gut ein, obwohl **jedes dritte Unternehmen** in den vergangenen zwei Jahren von Wirtschaftskriminalität **betroffen** war.

Dennoch sind **kaum Unterschiede in der Betroffenheit** zwischen den Unternehmen, die ihren Schutz als gut oder sehr gut beurteilen (zu **34 Prozent** betroffen), und den Unternehmen, die diesen als schlecht bzw. sehr schlecht einstufen (zu **38 Prozent** betroffen), zu erkennen.

Offenbar ergreifen die befragten Unternehmen **keine angemessenen Präventionsmaßnahmen**, sondern sind mit ihren bestehenden Maßnahmen zufrieden. Doch der vermeintliche Schutz besteht de facto nicht.

3

Unternehmen schätzen für den Fall kartellrechtlicher Ermittlungen ihre Reaktionsmöglichkeiten als gut ein; die Ermittlungs- und Folgekosten sind trotzdem erheblich.

86 Prozent der Unternehmen geben an, im Falle kartellrechtlicher Ermittlungen durch Aufsichtsbehörden einen umfassenden bzw. weitreichenden **Überblick** über die kartellrelevanten Daten, Dokumente und die Kommunikation zu haben, die für die Aufarbeitung des Sachverhalts relevant sind.

Rund **73 Prozent** der von Kartellrechtsverstößen betroffenen Unternehmen geben an, einen Gesamtschaden¹ von **einer Million Euro oder mehr** erlitten zu haben. Bei **50 Prozent** dieser Unternehmen machen die Ermittlungs- und Folgekosten davon **500.000 Euro oder mehr** aus. Dies sind im Vergleich aller Deliktsarten die **höchsten** Angaben zu Ermittlungs- und Folgekosten.

Die beachtlichen **von Kartellrechtsverstößen verursachten Schäden** belegen, dass Unternehmen sich nicht angemessen gewappnet haben, obwohl die meisten das von sich behaupten. Dies wirft erneut die Frage auf, warum die Befragten nicht in geeignete Präventionsmaßnahmen investieren.

¹ Der Gesamtschaden besteht aus den Ermittlungs- und Folgekosten zuzüglich Bußgeldern, Geldstrafen und eventuellen Gewinnabschöpfungen.

4

Die befragten Unternehmen missachten mit ihrer geringen Investitionsbereitschaft in Prävention das ökonomische Prinzip.

Lediglich **11 Prozent** der Befragten sind bereit, im Rahmen der Prävention 50.000 Euro oder mehr für **externe Unterstützung** auszugeben.

Je dringlicher die Situation, desto höher ist die **Investitionsbereitschaft** der Unternehmen in den Phasen der Detektion und Reaktion.

Offenbar lassen die befragten Unternehmen hier das **ökonomische Prinzip** außer Acht. Mit vergleichsweise geringen Ausgaben für das Implementieren und Aufrechterhalten präventiver Maßnahmen kann für eine deutliche Senkung des Schadenspotenzials im Falle einer wirtschaftskriminellen Handlung gesorgt werden. Die vermiedenen Kosten dürften die Kosten präventiver Maßnahmen mehr als kompensieren.

Prävention ist nicht nur Selbstzweck, sondern für ein gesundes Wirtschaften unabdingbar.

5

Menschliche Faktoren begünstigen wirtschaftskriminelle Handlungen; trotzdem wird wenig getan, um menschlichem Fehlverhalten entgegenzuwirken.

63 Prozent der Befragten sehen die Ursache für wirtschaftskriminelle Handlungen ausschließlich bzw. eher in **menschlichen Faktoren** (wie zum Beispiel finanzielle Motivation oder Rechtfertigungsmöglichkeiten) als in technischen Fähigkeiten oder mangelnden Kontrollen.

Dem „Tone at the Top“ wird lediglich geringe Bedeutung eingeräumt. Mehr als **80 Prozent** der Befragten halten fehlende **Vorbilder in der Geschäftsführung** für wenig relevant.

Ein offensichtlicher Widerspruch: Einerseits werden menschliche Faktoren als Hauptursache wirtschaftskriminellen Handelns ausgemacht, andererseits misst man dem „Tone at the Top“ kaum Bedeutung bei. Doch ist es unerlässlich, dass in der Geschäftsführung **gesetzeskonformes Verhalten vorgelebt** wird. Nur so können auch die Mitarbeiter in die Verantwortung genommen werden.

Lediglich ein Viertel der Befragten stuft einen **Mangel an Schulungen** als Faktor mit hoher bzw. sehr hoher Bedeutung ein, der wirtschaftskriminelle Handlungen begünstigt. Entsprechend führen über **40 Prozent** der Befragten keine Schulungen zur Vermeidung von Wirtschaftskriminalität durch.

Auch dies ist ein Widerspruch. **Schulungen** leisten einen wertvollen Beitrag zur Verhinderung wirtschaftskrimineller Handlungen durch Sensibilisierung und gesteigerte Aufmerksamkeit. Das Schadenspotenzial wird damit verringert, was die für die Durchführung von Trainings getätigten Ausgaben rechtfertigt. Schulungen sind in der heutigen Wirtschaft **als unabdingbar zu betrachten**.



1 Risikowahrnehmung entspricht nicht tatsächlicher Betroffenheit

Eine optimistische und gegebenenfalls medienorientierte Risikowahrnehmung der Unternehmen verstärkt die Gefahr wirtschaftskrimineller Handlungen.

Übergreifende Risikoeinschätzung versus Betroffenheit

Knapp 70 Prozent der 400 befragten Unternehmen² stufen das Risiko des eigenen Unternehmens, von wirtschaftskriminellen Handlungen betroffen zu sein, als gering ein. Dies steht in offensichtlichem Widerspruch zu der Einschätzung, dass 82 Prozent der befragten Unternehmen für andere Unternehmen in Deutschland ein hohes bzw. sehr hohes Risiko sehen, von Wirtschaftskriminalität betroffen zu sein. Vorangegangene KPMG-Studien bestätigen dieses Umfrageergebnis.

Je nach Umsatzstärke zeigen sich bei der Risikowahrnehmung beträchtliche Unterschiede (Abbildung 01, Seite 10). In Übereinstimmung mit den Ergebnissen von 2012 sehen sich kleinere Unternehmen einem deutlich geringeren Risiko ausgesetzt, selbst Opfer einer wirtschaftskriminellen Handlung zu werden. Dementsprechend geben lediglich 23 Prozent der Unternehmen mit einem Umsatz von unter 250 Millionen Euro an, dass für sie selbst ein hohes bzw. sehr hohes Risiko bestehe, von einer wirtschaftskriminellen Handlung betroffen zu sein. 35 Prozent der Befragten mit einem Umsatz zwischen 250 Millionen bis 3 Milliarden Euro sehen ein solches Risiko für sich selbst. Bei Unternehmen mit einem Umsatz von mehr als 3 Milliarden nehmen 40 Prozent der Befragten dieser Gruppe diese Einschätzung vor.

Im Folgenden werden die befragten Unternehmen zur Vereinfachung in die Kategorien „groß“, „mittel“ und „klein“ eingeteilt. Unternehmen mit einem Umsatz von mehr als 3 Milliarden Euro oder mit mehr als 500 Mitarbeitern werden als „groß“ bezeichnet. In der Kategorie „mittel“ finden sich die Unternehmen mit einem Umsatz zwischen 250 Millionen und 3 Milliarden Euro oder mit 101 bis 500 Mitarbeitern. Unternehmen mit einem Umsatz von unter 250 Millionen Euro oder bis zu 100 Beschäftigten werden der Kategorie „klein“ zugeordnet.

Es entsteht daher der Eindruck, dass sich große Unternehmen als lukratives oder häufiges Ziel von Wirtschaftskriminalität sehen. Dies liegt möglicherweise an der Unternehmensgröße und den damit einhergehenden Risiken durch komplexere Strukturen. Über 88 Prozent der mittleren und großen Unternehmen beurteilen ihren Schutz vor Wirtschaftskriminalität als gut oder sehr gut. Dennoch geben in der diesjährigen Studie 35 Prozent der befragten Unternehmen an, im Zeitraum der letzten zwei Jahre von wirtschaftskriminellen Handlungen betroffen gewesen zu sein. Dies steht zunächst im Einklang mit der Risikoeinschätzung für das eigene Unternehmen über diese relativ kurze Betrachtungsperiode. In der Vorgängerstudie von 2012 gaben 37 Prozent der befragten Unternehmen mit mehr als 50 Mitarbeitern³ an, in den letzten zwei Jahren Wirtschaftskriminalität zum Opfer gefal-

² Vergleiche Abschnitt „Über diese Studie“

³ Der Fokus der Studie aus dem Jahr 2012 lag auf Unternehmen aus dem Mittelstand, sodass eine Vergleichbarkeit nicht uneingeschränkt gegeben ist. Ausführungen zu Entwicklungen beziehen sich, sofern keine andere Festlegung erfolgt, im weiteren Verlauf auf die 2012 befragten Unternehmen mit mehr als 50 Mitarbeitern.

len zu sein. Der Anteil der Betroffenen bleibt somit nahezu gleich. Dies wirft Zweifel daran auf, dass die bislang seitens der Unternehmen ergriffenen und als gut oder sehr gut eingeschätzten Sicherungsmaßnahmen geeignet sind, ein höheres Maß an Sicherheit zu gewährleisten.

Es lassen sich zwei interessante Zusammenhänge erkennen: Mit steigender Anzahl der Mitarbeiter und Unternehmensgröße erhöht sich nach Einschätzung der Befragten sowohl das Risikobewusstsein für Wirtschaftskriminalität als auch die tatsächliche Betroffenheit.

Daher ist zu hinterfragen, ob von einer höheren Mitarbeiterzahl bzw. Unternehmenskomplexität tatsächlich eine größere Gefahr durch wirtschaftskriminelle Delikte ausgeht oder ob umfangreichere Investitionen von Großunternehmen in Prävention und Kontrollen mehr Möglichkeiten zur Aufdeckung bieten und damit das Risikobewusstsein erhöhen.

Trotz einer durch eine höhere Anzahl an Mitarbeitern bedingten Komplexität kann in Großunternehmen keine grundlegende Tendenz dazu festgestellt werden, dass die dort auftretenden Deliktsarten, zum Beispiel Diebstahl und Unterschlagung, hauptsächlich von Innentätern begangen werden.⁴

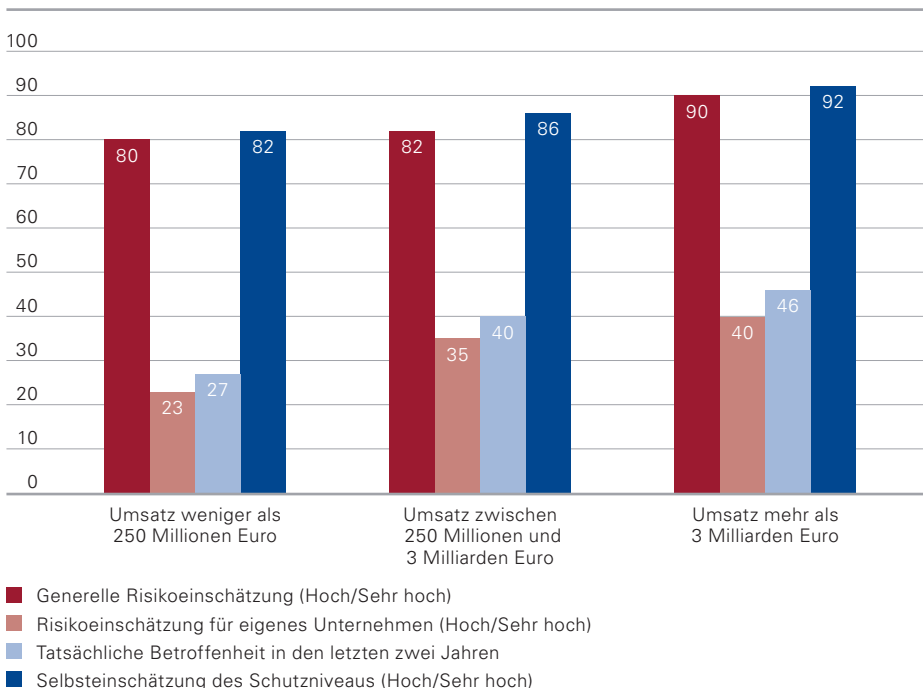
Im Gegenteil belegen die Angaben der befragten Unternehmen, dass große Unternehmen, zum Beispiel im Falle des Verrats von Geschäfts- und Betriebsgeheimnissen, mit steigender Mitarbeiterzahl eher kriminellen Handlungen externer denn interner Täter ausgesetzt sind. Bei dieser Deliktsart sind lediglich 13 Prozent der kleinen Unternehmen, jedoch 44 Prozent der Befragten der Kategorie „große Unternehmen“ von wirtschaftskriminellen Handlungen externer Täter betroffen.

Bei den weiteren abgefragten Deliktsarten (Abbildung 02, Seite 12) sind die Ergebnisse zur Täterherkunft unterschiedlich, sodass kein offensichtlicher Zusammenhang zwischen der Unternehmensgröße und der internen Täterschaft besteht (Abbildung 11, Seite 30).

Größere Unternehmen, gemessen an Mitarbeiter- und Umsatzstärke, sind bereit, mehr Geld in unterstützende Maßnahmen für Prävention und Detektion zu investieren (Abbildung 04, Seite 18).⁵ Damit wird die Wahrscheinlichkeit der Aufdeckung wirtschaftskrimineller Sachverhalte erhöht. Dies kann allerdings wiederum zu dem Kontrollparadoxon führen, dass größere Unternehmen aufgrund ihrer gegebenenfalls effektiveren Detektion eine stärkere Risikowahrnehmung für wirtschaftskriminelle Handlungen entwickelt haben als solche Unternehmen, die bei der Aufdeckung von Wirtschaftskriminalität weniger effektiv vorgehen.

01

Vergleich zwischen Risikoeinschätzung und Einschätzung des Schutzniveaus Angaben in Prozent der betroffenen Unternehmen



Quelle: KPMG, 2014

⁴ Vergleiche auch Kapitel 3 „Menschliche Faktoren begünstigen wirtschaftskriminelle Handlungen“

⁵ Vergleiche auch Kapitel 2 „Prävention – nach wie vor unterschätzt?“

Risikoeinschätzung und Selbstbewertung des Schutzes vor wirtschaftskriminellen Handlungen versus Betroffenheit hinsichtlich einzelner Deliktsarten

Fast zwei Drittel (63 Prozent) der in den letzten zwei Jahren von Wirtschaftskriminalität betroffenen Unternehmen geben als einschlägige Deliktsarten Diebstahl oder Unterschlagung an. 54 Prozent der Betroffenen nennen Betrugs- und Untreuedelikte. Weitere Delikte, wie zum Beispiel Datendiebstahl oder die Verletzung von Schutz- und Urheberrechten, folgen erst mit großem Abstand. Rund 50 Prozent der 400 befragten Unternehmen schätzen die Gefahr, von Diebstahl und Unterschlagung (54 Prozent) oder von Betrug und Untreue (49 Prozent) betroffen zu werden, als hoch bzw. sehr hoch ein. Bezüglich dieser Deliktsarten erweist sich die Risikoeinschätzung daher als zutreffend.

