KPMG

Tatort Deutschland

Wirtschaftskriminalität in Deutschland 2016
Studie

* Unter Wirtschaftskriminalität werden in dieser Studie in Anlehnung an die abgefragten Deliktsarten die Tatbestände Diebstahl und Unterschlagung, Betrug und Untreue, Korruption, Kartellrechtsverstöße, Verrat von Geschäfts- und Betriebsgeheimnissen, Verletzung von Schutz- und Urheberrechten, Datendiebstahl und -missbrauch, Manipulation jahresabschluss-relevanter Informationen sowie Geldwäsche verstanden.

Vorwort

Liebe Leserinnen und Leser,

Wirtschaftskriminalität ist in aller Munde. Kaum eine Woche vergeht ohne spektakuläre Fälle, keine Branche ist davor gefeit: die Automobilindustrie, das Finanzwesen, der Sport – hier ist alles dabei, woran wir Deutschen seit Jahrzehnten glauben und worauf wir vertrauen. Wird dieses Vertrauen durch die wirtschaftskriminellen Vorkommnisse beschädigt?

Um dieser Frage nachzugehen, wollen wir uns in unserer seit nunmehr 17 Jahren erscheinenden Studie zur Wirtschaftskriminalität in Deutschland in diesem Jahr nicht nur dem bekannten Phänomen der Wirtschaftskriminalität* widmen, sondern auch deren Auswirkungen auf die Reputation eines Unternehmens betrachten: Wie wirken sich Reputationsschäden aus? Sind Unternehmen in der Lage, diese Schäden richtig zu klassifizieren und zu quantifizieren? Und würden Unternehmen mit einem überführten Täter wieder zusammenarbeiten oder harte Auflagen verlangen? Hier zeigen sich unter anderem auch die Ethik und die Moral in der Unternehmensführung.

Wie bei den vorhergehenden Studien haben wir auch in diesem Jahr TNS Emnid beauftragt, 500 Unternehmen telefonisch zu befragen. Die Ergebnisse zeichnen einmal mehr ein komplexes Bild. Während nämlich einige Ergebnisse zum Denken und Handeln auffordern sollten, machen andere positive Tendenzen deutlich. So betrachten Unternehmen ihre Reaktionsfähigkeit auf wirtschaftskriminelle Handlungen zunehmend kritisch und erkennen Versäumnisse beim Umgang mit Wirtschaftskriminalität. Gleichzeitig verfolgen die Befragten im Vergleich zu vorherigen Studien einen deutlich breiter angelegten Präventionsansatz. Hier setzt unsere These an: Nur wenn sich Unternehmen mit eigenen Schwachstellen auseinandersetzen und diese angehen, können sie sich angemessen gegen wirtschaftskriminelle Handlungen wappnen.

Ich wünsche Ihnen eine spannende und erkenntnisreiche Lektüre.

Alexander Geschonneck
Partner, Leiter Forensic
KPMG in Deutschland

Geleitwort

Compliance gewinnt weltweit an Bedeutung und nimmt mittlerweile in der öffentlichen Diskussion einen hohen Stellenwert ein. Gerade die Privatwirtschaft steht im Fokus: Regulierungsbehörden, Geschäftspartner und Kunden verlangen nach mehr Transparenz, korrekten Rechenschaftsberichten und aufrechtem Handeln. Die vorliegende KPMG-Studie zur Wirtschaftskriminalität zeigt, dass es noch viel zu tun gibt. Doch mit der richtigen Strategie eröffnet das Thema Compliance für Unternehmen viele Chancen.

Denn Geld, das in Compliance und Korruptionsprävention investiert wird, zahlt sich aus. Die Stärkung von Integrität als Grundsatz der Unternehmensführung führt zu nachhaltigen Reputationsgewinnen bei Kunden, Geschäftspartnern und nicht zuletzt auch bei den Angestellten selbst. Wie die vorliegende Studie beweist, erhöht Compliance die Identifikation der Mitarbeiter mit ihrem Unternehmen. Gerade für die Generation Y trägt eine Kultur der Integrität wesentlich zur Arbeitsmotivation bei. Compliance leistet somit auch einen wichtigen Beitrag zur Anwerbung von Talenten sowie zur Innovationskraft und Wettbewerbsfähigkeit des Unternehmens.

Gegen Korruption und Wirtschaftskriminalität muss es im Unternehmen eine klare Linie geben. Die Erfahrung zeigt aber auch, dass Compliance mehr ist als nur Regeln. Denn das Regelwerk muss Teil der Unternehmenskultur sein und in die Praxis umgesetzt werden. Um langfristig eine erfolgreiche Compliance-Kultur aufzubauen, empfiehlt es sich, regelmäßige Aktivitäten im Bereich Korruptionsprävention durchzuführen. Collective Action-Initiativen eröffnen hierbei eine gute Möglichkeit, in den Erfahrungs- und Wissensaustausch mit anderen Unternehmen zu treten. Die Bereitschaft, sich unlauteren Praktiken und Wirtschaftskriminalität entgegenzustellen, ist in der heutigen Zeit groß. Nun liegt es an Staat, Wirtschaft und Zivilgesellschaft, zusammenzuarbeiten und Integrität in Unternehmen, bei ihren Geschäftspartnern und weiteren beteiligten Akteuren im Wirtschaftssystem zu fördern.

Noor Naqschbandi, Leiter, Allianz für Integrität
Noor Naqschbandi ist Leiter der wirtschaftsgetriebenen Multi-Stakeholder-Initiative Allianz für Integrität, die in Brasilien, Ghana, Indien, Indonesien sowie den jeweiligen Regionen aktiv ist. Noor Naqschbandi ist zudem zuständig für das Thema Antikorruption und Compliance im Deutschen Global Compact Netzwerk (DGCN).

Inhaltsverzeichnis

Executive Summary

Gesamtentwicklung

Unverändert gegenüber 2014 ist jedes dritte deutsche Unternehmen von Wirtschaftskriminalität betroffen. Wie hoch der durch Wirtschaftskriminalität entstandene monetäre Schaden ist, können Unternehmen häufig nicht beziffern.

» In den vergangenen zwei Jahren war mehr als jedes dritte der befragten Unternehmen von Wirtschaftskriminalität betroffen (36 Prozent), von den großen Unternehmen sogar fast die Hälfte (45 Prozent).

» Je nach Unternehmensgröße sind unterschiedliche Bereiche und Abteilungen betroffen: Insbesondere große Unternehmen verzeichnen einen Anstieg wirtschaftskrimineller Handlungen im Finanz- und Rechnungswesen (2016: 31 Prozent, 2014: 13 Prozent). Bei kleinen Unternehmen sind IT-Abteilungen erheblich stärker als früher betroffen (2016: 33 Prozent, 2014: 9 Prozent).

» Unternehmen können die Schäden im Vergleich zu 2014 seltener beziffern. Bei der Mehrzahl der Deliktsarten kann über ein Viertel der Unternehmen keine Angaben zu den entstandenen Schäden machen. Dabei ist dies die Voraussetzung, um die tatsächliche Gefahrenlage realistisch zu bewerten und betriebswirtschaftlich sinnvolle Präventionsmaßnahmen zu planen und umzusetzen.

Reputationsrisiken

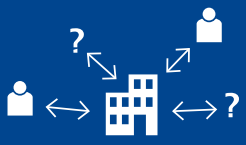
Reputationsrisiken sollten nicht unterschätzt werden: Ein Großteil der Befragten misstraut Unternehmen, die Täter wirtschaftskrimineller Handlungen waren.

» Das Risiko eines Reputationsschadens durch wirtschaftskriminelle Handlungen oder Compliance-Verstöße schätzen die Unternehmen mit einem Anteil von 27 Prozent ähnlich hoch ein wie das Risiko, überhaupt von Wirtschaftskriminalität betroffen zu sein. Einen tatsächlich erlittenen Reputationsschaden geben dabei 13 Prozent der Unternehmen an.

» Gleichzeitig sind Unternehmen kaum in der Lage, das monetäre Ausmaß dieser Reputationsschäden zu erfassen. Dies spricht dafür, dass es zwar eine grundlegende Sensibilität für das Thema gibt, die Unternehmen jedoch unsicher sind, wie sie mit Reputationsschäden umgehen und wie sie diese quantifizieren sollen. Eine Ursache ist möglicherweise in der nicht eindeutigen Messbarkeit dieser Schäden zu suchen.

» Mehr als die Hälfte der Befragten macht strenge Auflagen zur Voraussetzung, um weiterhin mit Unternehmen zusammenzuarbeiten, die Täter wirtschaftskrimineller Handlungen waren. Dazu gehört zum Beispiel, dass der jeweilige Sachverhalt durch eine unabhängige Stelle aufgeklärt bzw. bewertet wird oder dass ein Compliance Management-System eingerichtet wird. 35 Prozent der Befragten schließen Geschäftsbeziehungen mit diesen Unternehmen sogar grundsätzlich aus. Lediglich sechs Prozent der Befragten sehen die Geschäftsbeziehung auch bei Wirtschaftskriminalität unbelastet.

Investitionsbereitschaft



Unternehmen suchen immer öfter externe Unterstützung. Die Investitionsbereitschaft ist aber nicht in gleichem Maße vorhanden.

- Um Wirtschaftskriminalität in den eigenen Reihen zu bewältigen, greifen immer mehr Unternehmen auf die Unterstützung externer Dienstleister zurück.
- Die Investitionsbereitschaft in externe Unterstützung entspricht diesem Trend allerdings nicht: So ist mindestens ein Drittel der Befragten nicht bereit, für Prävention, Aufklärung und Reaktion jeweils mehr als 10.000 Euro in externe Dienstleister zu investieren.
- Wie 2014 wird nach wie vor eher in die Reaktion als in die Prävention investiert – was dem ökonomischen Prinzip widerspricht, denn die für präventive Maßnahmen notwendigen Investitionen dürften oftmals geringer ausfallen als die mit Wirtschaftskriminalität einhergehenden Schäden.

Reaktionsversäumnisse

Unternehmen setzen sich zunehmend kritisch mit ihrer Reaktionsfähigkeit auf Wirtschaftskriminalität auseinander. Versäumnisse werden vor allem in der unternehmensinternen Kommunikation und Koordination gesehen.

- 63 Prozent der durch dolose Handlungen Betroffenen gestehen Versäumnisse bei der Reaktion auf Wirtschaftskriminalität ein. Im Vergleich dazu gaben 2014 lediglich vier Prozent der Befragten an, nicht angemessen auf Wirtschaftskriminalität reagiert zu haben.
- Die unternehmensinterne Kommunikation der Sachverhalte (27 Prozent), die Beweissicherung (24 Prozent) sowie die Koordination bzw. Abstimmung des weiteren Vorgehens (23 Prozent) bereiten Unternehmen die größten Schwierigkeiten.
- Immer klarer sehen Unternehmen Nachholbedarf im Umgang mit Wirtschaftskriminalität. Entsprechend sollten vermehrt Ressourcen in Prävention und Reaktionsfähigkeit investiert werden.

Aufklärungsmaßnahmen

Datenanalysen entwickeln sich zu einem vierten Standbein bei der Aufklärung von Wirtschaftskriminalität. Kleine Unternehmen wenden diese Methode allerdings noch deutlich seltener an als große.

- Neben den klassischen Aufklärungsmaßnahmen Mitarbeiterbefragung (75 Prozent), Hintergrundrecherche (61 Prozent) und Auswertung von Unternehmensakten (59 Prozent) greifen mittlerweile 57 Prozent der Unternehmen bei der Aufklärung wirtschaftskrimineller Sachverhalte auf Datenanalysen zurück.
- Auch E-Mail-Reviews wurden von großen und mittleren Unternehmen in mehr als der Hälfte der Fälle durchgeführt. Kleine Unternehmen verlassen sich eher noch auf die klassischen Aufklärungsmaßnahmen – eventuell weil ihnen das technische Know-how bzw. die Mittel und Kapazitäten fehlen, um solche Tools einzusetzen.
- Angesichts der zunehmenden Digitalisierung und der Bedrohung durch e-Crime sind moderne Aufklärungsmaßnahmen allerdings zu empfehlen, da viele Delikte ohne digitale Aufklärungsmaßnahmen nicht mehr wirksam bekämpft werden können.

1. Aktuelle Entwicklungen der Wirtschaftskriminalität in Deutschland

Risikoeinschätzung und tatsächliche Betroffenheit von wirtschaftskriminellen Handlungen in der deutschen Wirtschaft haben sich gegenüber 2014 kaum verändert. Veränderungen ergeben sich allerdings, wenn man deliktsbezogene Betroffenheit und die betroffenen Unternehmensbereiche betrachtet.

Diskrepanz zwischen allgemeiner und eigener Risikoeinschätzung

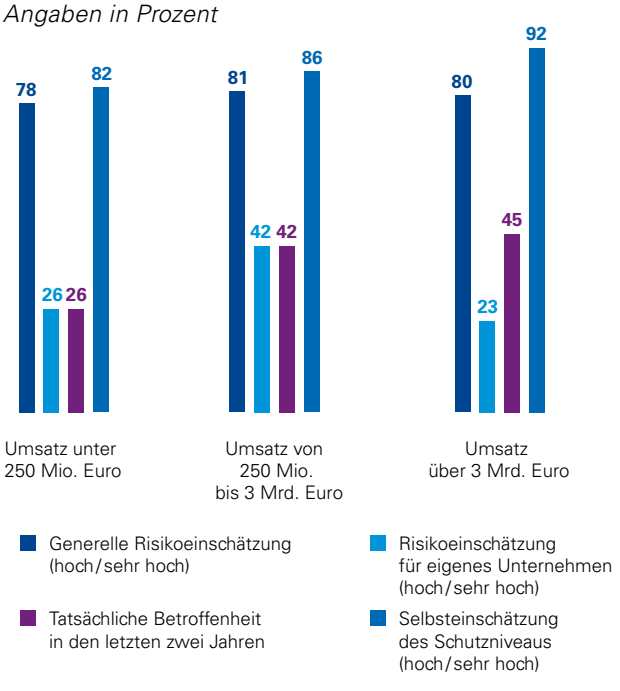
Die Einschätzung des allgemeinen Risikos von Wirtschaftskriminalität weicht stark von der Risikoeinstufung des eigenen Unternehmens ab. 80 Prozent der 500 befragten Unternehmen sehen ein hohes bzw. sehr hohes Risiko für deutsche Unternehmen, von wirtschaftskriminellen Handlungen betroffen zu sein. Bezogen auf das eigene Unternehmen sehen allerdings lediglich 32 Prozent der Befragten ein solches Risiko (Abb. 1). Diese Ambivalenz haben wir bereits in den vorangegangenen Studien festgestellt.