Bei den Deliktsarten Datendiebstahl oder Datenmissbrauch, Verletzung von Urheberrechten und Verrat von Geschäfts- und Betriebsgeheimnissen zeigt sich ein anderes Bild: Mehr als zwei Drittel der Befragten schätzen das Risiko, Opfer solcher Delikte

zu werden, als hoch bis sehr hoch ein (Verrat von Geschäfts- und Betriebsgeheimnissen 69 Prozent, Verletzung von Schutz- und Urheberrechten 78 Prozent, Datendiebstahl/Datenmissbrauch 87 Prozent). Beim Thema Datendiebstahl geht sogar ein Drittel der Befragten von einem sehr hohen Risiko aus. Jedoch geben lediglich jeweils circa 20 Prozent der 140 betroffenen Unternehmen an, in den vergangenen zwei Jahren tatsächlich von der Verletzung von Urheberrechten oder dem Verrat von Geschäfts- und Betriebsgeheimnissen betroffen gewesen zu sein. 30 Prozent der betroffenen Unternehmen geben Fälle von Datendiebstahl und Datenmissbrauch an. Wie in der Studie des Jahres 2012 waren rund 30 Prozent der Befragten von datenbezogenen Delikten betroffen. Damit ist dies nach Diebstahl und Unterschlagung sowie Betrug und Untreue, aber noch vor Korruption die am dritthäufigsten genannte Deliktsart (Abbildung 02, Seite 12).

Bei jenen Delikten, bei denen das Missverhältnis zwischen Wahrnehmung und tatsächlicher Betroffenheit besonders deutlich ist, werden in Zukunft steigende Risiken und somit

Es stellt sich die Frage, woher dieses Ungleichgewicht zwischen Risikowahrnehmung und tatsächlicher Betroffenheit kommt. Wie unsere Erfahrung zeigt, ist die Dunkelziffer gerade bei daten- und technikbezogenen Deliktsarten oftmals höher als die betroffenen Unternehmen ahnen. Vielfach fehlt ein Überblick über die komplexen Prozesse und Abläufe sowie die hochkomplizierte Technik. Ebenso mangelt es an der Implementierung von Kontrollmechanismen, um eben diesen Überblick zu behalten. Außerdem verschwinden, anders als beim Diebstahl materieller Güter, Daten nicht, sondern werden unzulässigerweise kopiert und dann andernorts verwendet. Der Umstand der unzulässigen Kopie fällt aber meist erst viel später auf – wenn überhaupt.

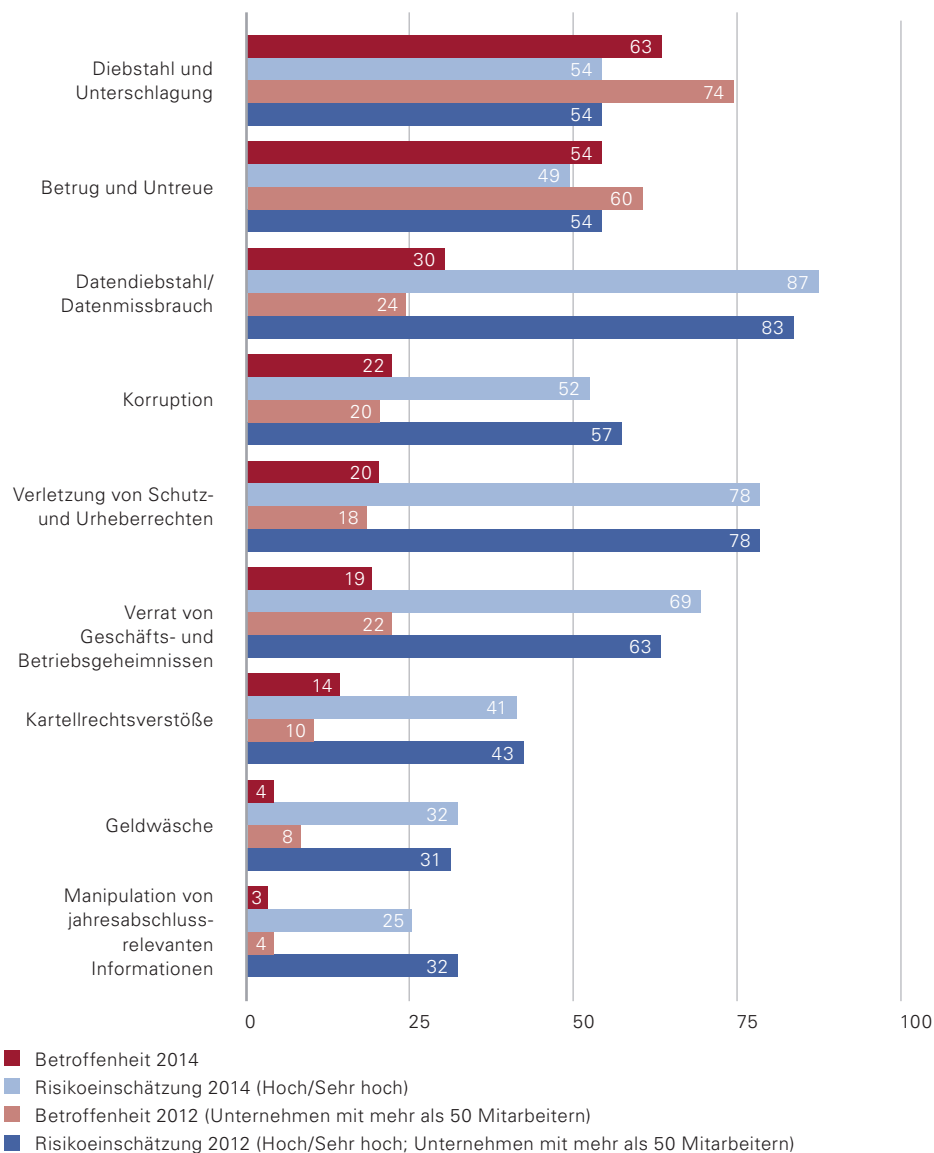


Alexander Geschonneck
Partner, Leiter Forensic

02

Vergleich zwischen Risikoeinschätzung und Betroffenheit

Angaben in Prozent



Quelle: KPMG, 2014

steigende Fallzahlen erwartet. Fast zwei Drittel der Befragten (64 Prozent) befürchten, dass das Risiko, Opfer eines „Datendelikts“ zu werden, in den nächsten zwei Jahren größer wird. 41 Prozent sind der gleichen Ansicht hinsichtlich der Verletzung von Schutz- und Urheberrechten. 31 Prozent der Unternehmen rechnen mit einem Anstieg des Verrats von Geschäfts- und Betriebsgeheimnissen. Bei keiner der weiteren abgefragten Deliktsarten ist in der Wahrnehmung der Befragten ein ähnlicher Anstieg zu verzeichnen.

Die Befürchtungen der Studienteilnehmer werfen die Frage auf, ob Unternehmen sich ausreichend wappnen, um den Eintritt genau dieser wirtschaftskriminellen Handlungen zu verhindern. Wie die Ergebnisse der Studie belegen, ist die Investitionsbereitschaft in externe Unterstützung in der Prävention sehr gering. Um ein höheres Schutzniveau zu gewährleisten, müssen allerdings höhere Ausgaben getätigt werden. Dies scheint jedoch nicht die Absicht der Befragten zu sein. Vielmehr sind sie bereits zufrieden mit ihrem Schutz vor Wirtschaftskriminalität: Wie erläutert, stuften 88 Prozent der mittleren und größeren Unternehmen ihr Schutzniveau als gut oder sehr gut ein.

Wie sind dann jedoch die Befürchtungen zu bewerten, dass das Eintrittsrisiko einzelner wirtschaftskrimineller Handlungen ansteigt? Hier besteht offensichtlich ein Widerspruch: Einerseits stuften sich die Unternehmen in den kommenden zwei Jahren als anfälliger gegenüber wirtschaftskriminellen Handlungen ein, andererseits sind sie mit ihrem Schutz vor eben diesen Handlungen zufrieden. Zwar haben die befragten Unternehmen offenkundig Bedenken hinsichtlich ihrer Anfälligkeit, doch spiegelt sich dies nicht in ihrer Investitionsbereitschaft wider.

Zudem war ein Drittel jener 341 Unternehmen, die ihren Schutz als gut bzw. sehr gut einstufen, in den letzten zwei Jahren trotzdem von Wirtschaftskriminalität betroffen. Überraschenderweise waren die 55 Unternehmen, die ihre Schutzmaßnahmen als schlecht oder sehr schlecht bewerteten, lediglich geringfügig häufiger – zu 38 Prozent – betroffen. Dieses Ergebnis wirft die Frage auf, wieso der Unterschied zwischen Unternehmen, die ihren Schutz als gut oder sehr gut beurteilen, und denen, die dieses nicht tun, lediglich so gering ist. Zum einen mag auch hier die Ursache im Kontrollparadoxon zu suchen sein. Wer Maßnahmen zur Prävention und Aufdeckung betreibt, erhöht die Wahrscheinlichkeit, einen Sachverhalt tatsächlich aufzudecken. Zum anderen ist der Schutz der Unternehmen, die sich hier gut aufgestellt sehen, möglicherweise doch nicht ausreichend. Dies ist angesichts

Die Ergebnisse zeigen, dass die Fokussierung der Medienberichterstattung auf bestimmte Deliktsarten einen erheblichen Einfluss auf die Risikoeinschätzung der Befragten zu haben scheint. Datenbezogene Vergehen sind nicht erst seit dem Fall Snowden in aller Munde. Auch urheberrechtliche Streitigkeiten sind derzeit regelmäßig in der Presse, beispielsweise die Kontroversen um unterschiedliche Streamingportale im Internet. Nicht so regelmäßig, jedoch mit mindestens gleichwertiger Intensität, wird in den Medien über den Verrat von Geschäfts- und Betriebsgeheimnissen berichtet. Die viel häufiger vorkommenden Diebstahls- und Unterschlagungsdelikte – mit im Vergleich oftmals geringeren Schäden – finden hingegen seltener auf die Titelseiten oder in die Headlines. Die subjektive Risikowahrnehmung des Einzelnen kann durch die Berichterstattung der Medien erheblich beeinflusst werden.



Barbara Scheben
Partner, Forensic

der geringen Investitionsbereitschaft denkbar. Demnach würden die implementierten Maßnahmen die Unternehmen nicht in dem erhofften oder erforderlichen Maße schützen.

Befragt nach dem generellen Risiko des Eintritts einer wirtschaftskriminellen Handlung sind die Unternehmen der Ansicht, dass in den kommenden zwei Jahren die Risiken wirtschaftskrimineller Handlungen entweder gleich bleiben (48 Prozent) oder ansteigen (47 Prozent) werden. Lediglich 6 Prozent der Unternehmen gehen von einem sinkenden Risiko aus.

Hinsichtlich ihrer Einschätzung des Risikos im eigenen Unternehmen in den nächsten zwei Jahren geben rund zwei Drittel der Befragten an, dass dieses gleich bleiben werde. Allerdings befürchten beachtliche 25 Prozent einen Anstieg, wohingegen lediglich 8 Prozent davon ausgehen, dass das Risiko sinken wird. Analog zur Einschätzung des aktuellen Risikos werden für die nächsten zwei Jahre größere Gefahren verstärkt bei anderen

Unternehmen und nicht beim eigenen gesehen. Dennoch kann festgestellt werden, dass für die befragten Unternehmen das Thema Wirtschaftskriminalität auch in Zukunft von hoher Relevanz sein wird.

Insgesamt zeigt sich im Vergleich von Risikoeinschätzung und Betroffenheit, dass die Unternehmen für einige Delikte eine zutreffende Risikoeinschätzung vornehmen, und zwar bei Diebstahls- und Unterschlagungs- sowie Betrugsdelikten. Dies könnte in deren „Alltäglichkeit“ begründet sein. Im Gegensatz dazu sehen die Befragten eine von der tatsächlichen Betroffenheit stark abweichende Bedrohung durch andere Deliktsarten. Dies gilt insbesondere für Delikte im Zusammenhang mit Daten, für den Verrat von Geschäfts- und Betriebsgeheimnissen sowie die Verletzung von Schutz- und Urheberrechten.

Risikoeinschätzung versus Schadenshöhe

Dass gerade Betrugs- und Untreuedelikte nicht zu unterschätzen sind, zeigen die von den Befragten geschätzten Schäden, die in Verbindung mit den verschiedenen Delikten eingetreten sind (Abbildung 03). Es werden knapp 300 Fälle der Deliktsart Betrug angegeben, bei denen über 52 Prozent der Unternehmen Gesamtschäden von 300.000 Euro oder mehr melden. Dies unterstreicht die Auswirkungen, die auch ein solches Delikt nach sich zieht.

Die Schäden aus dem Verrat von Geschäfts- und Betriebsgeheimnissen sowie die aus der Verletzung von Schutz- und Urheberrechten resultierenden Schäden liegen nach Schätzung der Befragten in einem ähnlichen Bereich. Bei dem Verrat von Geschäfts- und Betriebsgeheimnissen geben 63 Prozent der Betroffenen Gesamtschäden von 300.000 Euro oder höher an, bei der Verletzung von Schutz- und Urheberrechten sind es 57 Prozent.

Allerdings gehen die Befragten bei Betrugs- und Untreuedelikten von einem im Vergleich zu anderen Deliktsarten höheren Grundschaten aus. Oder umgekehrt: Die Ermittlungs- und Folgekosten sind bei Betrugs- und Untreuedelikten geringer. Knapp 62 Prozent der Befragten beziffern die Ermittlungs- und Folgekosten hier mit lediglich bis zu 50.000 Euro. Hingegen geben mehr als 76 Prozent der Unternehmen an, dass der Verrat von Geschäfts- und Betriebsgeheimnissen Ermittlungs- und Folgekosten von bis zu 100.000 Euro nach sich zieht. Gleiches gilt für die Verletzung von Schutz- und Urheberrechten, für die 84 Prozent der Unternehmen die Schadenshöhe auf bis zu 100.000 Euro beziffern. Daraus lässt sich schließen, dass sich wirtschaftskriminelle Handlungen wie Betrug und Untreue in den Augen der Befragten leichter aufklären lassen.

Was Risikoeinschätzung und Schadenshöhe anbelangt, verhält es sich im Hinblick auf Korruption⁶ ähnlich wie bei den Betrugs- und Untreuedelikten.

Hier schätzen 52 Prozent der Befragten das Risiko, von derartigen Fällen betroffen zu sein, als hoch bzw. sehr hoch ein. Somit wird die Eintrittswahrscheinlichkeit von Korruptionsfällen als wesentlich geringer empfunden als die von anderen Deliktsarten wie zum Beispiel Datendiebstahl oder Datenmissbrauch. 64 Prozent der betroffenen Unternehmen geben für Korruption einen Gesamtschaden von 300.000 Euro oder mehr an. Lediglich kartellrechtliche Verstöße sowie die Manipulation jahresabschlussrelevanter Finanzinformationen ziehen nach Einschätzung der Befragten noch höhere Schäden nach sich. Über 50 Prozent der Betroffenen geben für Korruptionsdelikte an, dass Ermittlungs- und Folgekosten 100.000 Euro oder mehr des Gesamtschadens ausmachen.