> Im Folgenden werden die befragten Unternehmen zur Vereinfachung in die Kategorien „groß", „mittel" und „klein" eingeteilt. Unternehmen mit einem Umsatz von mehr als drei Milliarden Euro werden als „groß" bezeichnet. In der Kategorie „mittel" finden sich die Unternehmen mit einem Umsatz zwischen 250 Millionen und drei Milliarden Euro. Unternehmen mit einem Umsatz von weniger als 250 Millionen Euro werden der Kategorie „klein" zugeordnet.

Im Vergleich zu den Studienergebnissen von 2014 zeigt sich allerdings, dass das wahrgenommene Risiko in Bezug auf das eigene Unternehmen nicht mehr zwangsläufig mit zunehmendem Umsatz steigt. Lediglich 23 Prozent der Befragten aus großen Unternehmen (gegenüber 40 Prozent im Jahr 2014) sehen sich einem großen oder sehr großen Risiko ausgesetzt. Eine tendenziell zunehmende Risikowahrnehmung ist bei den kleinen und mittleren Unternehmen zu verzeichnen: 26 Prozent (2014: 23 Prozent) der kleinen Unternehmen sehen ein hohes oder sehr hohes Risiko für das eigene Unternehmen, von Wirtschaftskriminalität betroffen zu sein. 42 Prozent (2014: 35 Prozent) der mittleren Unternehmen teilen diese Einschätzung.

Der Rückgang der Risikowahrnehmung bei den großen Unternehmen lässt darauf schließen, dass sich diese besser gegenüber wirtschaftskriminellen Handlungen gewappnet sehen als vor zwei Jahren: Wie schon 2014 zeigen sich große Teile der Befragten zufrieden mit dem eigenen Schutzniveau. Über 80 Prozent aller Befragten, bei großen Unternehmen sogar 92 Prozent, sehen sich gut oder sehr gut vor wirtschaftskriminellen Handlungen geschützt. Lediglich zwei Unternehmen aus dem Kreis der 500 Befragten gaben an, sehr schlecht gegen wirtschaftskriminelle Handlungen geschützt zu sein.

Abb. 1: Einschätzung des allgemeinen Risikos, Selbsteinschätzung des eigenen Schutzes und tatsächliche Betroffenheit von Wirtschaftskriminalität
Angaben in Prozent



Quelle: KPMG, 2016

Ungeachtet des hohen „gefühlten" Schutzniveaus stellt sich die tatsächliche Betroffenheit der Unternehmen im Wesentlichen unverändert gegenüber 2014 dar. In den vergangenen zwei Jahren war etwas mehr als jedes dritte befragte Unternehmen von Wirtschaftskriminalität betroffen (36 Prozent); bei großen Unternehmen gilt dies für 45 Prozent. Hier lag die Betroffenheitsrate vor zwei Jahren noch bei 53 Prozent. Jedoch herrscht bei den großen Unternehmen eine spürbare Diskrepanz zwischen eigener Risikowahrnehmung und tatsächlicher Betroffenheit. Nur 23 Prozent der großen Unternehmen schätzen das Risiko, von Wirtschaftskriminalität betroffen zu sein, als hoch oder sehr hoch ein. Gleichzeitig waren aber 45 Prozent der großen Unternehmen in den letzten beiden Jahren von wirtschaftskriminellen Handlungen betroffen. Große Unternehmen wähnen sich also in trügerischer Sicherheit.

Vergleicht man die Wahrnehmung des eigenen Risikos und die tatsächliche Betroffenheit in den vergangenen zwei Jahren bei kleinen und mittleren Unternehmen, stellt sich die Situation anders dar: Die Befragten dieser Unternehmenskategorien scheinen ihr Risikoniveau zutreffend einzuordnen. Bedeuten diese Ergebnisse nun, dass lediglich Betroffenheit und Risikowahrnehmung bei großen Unternehmen divergieren und dass die restlichen Befragten einen angemessenen Überblick über ihre Risikosituation und Betroffenheit haben? Die Ergebnisse dieser Studie legen eine andere Interpretation nahe. Denn hinsichtlich der operativen Prävention und Aufdeckung sowie der ergriffenen Maßnahmen[1] zeigt die Studie, dass gerade in kleinen und mittleren Unternehmen oft noch keine ausreichenden Ressourcen und Vorkehrungen zur Aufdeckung von Wirtschaftskriminalität vorhanden sind. Die tatsächliche Betroffenheit dieser Unternehmen könnte also deutlich höher liegen.

Ein weiteres interessantes Ergebnis ist der Unterschied zwischen der Selbsteinschätzung des Schutzes vor Wirtschaftskriminalität und der tatsächlichen Betroffenheit. Wie schon 2014 gibt es nur marginale Unterschiede zwischen den betroffenen Unternehmen, die ihren eigenen Schutz als gut oder sehr gut einschätzen (35 Prozent Betroffenheit) und solchen, die ihn als schlecht bzw. sehr schlecht einstufen (38 Prozent Betroffenheit). Wie ist dieser geringe Unterschied zu erklären? Das sogenannte Kontrollparadoxon könnte einen Erklärungsansatz liefern: Ist ein befragtes Unternehmen tatsächlich besser vor wirtschaftskriminellen Handlungen geschützt, dürfte das in der Regel zugleich bedeuten, dass effektivere Aufdeckungsmaßnahmen zur Verfügung stehen. Somit würden tatsächlich mehr Delikte erfasst, als es bei einem Unternehmen mit geringeren Schutzmechanismen der Fall wäre.

Bei der Frage nach dem erwarteten Risiko, in den kommenden zwei Jahren von wirtschaftskriminellen Handlungen betroffen zu sein, öffnet sich ebenfalls die Schere. So geht etwa die Hälfte (47 Prozent) der befragten Unternehmen davon aus, dass dieses Risiko für deutsche Unternehmen allgemein steigen wird. Für das eigene Unternehmen sieht diese Entwicklung allerdings lediglich etwa ein Drittel (29 Prozent) der Befragten.

Betrug und Untreue an der Spitze. Geldwäsche gewinnt stark an Relevanz.

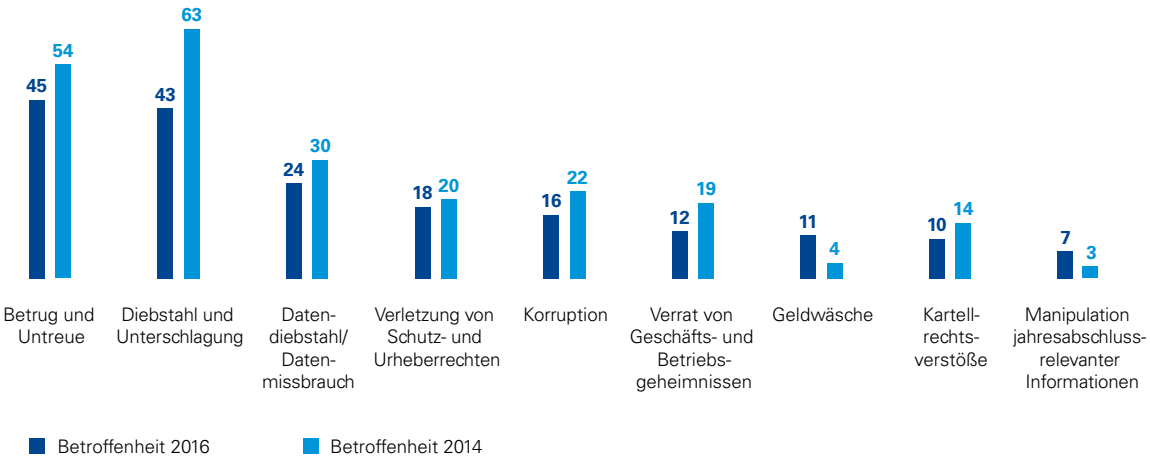
Die Unternehmen geben für fast alle Deliktsarten gegenüber 2014 eine geringere Betroffenheit an (Abb. 2, Seite 11). Dabei sind einzelne Delikte insbesondere in kleinen und mittleren Unternehmen deutlich zurückgegangen. Gleiches gilt für das wahrgenommene Risiko im Hinblick auf die abgefragten Deliktsarten (Abb. 3, Seite 11). Diese Ergebnisse überraschen insoweit, als die generelle Betroffenheit gegenüber 2014 sogar leicht gestiegen ist. Auch die von den betroffenen Unternehmen gemeldeten Fallzahlen sind mit jeweils rund 13 Fällen wirtschaftskrimineller Handlungen pro betroffenem Unternehmen vergleichbar mit 2014 (zwölf angegebene Fälle). Die von Wirtschaftskriminalität betroffenen Unternehmen hatten es in jüngster Zeit also möglicherweise mit einer geringeren Bandbreite an Deliktsarten zu tun.

Mit 45 Prozent sind Betrug und Untreue in diesem Jahr die am häufigsten genannte Deliktsart. 2014 waren es mit 63 Prozent noch Diebstahl und Unterschlagung. Allerdings rangiert dieses Delikt bei mehr als zwei Dritteln der betroffenen großen Unternehmen nach wie vor an der Spitze.

Wie schon in der vorangegangenen Studie gibt etwa die Hälfte der Befragten für diese „alltäglichen" Delikte ein hohes bzw. sehr hohes Risiko an. Für Betrug und Untreue gilt dies für 46 Prozent der Befragten, für Diebstahl und Unterschlagung für 45 Prozent.

1 Vgl. dazu Abschnitt 3 „Umgang mit Wirtschaftskriminalität"

Abb. 2: Betroffenheit nach Deliktsarten
Angaben in Prozent

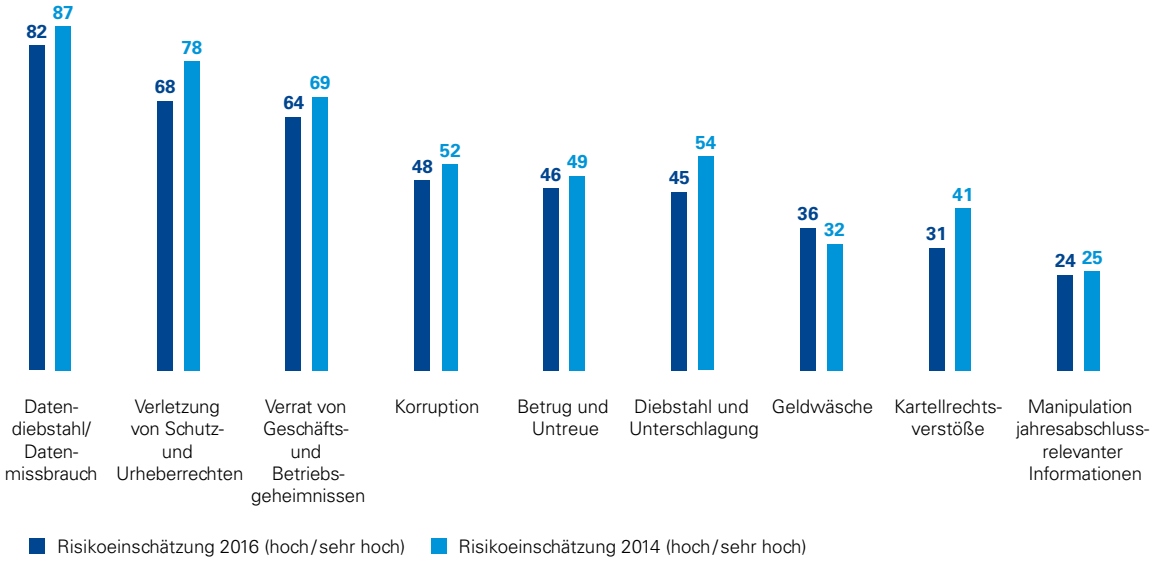


Quelle: KPMG, 2016

Ähnlich wie 2014 stellen sich auch Betroffenheit und Risikowahrnehmung bei Datendiebstahl bzw. -missbrauch, Verrat von Geschäfts- und Betriebsgeheimnissen sowie Verletzung von Schutz- und Urheberrechten dar. Die von den Befragten wahrgenommenen Risiken sind gegenüber 2014 zwar leicht rückläufig, aber dennoch anhaltend hoch. Mit der tatsächlichen Betroffenheit sieht es anders aus: 82 Prozent der befragten Unternehmen empfinden ein hohes bzw. sehr hohes Risiko in Verbindung mit Datendelikten. Betroffen hiervon waren in den letzten zwei Jahren allerdings lediglich 24 Prozent. In etwa der Hälfte der Fälle handelte es sich dabei um Datendiebstahl (52 Prozent), bei immerhin 15 Prozent der Betroffenen kam es zu Verstößen gegen den Datenschutz.

Für die Verletzung von Schutz- und Urheberrechten sowie der Verrat von Geschäfts- und Betriebsgeheimnissen ergibt sich ein ähnlich divergierendes Bild: Das Risiko wird von jeweils 68 bzw. 64 Prozent der befragten Unternehmen als hoch oder sehr hoch eingeschätzt. Tatsächlich nahmen die Delikte nur einen Anteil von 18 bzw. zwölf Prozent der Fälle bei den betroffenen Unternehmen ein.

Abb. 3: Risikowahrnehmung nach Deliktsarten
Angaben in Prozent



Quelle: KPMG, 2016

Für die Delikte mit ausgeprägt hoher Risikowahrnehmung bei gleichzeitig verhaltenen Betroffenheitszahlen erwarten befragte Unternehmen gleichwohl steigende Risiken für die kommenden zwei Jahre. Mehr als die Hälfte der Befragten befürchtet dies für Datendelikte, etwas mehr als ein Drittel für die Verletzung von Schutz- und Urheberrechten und etwas mehr als ein Viertel hinsichtlich des Verrats von Geschäfts- und Betriebsgeheimnissen.

Zumindest für Datendelikte lässt sich diese auffällige Diskrepanz zwischen Risikowahrnehmung und tatsächlicher Betroffenheit wohl zum Teil damit erklären, dass Unternehmen ihre Betroffenheit nicht immer zutreffend angeben können. Die Praxis zeigt, dass hier oft die erforderlichen Prozesse und Kontrollen für die Aufdeckung und Aufklärung fehlen. So dürfte die tatsächliche Dunkelziffer an Datendelikten höher liegen, als sie aus den Ergebnissen der Befragung ersichtlich wird.