Interessant ist der Gegensatz der genannten Ergebnisse für Korruption oder Betrug und Untreue im Vergleich zu der Deliktsart Datendiebstahl und Datenmissbrauch. Bei letztgenannter wird das Risiko eines Vorfalls als am größten eingeschätzt. Allerdings verursacht sie nach Angabe von rund 61 Prozent der Betroffenen einen im Vergleich geringeren Gesamtschaden von bis zu 200.000 Euro. Einzig die Schäden von Diebstahls- und Unterschlagungsdelikten (59 Prozent) sowie Geldwäsche (67 Prozent) fallen mit Gesamtschäden von lediglich bis zu 100.000 Euro geringer aus. Es ist allerdings hervorzuheben, dass der Anteil der Ermittlungs- und Folgekosten an den Gesamtkosten bei Datendiebstahl und Datenmissbrauch im Vergleich zu jenen anderer Deliktsarten höher ist (beispielsweise im Vergleich zu Betrug und Untreue). Über 60 Prozent der Befragten beziffern diesen Anteil mit 60.000 Euro oder mehr. Somit ist davon auszugehen, dass Datendiebstahl und Datenmissbrauch nach Einschätzung der befragten Unternehmen einen höheren Aufwand bei der Aufklärung verursachen als andere Deliktsarten. Dies ist möglicherweise in der Anonymität begründet, die der Bereich der Cyberkriminalität den Tätern bietet.

⁶ Unter dem Begriff „Korruption“ werden vereinfacht die Deliktsarten der §§ 299, 300, 331–335 StGB verstanden.

Dennoch stellen die tatsächlichen Schadenshöhen keine Begründung dafür dar, warum gerade Datendiebstahl und Datenmissbrauch von den Befragten als besonders bedrohlich empfunden werden. Eine Erklärung könnte sein, dass Delikte im Zusammenhang mit Daten seit einigen Jahren stark in den Fokus der Öffentlichkeit gerückt sind. Sie können Reputationsschäden nach sich ziehen, deren tatsächliches Ausmaß schwer messbar ist.

Allerdings wird, im Einklang mit der Studie des Jahres 2012, die Gefahr von Reputationsschäden durch wirtschaftskriminelle Handlungen von mehr als drei Vierteln der Befragten (77 Prozent) als niedrig bzw. sehr niedrig eingestuft (2012: 81 Prozent). Es entsteht der Eindruck, dass Unternehmen die Gefahr von Reputationsschäden grundsätzlich als nachrangig

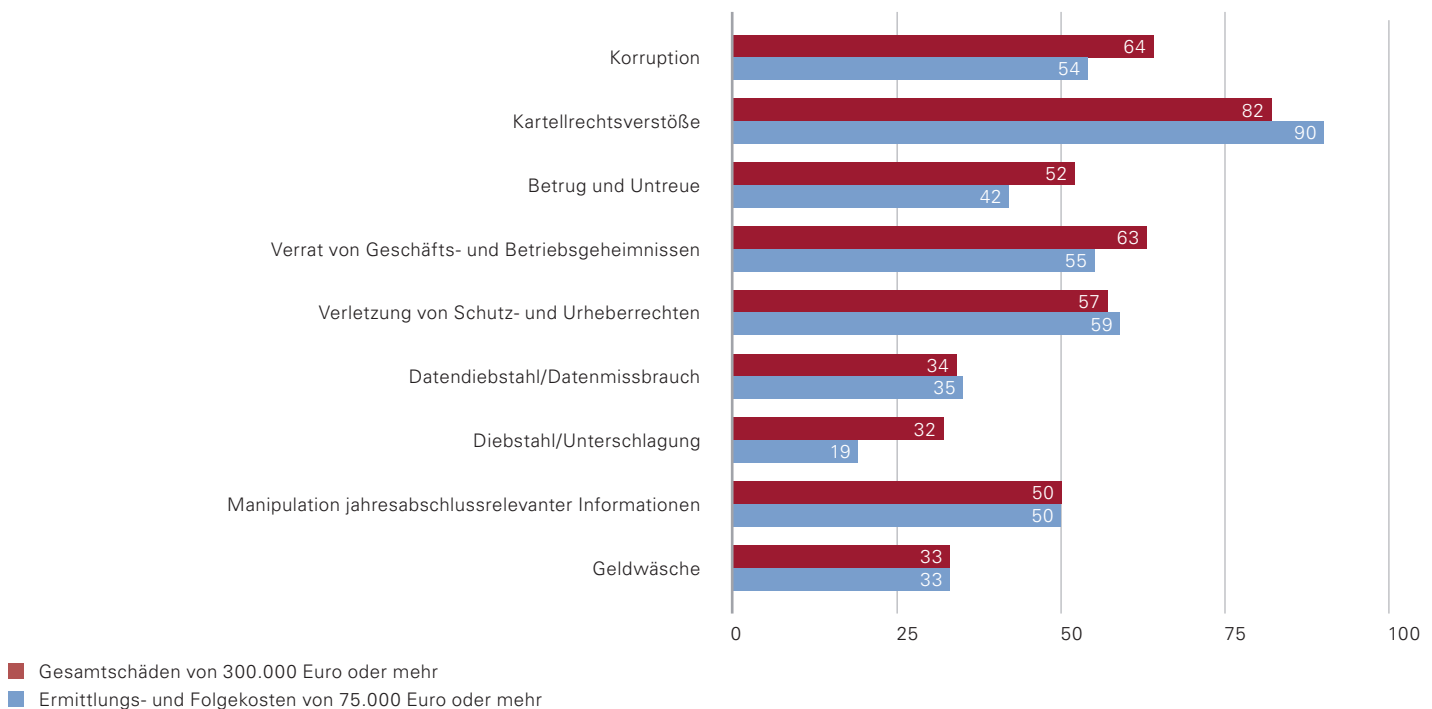
betrachten. Dennoch lassen sie sich anscheinend durch die mediale Fokussierung auf einzelne Delikte (zum Beispiel Datendiebstahl/Datenmissbrauch) in ihrer Risikoeinschätzung beeinflussen.

Analog zur Vorgängerstudie halten die Befragten den Eintritt von Reputationsschäden in zwei Jahren nicht für wahrscheinlicher als aktuell. In beiden Studien sind jeweils über 80 Prozent der Befragten der Ansicht, dass das Risiko gleich bleiben wird. Weniger als 15 Prozent der Unternehmen erwarten eine steigende Gefahr für das eigene Image bei Betroffenheit.

03

Übersicht Gesamtschäden sowie Ermittlungs- und Folgekosten

Angaben in Prozent



Quelle: KPMG, 2014

Exkurs: Kartell

Interessanterweise werden Kartellrechtsverstöße in der Risikowahrnehmung der befragten Unternehmen im Vergleich zu den weiteren abgefragten Deliktsarten nicht besonders betont. Dies verwundert angesichts des erheblichen Schadenspotenzials.

Von den 140 Unternehmen, die innerhalb der vergangenen zwei Jahre wirtschaftskriminellen Sachverhalten ausgesetzt waren, gibt circa ein Siebtel (14 Prozent) an, von kartellrechtlichen Verstößen betroffen gewesen zu sein.

Auch in Bezug auf Kartellrechtsverstöße belegen die Ergebnisse der Studie, dass umsatzstärkere Unternehmen häufiger von diesem Delikt betroffen sind als umsatzschwächere (22 Prozent der befragten großen Unternehmen gegenüber 9 Prozent der Befragten der Kategorie „kleine Unternehmen“).

Die Befragten schätzen zu 41 Prozent die Eintrittswahrscheinlichkeit eines Kartelldelikts bei ihrem Unternehmen als hoch bzw. sehr hoch ein. Dies ist im Vergleich zu der zuvor genannten Risikoeinschätzung im Hinblick auf Datendiebstahl oder Datenmissbrauch ein niedriger Wert. Obgleich Kartellrechtsverstöße zumeist hohe Wellen in den Medien schlagen, empfinden die Befragten das Risiko, Opfer eines solchen Delikts zu werden, als gering. Daher entsteht der Eindruck, dass die Befragten kartellrechtliche Verstöße zunächst nicht mit dem eigenen Unternehmen assoziieren. Des Weiteren geben lediglich 20 Prozent der Befrag-

ten die Einschätzung ab, dass ein hohes bzw. sehr hohes Risiko bestehe, von einem Kartell Dritter beeinträchtigt zu werden. Obwohl Kartellrechtsverstöße in der letzten Zeit häufiger im Blickfeld der Öffentlichkeit standen, zeigen diese Angaben, dass ihr Eintrittsrisiko trotz des enormen potenziellen Schadens vernachlässigt wird.

Dabei wird dieses hohe Schadenspotenzial sogar von der Einschätzung der Befragten untermauert. So schätzen die Betroffenen die durch Kartellrechtsverstöße entstandenen Schäden mit großem Abstand zu den anderen abgefragten Deliktsarten am höchsten ein. Fast drei Viertel (73 Prozent) der von Kartellrechtsverstößen betroffenen Unternehmen beziffern die Gesamtschäden aus dieser Deliktsart auf 1.000.000 Euro oder mehr. Lediglich die Gesamtschäden infolge von Manipulationen von für den Jahresabschluss relevanten Finanzinformationen werden ähnlich hoch eingeschätzt.

Von den angegebenen entstandenen Gesamtschäden im Rahmen eines Kartellrechtsverstoßes entfallen laut 60 Prozent der Betroffenen allein 400.000 Euro oder mehr auf Ermittlungs- und Folgekosten. Dieser Wert liegt deutlich höher als bei jeder anderen Deliktsart. Die Ermittlungs- und Folgekosten von Kartellrechtsverstößen lassen sich somit oftmals höher beziffern als die geschätzten Gesamtkosten anderer Deliktsarten. Dies unterstreicht, dass ein stärkeres Bewusstsein für kartellrechtliche Delikte angebracht ist.



Alexander Geschonneck
Partner, Leiter Forensic

In der Praxis beobachten wir häufig, dass im Zuge von kartellrechtlichen Ermittlungen in den Unternehmen keine Klarheit über die verfügbaren Informationsquellen herrscht. Dies fängt bei der angemessenen Reaktion auf eine kartellrechtliche Untersuchung an und hört bei der Identifikation entsprechender Frühwarnindikatoren in den Daten auf.

Interessanterweise geben dennoch 86 Prozent der Unternehmen an, im Falle möglicher kartellrechtlicher Ermittlungen einen umfassenden oder weitreichenden Überblick über die für die Aufklärung relevanten Daten, Dokumente und die Kommunikation zu besitzen. Der Großteil der Befragten betrachtet sich im Falle einer solchen Untersuchung demnach als gut aufgestellt. Angesichts der geringen Investitionsbereitschaft in unterstützende Maßnahmen in der Präventionsphase (Abbildung 04, Seite 18) und des hohen Anteils an Ermittlungs- und Folgekosten ist diese Selbsteinschätzung überraschend. Offensichtlich fallen in der Regel hohe Kosten an, wenn ein Unternehmen in eine kartellrechtliche

Ermittlung verwickelt ist. Diese Kosten sind schwer zu erklären, wenn sich die Befragten doch gut gewappnet fühlen. Eine funktionierende sensibilisierende Prävention bedeutet mehr als einen Überblick über Daten und Dokumente.



2 Prävention – nach wie vor unterschätzt?

Die Investitionsbereitschaft in externe Unterstützung im Bereich der Prävention ist geringer als der Wille, Ausgaben für die Aufklärung von und die Reaktion auf wirtschaftskriminelle Handlungen zu tätigen.

Der Umgang mit wirtschaftskriminellen Sachverhalten kann in drei Phasen eingeteilt werden: die Prävention (Vorbeugung), die Detektion (Aufdeckung) und die Reaktion (Aufklärung und Sanktionen). In dieser Studie wurden Unternehmen erstmals nach ihrer Investitionsbereitschaft für Unterstützungsleistungen in den unterschiedlichen Phasen befragt.

Ein Großteil der befragten Unternehmen ist in keiner der drei Phasen bereit, mehr als 50.000 Euro in externe Unterstützung zu investieren. Für die Prävention käme dies lediglich für 11 Prozent infrage. In der Detektionsphase gilt dies für 13 Prozent und in der Reaktionsphase für 17 Prozent der Befragten (Abbildung 04).

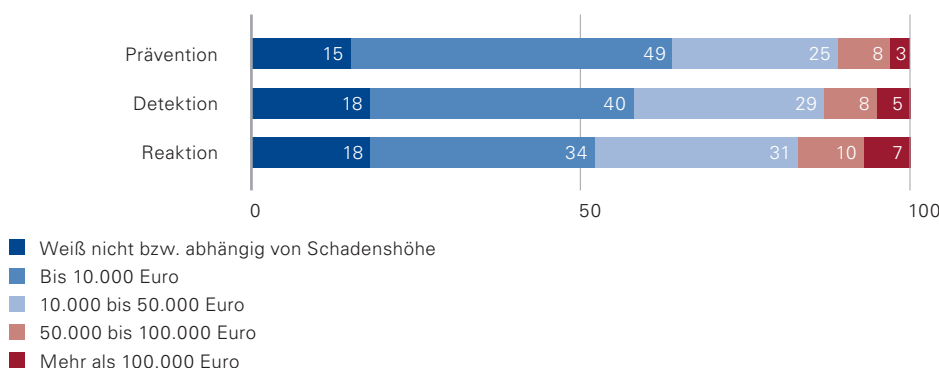
Von den befragten Unternehmen sind 49 Prozent lediglich bereit, bis zu 10.000 Euro in externe Unterstützung bei präventiven Maßnahmen zu investieren. Bei der Detektion wollen 40 Prozent der Befragten nicht mehr als 10.000 Euro aufwenden; hinsichtlich der Reaktion traf dies auf etwa ein Drittel der Befragten zu. Der Wille zur Investition in externe Unterstützung im Rahmen vorbeugender Maßnahmen ist somit geringer als in der Phase der Detektion und der Reaktion. Darüber hinaus zeigt sich auch hier der Trend, dass die Investitionsbereitschaft der Unternehmen in externe Unterstützung je nach Mitarbeiterstärke und Umsatz steigt.

Beispielsweise sind in der Prävention rund 20 Prozent der befragten großen Unternehmen bereit, mehr als 50.000 Euro in externe Unterstützung zu investieren, wohingegen dies lediglich bei rund 6 Prozent der kleinen Unternehmen der Fall ist. Ein identisches Bild zeigt sich für Detektion und Reaktion.

Die Investitionsbereitschaft ist in großem Maße davon abhängig, in welcher Phase des Umgangs mit einer wirtschaftskriminellen Handlung sich das jeweilige Unternehmen befindet. Je akuter und greifbarer die Situation ist, desto höher fällt die Bereitschaft der Unternehmen aus, zu investieren. Damit unterstreichen die Ergebnisse der Studie, dass in der Phase der Prävention der im Vergleich monetär geringste Aufwand betrieben wird. Es entsteht daher der Eindruck, dass Unternehmen von Fall zu Fall handeln und das Augenmerk nicht auf die Vermeidung zukünftiger Fälle legen. Prävention wird damit nach wie vor unterschätzt.

04 Bereitschaft zur Investition in externe Unterstützung bei Prävention, Detektion und Reaktion

Angaben in Prozent



Quelle: KPMG, 2014

Einzelne Präventionsmaßnahmen im Unternehmen

Es zeigen sich auffallende Abweichungen zwischen den tatsächlich von den Befragten umgesetzten präventiven Maßnahmen (Abbildung 05, Seite 21) sowie deren Zielrichtung einerseits und den Risikofaktoren, die von betroffenen Unternehmen als bedeutsam eingestuft werden, andererseits (Abbildung 06, Seite 22).