Eine weitere interessante Entwicklung zeigt sich bei der Korruption. Nach wie vor schätzt etwa die Hälfte (48 Prozent) der befragten Unternehmen die Gefahr, von Korruption betroffen zu sein, als hoch bzw. sehr hoch ein. Unter den betroffenen Unternehmen wird Korruption jedoch lediglich in 16 Prozent der Fälle genannt – ein Rückgang von sechs Prozent gegenüber 2014. Allerdings verbreitet sich diese Deliktsart in den großen Unternehmen deutlich: Knapp die Hälfte der betroffenen Unternehmen dieser Größenkategorie nennen dieses Delikt (45 Prozent). Das entspricht einem Anstieg von 50 Prozent gegenüber 2014 (30 Prozent). Kleine Unternehmen sind lediglich zu vier Prozent, mittlere zu 15 Prozent von dieser Deliktsart betroffen.

Die große Ausnahme zu der ansonsten eher rückläufigen Entwicklung im Rahmen der deliktsspezifischen Betroffenheit und Risikowahrnehmung stellt die Geldwäsche dar. Mit Abstrichen gilt dies auch für die Manipulation jahresabschlussrelevanter Informationen. So wurde Geldwäsche von den betroffenen Unternehmen fast dreimal so oft angegeben wie 2014 (von vier auf elf Prozent); bei der Manipulation jahresabschlussrelevanter Informationen haben sich die Nennungen mehr als verdoppelt (von drei auf sieben Prozent). Die Geldwäsche ist zudem die einzige Deliktsart, für die die Befragten eine höhere Risikoeinschätzung abgeben als in der Vorgängerstudie (2016: 36 Prozent, 2014: 32 Prozent).

Geldwäsche im Fokus

Nicht zuletzt durch die zunehmende Medienberichterstattung – man denke an die Panama Papers oder die 4. EU-Geldwäscherichtlinie – wird Geldwäsche immer mehr zu einem öffentlich wahrgenommenen Fokus der Wirtschaftskriminalität, der nicht nur für Banken relevant ist. Die Ergebnisse dieser Studie unterstreichen die steigende Relevanz dieses Delikts. Ablesen lässt sich diese Entwicklung auch an den zahlreichen aktuellen Gesetzesvorhaben oder schon in Kraft getretenen Regelungen, die sich der Bekämpfung dieser Deliktsart widmen.

Die Ergebnisse lassen erkennen, dass gerade Finanzdienstleister von Geldwäschedelikten betroffen waren (47 Prozent). Folgerichtig messen sie dieser Deliktsart auch ein höheres Risiko (47 Prozent hohes bzw. sehr hohes Risiko) bei. Auch Nichtfinanzunternehmen sollten die Bekämpfung von Geldwäsche nicht vernachlässigen, zumal die Umsetzung der 4. EU-Geldwäscherichtlinie in deutsches Recht verschärfte Regelungen auch für sogenannte Güterhändler vorsieht.

Schadenssummen schwierig zu beziffern

Dass Geldwäschedelikte eine große Bedeutung erlangt haben, zeigt sich auch in den angegebenen Schäden. Die Höhe des jeweils angegebenen Gesamtschadens fällt dabei allerdings höchst unterschiedlich aus:

Der Gesamtschaden besteht aus dem eingetretenen Verlust, entgangenen Gewinn, Ermittlungs- und Folgekosten zuzüglich Bußgeldern, Geldstrafen und eventuellen Gewinnabschöpfungen.

70 Prozent der Betroffenen beziffern den Gesamtschaden durch Geldwäsche auf 50.000 bis 500.000 Euro. Das Schadenspotenzial von Geldwäsche liegt allerdings weitaus höher. Darauf weist hin, dass 15 Prozent der Opfer von Geldwäsche Gesamtschäden von einer Million Euro oder mehr, in Einzelfällen sogar von mehr als 50 Millionen Euro angeben. Je nach Schwere des Verstoßes müssen Betroffene bereits jetzt insbesondere mit hohen Geldbußen rechnen. Ermittlungs- und Folgekosten machen bei Geldwäschedelikten hingegen einen deutlich geringeren Anteil am Gesamtschaden aus. Sie belaufen sich in drei von vier Fällen lediglich auf bis zu 50.000 Euro. Möglicherweise ist diese Summe jedoch auf eine ungenaue Messung bzw. Zuordnung der Folgekosten zurückzuführen.

Gegenüber der Studie von 2014 zeigt sich, dass betroffene Unternehmen tendenziell seltener in der Lage sind, konkrete Schadenssummen zu benennen. 2014 konnte lediglich für die Deliktsarten Korruption (26 Prozent) und Kartellrechtsverstöße (42 Prozent) mehr als ein Viertel der Betroffenen keine Angaben zu den entstandenen Schäden machen. Bei der diesjährigen Befragung trifft dies, mit Ausnahme von Geldwäsche und der Manipulation jahresabschlussrelevanter Informationen, auf alle Deliktsarten zu. Bei dem Verrat von Geschäfts- und Betriebsgeheimnissen konnten gar 82 Prozent der betroffenen Unternehmen keine Angaben zum Gesamtschaden machen. Im Gegensatz dazu konnten 2014 noch 81 Prozent der Opfer dieses Delikts konkrete Schadenssummen benennen.

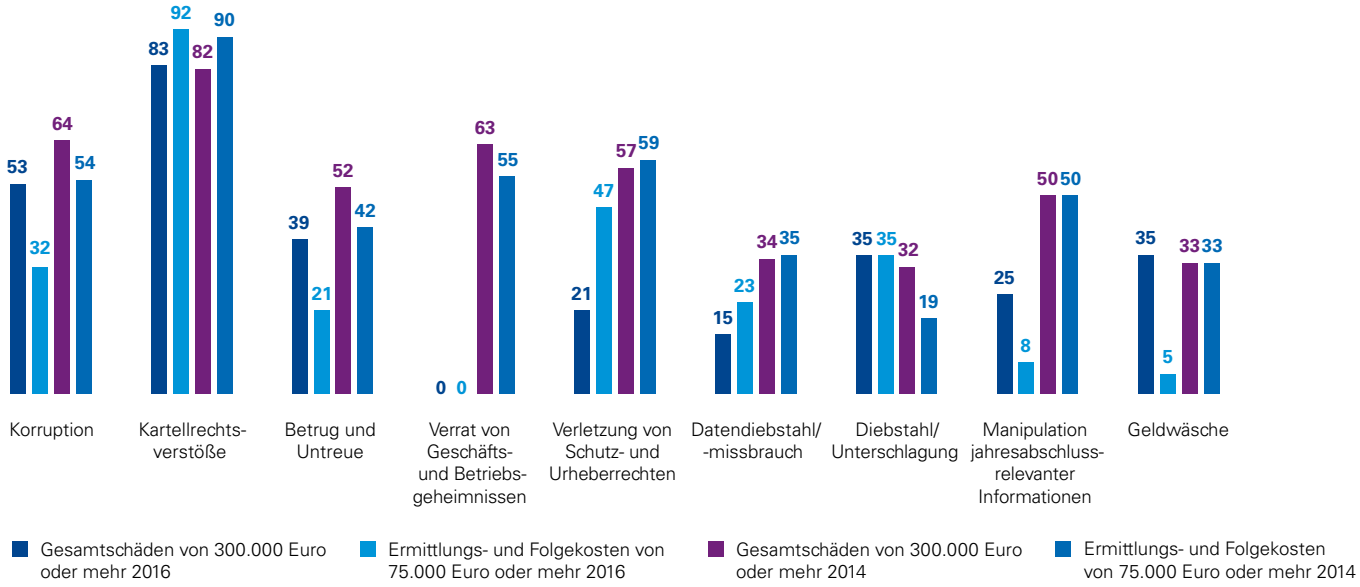
2 Vgl. Jahresbericht 2014 Financial Intelligence Unit, S. 9, sowie Grafik 2; abzurufen unter: http://www.bka.de/nn_193364/SharedDocs/Downloads/EN/Publications/AnnualReportsAndSituationAssessments/FIU/fiuJahresbericht2014Englisch,templateId=raw,property=publicationFile.pdf/fiuJahresbericht2014Englisch.pdf

Dabei ist es für die Unternehmen entscheidend, die entstandenen Schadenssummen einschätzen zu können: Effektives Risikomanagement setzt voraus, Eintrittswahrscheinlichkeiten und deliktsspezifische Schäden zu identifizieren und zu quantifizieren. Nur so kann die eigene Gefahrenlage zutreffend eingeschätzt und können angemessene Maßnahmen auch unter ökonomischen Gesichtspunkten eingeleitet werden.

Deliktsübergreifend zeigt sich der Trend, dass der Gesamtschaden pro Deliktsart ebenso wie die Ermittlungs- und Folgekosten für die meisten Unternehmen gegenüber 2014 gesunken sind (Abb. 4). Allerdings verzerrt der hohe Anteil der Betroffenen, die im Rahmen der diesjährigen Befragung keine Angaben machen konnten, die Ergebnisse. Gleichzeitig wurden nämlich auch extreme Spitzenwerte festgestellt. So geben beispielsweise sechs Prozent der von Betrug und Untreue betroffenen Unternehmen Gesamtschäden von 20 Millionen Euro oder mehr an. 2014 lag die maximal angegebene Schadenssumme für diese Deliktskategorie bei zehn Millionen Euro.

Die geringe Anzahl der Angaben sowie die Ausreißer bei einzelnen Schadensangaben erschweren die Bewertung der rechnerisch ermittelten durchschnittlichen Schadenssummen. So haben sich etwa die durchschnittlich pro Deliktsart entstandenen Gesamtschäden für Betrug und Untreue sowie Diebstahl und Unterschlagung mehr als verdreifacht. Betrug und Untreue verursachten im Durchschnitt eine Gesamtschadenssumme von über vier Millionen Euro pro Unternehmen. 2014 lagen die Angaben bei 1,2 Millionen Euro. Für Diebstahl und Unterschlagung wurden durchschnittliche Gesamtschäden von 1,6 Millionen Euro festgestellt, im Vergleich zu 539.000 Euro im Jahr 2014. Der Schadensmedian illustriert diese Problematik zusätzlich. So liegen die medianen Schäden für Betrug und Untreue bei lediglich 160.000 Euro, für Diebstahl und Unterschlagung bei 100.000 Euro.

Abb. 4: Vergleich Gesamtschäden sowie Ermittlungs- und Folgekosten 2016 zu 2014[3]
Angaben in Prozent



Quelle: KPMG, 2016

Die höchsten Schäden, abgesehen von Ausreißern, fallen nach wie vor bei Kartellrechtsverstößen an. Die durchschnittlichen Gesamtschäden werden hier mit 4,6 Millionen Euro beziffert. Lediglich die durchschnittlich durch Betrug entstandenen Schäden reichen an diese Summe heran.

3 Werte beziehen sich lediglich auf Befragte, die tatsächlich Angaben zur Schadenshöhe machen konnten

Externe und interne Täter fast gleichauf

2016 wurden wirtschaftskriminelle Handlungen zu nahezu gleichen Anteilen von externen (50 Prozent) wie internen Tätern (51 Prozent) begangen.[4] 2014 wurden noch 55 Prozent interne Täter festgestellt, 2012 lag der Anteil sogar noch bei 56 Prozent.

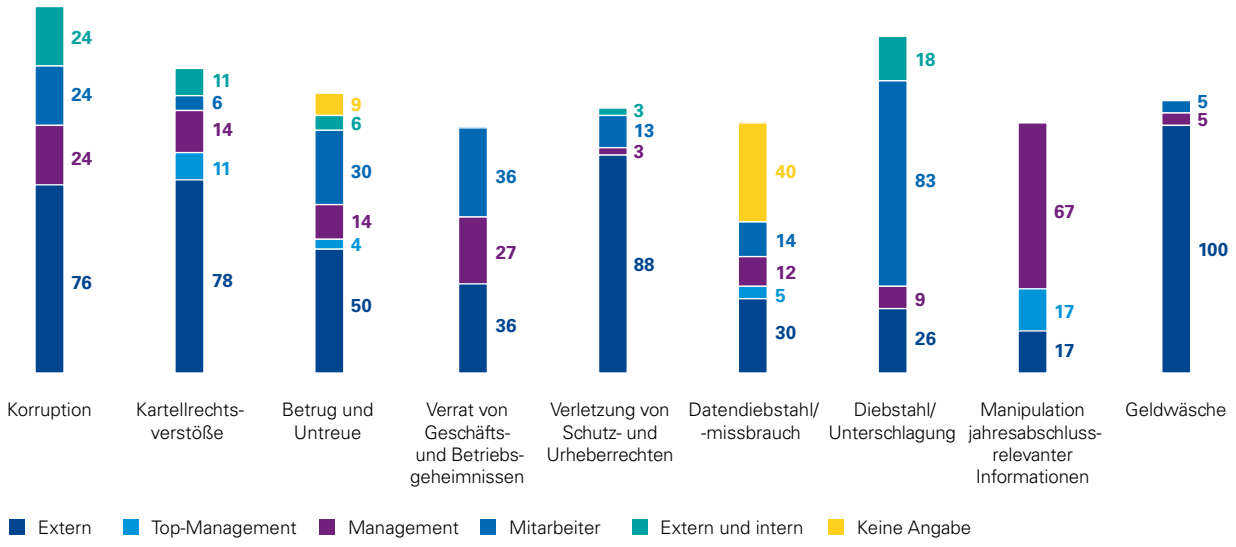
Acht Prozent der Befragten geben an, dass sowohl interne als auch externe Täter an einer wirtschaftskriminellen Handlung beteiligt waren. Dieser Wert hat sich gegenüber 2014 halbiert und ist auch in Bezug auf jede einzelne Deliktsart gesunken.

Deliktsspezifische Auffälligkeiten zeigen sich bei der Deliktsart Korruption. Bei diesem Delikt ist der Anteil externer Täter gegenüber 2014 von damals 45 auf nun 76 Prozent gestiegen. Gleichzeitig sank die angegebene Beteiligung interner Täter von 84 Prozent 2014 auf nunmehr 48 Prozent (Abb. 5). In lediglich rund einem Viertel der Fälle geben betroffene Unternehmen an, dass interne und externe Täter gemeinschaftlich tätig waren. 2014 traf das noch auf ein Drittel der betroffenen Unternehmen zu.

Nach Angaben der Betroffenen werden insbesondere Diebstahl und Unterschlagung (92 Prozent), Manipulation von jahresabschlussrelevanten Informationen (84 Prozent) und Verrat von Geschäfts- und Betriebsgeheimnissen (63 Prozent) – nicht überraschend – von internen Tätern begangen. Durch Präventionsmaßnahmen, beispielsweise zur Kontrolle und Sensibilisierung der Mitarbeiter, können Unternehmen diesem Risiko entgegenwirken.

Die prozentuale Aufteilung innerhalb der internen Täter ist gegenüber der Vorgängerstudie konstant geblieben. Nach wie vor machen Mitarbeiter unterhalb der Managementebene zwei Drittel der Täter aus, auch der Anteil der Täter aus dem Top-Management bleibt mit fünf Prozent konstant. Deliktsarten, bei denen Mitglieder des Top-Managements als Täter angegeben werden, sind insbesondere die Manipulation jahresabschlussrelevanter Informationen (17 Prozent), Kartellrechtsverstöße (elf Prozent) sowie Betrug und Untreue (vier Prozent). Als Tätergruppe tritt das Top-Management gemäß Angaben der betroffenen Unternehmen auch erstmals in Zusammenhang mit Datendelikten in Erscheinung (fünf Prozent).

Abb. 5: Täterherkunft[5]
Angaben in Prozent



Quelle: KPMG, 2016

4 Dadurch, dass auch ein mögliches Zusammenwirken interner und externer Täter abgefragt wurde, ergeben die Angaben zusammen nicht 100 Prozent.

5 Werte über 100 Prozent resultieren aus der Antwortmöglichkeit des Zusammenwirkens externer und interner Täter.

Die Bestimmung der Täterherkunft bei Datendelikten stellt für Unternehmen eine unverändert große Herausforderung dar. Wie schon 2014 können 40 Prozent der betroffenen Unternehmen keine Angaben zu den Tätern bei Datendelikten machen. Dies belegt, dass Unternehmen weiterhin nicht entsprechend vorbereitet sind, um eine effektive und umfassende Aufklärung derartiger Vorfälle zu gewährleisten. Vielmehr können sich potenzielle Täter auf dem Feld der Datendelikte weitgehend anonym bewegen. Durch Präventions- und Aufklärungsmaßnahmen sowie Vorkehrungen für Datensicherheit und Datenschutz könnten Unternehmen hier gegensteuern. Angesichts der geringen Investitionsbereitschaft[6] erscheint es jedoch zumindest zweifelhaft, ob Unternehmen hier schon eine angemessene Gewichtung vornehmen und sich entsprechend wappnen.

Betrugsmasche: „Fake-President“

Neben den Datendelikten können die betroffenen Unternehmen auch bei neun Prozent der Betrugs- und Untreuedelikte keinen Täter benennen. Bei allen übrigen Deliktsarten dagegen ist das möglich. Eine denkbare Erklärung hierfür ist das vermehrte Auftreten sogenannter Fake-President-Fälle bzw. CEO-Fraud-Fälle. Dabei wird unter Vorspiegelung einer falschen Identität, meistens der einer Führungskraft, gezielt ein für Finanztransaktionen zuständiger Mitarbeiter aufgefordert, eine dringende und geheim zu haltende Überweisung in Millionenhöhe durchzuführen. Diese Überweisungen erfolgen nahezu ausschließlich auf Offshore-Konten, die bei Aufdeckung des Betrugs längst leergeräumt sind. Möglicherweise sind auch die zuvor beschriebenen Meldungen extremer Schadenssummen durch Betrug und Untreue in Verbindung mit solchen Fällen zu sehen.

Betroffene Bereiche unterscheiden sich nach Unternehmensgröße

Wie schon 2014 ist der Vertrieb der von Wirtschaftskriminalität am meisten betroffene Bereich in Unternehmen: 40 Prozent aller betroffenen Unternehmen geben an, dass er das Ziel wirtschaftskrimineller Handlungen war (Abb. 6, Seite 17). Das sind zwar zehn Prozent weniger als noch 2014, gleichzeitig vermelden aber gerade große Unternehmen einen Anstieg wirtschaftskrimineller Handlungen in diesem Bereich – und zwar von 43 Prozent auf nun 52 Prozent. Kleine und mittlere Unternehmen waren hier hingegen zuletzt wesentlich seltener betroffen.

Das Finanz- und Rechnungswesen ist laut den Betroffenen vermehrt Zielscheibe von Wirtschaftskriminalität geworden. Fast jedes dritte Großunternehmen (31 Prozent) zählt sich zu den Betroffenen – tatsächlich ein massiver Anstieg im Vergleich zu den Angaben von 2014 (13 Prozent). Zwar war dieser Bereich auch bei kleinen und mittleren Unternehmen von wirtschaftskriminellen Handlungen betroffen, jedoch gab es hier nur eine vergleichsweise geringfügige Steigerung von jeweils fünf Prozent, mit einer aktuellen Betroffenheitsrate von 18 bzw. 21 Prozent.

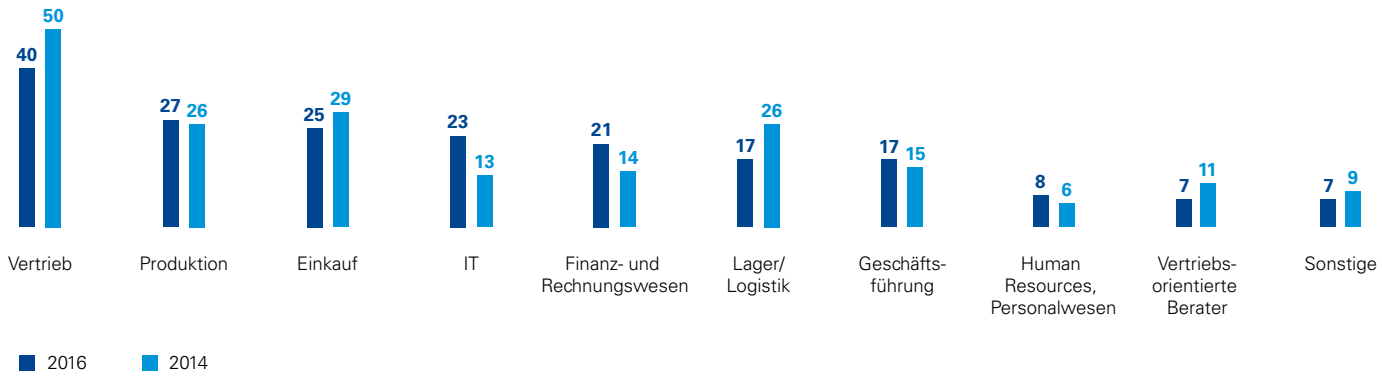
So gut wie unverändert sind auch Lager und Logistik in großen Unternehmen regelmäßig Ziel von Wirtschaftskriminalität. Wie 2014 führt mehr als ein Drittel (38 Prozent) der betroffenen großen Unternehmen diesen Bereich auf. Bei kleinen und mittleren Unternehmen liegen die Angaben jeweils bei elf und 15 Prozent.

6 Vgl. dazu Abschnitt 3 „Umgang mit Wirtschaftskriminalität“.

Produktion und IT waren in großen Unternehmen weit weniger betroffen als noch 2014 – bei großen Unternehmen war die Produktion statt zu 43 nur noch zu 21 Prozent betroffen. Die IT verzeichnete einen Rückgang von 30 auf 17 Prozent. Interessanterweise sind es genau die Bereiche, in denen es bei kleinen Unternehmen einen deutlichen Anstieg an wirtschaftskriminellen Handlungen gegeben hat: 2014 wurde die Produktion von etwa jedem fünften kleinen Unternehmen genannt (19 Prozent). Aktuell wird er von fast jedem dritten kleinen Unternehmen aufgeführt (32 Prozent). Bei der IT fällt der Anstieg noch deutlicher aus. Während die IT 2014 von jedem zehnten kleinen Unternehmen genannt wurde (neun Prozent), wird sie jetzt von jedem dritten kleinen Unternehmen (33 Prozent) angegeben.

Dass gerade die IT in kleinen Unternehmen immer häufiger Ziel wirtschaftskrimineller Handlungen wird, zeigt, dass elektronische Prozesse unabhängig von der Unternehmensgröße ein vermehrt genutztes Einfallstor für Wirtschaftskriminalität geworden sind. Angesichts der zunehmenden Digitalisierung ist zu erwarten, dass die digitale Kriminalität (e-Crime bzw. Cybercrime) steigen wird. Da es sich bei e-Crime um ein sich permanent wandelndes Feld der Kriminalität handelt, müssen speziell hierauf abzielende Präventivmaßnahmen implementiert und regelmäßig auf ihre Wirksamkeit geprüft werden. Das erfordert einen Mindestaufwand an Ressourcen. Es wundert daher nicht, dass sich kleine Unternehmen hier anfälliger zeigen.

Abb. 6: Betroffene Abteilungen
Angaben in Prozent



Quelle: KPMG, 2016

Einkauf und Geschäftsführung sind in etwa so häufig betroffen wie 2014. Über alle Unternehmensklassen hinweg werden sie nach wie vor von etwa 25 bzw. 17 Prozent aller Betroffenen genannt. Die weiteren abgefragten Abteilungen wurden von jeweils mehr als 90 Prozent aller betroffenen Unternehmen nicht genannt und spielen somit im Rahmen der Betroffenheit eine eher nachgelagerte Rolle.

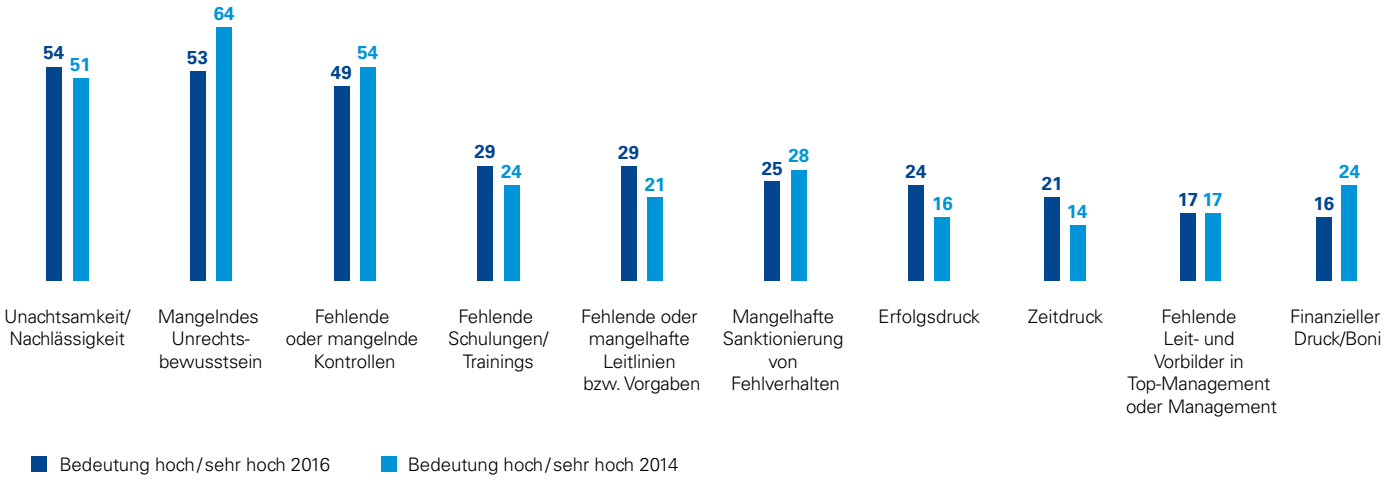
Faktor Mensch entscheidet

Analog zu den Studienergebnissen von 2012 und 2014 begünstigen vor allem menschliche Faktoren auch aktuell wirtschaftskriminelle Handlungen – allen voran Unachtsamkeit bzw. Nachlässigkeit sowie mangelndes Unrechtsbewusstsein. Beide Faktoren werden von mehr als jedem zweiten betroffenen Unternehmen (54 Prozent und 53 Prozent) als begünstigender Faktor für wirtschaftskriminelle Handlungen aufgeführt (Abb. 7). Fehlende oder mangelhafte Kontrollen sind wie schon 2014 der einzige nicht menschliche Faktor, dem die von Wirtschaftskriminalität betroffenen Unternehmen eine vergleichsweise hohe Bedeutung beimessen (49 Prozent).

Welche Konsequenzen ziehen die Unternehmen daraus, dass menschliche Eigenschaften weiterhin ausschlaggebend für wirtschaftskriminelle Handlungen sind? Die Studienergebnisse zeigen, dass gerade Schulungen, die einen wesentlichen Beitrag zur Sensibilisierung der Mitarbeiter leisten, einen höheren Stellenwert in der Prävention genießen als noch 2014 und entsprechend auch häufiger durchgeführt werden.[7] Die gestiegene Bedeutung von Schulungen untermauert auch, dass nunmehr 29 Prozent der betroffenen Unternehmen (2014: 24 Prozent) fehlende Schulungen als wichtigen begünstigenden Faktor für wirtschaftskriminelle Handlungen nennen.

2014 wurde fehlenden Leit- und Vorbildern in Management und Top-Management lediglich eine geringe Bedeutung für die Begehung von wirtschaftskriminellen Handlungen im Unternehmen beigemessen. Auch bei der diesjährigen Befragung empfinden nur 17 Prozent der betroffenen Unternehmen, dass dieser Faktor eine hohe Bedeutung hat. In der Rangfolge der Faktoren ist er sogar weiter nach hinten gerückt – obwohl laut Angaben der betroffenen Unternehmen nach wie vor 50 Prozent der wirtschaftskriminellen Täter aus dem eigenen Unternehmen stammen; im Falle von Diebstahl und Unterschlagung sogar über 90 Prozent. Insofern sollte ein angemessener „Tone at the Top" Mitarbeiter zu gesetzes- und richtlinientreuem Verhalten anhalten und dazu beitragen können, eine Compliance-Kultur im Unternehmen zu schaffen.