Ein Widerspruch zwischen den von den Befragten als wichtig erachteten Risikofaktoren und den tatsächlich getroffenen Maßnahmen besteht

darin, dass Schulungen gerade von kleinen und mittleren Unternehmen anscheinend lediglich als zweitrangig betrachtet werden. Dabei werden menschliche Faktoren als besonders wichtig bei der Begehung einer wirtschaftskriminellen Handlung angesehen.

Lediglich 17 Prozent der kleinen und rund ein Viertel der mittleren Unternehmen stufen den Einfluss fehlender Schulungen auf wirtschaftskriminelle Handlungen als hoch oder sehr hoch ein. In der Folge führen lediglich 54 Prozent der Befragten dieser

Präventionsmaßnahmen werden, sofern noch keine konkrete Gefahrenlage besteht, im Vergleich zu Detektion und Reaktion eher vernachlässigt. Der Anruf bei der Feuerwehr liegt eben näher als die Investition in individuelle Schulungsmaßnahmen zur Brandverhütung. Die Vorteile effektiver Prävention liegen damit nicht im unmittelbaren Blickfeld der Unternehmen. Allerdings leisten gerade risikoorientierte vorbeugende Maßnahmen wesentliche Beiträge zur Minimierung der Ermittlungs- und Folgekosten. Unternehmen, die eine professionelle Prävention betreiben, laufen aufgrund der getroffenen Maßnahmen weniger Gefahr, von wirtschaftskriminellen Handlungen und den daraus resultierenden Imageschäden betroffen zu sein.

Eine derartige Vernachlässigung der Prävention widerspricht dem ökonomischen Prinzip. Werden Schäden und Folgekosten einer wirtschaftskriminellen Handlung in Relation zu den vergleichsweise geringen Implementierungs- und Instandhaltungskosten und dem daraus resultierenden geringeren Risiko wirtschaftskrimineller Handlungen gesehen, sollte deutlich werden, dass derartige Investitionen von hohem Wert sind und sich auf Dauer auszahlen. Wer gut wirtschaften will, sollte auch gute Prävention betreiben.



Christoph Kampmeyer
Director, Forensic

Unternehmensgrößen solche Schulungen durch. Im Gegensatz dazu schätzen die Befragten, und zwar vor allem kleinere Unternehmen, mangelndes Unrechtsbewusstsein und Unachtsamkeit bzw. Nachlässigkeit als Faktoren mit hohem oder sehr hohem Einfluss auf wirtschaftskriminelle Handlungen ein.

Schulungen tragen allerdings dazu bei, genau diese als wichtig betrachteten Gefährdungsfaktoren einzudämmen. Sie sollten eine grundlegende Maßnahme in jedem Unternehmen sein. Zudem zeigen unsere Erfahrungen, dass das Verhältnis von Kosten und Nutzen für die Durchführung von Schulungen und Trainings spricht.

54 Prozent der Befragten führen fehlende oder mangelnde Kontrollen als Risikofaktor mit einer hohen oder sehr hohen Bedeutung für die Begehung einer wirtschaftskriminellen Handlung an. Dies ist der am zweithäufigsten genannte Faktor. Allerdings spiegelt sich seine Relevanz zum Teil nicht in den Präventionsmaßnahmen wider. Beispielsweise wird die proaktive systematische Erfassung von Frühwarnindikatoren (Red Flags) lediglich von rund 30 Prozent der kleinen und mittleren Unternehmen betrieben, obwohl die Befragten dem Aspekt der Kontrollen offensichtlich eine hohe Bedeutung zumessen. Einzig große Unternehmen nehmen eine solche Erfassung vermehrt vor (56 Prozent).

Hinzu kommt, dass Bewerber vor einer möglichen Anstellung nicht einmal von der Hälfte der Befragten auf Integrität überprüft werden. Eine frühzeitige Gefahrenerkennung kann somit nicht stattfinden. Dadurch, dass Unternehmen es unterlassen, derartige Frühwarnsysteme einzurichten, steigern sie das Risiko, Opfer einer wirtschaftskriminellen Handlung zu werden. Deren Schäden und Folgekosten wiederum dürften die Anschaffungs- und Unterhaltungskosten solcher Systeme bei Weitem übertreffen.

Unachtsamkeit bzw. Nachlässigkeit werden von etwas mehr als der Hälfte der Befragten als Risikofaktor mit einem hohen oder sehr hohen Einfluss auf die Begehung wirtschaftskrimineller Handlungen genannt. Neben den fehlenden Schulungen und Trainings fällt bezüglich dieses Faktors auf, dass etwa ein Drittel der Befragten über keine sichtbare Organisationsstruktur mit Compliance-Verantwortung verfügt. Diese dient den Beschäftigten als Maßgabe für gesetzeskonformes Verhalten und nimmt sie entsprechend in die Verantwortung, aktiv auf die Einhaltung gesetzlicher Vorgaben einzuwirken. Hinsichtlich kleiner Unternehmen ist es sogar knapp die Hälfte, die keine solche Struktur aufweist. Dabei ist es von unschätzbarem Wert, dass die Organisationsstruktur den Mitarbeitern Compliance-Grundsätze verdeutlicht und zu deren Einhaltung anhält.

Die Ergebnisse zeigen allerdings auch einige positive Tendenzen auf. 83 Prozent der Befragten verfügen über eine Definition von Leitbildern und Verhaltensgrundsätzen im Unternehmen. Dies unterstreicht, dass Unternehmen tatsächlich bemüht sind, den „Faktor Mensch“, der sich zum Beispiel in mangelndem Unrechtsbewusstsein oder Nachlässigkeit zeigt, zu beeinflussen. Leitbilder und Verhaltensgrundsätze sind unerlässlich, um die Beschäftigten zu gesetzeskonformem Verhalten zu ermutigen. Auffallend ist hingegen, dass 75 Prozent der betroffenen Unternehmen fehlenden Leitlinien oder Vorgaben lediglich eine geringe Bedeutung bei der Begehung einer wirtschaftskriminellen Handlung beimessen.

Die Ergebnisse der Studie verweisen zudem darauf, dass die Befragten durchaus präventive Maßnahmen zu Kontrollzwecken implementiert haben. 73 Prozent der Befragten erfassen und bewerten systematisch besonders schützenswerte Daten und können anhand dieser Bewertung geeignete Schutzkonzepte erarbeiten. Gerade in der heutigen Zeit, in der die Wichtigkeit des Datenschutzes und der Datensicherheit nicht oft genug betont werden kann, ist dies ein erfreulich hoher Anteil an Unternehmen, die Präven-

tion aktiv betreiben. Überdies sehen 69 Prozent der Studienteilnehmer in der Integritätsüberprüfung ihrer Geschäftspartner und Lieferanten eine wichtige Präventionsmaßnahme.

Knapp drei Viertel der Unternehmen haben einen Ansprechpartner für Fragen zu möglicherweise wirtschaftskriminellen Handlungen eingesetzt. Dies belegt, dass die Befragten sich der Sensibilität dieser Thematik bewusst sind.

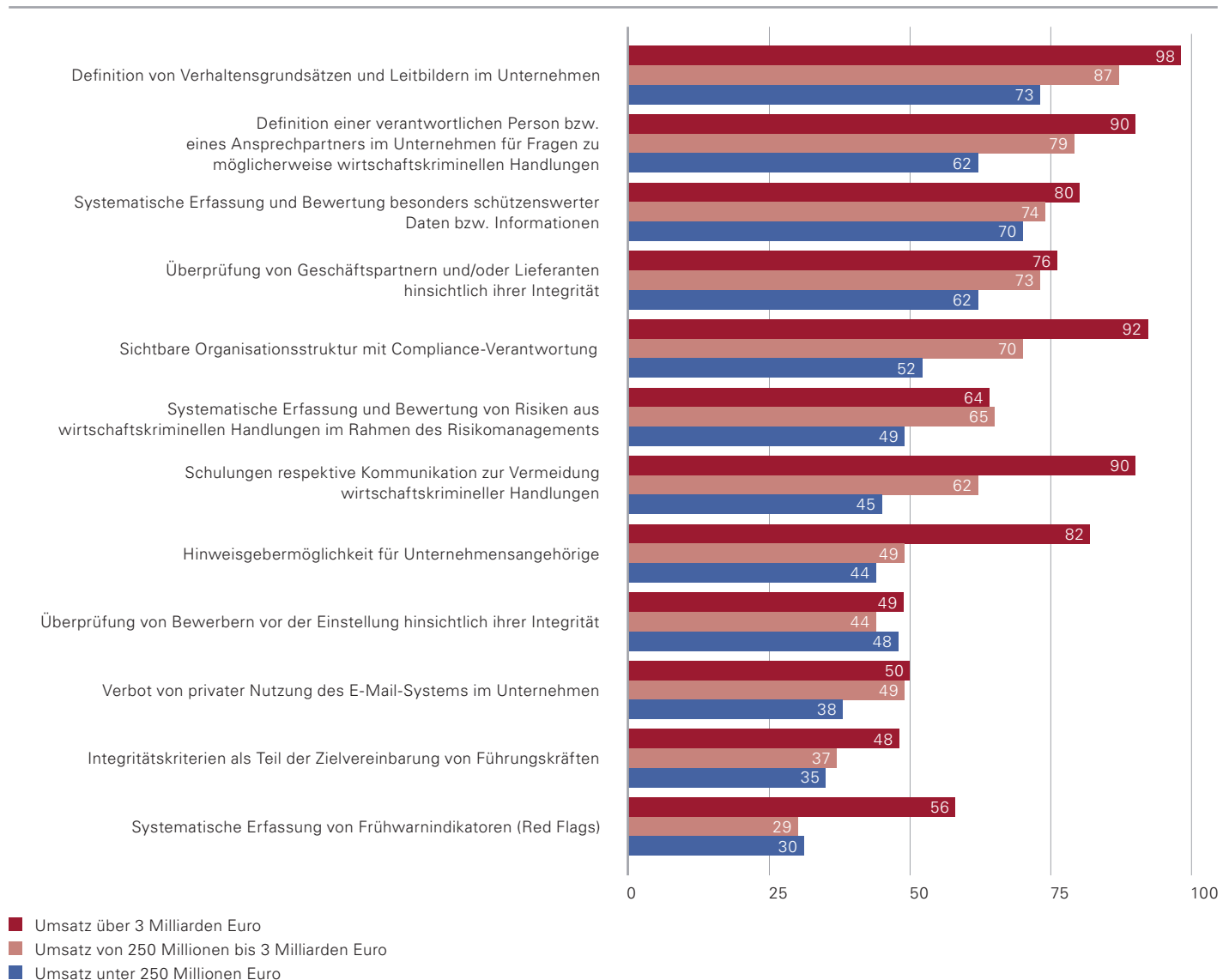
Bei der Betrachtung einzelner Unternehmensklassen fällt auf, dass große Unternehmen ein deutlich höheres Maß an präventiven Maßnahmen vorsehen als die übrigen Teilnehmer

der Studie. Im Vergleich zu den kleineren Unternehmensklassen legen große Unternehmen insbesondere wesentlich mehr Wert auf Schulungen (90 Prozent gegenüber 54 Prozent bei den restlichen Teilnehmern der Studie), eine Organisationsstruktur mit Compliance-Verantwortung (92 Prozent gegenüber 61 Prozent) sowie auf das Einräumen einer Hinweisgebermöglichkeit hinsichtlich wirtschaftskrimineller Handlungen für Unternehmensangehörige (82 Prozent gegenüber 47 Prozent). Diese Zahlen belegen, dass bei kleinen und mittleren Unternehmen hier Nachholbedarf besteht.

05

Vorhandene Präventionsmaßnahmen nach Umsatz

Angaben in Prozent, Mehrfachnennungen möglich



Quelle: KPMG, 2014

Entdeckung, betroffene Bereiche und Aufklärung

Nach Einschätzung von drei Vierteln der Betroffenen vergehen zwischen der Tat und ihrer Entdeckung durchschnittlich weniger als zwei Jahre. 16 Prozent der Befragten geben einen Zeitraum von zwei bis fünf Jahren an, lediglich 5 Prozent schätzen, dass zwischen Begehung und Entdeckung der wirtschaftskriminellen Handlung mehr als fünf Jahre liegen.

Die Ergebnisse der Studie zeigen, dass bei großen Unternehmen zwischen Begehung und Entdeckung der Tat wesentlich mehr Zeit vergeht als bei kleineren Unternehmen. Lediglich 4 Prozent der kleinen bzw. 1 Prozent der mittleren Unternehmen geben mehr als fünf Jahre an. Im Gegensatz dazu nennen 17 Prozent der großen Unternehmen diesen Zeitraum. In Großunternehmen sind somit entweder die wirtschaftskriminellen Handlungen komplexer und die Aufdeckung gestaltet sich daher schwieriger oder

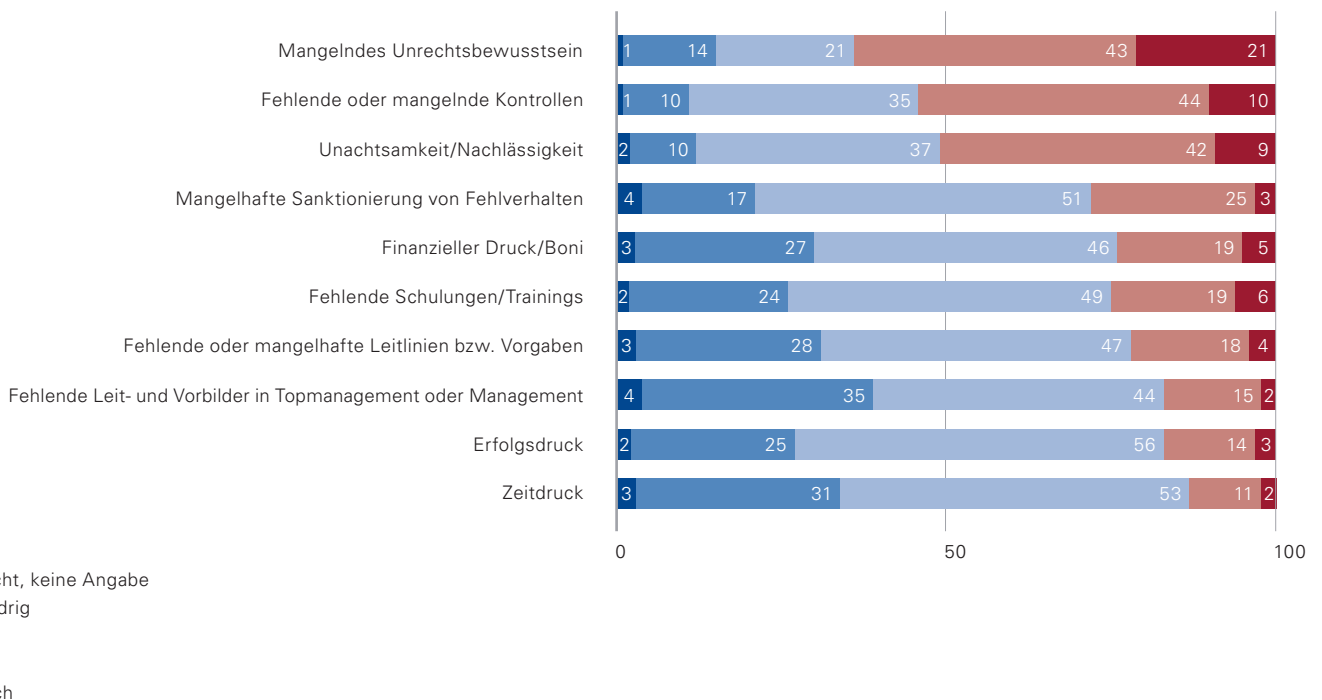
die Sachverhalte können aufgrund der Größe und Komplexität der Unternehmensstruktur nicht schnell aufgedeckt und aufgeklärt werden. Dies hat jedoch Konsequenzen: Eine frühzeitige Aufdeckung erleichtert sowohl Aufklärung als auch Reaktion und trägt somit dazu bei, die Höhe der jeweiligen Schäden über den Zeitverlauf in Grenzen zu halten.