Abb. 7: Risikofaktoren für Begehung einer wirtschaftskriminellen Handlung
Angaben in Prozent



Quelle: KPMG, 2016

7 Vgl. dazu Abschnitt 3 „Umgang mit Wirtschaftskriminalität".

Unter den weiteren, von den betroffenen Unternehmen als begünstigend angesehenen Faktoren finden sich in je einem von vier Fällen auch fehlende oder mangelhafte Leitlinien bzw. Vorgaben und mangelhafte Sanktionierung von Fehlverhalten. Gemäß den Betroffenen ergreifen 22 Prozent nach wie vor keine Sanktionen gegen die Täter. Dies mag teilweise darin begründet sein, dass Täter nicht zweifelsfrei ermittelt werden können. Die abschreckende Wirkung von Sanktionen ist jedoch nicht zu unterschätzen. Gerade in Bezug auf mangelndes Unrechtsbewusstsein, den ein Großteil der betroffenen Unternehmen als Ursache für Wirtschaftskriminalität ausmacht, kann die konsequente Kommunikation und Umsetzung von Sanktionsmaßnahmen ein wirksames Gegenmittel darstellen.

Die weiteren abgefragten Faktoren fokussieren persönliche Drucksituationen – Erfolgsdruck, Zeitdruck und finanziellen Druck. Nach wie vor zählen diese drei zu den am seltensten genannten Einflussfaktoren für Wirtschaftskriminalität. Dennoch nimmt Erfolgsdruck für ein Viertel aller betroffenen Unternehmen einen hohen bzw. sehr hohen Stellenwert ein; für Zeitdruck geben 21 Prozent diese Einschätzung ab, für finanziellen Druck 16 Prozent. Es zeigt sich also, dass aus Sicht der Betroffenen weniger die finanzielle Motivation im Vordergrund steht als vielmehr die generelle Situation und der Stress im Arbeitsumfeld.

2. Themenschwerpunkt Reputation

Reputationsrisiken spielen für deutsche Unternehmen eine große Rolle. Die Bestimmung etwaiger (monetärer) Auswirkungen stellt jedoch eine Herausforderung dar.

Reputationsrisiko wird ähnlich wie Betroffenheitsrisiko eingeschätzt

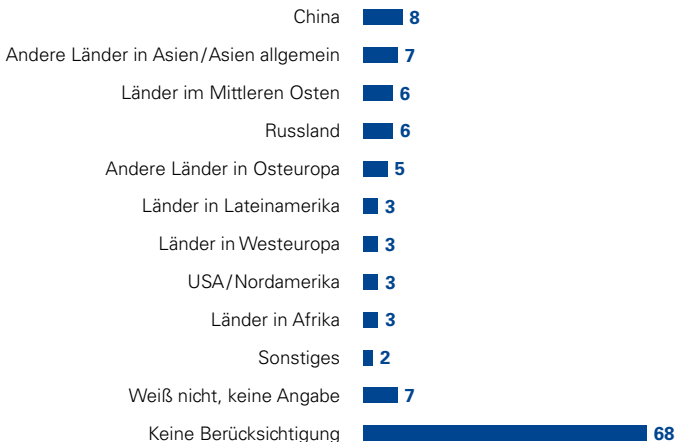
Die Reputation eines Unternehmens bestimmt das Ansehen und das Vertrauen, das ihm Kunden, Lieferanten, Kapitalgeber und andere Stakeholder entgegenbringen. Insofern ist sie unbestritten ein schützenswertes Gut. In der Praxis ist allerdings häufig zu beobachten, dass Unternehmen ihrer Reputation zwar grundsätzlich großes Gewicht beimessen, im Rahmen des Risikomanagements dieses Thema jedoch stiefmütterlich behandeln. Dabei können gerade wirtschaftskriminelle Handlungen neben den unmittelbaren Schäden auch massive Reputationsschäden mit sich bringen.

Befragt nach der Gefahr für das eigene Unternehmen, einen Reputationsschaden durch Wirtschaftskriminalität und Compliance-Verstöße zu erleiden, geben 27 Prozent der Unternehmen an, ein hohes bzw. sehr hohes Gefahrenpotenzial zu sehen. Dieses Ergebnis korrespondiert in etwa mit der Einschätzung der Unternehmen, grundsätzlich von wirtschaftskriminellen Handlungen betroffen zu sein (32 Prozent).

Betrachtet man die Angaben differenziert nach Unternehmensgröße, zeigt sich folgendes Bild: Die großen Unternehmen geben zu 23 Prozent an, ein hohes bzw. sehr hohes Risiko zu haben, von wirtschaftskriminellen Handlungen betroffen zu sein. Gleichzeitig schätzen 32 Prozent dieser Befragten die Gefahr von Reputationsschäden durch Wirtschaftskriminalität und Compliance-Verstöße für das eigene Unternehmen als hoch bzw. sehr hoch ein. In den Kategorien der kleinen und mittleren Unternehmen liegt der umgekehrte Effekt vor. Sie sehen ein im Vergleich zum Risiko, von wirtschaftskriminellen Handlungen betroffen zu sein, geringes Risiko eines Reputationsschadens.

Ein Viertel der befragten Unternehmen verknüpft Reputationsrisiken mit bestimmten Ländern im Rahmen ihrer Marken- und Produktentwicklung sowie ihrer Expansionsstrategie (Abb. 8). Dabei nimmt der Anteil mit steigendem Umsatz zu: Während lediglich jedes fünfte kleine Unternehmen Reputationsrisiken in Verbindung mit bestimmten Ländern berücksichtigt, bezieht jedes dritte große Unternehmen diese Risikobetrachtung ein.

Abb. 8: Berücksichtigung länderspezifischer Reputationsrisiken
Angaben in Prozent

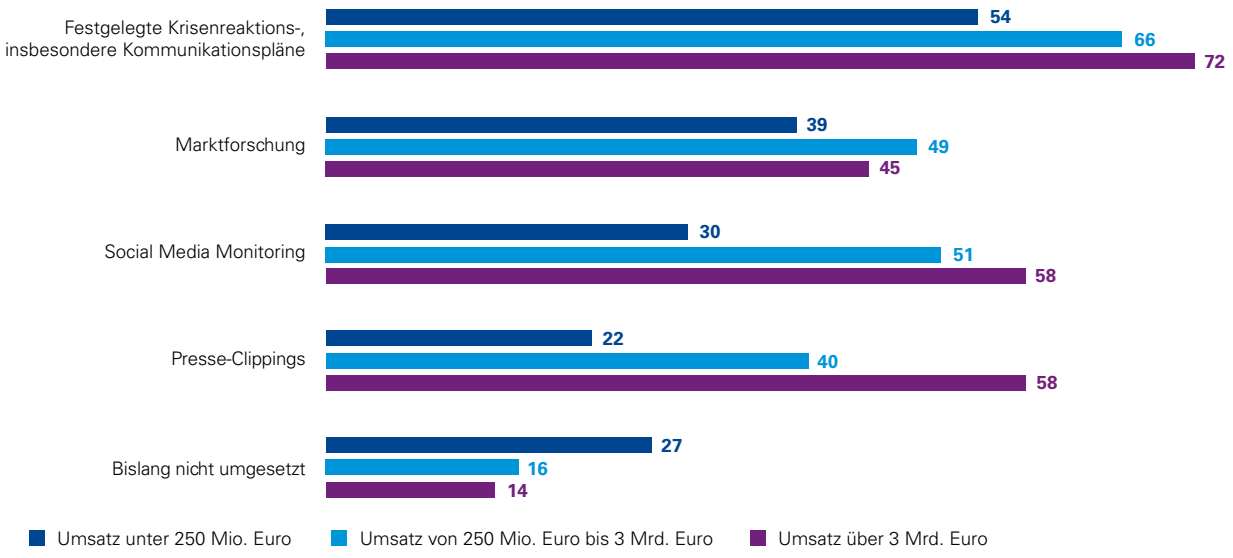


Quelle: KPMG, 2016

Kein Land bzw. keine Region wurde von mehr als acht Prozent der Befragten bei der Frage nach der Berücksichtigung von Reputationsrisiken im Rahmen der Expansionsstrategie genannt. Dennoch lässt sich ablesen, dass Reputationsrisiken vor allem mit asiatischen und osteuropäischen Ländern und Regionen in Verbindung gebracht werden. So zählen China (acht Prozent), Asien allgemein (sieben Prozent), der Mittlere Osten (sechs Prozent), Russland (sechs Prozent) und Osteuropa (fünf Prozent) zu den meistgenannten Ländern und Regionen. Westeuropa, westlich davon gelegene Regionen, aber auch Afrika werden nur von jeweils drei Prozent der Befragten angeführt.

Knapp 80 Prozent der befragten Unternehmen haben bereits Präventionsmaßnahmen gegenüber Reputationrisiken eingeführt. Über 60 Prozent der Befragten geben an, über festgelegte Krisenreaktions-, insbesondere Kommunikationspläne zu verfügen (Abb. 9). 44 Prozent der befragten Unternehmen betreiben Marktforschung, 43 Prozent führen Social Media Monitorings durch. Presse-Clippings[8] betreibt etwas mehr als ein Drittel der befragten Unternehmen.

Abb. 9: Präventionsmaßnahmen hinsichtlich Reputationsrisiken
Angaben in Prozent



Quelle: KPMG, 2016

8 Presse-Clipping bezeichnet die regelmäßige Auswertung von Pressemeldungen.

Reputationsschäden haben interne und externe Auswirkungen – bei oft unklarem monetärem Ausmaß

13 Prozent aller befragten Unternehmen geben an, schon einmal einen Reputationsschaden durch Wirtschaftskriminalität oder Compliance-Verstöße erlitten zu haben. Dabei gilt: je höher der Umsatz, desto stärker die Betroffenheitsrate.

Insgesamt geben 77 Prozent der von Reputationsschäden betroffenen Unternehmen an, spürbare Auswirkungen nach der Veröffentlichung von Straftaten erlebt zu haben. Die Folgen wirkten sich dabei sowohl auf unternehmensinterne Bereiche als auch auf externe Dimensionen wie Kunden, Geschäftspartner oder Auftraggeber aus.

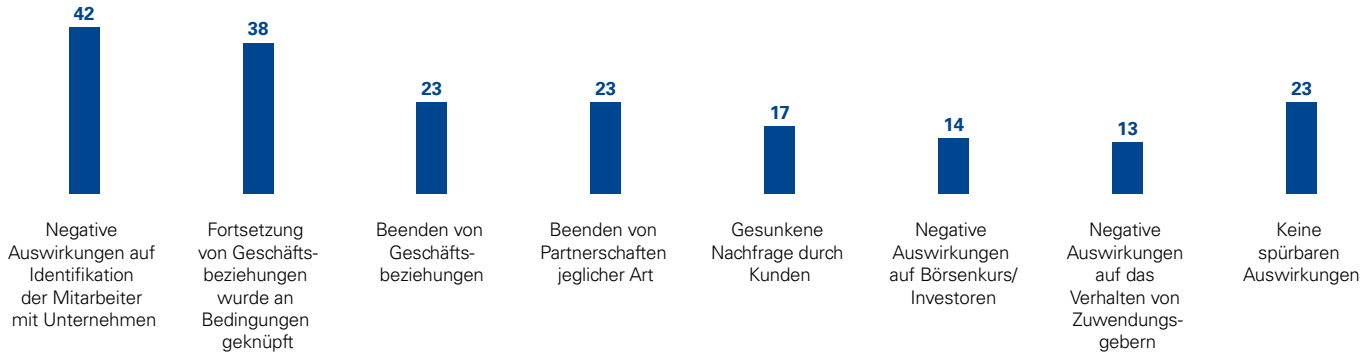
Am häufigsten wirken sich wirtschaftskriminelle Taten auf die Identifikation der Mitarbeiter mit ihrem Unternehmen aus. 42 Prozent der betroffenen Unternehmen nennen diesen Aspekt (Abb. 10). Nach außen, so ein Viertel der von Reputationsschäden betroffenen Unternehmen, kommt es zunächst interessanterweise nur zu einem marginalen Kundenverlust. Bei einem Fünftel der betroffenen Unternehmen ging der Umsatz zurück – bei immerhin sechs Prozent der Unternehmen erheblich.

Befragt nach den Auswirkungen auf ihre Beziehung zu öffentlichen Auftraggebern nach Bekanntwerden wirtschaftskrimineller Handlungen oder Compliance-Verstößen gibt jedes sechste mit öffentlichen Auftraggebern zusammenarbeitende Unternehmen an, dass ihm spürbar strengere Kontrollen oder Auflagen zur Selbstreinigung auferlegt wurden.

Für mehr als ein Drittel (38 Prozent) der betroffenen Unternehmen hatte die Veröffentlichung von wirtschaftskriminellen Handlungen zur Folge, dass die Fortsetzung der Geschäftsbeziehung an Bedingungen geknüpft wurde. In jeweils 23 Prozent der Fälle wurden die Geschäftsbeziehung bzw. die Partnerschaft gar beendet.

Das monetäre Ausmaß von Reputationsschäden können die betroffenen Unternehmen nur in wenigen Fällen tatsächlich benennen. Vielfach geben sie an, keinen monetären Schaden in Verbindung mit einem Reputationsschaden erlitten zu haben. Dieses Ergebnis überrascht, da jedes vierte Unternehmen ein hohes Gefahrenpotenzial durch Reputationsschäden sieht. Auch mit Blick auf die Angaben von Unternehmen hinsichtlich der negativen Auswirkungen auf Kundenbeziehungen und Geschäftspartner sind diese Angaben bemerkenswert. Die wenigen konkret festgestellten Schäden variieren zudem ausgesprochen stark: In einigen Fällen wurden die Reputationsschäden auf 10.000 Euro beziffert, zwei von Diebstahl betroffene Unternehmen geben an, Reputationsschäden von jeweils fünf Millionen Euro erlitten zu haben. Diese Ergebnisse deuten darauf hin, dass die Bestimmung der monetären Schäden durch einen Reputationsverlust eine Herausforderung darstellt.

Abb. 10: Auswirkungen durch Reputationsschäden
Angaben in Prozent

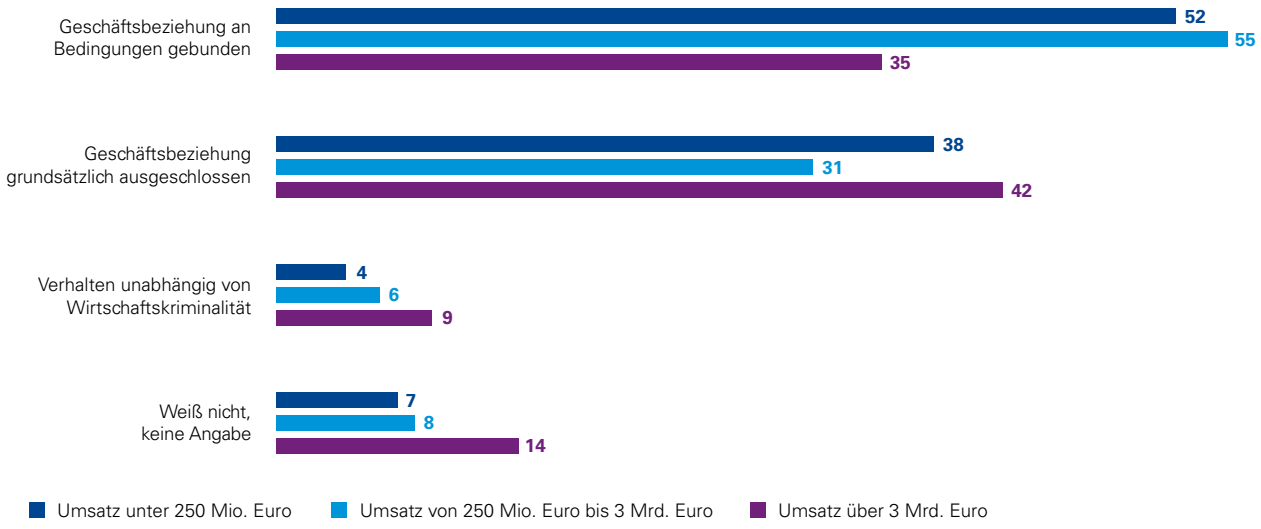


Quelle: KPMG, 2016

Großes Misstrauen gegenüber Unternehmen, die Täter von Wirtschaftskriminalität wurden

Die Studienteilnehmer wurden auch danach gefragt, wie sie sich gegenüber Unternehmen verhalten, die Täter von Wirtschaftskriminalität wurden. Hier gibt jedes dritte (35 Prozent) der befragten Unternehmen an, dass eine Geschäftsbeziehung zu solchen Unternehmen grundsätzlich ausgeschlossen ist (Abb. 11). Bei den großen Unternehmen sagen das sogar 42 Prozent. Jedes zweite Unternehmen würde die Geschäftsbeziehung an konkrete Bedingungen knüpfen. Lediglich sechs Prozent der Befragten geben an, dass ihr Verhalten nicht davon beeinflusst wird, ob ein Unternehmen in wirtschaftskriminelle Handlungen involviert ist.

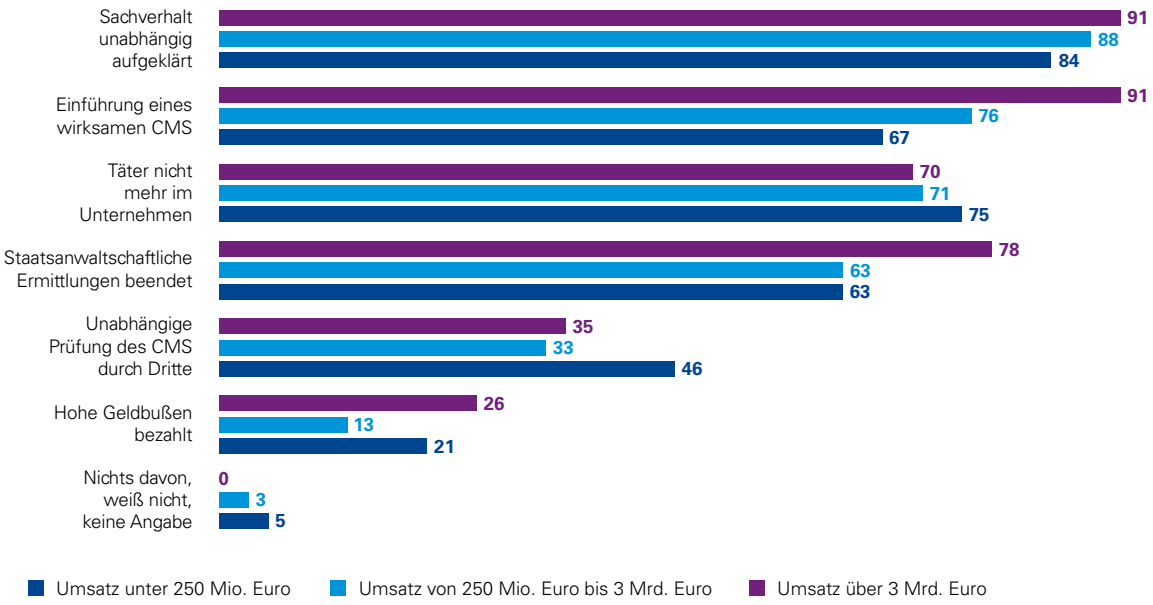
Abb. 11: Verhalten gegenüber Tätern wirtschaftskrimineller Handlungen
Angaben in Prozent



Quelle: KPMG, 2016

Die von den Befragten meistgenannte Bedingung für eine Fortsetzung der Geschäftsbeziehung mit einem Unternehmen, das Täter von Wirtschaftskriminalität wurde, war eine unabhängige Aufklärung des Sachverhalts (87 Prozent). Auch die zuverlässige und zeitnahe Ermittlung der Täter ist von Bedeutung: 72 Prozent der befragten Unternehmen machen es zur Bedingung für eine Fortsetzung der Geschäftsbeziehung, dass die handelnde Person nicht mehr im Unternehmen arbeitet (Abb. 12, Seite 25). Dies unterstreicht, wie wichtig es ist, die verantwortlichen Instanzen bzw. Personen zu ermitteln und mit Sanktionen zu belegen sowie die Straftat aufzuklären, um das Vertrauen der Geschäftspartner zurückzugewinnen. Gerade bei Datendelikten können sich hier besondere Schwierigkeiten ergeben. Unternehmen können diesen durch die Implementierung von Aufklärungsmaßnahmen entgegenwirken, um eine effektive Täterermittlung sicherzustellen.

Abb. 12: Bedingungen für eine Fortsetzung der Geschäftsbeziehung
Angaben in Prozent



Quelle: KPMG, 2016

Knapp drei Viertel der Befragten (73 Prozent) stellen für eine weitere Zusammenarbeit die Bedingung, dass ein wirksames Compliance-Management-System (CMS) eingeführt wird. Ein solches CMS stellt vor allem für große Unternehmen eine Muss-Bedingung dar: 91 Prozent der Befragten nennen dieses Kriterium. Auch bei kleineren Unternehmen wird diese Bedingung von jeweils mehr als zwei Dritteln der Befragten genannt.

Knapp 40 Prozent der Befragten nennen außerdem die unabhängige Prüfung des CMS durch Dritte als Bedingung für die Fortführung der Zusammenarbeit. Durch eine Zertifizierung der Angemessenheit, der Implementierung und der Wirksamkeit ihres CMS gewinnen die betroffenen Unternehmen an Sicherheit und können diese auch gegenüber Geschäftspartnern und anderen Stakeholdern demonstrieren.

Knapp zwei Drittel der Befragten (64 Prozent) erachten die Beendigung der staatsanwaltschaftlichen Ermittlungen als notwendige Bedingung für eine Fortsetzung der geschäftlichen Beziehungen. Bereits ausgesprochene, hohe Geldbußen sind für die Befragten dagegen von nachrangiger Bedeutung: Lediglich 18 Prozent knüpfen die weitere Geschäftsbeziehungen an die Zahlung von Geldbußen.

Die Studie belegt, dass wirtschaftskriminelle Handlungen zu ausgeprägtem Misstrauen gegenüber Unternehmen, die Täter von Wirtschaftskriminalität waren, führen und dies erhebliche Konsequenzen für eine weitere Zusammenarbeit hat. Mehr noch: Eine Fortsetzung der Zusammenarbeit gibt es – wenn überhaupt – nur gegen Sicherheiten.

3. Umgang mit Wirtschaftskriminalität

Unternehmen sehen den eigenen Umgang mit wirtschaftskriminellen Handlungen zunehmend kritisch. Der Stellenwert präventiver Maßnahmen ist gestiegen, das Maß an Investitionsbereitschaft in externe Unterstützung bleibt allerdings noch gering.

Externe Unterstützung immer mehr gefragt

Die Studienteilnehmer wurden auch nach ihrer Vorgehensweise in Sachen Prävention und Aufklärung von sowie Reaktion auf Wirtschaftskriminalität befragt.

Zur Prävention nimmt etwa die Hälfte der befragten Unternehmen externe Unterstützung in Anspruch – beispielsweise für die Ausarbeitung von Richtlinien (46 Prozent), zur Durchführung von Trainings (43 Prozent) sowie von Integrity Due Diligences bzw. Hintergrundrecherchen (43 Prozent). Außerdem werden externe Dienstleister zur Durchführung von Datenanalysen mit Fraud-Routinen (36 Prozent) sowie Risiko-Assessments mit dem Fokus Wirtschaftskriminalität (33 Prozent) beauftragt (Abb. 13).

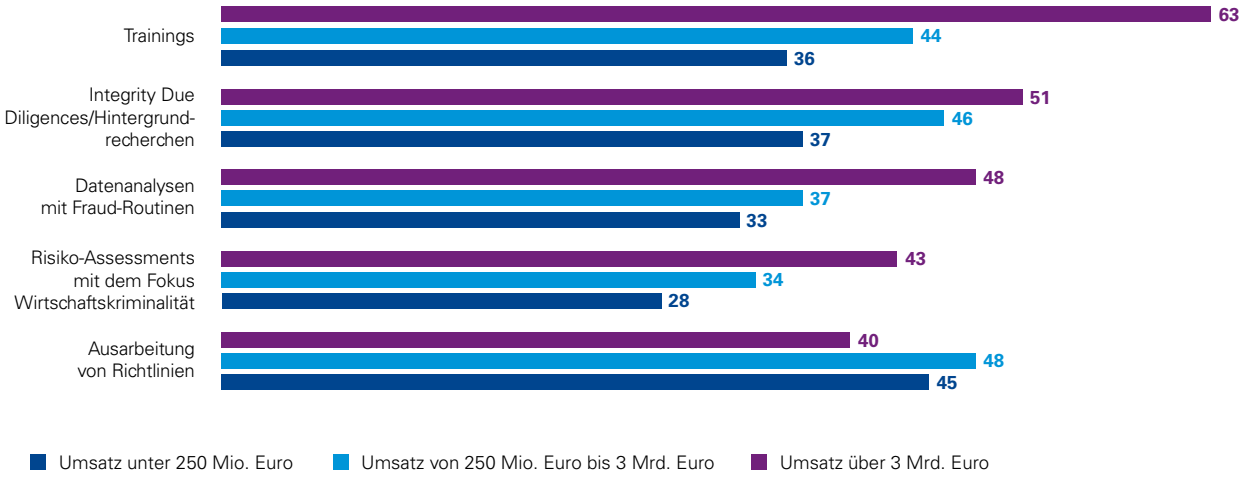
Abb. 13: Externe Unterstützung in der Prävention
Angaben in Prozent

Quelle: KPMG, 2016

Dabei ist der Anteil der Unternehmen, die sich externer Unterstützung bedienen, gegenüber 2014 insgesamt gestiegen. Unternehmen scheinen also deutlicher die Notwendigkeit zu sehen, auf externe Dienstleister zurückzugreifen bzw. über mehr finanzielle Mittel zu verfügen, um dies zu tun.

Differenziert nach Größenkategorien ist fast durchgängig zu beobachten, dass mit zunehmendem Umsatz auch mehr externe Unterstützung eingeholt wird. Beispielsweise binden kleine Unternehmen nur zu 36 Prozent externe Expertise für Schulungen ein, während große Unternehmen zu 63 Prozent auf externe Unterstützung bei Trainings zurückgreifen (Abb. 14).

Abb. 14: Externe Unterstützung in der Prävention
Angaben in Prozent



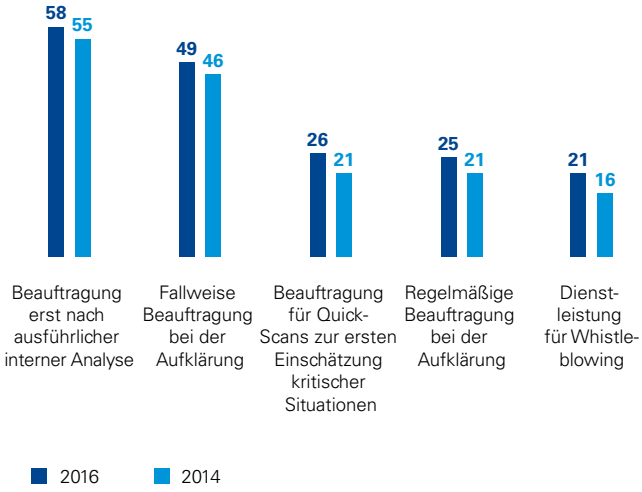
Quelle: KPMG, 2016

Setzt man die Selbsteinschätzung der Unternehmen hinsichtlich ihres Schutzes gegenüber wirtschaftskriminellen Handlungen ins Verhältnis zur Einbindung externer Dienstleister bei Präventionsmaßnahmen, zeigt sich, dass 39 Prozent der Unternehmen, die ihren Schutz als gut bzw. sehr gut bewerten, auf externe Unterstützung bei der Durchführung von Datenanalysen mit Fraud-Routinen zurückgreifen. Für Unternehmen, die sich schlecht auf Wirtschaftskriminalität vorbereitet sehen, liegt dieser Wert bei gerade einmal 18 Prozent. Aus Sicht der Unternehmen erhöht die professionelle Durchführung solcher Analysen demnach den Schutz gegen Wirtschaftskriminalität.

Im Rahmen der Aufklärung von Wirtschaftskriminalität gibt jedes vierte Unternehmen (25 Prozent) an, regelmäßig externe Unterstützung in Anspruch zu nehmen (Abb. 15). Bei mittleren Unternehmen trifft dies gar auf jedes dritte Unternehmen (30 Prozent) zu. Ebenfalls ein Viertel aller Unternehmen (26 Prozent) greift für Quick-Scans zur ersten Einschätzung kritischer Situationen auf externe Ressourcen zurück. Darüber hinaus gibt fast jedes zweite Unternehmen (49 Prozent) an, externe Unterstützung fallweise für die Aufklärung hinzuzuziehen. Mehr als jedes zweite Unternehmen (58 Prozent) führt zunächst ausführliche interne Analysen durch.

21 Prozent der Befragten engagieren externe Dienstleister, um sogenannten Whistleblowern eine Möglichkeit zur Meldung zu geben.