Analog zur Studie des Jahres 2012 (44 Prozent) ist der Vertrieb der am häufigsten von Wirtschaftskriminalität betroffene Bereich in den befragten Unternehmen (50 Prozent) (Abbildung 07). Die Betroffenheit der Bereiche Lager/Logistik sowie der Produktion zeigt sich im Vergleich zur Vorstudie als rückläufig, doch werden sie weiterhin von etwa einem Viertel der Befragten genannt. Hingegen stellt der Einkauf trotz eines lediglich marginalen Anstiegs auf 29 Prozent in der aktuellen Studie den am zweithäufigsten genannten Bereich dar. Die übrigen abgefragten Bereiche, wie

06

Einschätzung von Risikofaktoren wirtschaftskrimineller Handlungen

Angaben in Prozent, Mehrfachnennungen möglich



Quelle: KPMG, 2014

beispielsweise die Geschäftsführung oder die IT, werden von über 80 Prozent der Befragten nicht angeführt und somit als nachrangiges Ziel wirtschaftskrimineller Handlungen eingeschätzt. Es lässt sich hier ein leichter Rückgang der Betroffenheit gegenüber der Vorgängerstudie feststellen (2012: Geschäftsführung 26 Prozent, Informationstechnologie 18 Prozent).

Die Antworten der Befragten zeigen, dass Unternehmen hauptsächlich infolge offener Hinweise sowohl von Unternehmensinternen (57 Prozent) als auch Unternehmensexternen (47 Prozent) sowie durch Erkenntnisse der internen Revision oder einer sonstigen internen Ermittlungseinheit (52 Prozent) auf wirtschaftskriminelle Handlungen aufmerksam werden (Abbildung 08, Seite 24).

Die Entdeckung aufgrund von Hinweisen Unternehmensexternen sowie der Internen Revision wird in der diesjährigen Studie von einem größeren Anteil der Befragten genannt.

Nahezu unverändert häufig (54 Prozent) spielt „Kommissar Zufall“ eine Rolle bei der Entdeckung einer wirtschaftskriminellen Handlung. Er bleibt der am zweithäufigsten angeführte Grund für die Entdeckung der Tat. Gerade die hohe Zahl der zufällig ans Tageslicht gekommenen Hinweise verdeutlicht, dass offenbar nach wie vor weitreichende Möglichkeiten bestehen, die von den Unternehmen implementierten Mechanismen zur Aufdeckung zu umgehen.

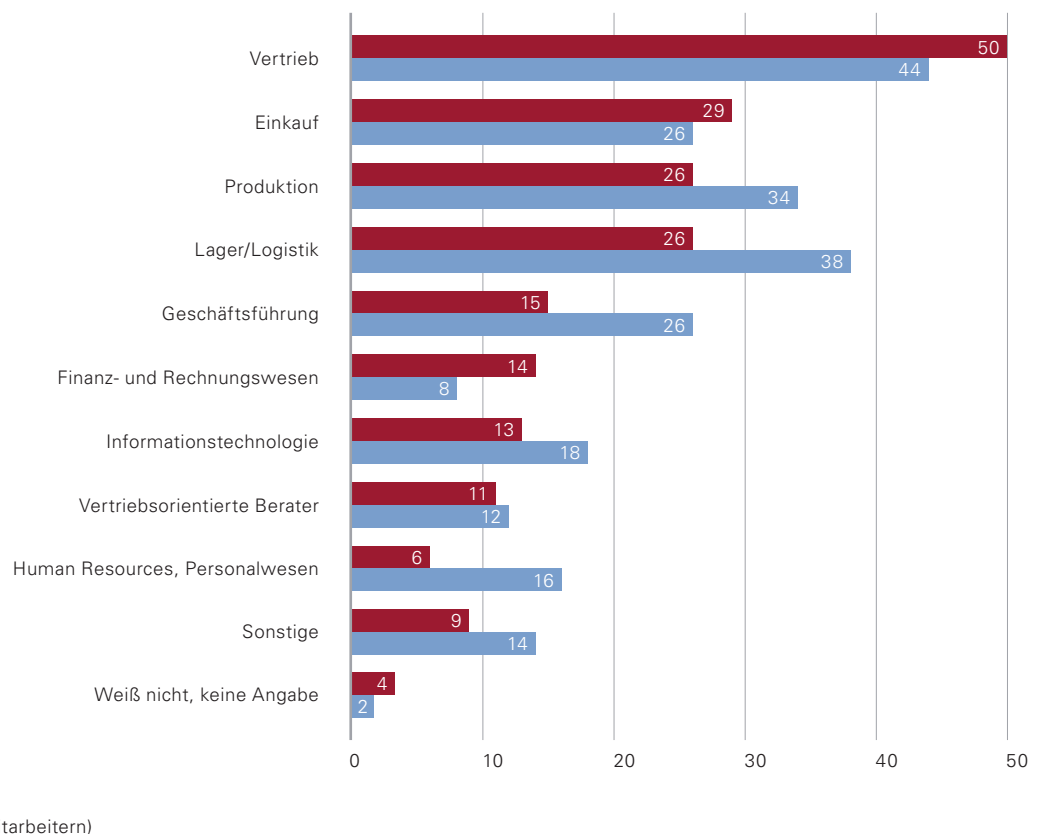
Von zunehmender Bedeutung sind Hinweise der Strafverfolgungsbehörden, die von 29 Prozent der betroffenen Unternehmen angegeben werden. Dies deutet auf eine Verbesserung der Aufdeckungsmethoden oder eine höhere Aktivität der zuständigen Behörden hin.

Wie in der Studie des Jahres 2012 nennt etwa ein Viertel der Befragten anonyme Hinweise; Hinweisen aus der Öffentlichkeit sowie aus der Jahresabschlussprüfung wird von den Befrag-

07

Betroffene Abteilungen im Unternehmen

Angaben in Prozent, Mehrfachnennungen möglich



■ 2014

■ 2012 (Unternehmen mit mehr als 50 Mitarbeitern)

Quelle: KPMG, 2014

ten im Vergleich dazu ein sehr geringer Stellenwert eingeräumt.

In der Phase der operativen Aufklärung zeichnet sich die Tendenz ab, dass die befragten Unternehmen zuerst intern agieren wollen. Dabei sind die Interne Revision (60 Prozent) sowie die Compliance- und Rechtsabteilung (55 Prozent) die nach Einschätzung der Betroffenen meistgenutzten Ressourcen der operativen Erstaufklärung. Unwesentlich geringer ist die Rolle der Strafverfolgungsbehörden (54 Prozent). Externe Berater in Gestalt von Rechtsanwälten oder Wirtschaftsprüfern wurden in 41 Prozent der Fälle mit der operativen Erstaufklärung beauftragt. Detekteien werden laut den Befragten lediglich in 10 Prozent der Fälle mit der operativen Aufklärung betraut.

Die befragten Unternehmen scheinen demnach dazu zu tendieren, sich zunächst intern mit der operativen Erstaufklärung zu befassen, solange dies

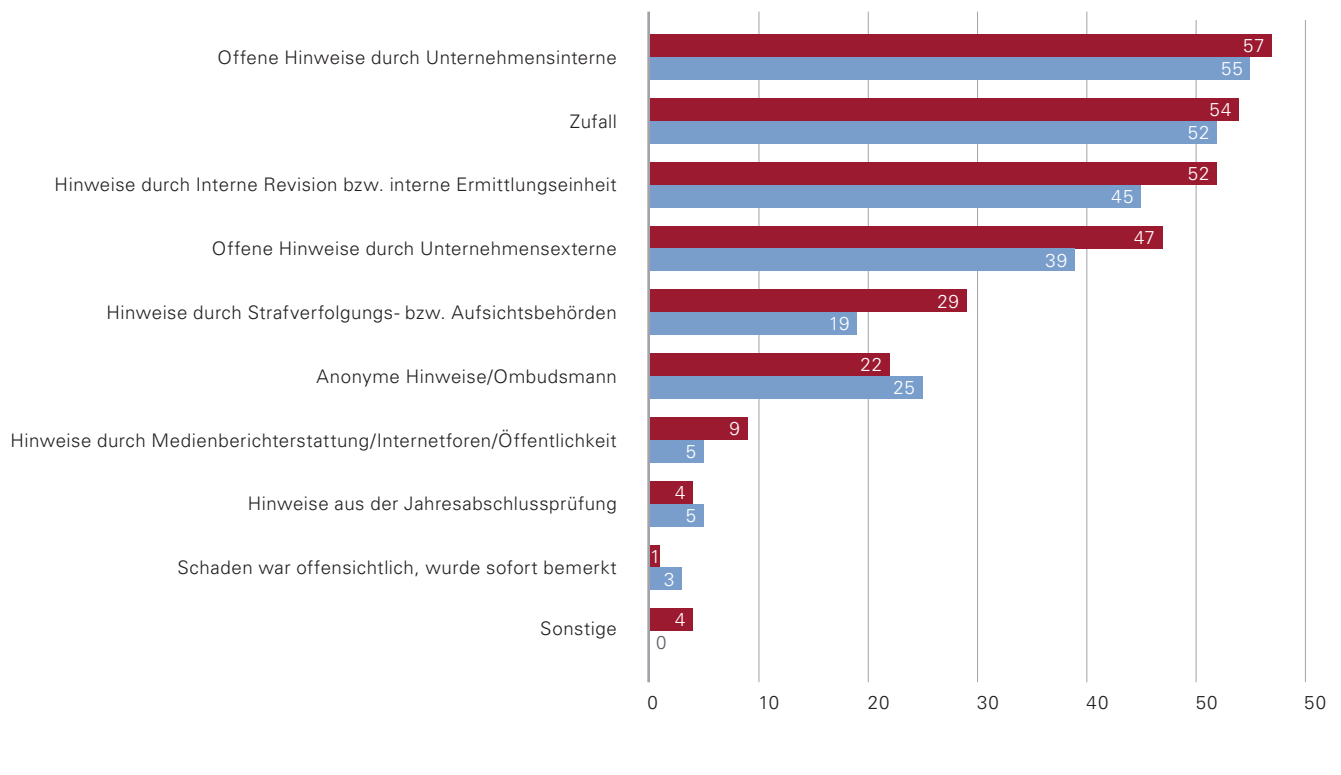
möglich ist. Zudem greifen Unternehmen mit höherem Umsatz zu verschiedenartigen Aufklärungsansätzen (Abbildung 09).

Bei der Aufklärung der entdeckten Sachverhalte zeichnet sich ab, dass die befragten Unternehmen zumeist auf Maßnahmen zurückgreifen, die im Vergleich einfach umzusetzen und unter geringem Einsatz technischer Hilfsmittel durchzuführen sind. Daher sind im Einklang mit der Studie des Jahres 2012 Mitarbeiterbefragungen, die von 71 Prozent der Betroffenen genannt werden, die am häufigsten durchgeführte Maßnahme. Ähnlich verhält es sich mit der Auswertung physischer Unternehmensakten, die von fast zwei Dritteln der Betroffenen genutzt wird. In der Vorgängerstudie war ein deutlich größeres Ungleichgewicht zwischen Befragungen und der Auswertung von Akten festzustellen, da Mitarbeiterbefragungen derzeit im Vergleich häufiger durchgeführt wurden (in 92 Prozent der Fälle von betroffe-

08

Quellen der Entdeckung von wirtschaftskriminellen Handlungen

Angaben in Prozent⁷, Mehrfachnennungen möglich



■ 2014
■ 2012

Quelle: KPMG, 2014

⁷ Um eine bessere Vergleichbarkeit zu gewährleisten, wurde bei dieser Grafik auf die Gesamtergebnisse der Studie 2012 zurückgegriffen.

nen Unternehmen mit mehr als 50 Mitarbeitern). Die Auswertung von physischen Unternehmensakten wurde 2012 von 64 Prozent der Befragten als Maßnahme genannt.

Hintergrundrecherchen stellen die drittwichtigste Maßnahme dar, die von mehr als der Hälfte der Betroffenen ergriffen wird (54 Prozent). Gegenüber 2012 ist diesbezüglich allerdings ein geringer Rückgang in der geschätzten Nutzung festzustellen.

Bezüglich weiterer abgefragter Maßnahmen bestätigt sich bei großen Unternehmen der Trend, dass die Betroffenen bei der Aufklärung des Sachverhalts technische Hilfsmittel einsetzen. Instrumentarien wie elektronische Datenanalysen sowie der Zugriff auf E-Mail-Konten der Mitarbeiter und die Analyse dieser Konten etablieren sich bei diesen Unternehmen als anerkannte Maßnahmen. Beide werden laut den betroffenen großen Unternehmen in 71 Prozent der Fälle genutzt. Im Gegensatz dazu greifen lediglich 29 Prozent der betroffenen kleinen Unternehmen auf solche Maßnahmen zurück; Unternehmen mittlerer Größe nehmen zu 41 Prozent elektronische Datenanalysen vor. Gegenüber 2012 zeigt sich bei großen Unternehmen ein deutlicher Anstieg der Nutzung elektronischer Daten- und E-Mail-Analysen (elektronische Datenanalyse 2012: 53 Prozent; Zugriff auf und Analyse von E-Mail-Konten der Mitarbeiter 2012: 44 Prozent). Im Hinblick auf kleinere Unternehmensklassen blieben die Zahlen in etwa gleich (Abbildung 10, Seite 26). In Anbetracht der immensen Bedeutung technischer Aufklärungsmaßnahmen beim Umgang mit wirtschaftskriminellen Handlungen wäre es wünschenswert, dass in Zukunft nicht nur große Unternehmen regelmäßig darauf zurückgreifen, sondern auch kleinere Unternehmen diese Maßnahmen häufiger anwenden.

Mit Blick auf große Unternehmen zeigt sich die Tendenz, dass sich technisch umsetzbare Maßnahmen, zum Beispiel elektronische Datenanalysen,

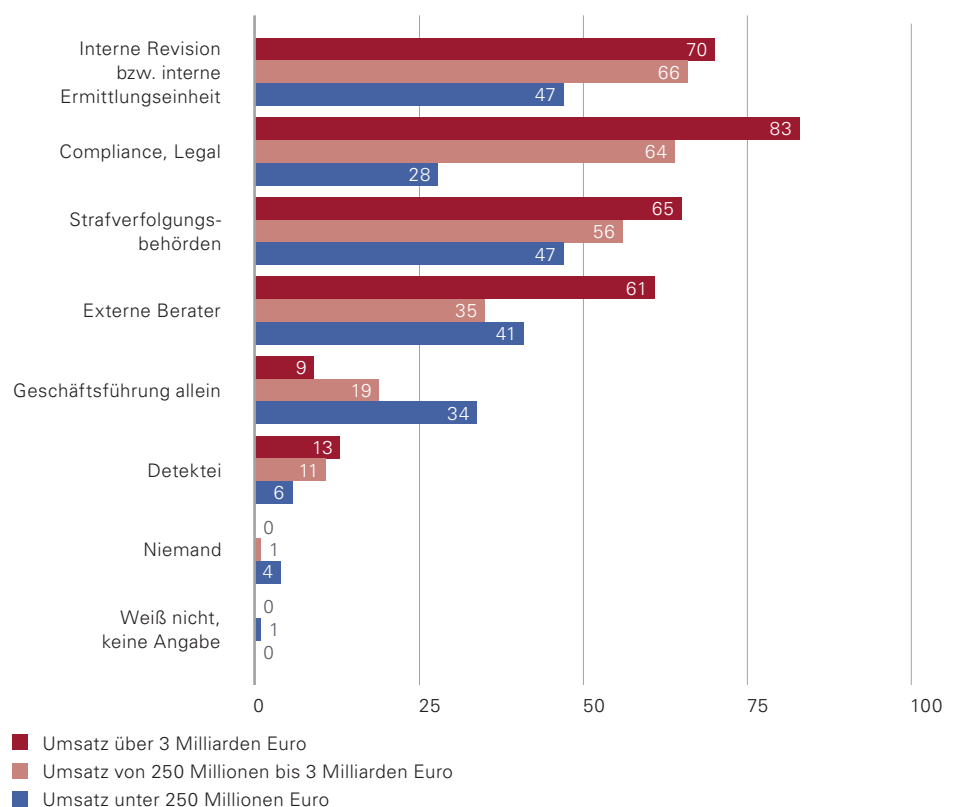
immer mehr im Rahmen der Aufklärung von wirtschaftskriminellen Handlungen etablieren. Diese Entwicklung ist positiv zu betrachten, da sie belegt, dass sich große Unternehmen in den angewandten Maßnahmen dem aktuellen technischen Stand anpassen. Sie nehmen diesbezüglich eine Vorreiterrolle ein.

In Bezug auf Unternehmensgröße und Umsatz lässt sich festhalten, dass Unternehmen mit wachsender Größe und steigendem Umsatz, insbesondere mit zunehmender Anzahl an Mitarbeitern, im Rahmen der Aufklärung zu verschiedenen, einander ergänzenden Maßnahmen greifen. Außerdem wenden mehr als zwei Drittel der betroffenen Unternehmen dieser Größe jede der fünf insgesamt am häufigsten genannten Maßnahmen kumulativ an (Mitarbeiterbefragungen, Auswertung von Unternehmensakten, Hintergrundrecherchen, elektronische Datenanalysen und die Analyse von E-Mail-Konten).

09

Operative Aufklärung nach Umsatz

Angaben in Prozent, Mehrfachnennungen möglich



Quelle: KPMG, 2014

Reaktion und Sanktion

Lediglich rund 4 Prozent der Betroffenen sind der Ansicht, dass sie nicht angemessen auf wirtschaftskriminelle Handlungen reagiert haben. Darauf beruht gegebenenfalls die positive Selbsteinschätzung der Unternehmen bezüglich ihres Schutzniveaus vor wirtschaftskriminellen Handlungen (85 Prozent stufen dieses als gut bzw. sehr gut ein).

Nach abgeschlossener Aufklärung reagieren etwas mehr als drei Viertel der betroffenen Unternehmen damit, die Täter zu sanktionieren und die bestehenden Präventionsmaßnahmen zu verändern. In etwas mehr als

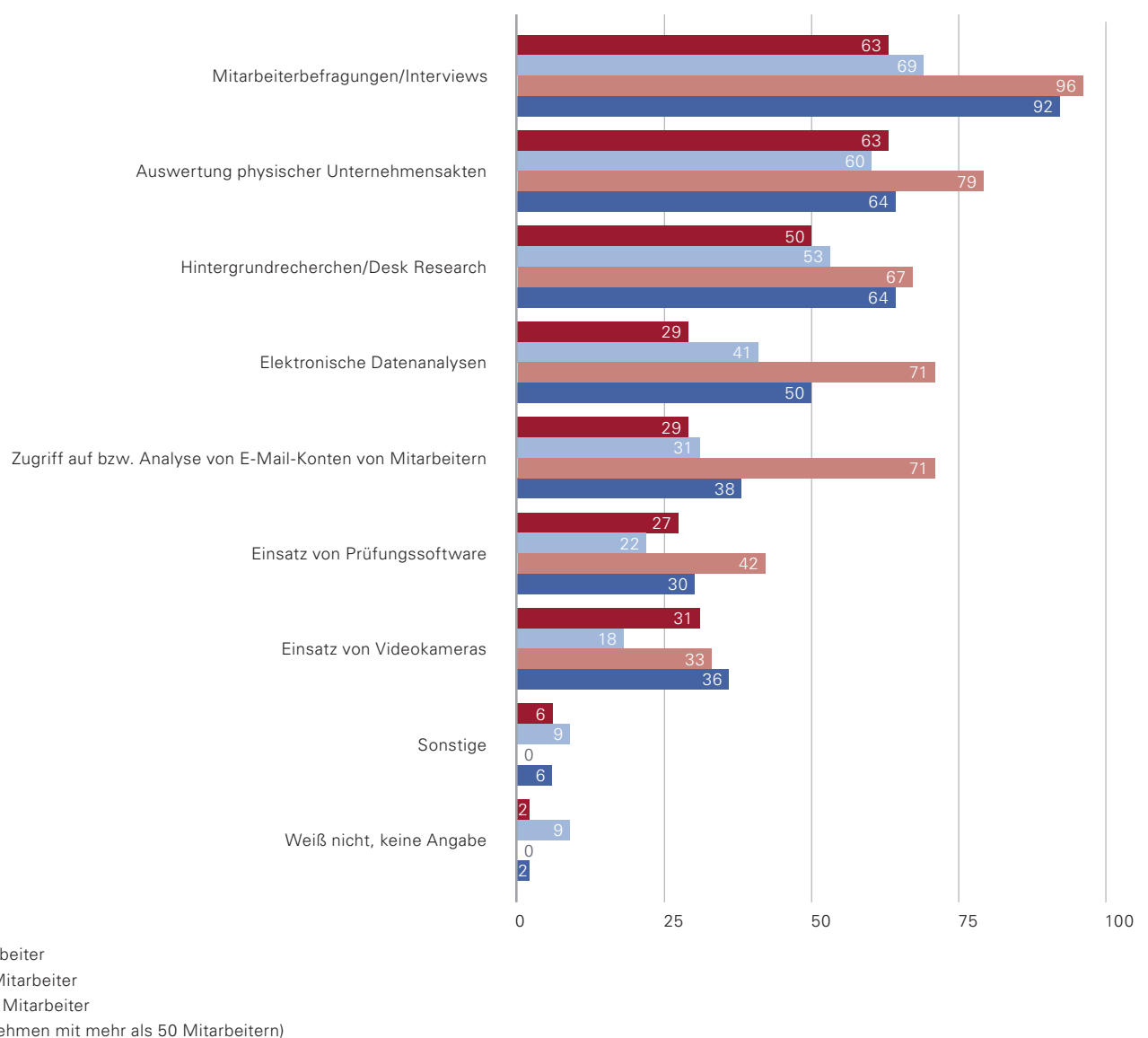
20 Prozent der Fälle kommen die Täter ohne rechtliche Konsequenzen davon. Dies kann allerdings auch darauf beruhen, dass Täter beispielsweise bei datenbezogenen Verstößen nicht eindeutig identifiziert werden können. Somit werden nicht alle Delikte tatsächlich aufgeklärt. Befragt danach, ob es sich um interne oder externe Täter handelte, können 8 Prozent der Unternehmen keine Angabe machen.

Werden den Tätern Sanktionen auferlegt, handelt es sich zumeist um arbeitsrechtliche Konsequenzen (73 Prozent). Im Vergleich zur Studie des Jahres 2012 scheuen sich weniger Unternehmen davor, straf- (55 Prozent)

10

Maßnahmen zur Aufklärung

Angaben in Prozent, Mehrfachnennungen möglich



Quelle: KPMG, 2014

oder zivilrechtliche Konsequenzen (58 Prozent) zu ziehen (2012: 52 Prozent strafrechtliche bzw. 39 Prozent zivilrechtliche Konsequenzen). Diese üben aufgrund der zu befürchteten Strafverfolgung oder Schadensersatzleistungen eine erheblich stärkere abschreckende Wirkung aus als arbeitsrechtliche Maßnahmen. Dennoch werden nicht alle Delikte geahndet und die abschreckende Wirkung von Sanktionen bleibt zum Teil ungenutzt.

Neben Sanktionen reagierten zwei Drittel der Betroffenen mit organisatorischen Maßnahmen und Strukturveränderungen. Bei der Hälfte der Betroffenen hatte dies auch Veränderungen der personellen Zuständigkeiten und Verantwortlichkeiten zur Folge.

Entwicklung des Compliance-Budgets

Rund 50 Prozent der Befragten geben an, dass ihr Compliance-Budget in den letzten zwei Jahren gleich geblieben sei. Jeweils ein Viertel der Befragten gibt an, dass es gesunken bzw. gestiegen sei. Dies widerspricht den Erwartungen der Teilnehmer der Studie des Jahres 2012. Dort hatten 41 Prozent der Unternehmen angegeben, sie seien der Ansicht, dass das Compliance-Budget steigen werde. Nur 3 Prozent gingen von einer Senkung aus. Angesichts der Tatsache, dass in der aktuellen Studie lediglich 30 Prozent der Unternehmen das Risiko, selbst Opfer einer wirtschaftskriminellen Handlung zu werden, als hoch bzw. sehr hoch einschätzen, verwundert es nicht, dass sich kein beachtlicher Anstieg der Budgets feststellen lässt, obwohl die Unternehmen dies angenommen hatten.

Für die kommenden zwei Jahre erwarten die Befragten jedoch wiederum zu 40 Prozent einen Anstieg ihres Compliance-Budgets. Weitere 55 Prozent gehen davon aus, dass das Budget gleich bleiben wird. Nur 2 Prozent sind der Ansicht, dass es sinken wird.

Aus der Erfahrung zeigt sich, dass sowohl rechtlich als auch investigativ in der Mehrzahl der Fälle ein hohes Spezialistentum notwendig ist, um Fehler zu vermeiden, die sich in gerichtlichen Auseinandersetzungen bzw. weiterführenden Ermittlungen schädlich auswirken können. Die oft vorherrschende Komplexität sowie die Herausforderungen einer gerichtssicheren Beweisführung übertreffen die Erwartungshaltungen der Unternehmen bezüglich des zu investierenden Budgets häufig.



Rüdiger Birkental
Partner, Forensic

3 Menschliche Faktoren begünstigen wirtschaftskriminelle Handlungen

Unabhängig von technischen Kenntnissen finden Kriminelle ihren Weg. Die kriminelle Motivation des Täters ist ausschlaggebend bei der Begehung eines wirtschaftskriminellen Delikts.

Wie in der Studie des Jahres 2012 nennen die Befragten persönliche Eigenschaften der Täter als den wichtigsten Einflussfaktor für das Risiko, von wirtschaftskriminellen Handlungen betroffen zu werden. 63 Prozent der Befragten geben an, dass eher oder ausschließlich menschliche Faktoren wie finanzielle Motivation oder Rechtsfertigungsmöglichkeiten das Risiko, wirtschaftskriminell zu handeln, am stärksten beeinflussen. 25 Prozent benennen technische und organisatorische Schwachstellen im System, die dem Täter die Tat erst ermöglichen, als einflussreichsten Faktor.

Lediglich 11 Prozent der Befragten betrachten eher bzw. ausschließlich fachliches Spezialwissen der beteiligten Personen als einen wichtigen Faktor.

Den Täter machen gemäß den Ergebnissen nicht etwa die technischen Kenntnisse aus, sondern bestimmte Charaktereigenschaften oder das individuelle Umfeld. Somit entspricht ein brillanter Hacker, dem es jedoch an krimineller Motivation mangelt, weniger dem Bild eines möglichen Täters als eine Person mit finanziellem Motiv, die ihre Taten als gerechtfertigt ansieht.

Der Stellenwert der menschlichen Eigenschaften als Hauptursache für die Durchführung wirtschaftskrimineller Handlungen wird weiterhin von den Ergebnissen zur Frage nach der Bedeutung einzelner Faktoren innerhalb des Unternehmens untermauert. 64 Prozent der Befragten antworten auf diese Frage, dass mangelndes Unrechtsbewusstsein beim Täter eine

hohe bzw. sehr hohe Bedeutung für die Begehung der Tat habe. 51 Prozent sind zudem der Ansicht, dass Unachtsamkeit und Nachlässigkeit ebenfalls wichtige Faktoren seien.

Somit handelt es sich bei zwei der drei meistgenannten Faktoren um menschliche Eigenschaften (Abbildung 06, Seite 22).

Daneben geben 54 Prozent der Befragten fehlende und mangelnde Kontrollen als bedeutsamen Faktor bei der Begehung wirtschaftskrimineller Handlungen an. Technische und organisatorische Faktoren werden somit nicht vollständig außer Acht gelassen. Dies belegt, dass die Teilnehmer der Studie sich der Wichtigkeit funktionierender Kontrollmechanismen zwar bewusst sind, jedoch auch wahrnehmen, dass dort weiterer Handlungsbedarf besteht. Wiederum steht diese Einschätzung nicht in Einklang mit der tatsächlichen Bereitschaft zu Investitionen in externe Unterstützung innerhalb der Prävention. Zur Implementierung effektiverer Kontrollmechanismen sind höhere Ausgaben notwendig als die von den Befragten nach eigener Aussage getätigten.

Da gerade der „Faktor Mensch“ eine beachtliche Rolle für die Ausführung wirtschaftskrimineller Handlungen spielt, ist es empfehlenswert, ihn bei der Implementierung präventiver Maßnahmen besonders zu berücksichtigen. Daher sollten spezielle Schulungen durchgeführt werden, um eine Sensibilisierung der Mitarbeiter zu gewährleisten und diesem Faktor entgegenzuwirken.

Laut den befragten Unternehmen ist nahezu allen weiteren abgefragten Faktoren eine nachrangige Bedeutung einzuräumen. Dass 68 Prozent der befragten Unternehmen der mangelhaften Sanktionierung von Fehlverhalten lediglich eine niedrige bzw. sehr niedrige Bedeutung zugestehen, erscheint in diesem Zusammenhang überraschend. Sanktionierung bedeutet schließlich auch Abschreckung. Dennoch belegen die Ergebnisse der Studie, dass in über einem Viertel der Fälle keinerlei Sanktionierung erfolgt.

Fehlende Vorgaben oder Vorbildfunktionen der Geschäftsführung werden von den Befragten nicht als bedeutsame Faktoren für die Begründung einer höheren Gefahr angesehen, von

einer wirtschaftskriminellen Handlung betroffen zu werden. Neben der mangelhaften Sanktionierung gehören auch fehlende Leitlinien des Topmanagements sowie eine nicht vorhandene Vorbildfunktion der Geschäftsführung zu den Faktoren, denen nur von weniger als einem Viertel der Befragten eine hohe Bedeutung beigegeben wird.