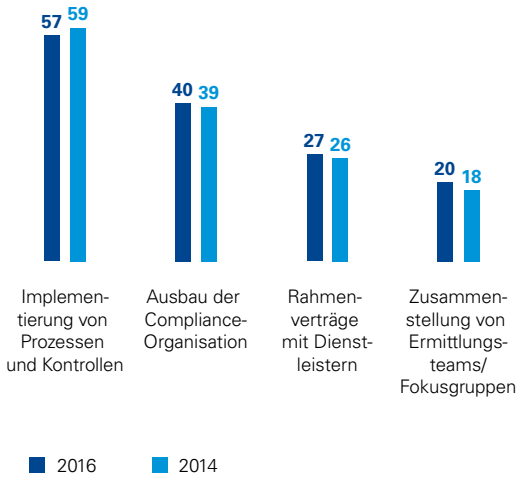
Abb. 15: Externe Unterstützung in der Aufklärung
Angaben in Prozent



Quelle: KPMG, 2016

Insbesondere bei der Implementierung von Prozessen und Kontrollen nehmen betroffene Unternehmen Unterstützung durch externe Dienstleister in Anspruch (57 Prozent). Zwei von fünf Unternehmen holen zudem beim Ausbau der Compliance-Organisation externe Expertise ins Haus (Abb. 16). Beide Entscheidungen sorgen dafür, dass im Rahmen der Aufklärung festgestellte Schwachstellen zeitnah und nachhaltig behoben werden können. Dabei erleichtert das Zusammenspiel zwischen internen und externen Ressourcen die zielgerichtete Überarbeitung, Ergänzung bzw. Neuausrichtung bestehender Maßnahmen.

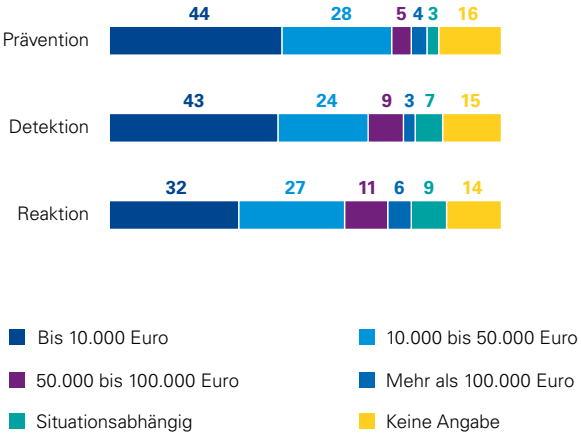
Abb. 16: Externe Unterstützung in der Aufklärung
Angaben in Prozent



Quelle: KPMG, 2016

Obwohl die betroffenen Unternehmen zur Bewältigung von Wirtschaftskriminalität in vielfältiger Weise auf externe Dienstleister zurückgreifen, sind sie nicht bereit, entsprechend in externe Unterstützung zu investieren. Beabsichtigte Investitionen von mehr als 50.000 Euro pro Geschäftsjahr bleiben in jeder Phase des Umgangs mit Wirtschaftskriminalität die Ausnahme. So sind in der Prävention lediglich neun Prozent der Befragten gewillt, einen Betrag dieser Höhe in externe Unterstützung zu investieren (Abb. 17). Für die Detektion gilt dies für zwölf Prozent der Studienteilnehmer, für die Reaktion für 17 Prozent. Diese Zahlen entsprechen nahezu unverändert denen der Vorgängerstudie.

Abb. 17: Investitionsbereitschaft in externe Unterstützung
Angaben in Prozent



Quelle: KPMG, 2016

Viele der Befragten sind lediglich bereit, bis zu 10.000 Euro in externe Unterstützung zu investieren. Im Rahmen der Prävention und bei der Detektion geben dies 44 Prozent bzw. 43 Prozent der Unternehmen an. Lediglich im Zuge der Reaktion ist die Investitionsbereitschaft etwas höher: Hier gibt etwa die Hälfte der Befragten an, mehr als 10.000 Euro pro Geschäftsjahr investieren zu wollen.

Unverändert sind Unternehmen weiterhin eher bereit, in die Reaktion als in die Prävention zu investieren. Dabei sind im Sinne des ökonomischen Prinzips gerade Investitionen in die Prävention von Wirtschaftskriminalität gut angelegtes Kapital: Die durch einen effektiven Präventionsansatz verhinderten Schäden und Folgekosten dürften die notwendigen Investitionskosten oft deutlich übersteigen.

Bewusstsein für Versäumnisse im Umgang mit wirtschaftskriminellen Handlungen steigt

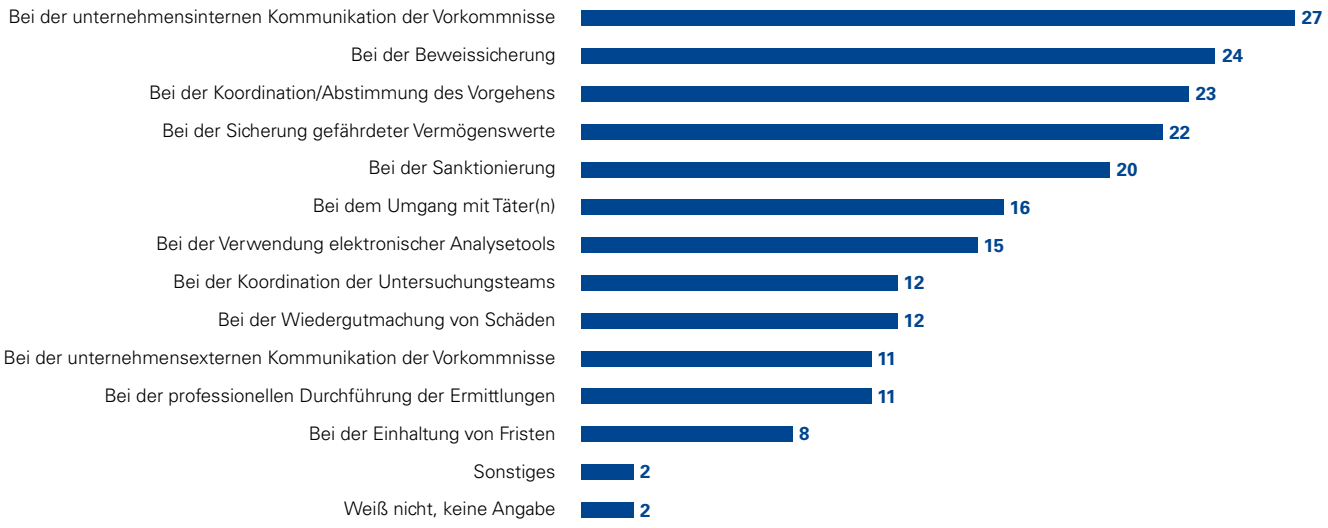
Im Umgang mit Wirtschaftskriminalität geben 63 Prozent der von wirtschaftskriminellen Handlungen betroffenen Unternehmen an, dass Versäumnisse bei der Reaktion auf wirtschaftskriminelle Handlungen aufgetreten sind. Unter den Unternehmen, die ihren Schutz gegenüber wirtschaftskriminellen Handlungen als schlecht bewerten, liegt dieser Anteil sogar bei 87 Prozent.

Diese Angaben sind insofern bemerkenswert, als im Rahmen früherer KPMG-Studien gegensätzliche Aussagen zu finden waren: 2014 etwa gaben lediglich vier Prozent der Befragten an, nicht angemessen auf wirtschaftskriminelle Handlungen reagiert zu haben.

Differenziert nach Art der konkreten Versäumnisse geben Unternehmen eine große Bandbreite unterschiedlicher Aspekte an. Fünf der abgefragten Aspekte wurden jeweils von mehr als einem Fünftel der betroffenen Unternehmen genannt (Abb. 18).

Jedes vierte Unternehmen sieht demnach Versäumnisse in der unternehmensinternen Kommunikation über die Vorkommnisse (27 Prozent). Diese Schwierigkeit wurde insbesondere von Befragten aus großen Unternehmen genannt (48 Prozent). Ein anderer Aspekt ist die Koordination bzw. Abstimmung des Vorgehens nach einem Vorfall (23 Prozent). In diesem Zusammenhang können klare Prozesse und Zuständigkeiten, beispielsweise in Form von definierten Krisenreaktions- und -kommunikationsplänen, dazu beitragen, eine angemessene interne Kommunikation und Koordination im Unternehmen zu gewährleisten. Insbesondere Unternehmen, die ihren Schutz vor Wirtschaftskriminalität als schlecht bewerten, nennen Versäumnisse in der internen Kommunikation und bei der internen Abstimmung.

Abb. 18: Versäumnisse beim Umgang mit wirtschaftskriminellen Handlungen
Angaben in Prozent



Quelle: KPMG, 2016

Knapp ein Viertel der betroffenen Unternehmen (24 Prozent) gesteht sich Versäumnisse bei der Beweissicherung ein. Bei großen Unternehmen liegt der Wert gar bei 41 Prozent. Auch elektronische Analysetools werden aus Sicht von 15 Prozent der Unternehmen nicht ausreichend oder mangelhaft eingesetzt. In Verbindung mit drohenden rechtlichen Auseinandersetzungen und Regressansprüchen, aber auch mit der Vermögenssicherungspflicht der Unternehmensleitung stellt die Beweissicherung einen zentralen Bestandteil jeder Untersuchung wirtschaftskrimineller Sachverhalte dar. Eine belastbare (gerichtsverwertbare) Beweissicherung kann dazu beitragen, Schäden, beispielsweise durch Schadensersatzansprüche an die Täter, zu verringern bzw. zu vermeiden – indem etwa Strafzahlungen abgewendet werden.

Elektronische Analysetools können zusätzliche Instrumente der Beweissicherung sein und die Verarbeitung und Auswertung großer Datenmengen möglich machen. Ob hier Versäumnisse benannt werden, hängt mit der Einstufung des eigenen Schutzniveaus zusammen: Knapp die Hälfte der Unternehmen, die sich als schlecht geschützt einstufen, beklagen Versäumnisse in Zusammenhang mit der Anwendung dieser Analysemethoden. Dies äußert dagegen nur eines von zehn Unternehmen mit gefühlt gutem Schutzniveau.

Die Befragten nennen zudem Versäumnisse bei der Sicherung gefährdeter Vermögenswerte (22 Prozent), der Koordination der Untersuchungsteams (zwölf Prozent) sowie der professionellen Ermittlung (elf Prozent).

Versäumnisse in Verbindung mit der Reaktion auf Wirtschaftskriminalität betreffen die Sanktionierung (20 Prozent), den Umgang mit dem Täter (16 Prozent), die Wiedergutmachung von Schäden (zwölf Prozent) sowie die Einhaltung von Fristen (acht Prozent). Die Sanktionierung bereitet insbesondere großen Unternehmen Schwierigkeiten (31 Prozent), obwohl sie angeben, in 93 Prozent der Fälle den Täter zur Rechenschaft gezogen zu haben. Möglicherweise werden die Sanktionsmaßnahmen als nicht angemessen betrachtet.

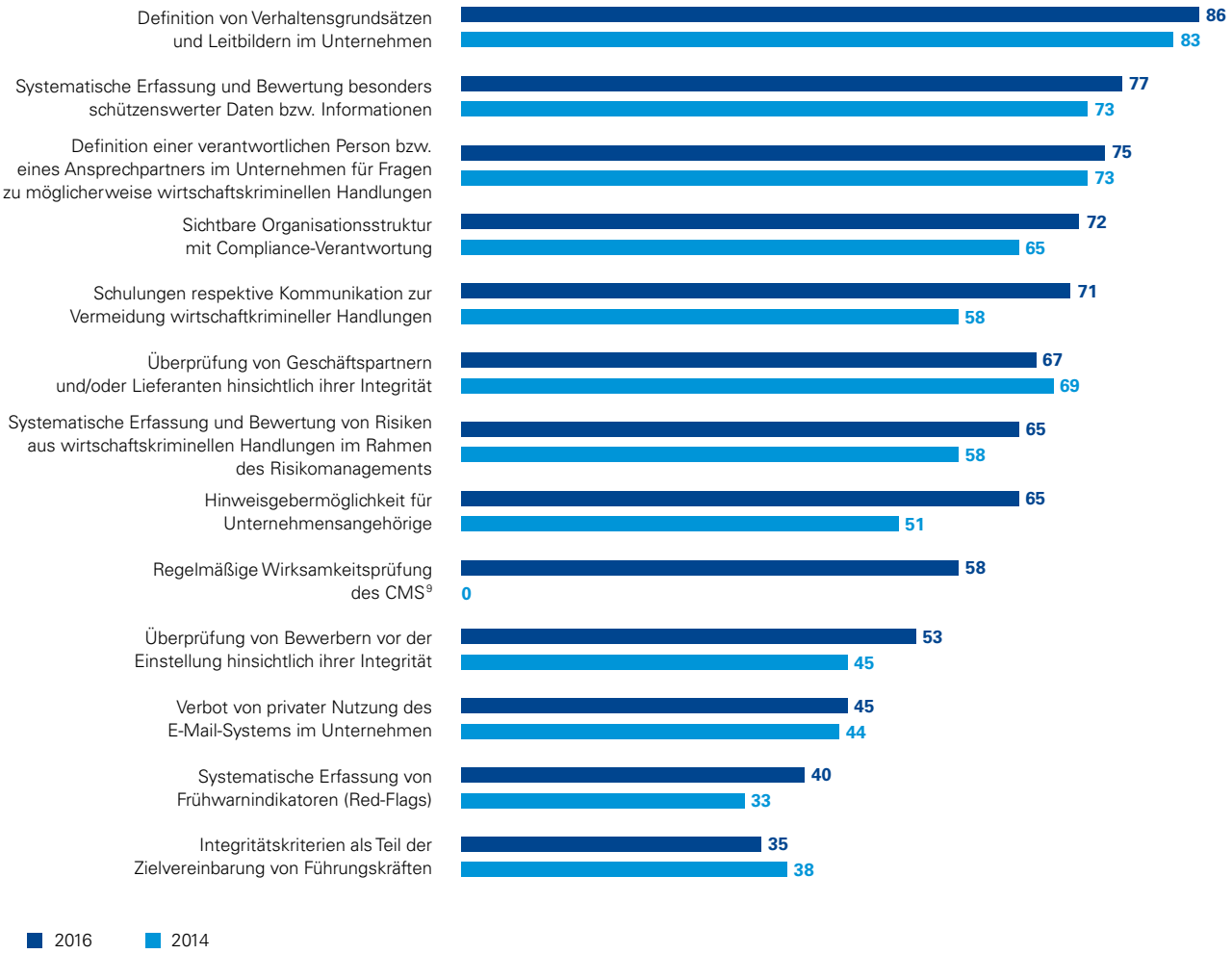
Bandbreite an Präventionsmaßnahmen steigt

Die Studienergebnisse belegen: Die Bedeutung der Prävention steigt. So wurden viele der abgefragten Maßnahmen prozentual häufiger verwirklicht als noch 2014. Sichtbar wird die gestiegene Bedeutung auch durch das größere Spektrum an Präventionsmaßnahmen.