Hinsichtlich psychologisch schwieriger Situationen wie Zeit-, Erfolgs- und finanzieller Druck, denen über drei Viertel der Befragten lediglich eine niedrige oder sehr niedrige Bedeutung für die Begehung einer wirtschaftskriminellen Handlung einräumen, verhält es sich ähnlich.

Die Tatsache, dass zwischen fehlenden positiven Vorbildern in der Geschäftsführung und der Neigung, sich wirtschaftskriminell zu betätigen, kein wesentlicher Zusammenhang gesehen wird, ist ein offensichtlicher Widerspruch. Wenn der menschliche Faktor so wichtig erscheint, kann das Verhalten der Führungskräfte aus dem Topmanagement nicht so unwichtig sein wie angegeben. Sind dann die Mitarbeiter auf der gleichen Hierarchieebene die wahren Vorbilder? Sicherlich ist der unmittelbare Kollege die häufigste Bezugsperson und dessen Fehlverhalten dann die Rechtfertigung für eigene Delikte, aber dennoch scheint hier eine Wahrnehmungslücke vorhanden zu sein, zumal die bessere Sensibilisierung als wichtiger Faktor für Wirtschaftskriminalitätsvermeidung angegeben wird. Lassen sich Mitarbeiter heutzutage nicht mehr vom Topmanagement sensibilisieren? Im Zusammenhang mit der Erkenntnis, dass immer mehr Täter der Ebene unter dem Topmanagement entstammen, scheint hier eine beachtliche Gefahrenverschiebung stattzufinden.



Alexander Geschonneck
Partner, Leiter Forensic

Überraschenderweise geben trotz des Stellenwerts menschlicher Eigenschaften 54 Prozent der Befragten an, sie seien nicht der Ansicht, dass eine bessere Sensibilisierung der Mitarbeiter die wirtschaftskriminellen Handlungen hätte verhindern können.

Damit übereinstimmend machen lediglich 24 Prozent der Befragten fehlende Schulungen oder Trainings als bedeutsamen Faktor für die Begehung wirtschaftskrimineller Delikte aus. Schulungen wird somit kein hoher Stellenwert bei der Verhinderung wirtschaftskrimineller Handlungen eingeräumt.

Täter in den eigenen Reihen

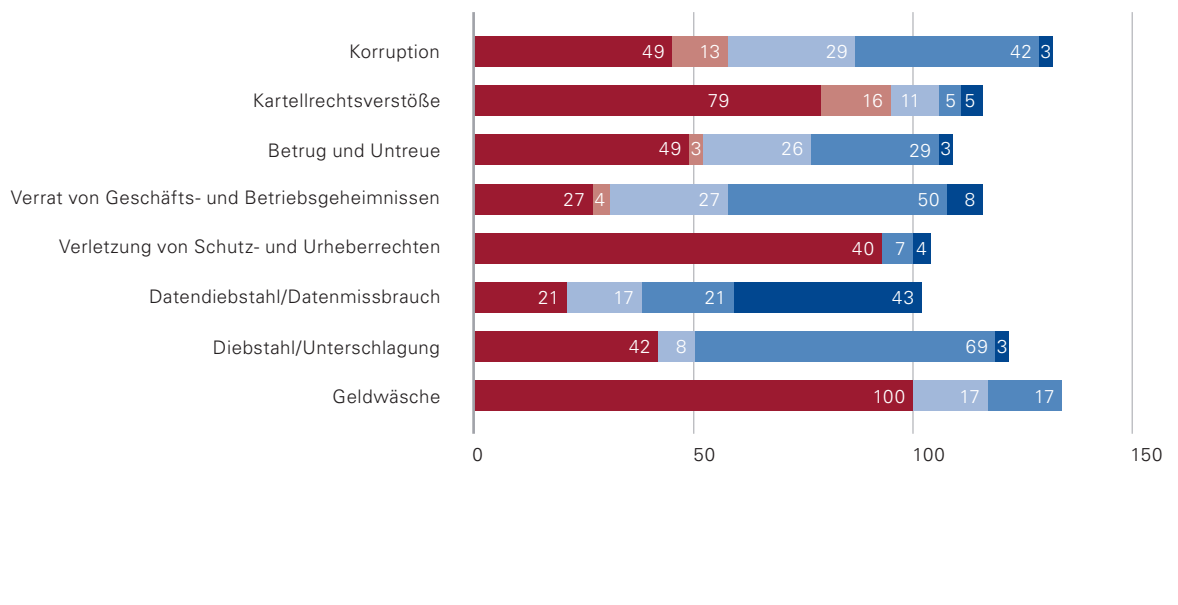
Insgesamt wurden von den betroffenen Unternehmen in den letzten zwei Jahren durchschnittlich rund zwölf Fälle wirtschaftskrimineller Handlungen gemeldet. In 8 Prozent aller angegebenen Fälle können die Befragten keine Angabe dazu machen, ob es sich um einen internen oder einen externen Täter gehandelt hat. Ähnlich zur Vorgängerstudie (60 Prozent) geht das generelle Risiko eher von Innentätern (64 Prozent) aus. Außerdem benennen die Befragten die Unternehmensebene, auf der sich die internen Täter bewegen (Abbildung 11).

Befragt nach den einzelnen Deliktsarten und den tatsächlich festgestellten Tätern wird deutlich, dass die Einschätzung der Innentäterschaft etwas zu hoch gegriffen ist. Im Einklang mit der Vorgängerstudie, gemäß der 56 Prozent der Täter aus dem Unter-

11

Täterherkunft nach Deliktsart

Angaben in Prozent, Mehrfachnennungen möglich



Quelle: KPMG, 2014

nehmen selbst stammen, sind in der aktuellen Studie bei der Betrachtung aller Fälle, in denen die Befragten einen Täter ermitteln konnten, interne Täter mit 55 Prozent in der Überzahl. 45 Prozent der Delikte werden von unternehmensexternen Personen verübt, in 16 Prozent der Fälle sind sowohl interne als auch externe Täter an einer wirtschaftskriminellen Handlung beteiligt.

Innerhalb der Gruppe der internen Täter ist der Prozentanteil von Mitarbeitern unterhalb der Managementebene inzwischen auf 66 Prozent gegenüber 56 Prozent aus der Vorgängerstudie angestiegen. Im Unterschied dazu ist die Anzahl der Täter aus dem Topmanagement deutlich von 18 Prozent auf 5 Prozent gesunken.

92 Prozent der Täter können entweder klar einem bestimmten Bereich des Unternehmens oder der externen Täterschaft zugeordnet werden. Die einzige Ausnahme zeigt sich in den Ergebnissen zu Datendiebstahl und Datenmissbrauch. Diesbezüglich geben 43 Prozent der Befragten an, dass sie nicht wissen, welchem Ressort der Täter angehörte. Diese Aussagen bestätigen, dass die Erfassung der Täter in derartigen Fällen große Schwierigkeiten bereitet, da dieses Feld umfassende Möglichkeiten bietet, anonym bzw. unentdeckt zu bleiben.

Unternehmen müssen weiterhin daran arbeiten, sich im Bereich des Datenschutzes und der Datensicherheit besser aufzustellen, um eventuelle Verstöße vermeiden zu können oder einen effektiveren Umgang damit zu gewährleisten.

Es ist bemerkenswert: Bei Delikten in Zusammenhang mit Daten, wie Datendiebstahl und Datenmissbrauch, oder auch beim Verrat von Geschäfts- und Betriebsgeheimnissen schätzen die befragten Unternehmen das Risiko, künftig selbst als Opfer betroffen zu sein, als hoch oder sehr hoch ein. Zugleich geben die Unternehmen, die bereits Opfer eines solchen Delikts waren, an, dass sie Schwierigkeiten hatten, den Täter zu ermitteln bzw. diesen nicht ermitteln konnten. Hieraus lässt sich der Schluss ableiten, dass nicht nur die Maßnahmen und Prozesse zur Prävention der Verbesserung bedürfen, sondern auch jene zur Aufdeckung und Aufklärung derartiger Sachverhalte. Angesichts des komplexen Zusammenspiels von juristischen und technischen Aspekten, die bei Datenschutzdelikten und Geheimnisverrat eine Rolle spielen, erwarte ich hier in der Zukunft einen vermehrten Einsatz externer Spezialisten.



Barbara Scheben
Partner, Forensic

4 Wirtschaftskriminalität in einzelnen Sektoren – eine branchenspezifische Betrachtung

Die Investitionsbereitschaft in externe Unterstützung beim Umgang mit wirtschaftskriminellen Handlungen variiert je nach Branche zum Teil stark. Des Weiteren zeigt sich, dass abhängig von der jeweiligen Branche unterschiedliche Bereiche der Unternehmen von wirtschaftskriminellen Sachverhalten betroffen sind.

Betrachtet man die befragten Unternehmen vor dem Hintergrund ihrer jeweiligen Geschäftstätigkeit (Abbildung 15, Seite 37), werden branchenspezifische Unterschiede ersichtlich. Im Folgenden sind einige Branchen gesondert dargestellt.

Handel

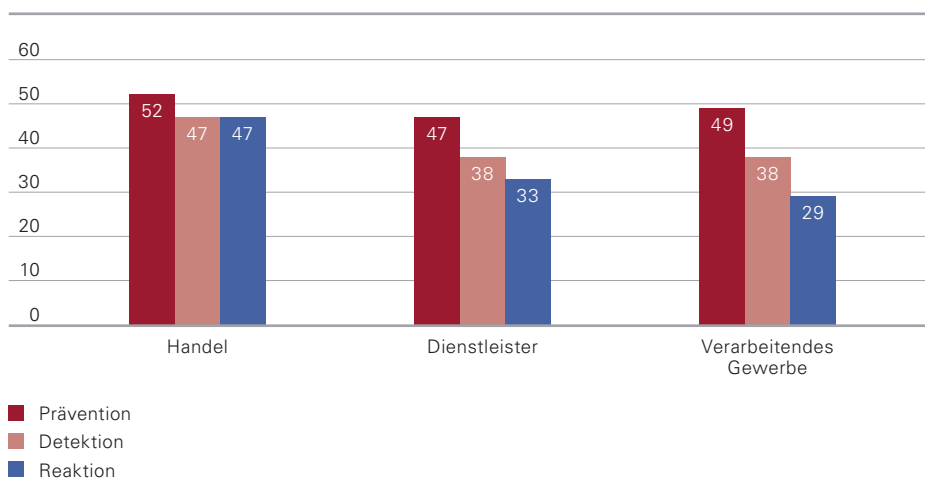
Die Angaben der 81 Befragten aus dem Bereich Handel weichen am deutlichsten von jenen anderer Branchen sowie von den Ergebnissen der Gesamtbetrachtung ab. Dies zeigt sich beispielsweise an der im Vergleich geringen Investitionsbereitschaft.

In der Betrachtung des Risikos, Opfer von Wirtschaftskriminalität zu werden, gleichen sich Industrie, Dienstleister und Handel. Allerdings gibt es bezüglich einzelner Deliktsarten Ausnahmen, bei denen Befragte der Handelsbranche von geringeren Risiken für sich ausgehen: Zum Beispiel schätzen lediglich 35 Prozent des Handels das Risiko eines Kartellrechtsverstoßes als hoch bzw. sehr hoch ein gegenüber 39 Prozent der Industrie und 45 Prozent der Dienstleister.

Unterschiede bei der tatsächlichen Betroffenheit der vergangenen zwei Jahre, die diese im Vergleich weniger gravierend ausfallende Risikoeinschätzung rechtfertigen würden, sind nicht ersichtlich. Darüber hinaus wollen die Befragten der Handelsbranche deutlich weniger in externe Unterstützung bei Prävention, Detektion und Reaktion investieren (Abbildung 12). In jeder dieser Phasen sind rund 50 Prozent der hier Befragten gewillt, maximal 10.000 Euro zu diesem Zweck einzusetzen. Die Differenz zu Industrie und Dienstleistern hinsichtlich der Investitionsbereitschaft wird im Verlauf der Phasen immer deutlicher. In der Reaktionsphase geben jeweils rund 70 Prozent der Befragten der anderen Branchen an, mehr als 10.000 Euro investieren zu wollen, und sind daher eher bereit, Investitionen in größerem Umfang zu tätigen.

12 Investitionsbereitschaft bis zu 10.000 Euro nach Branche

Angaben in Prozent



Quelle: KPMG, 2014

Diese im Vergleich geringe Bereitschaft, Ausgaben zum Zweck des Umgangs mit wirtschaftskriminellen Handlungen zu tätigen, wird dadurch untermauert, dass die Befragten der Handelsbranche in der Regel einzelne Präventionsmaßnahmen im Unternehmen zu einem geringeren Anteil umsetzen als die übrigen Teilnehmer der Studie. Hier besteht Nachholbedarf. Zudem rechnen zwei Drittel der Befragten dieser Branche damit, dass ihr Compliance-Budget in den kommenden zwei Jahren gleich bleiben wird. Der Weg zu größeren Ausgaben für Schutzinstrumente scheint somit versperrt.

In der Aufklärungsphase zeigt sich, dass bei Vertretern der Handelsbranche in fast drei Vierteln der Fälle Strafverfolgungsbehörden mit der Aufklärung befasst sind (lediglich zu rund 50 Prozent in anderen Branchen). Es fällt außerdem auf, dass die operative Aufklärung wesentlich seltener unter Einsatz moderner elektronischer Mittel abläuft; weniger als 30 Prozent der Befragten bedienen sich elektronischer Daten- oder E-Mail-Analysen. Hintergrundrecherchen zu Geschäftspartnern werden dafür von fast zwei Dritteln der Befragten des Handels zur operativen Aufklärung herangezogen und somit deutlich häufiger als bei Dienstleistern (55 Prozent) und insbesondere der Industrie (50 Prozent).

Bezüglich der einzelnen Abteilungen eines Unternehmens innerhalb des Handels ist eine branchenspezifische Besonderheit zu erkennen. In zwei Dritteln der Fälle war der Vertrieb von wirtschaftskriminellen Handlungen tangiert, zu jeweils rund einem Drittel außerdem die Bereiche Einkauf und Lager/Logistik.

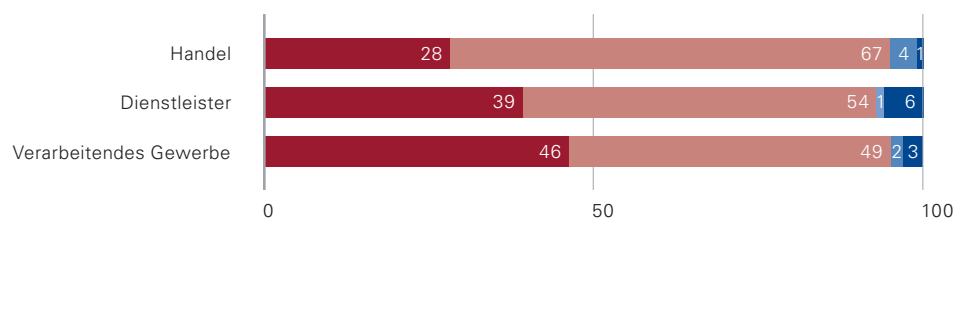
Abschließend ist zu konstatieren, dass die Vertreter der Handelsbranche die Wichtigkeit einzelner risikoerhöhender Faktoren in erheblichem Maße anders bewerten als die anderen Teilnehmer der Studie. Faktoren wie der finanzielle Druck, dem 44 Prozent dieser Branche eine hohe bzw. sehr hohe Bedeutung zuweisen, sowie der Erfolgsdruck nehmen eine wesentlich gewichtigere Rolle ein, wohingegen der insgesamt als am höchsten eingeschätzte Faktor des mangelnden Unrechtsbewusstseins im Handel einiges an Bedeutung verliert (48 Prozent gegenüber 64 Prozent in der Gesamtauswertung).

Industrie

Bei der Betrachtung der Antworten von 184 Befragten der Industrie zeigen sich bezüglich der tatsächlichen Betroffenheit keine markanten Branchenunterschiede, abgesehen davon, dass prozentual deutlich seltener die Delikte Betrug und Untreue verübt werden (45 Prozent) als im Handel (63 Prozent) und bei Dienstleistern (59 Prozent).

13

Entwicklung des Compliance-Budgets in den nächsten zwei Jahren nach Branche Angaben in Prozent



Quelle: KPMG, 2014

In der Risikoeinschätzung liegen die Industrie und der Dienstleistungssektor meistens auf einer Linie, jedoch zeigt sich insbesondere für die Industrie die Tendenz, dass in den Medien im Fokus stehende Delikte mehr gefürchtet werden. Entsprechend der Gesamtheit der Angaben ist erkennbar, dass die tatsächliche Betroffenheit dies nicht rechtfertigt. Selbiges gilt auch für die Einschätzung des Trends in den kommenden zwei Jahren.

Die Industrie ist im Vergleich zu den anderen Branchen bereit, die höchsten Ausgaben für externe Unterstützung beim Umgang mit einer wirtschaftskriminellen Handlung zu tätigen. In jeder Phase stellen industrielle Unternehmen den größten Anteil an Unternehmen, die mehr als 100.000 Euro investieren würden (beispielsweise in der Reaktionsphase 11 Prozent gegenüber 2 Prozent des Handels und 4 Prozent der Dienstleister).

In Einklang mit dem Investitionswillen sind die Befragten aus diesem Sektor wesentlich optimistischer bezüglich der Entwicklung des Compliance-Budgets (Abbildung 13, Seite 33). Fast die Hälfte ist der Ansicht, dass das Budget in den kommenden zwei Jahren steigen wird (Dienstleister 39 Prozent, Handel 28 Prozent). Somit scheint die Industrie zukünftig weiterhin gewillt, die im Vergleich höchsten Ausgaben zu tätigen, um sich präventiv vor Wirtschaftskriminalität zu schützen.

Im Rahmen der Aufklärung zeigt sich die Tendenz, dass sie in der Industrie im Vergleich deutlich öfter unter Einsatz moderner Methoden oder elektronischer Daten- und E-Mail-Analysen abläuft. Fast die Hälfte der Befragten der Industrie bedient sich dieser Methoden, aber beispielsweise weniger als 30 Prozent des Handels. Dafür werden die „klassischen Methoden“ der Auswertung physischer Unternehmensakten und der Hintergrundrecherchen seltener angewandt.

Nahezu vollständig in Einklang mit den Gesamtergebnissen stehen die Angaben der betroffenen Unternehmen der Industrie bezüglich der Bereiche Ver-

trieb und Einkauf, welche die häufigsten Angriffspunkte wirtschaftskrimineller Handlungen waren. Lediglich die für diese Branche sehr wichtige Produktion ist mit 36 Prozent im Vergleich zu den Gesamtergebnissen (26 Prozent) mehr betroffen.

Dienstleister

Die Ergebnisse der Dienstleistungsbranche weichen insgesamt am geringfügigsten von den Gesamtergebnissen der Studie ab.

Die Dienstleistungsbranche ist bei der Mehrzahl der Deliktsarten, aber insbesondere bei spezifischen Delikten, die meistbetroffene Branche, auch wenn dies in den Gesamtzahlen nicht eindeutig zum Ausdruck kommt. Gerade von Korruption sind Vertreter dieser Branche deutlich häufiger betroffen als die anderen Befragten, nämlich zu 31 Prozent (Industrie 22 Prozent, Handel 7 Prozent).

Bei den Fragen zur Investitionsbereitschaft und Risikoeinschätzung ist die Differenz zwischen den Gesamtergebnissen und den Ergebnissen dieser Branche nicht nennenswert.

Wie in der Industrie und dem Handel ist der Vertrieb auch im Dienstleistungssektor der meistbetroffene Bereich im Unternehmen (39 Prozent). Im Vergleich zu den anderen Branchen ist der Vertrieb prozentual dennoch erheblich seltener tangiert (Abbildung 14). Demgegenüber sind folgende abgefragte Bereiche in mindestens 18 Prozent der Fälle betroffen: Einkauf, Finanz- und Rechnungswesen, Produktion, Lager/Logistik, Geschäftsführung und vertriebsorientierte Beratung. Dienstleister müssen sich daher in hohem Maße in diversen Bereichen gegen wirtschaftskriminelle Handlungen wappnen und können sich nicht auf spezifische Kernbereiche konzentrieren. Zudem dürfte es nicht unwahrscheinlich sein, dass im Dienstleistungssektor mehrere Bereiche des Unternehmens simultan von der gleichen wirtschaftskriminellen Handlung betroffen sind.

Auch dies kann Ursache dafür sein, dass gemäß den Angaben der betroffenen Unternehmen der Zeitraum zwischen Begehung und Entdeckung der Tat in der Dienstleistungsbranche am größten ist. 22 Prozent sagen aus, dass zwei bis fünf Jahre vergangen seien. Gegenüber rund 80 Prozent im Handel und in der Industrie geben lediglich rund zwei Drittel der betroffenen Dienstleister an, dass dieser Zeitraum sich über weniger als zwei Jahre erstreckt hat.

Ein weiterer Grund dafür kann sein, dass lediglich in 47 Prozent der Fälle der Zufall die maßgebliche Rolle bei der Entdeckung einer wirtschafts-

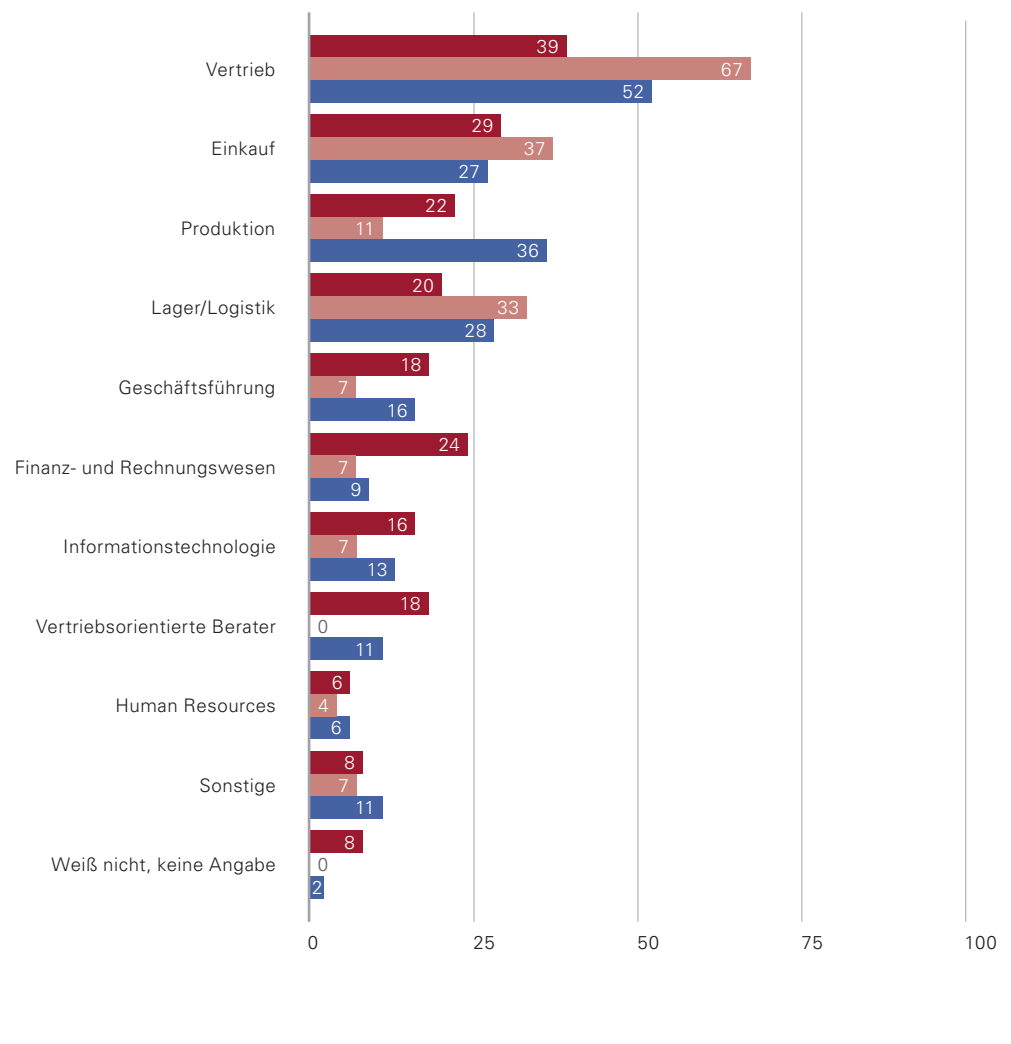
kriminellen Handlung im Dienstleistungssektor spielte. In den anderen Branchen lässt sich jeweils in rund 60 Prozent der Fälle die Entdeckung auf „Kommissar Zufall“ zurückführen.

Im Rahmen der risikoerhöhenden Faktoren stimmen das Gesamtergebnis und die Ergebnisse der Befragung der Teilnehmer aus der Dienstleistungsbranche ungefähr überein, wobei sie sowohl dem mangelnden Unrechtsbewusstsein (73 Prozent hohe/sehr hohe Bedeutung) als auch fehlenden Schulungen (31 Prozent) eine etwas höhere Bedeutung einräumen als die Befragten anderer Branchen.

14

Betroffene Bereiche nach Branche

Angaben in Prozent, Mehrfachnennungen möglich



Quelle: KPMG, 2014



Über diese Studie

In der diesjährigen Studie wurden 400 repräsentativ nach Branche⁸, Mitarbeiterzahl und Umsatz ausgewählte Unternehmen zu ihren Erfahrungen im Feld der Wirtschaftskriminalität befragt.

Wie in den vorherigen Studien zur Wirtschaftskriminalität 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 sind gegenüber KPMG nicht bekannt gemacht worden. Die Erfahrung hat gezeigt, dass aufgrund der Komplexität des Themas von den Teilnehmern der Studie eine persönliche Befragung erwünscht ist. Die Interviews wurden im April/Mai 2014 durchgeführt.

Der standardisierte Fragebogen orientiert sich an der Struktur der Vorgängerstudie mit Anpassungen bezüglich

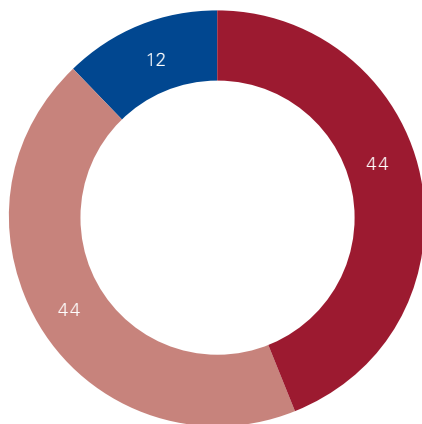
der diesjährigen Schwerpunkte der Studie und ohne den Fokus auf kleine und mittlere Unternehmen. Außerdem soll, wie bei den Vorgängerstudien, eine Vergleichbarkeit zu der ebenfalls von KPMG veröffentlichten „e-Crime-Studie“ ermöglicht werden.

Der Fragebogen wurde vom Bereich Forensic der KPMG AG Wirtschaftsprüfungsgesellschaft konzipiert.

15

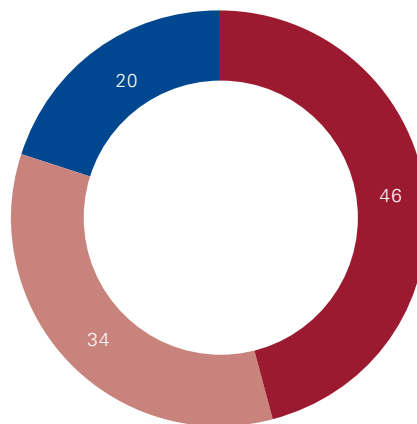
Eckdaten der Studie

Umsatz der befragten Unternehmen



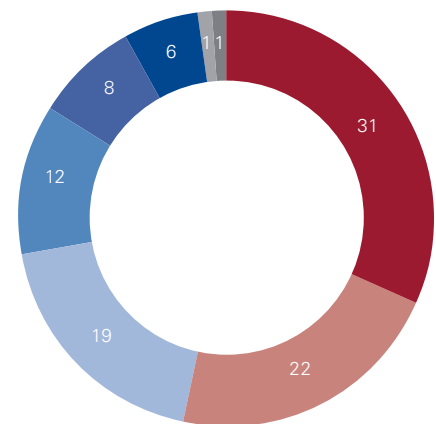
- Unter 250 Millionen Euro
- Von 250 Millionen bis 3 Milliarden Euro
- Über 3 Milliarden Euro

Branchen



- **Industrie**
Automobilindustrie, Chemie und Pharma, Energie und Rohstoffe, industrielle Produktion, Technologie
- **Dienstleister**
Gesundheitswirtschaft, Kreditinstitute, Medien und Telekommunikation, öffentlicher Sektor, Versicherungen
- **Handel**
Handel und Konsumgüter

Interviewpartner



- Mitglieder Vorstand/Geschäftsführung
- Leitung Controlling/Rechnungswesen
- Leitung Recht
- Compliance Officer
- Leitung Interne Revision
- Leitung Risikomanagement
- Leitung Unternehmenssicherheit
- Leitung Personal

⁸ Für die Aufteilung in die drei betrachteten Branchen wurde die im Grafikteil „Branchen“ dargestellte Zuteilung gewählt (Abbildung 15). Die Prozentangaben sind auf ganze Zahlen gerundet.

Über uns

Der Bereich Forensic von KPMG erbringt Leistungen rund um die Prävention, Aufdeckung und Aufklärung von Wirtschaftskriminalität und anderen Bedrohungslagen. Das Leistungsspektrum umfasst die folgenden Solutions:

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 Schadensbeurteilung, 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 der 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- bzw. datenbezogenen Sicherheitsvorfällen.

Des Weiteren geben wir Hilfestellung bei der Optimierung des Zusammenspiels technologischer, organisatorischer und datenschutzrechtlicher Herausforderungen im Zusammenhang mit Cyber Security Incidents 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.

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

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

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-informations-sicherheitszertifiziert.

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft

Alexander Geschonneck

Partner, Leiter Forensic
T +49 30 2068-1520
ageschonneck@kpmg.com

An dieser Studie haben mitgewirkt:

Nina Kiehne

Senior Manager, Consulting
T +49 89 9282-4765
nkiehne@kpmg.com

Marc Oliver Scheben

T +49 221 2073-1644
mscheben@kpmg.com

www.kpmg.de/forensic



Follow us!

www.kpmg.de/twitter_forensic

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.

© 2014 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity“ sind eingetragene Markenzeichen von KPMG International.