Inzwischen haben etwa zwei Drittel der befragten Unternehmen acht der im Rahmen der Studie abgefragten Präventionsmaßnahmen umgesetzt (Abb. 19); 2014 waren es lediglich fünf dieser Maßnahmen.

Die Definition von Verhaltensgrundsätzen und Leitbildern im Unternehmen ist nach wie vor die meistgenannte präventive Maßnahme (86 Prozent). Ihre Bedeutung wird auch dadurch unterstrichen, dass 28 Prozent der Unternehmen fehlende Leitbilder und Verhaltensgrundsätze als Nährboden für wirtschaftskriminelle Handlungen ansehen. Insbesondere wenn es darum geht, die Unternehmenskultur zu stärken und die Mitarbeiter für mangelndes Unrechtsbewusstsein und Nachlässigkeit bei Unternehmensangehörigen zu sensibilisieren, können definierte und vorgelebte Verhaltensgrundsätze und Leitbilder eine präventive Wirkung gegen Wirtschaftskriminalität entfalten.

Abb. 19: Präventionsmaßnahmen
Angaben in Prozent



Quelle: KPMG, 2016

9 Diese Antwortmöglichkeit wurde in der diesjährigen Studie erstmalig abgefragt.

Drei Viertel der befragten Unternehmen geben an, im Rahmen ihrer Präventionsmaßnahmen besonders schützenswerte Daten und Informationen systematisch zu erfassen und zu bewerten. Knapp zwei Drittel der Studienteilnehmer nehmen diese systematische Einordnung auch im Rahmen ihres Risikomanagements vor. Sowohl die gestiegene Rolle von IT-Abteilungen im Rahmen wirtschaftskrimineller Handlungen als auch die vermehrte Anwendung von Datenanalysen nach Vorfällen zeigen, dass Daten zu immer wichtigeren Rohstoffen der Wirtschaft werden. Nur wer die eigenen Daten- und Informationsbestände kennt und bewerten kann, ist auch in der Lage, ein angemessenes Schutzkonzept zu entwickeln.

Drei von vier befragten Unternehmen geben an, über einen zentralen Ansprechpartner im Unternehmen für Fragen im Zusammenhang mit wirtschaftskriminellen Handlungen zu verfügen. Im Kontext mit den von Betroffenen genannten Versäumnissen im Rahmen der unternehmensinternen Kommunikation kann die Bestellung einer Ansprechperson dafür Sorge tragen, dass die internen Kommunikationskanäle gestrafft und zentriert werden. Hierdurch kann die Nachverfolgung etwaiger Hinweise in Bezug auf wirtschaftskriminelle Sachverhalte erleichtert werden.

Im Vergleich zu 2014 setzen heute mehr Unternehmen auf eine sichtbare Organisationsstruktur mit Compliance-Verantwortung (72 Prozent) sowie Schulungen bzw. Kommunikation zur Vermeidung von Wirtschaftskriminalität (71 Prozent). Diese Maßnahmen unterstützen die Sensibilisierung von Unternehmensangehörigen und können dazu beitragen, die Compliance-Kultur intern zu verankern und zu stärken. Allerdings gilt dies überwiegend für die großen Unternehmen, denn lediglich zwei von fünf kleinen Unternehmen haben diese Maßnahmen bislang ergriffen.

Jens C. Laue, Partner, KPMG in Deutschland, Head of Governance & Assurance Services Germany:

„Wenn es darum geht, Wirtschaftskriminalität zu verhindern, zählt die Erweiterung der Sichtweise von einer Aggregation einzelner Maßnahmen zur Prävention oder Sanktionierung von Verstößen hin zu einem geschlossenen Compliance-Management-System zu den wesentlichen Entwicklungen der letzten fünf Jahre. Erst diese Betrachtungsweise und Implementierung stellt sicher, dass alle Risiken von der Identifizierung bis zur Überwachung der dafür eingerichteten Programme erfasst werden. Und das spiegelt sich in den Ergebnissen wider: Obwohl Unternehmen beispielsweise Verhaltensgrundsätze und Leitbilder (86 Prozent) eingerichtet haben, sind sie offenbar in großem Maße von Wirtschaftskriminalität betroffen. Ähnliches lässt sich für Maßnahmen im Rahmen der Compliance-Organisation (zum Beispiel Definition von Ansprechpartnern, Aufbau einer Organisationsstruktur) oder der Compliance-Kommunikation (Schulungen, Whistleblowing) ablesen. Ein Grund für die dennoch hohe Anfälligkeit für Wirtschaftskriminalität liegt demnach darin, dass Einzelmaßnahmen häufig nicht systemisch eingeführt worden sind: Weniger als die Hälfte der Unternehmen erfasst beispielsweise Frühwarnindikatoren wirklich konsequent. Viel entscheidender aber: Nur 58 Prozent der Befragten lassen ihr CMS regelmäßig auf Wirksamkeit durch einen Dritten (zum Beispiel einen Wirtschaftsprüfer) kontrollieren. Für Unternehmen, die ihren Schutz gegenüber wirtschaftskriminellen Handlungen als schlecht bewerten, trifft dies sogar nur auf 26 Prozent zu. Dabei stellt eine solche Überwachung ein ganz wesentliches Element effektiver Prävention dar.

Die Wirksamkeitsprüfung unterstreicht den systemischen Charakter eines Compliance-Management-Systems und stellt anhand der vom Institut der Wirtschaftsprüfer (IDW) in Prüfungsstandard 980 definierten Grundelemente sicher, dass die von den Unternehmen eingeführten Grundsätze und Maßnahmen über einen Zeitraum tatsächlich so umgesetzt und eingehalten werden. Das Ergebnis ist eine holistische Betrachtung des Compliance-Systems statt einer isolierten Einschätzung einzelner Compliance-Elemente. Überwachung heißt dabei, Prozesse und Kontrollen permanent auf deren Wirksamkeit zu testen und somit für einen kontinuierlichen Verbesserungsprozess zu sorgen.

Unternehmen reagieren leider oft erst zu spät – zumal 39 Prozent der Befragten nach einem Fraud-Fall bei einem Geschäftspartner eine Wirksamkeitsprüfung des CMS fordern. In vielen Branchen ist es durchaus üblich, dass eine Liefer- und Leistungsbeziehung an den Nachweis eines wirksamen CMS durch den Kunden oder Lieferanten geknüpft wird. Auch hier stellt sich die Frage, ob durch eine proaktive Prüfung entsprechende Fälle nicht wirksam hätten verhindert werden können.

Betrachtet man die von den Studienteilnehmern geplanten Präventionsmaßnahmen der nächsten zwei Jahre, so überrascht es aufgrund der weiterhin hohen Betroffenheit von Wirtschaftskriminalität nicht, dass die Wirksamkeitsprüfung eine der am meisten benannten (zwölf Prozent) zukünftigen Maßnahmen darstellt. Dem steht allerdings auch eine in Teilen ablehnende Haltung gegenüber: Jedes vierte Unternehmen hat nicht vor, in nächster Zeit eine Prüfung durchführen zu lassen. Allerdings rührt diese Ablehnung nicht unbedingt daher, dass der Mehrwert einer solchen Überwachung nicht gesehen werden würde. Vielmehr legen die Ergebnisse nahe, dass eine Überprüfung durchaus als sinnvolles Element zum Schutz vor wirtschaftskriminellen Handlungen eingestuft wird. Die Ablehnung könnte darauf zurückzuführen sein, dass eine Überprüfung erst erfolgt, wenn das CMS eingeführt worden ist – sie steht also am Ende des erst begonnenen Prozesses.

Wie schon 2014 geben zwei Drittel der befragten Unternehmen an, Geschäftspartner und/oder Lieferanten auf Integrität zu überprüfen. Gerade im Zusammenhang mit möglichen Reputationsrisiken, die durch Geschäftspartner bzw. Lieferanten entstehen können, sind Integritätsprüfungen und Hintergrundrecherchen ein sinnvolles Mittel zur Risikominderung. Zudem sollte eine derartige Überprüfung mit nicht allzu hohem Aufwand zu bewerkstelligen sein. Hinsichtlich der eigenen Mitarbeiter führt etwa die Hälfte der Unternehmen derartige Überprüfungen durch.

Nur zwei von fünf Unternehmen geben an, Warnsignale, sogenannte „Red Flags", systematisch zu erfassen. Mit Blick auf die Unternehmensgröße zeigen sich hier allerdings einmal mehr enorme Unterschiede. 62 Prozent der großen Unternehmen führen diese Analyse durch. Unter den kleinen Unternehmen ist es nur ein Drittel. Proaktive Kontrollmöglichkeiten werden daher nach wie vor vergleichsweise selten umgesetzt.

Betrachtet man in dieser Hinsicht wiederum gesondert Unternehmen, die ihren Schutz vor wirtschaftskriminellen Handlungen als schlecht einschätzen, fällt auf, dass diese insbesondere im Hinblick auf organisatorische Maßnahmen gegenüber den übrigen Studienteilnehmern zurückfallen. Dies betrifft neben der schon genannten Wirksamkeitsprüfung des CMS insbesondere die Benennung eines zentralen Ansprechpartners (47 Prozent), eine Organisationsstruktur mit Compliance-Verantwortung (32 Prozent) sowie Schulungen zur Vermeidung wirtschaftskrimineller Handlungen (49 Prozent). Wie wichtig gleichwohl präventive Maßnahmen für das eigene Schutzniveau sind, scheint diesen Unternehmen angesichts der wenig positiven Eigenbewertung durchaus bewusst zu sein.

„Kommissar Zufall" seltener für Aufdeckung verantwortlich

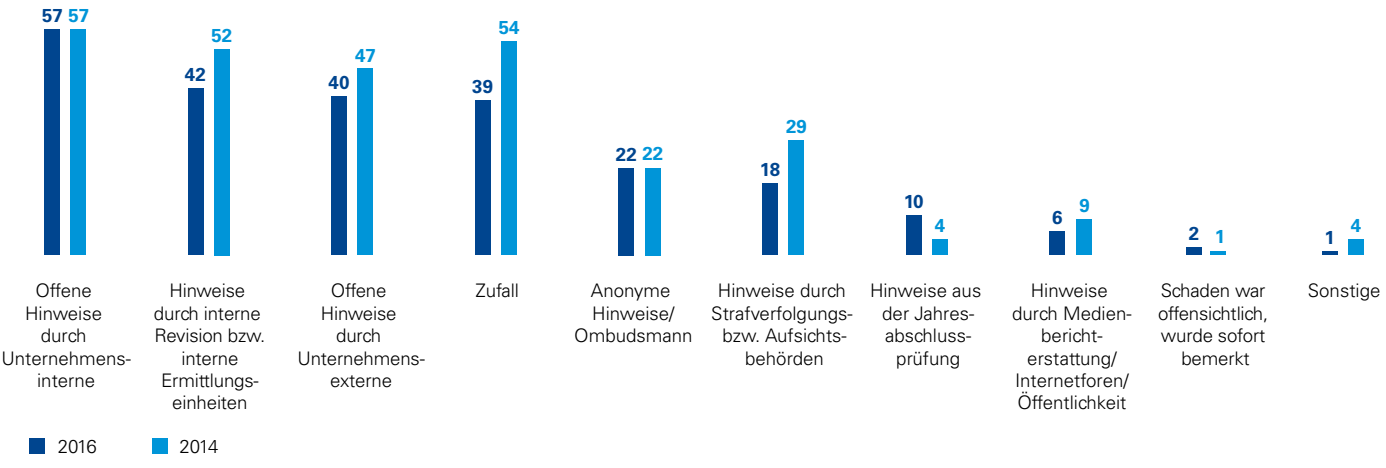
Wirtschaftskriminelle Handlungen werden weiterhin hauptsächlich durch offene Hinweise Unternehmensinterner aufgedeckt. Wie 2014 gilt dies für 57 Prozent der Fälle (Abb. 20). Dies spricht grundsätzlich dafür, dass bei den befragten Unternehmen eine gute Meldekultur herrscht. In diesem Zusammenhang geben zwei von drei Unternehmen an, über Hinweisgebermöglichkeiten für Unternehmensangehörige zu verfügen (65 Prozent).

Zufällige Entdeckungen verlieren an Bedeutung. Während 2014 noch mehr als die Hälfte (54 Prozent) der betroffenen Unternehmen angab, Vorfälle per Zufall entdeckt zu haben, trifft dies nun für weniger als zwei Fünftel der Unternehmen zu (39 Prozent). Gleichwohl zeigen sich Unterschiede hinsichtlich der Unternehmenskategorien: In kleinen Unternehmen gibt nur eines von vier an, wirtschaftskriminelle Sachverhalte durch Zufall aufgedeckt zu haben. In großen Unternehmen gilt dies für jedes zweite Unternehmen. Dies zeigt, dass größere und möglicherweise komplex strukturierte Unternehmen nach wie vor häufig von „Kommissar Zufall" bei der Aufdeckung wirtschaftskrimineller Sachverhalte abhängig sind.

Neben den offenen Hinweisen durch Unternehmensinterne spielen Hinweise durch die Interne Revision bzw. interne Ermittlungseinheiten (42 Prozent) sowie offene Hinweise durch Unternehmensexterne wie Geschäftspartner, Lieferanten oder Kunden (40 Prozent) eine wichtige Rolle. Weniger relevant sind hingegen wie schon 2014 anonyme Hinweise (22 Prozent), Hinweise durch Strafverfolgungs- bzw. Aufsichtsbehörden (18 Prozent) sowie Hinweise durch die Medienberichterstattung oder durch die Öffentlichkeit (sechs Prozent).

Hinweise aus der Jahresabschlussprüfung werden nur von jedem zehnten Unternehmen genannt (2014: jedes 25. Unternehmen).

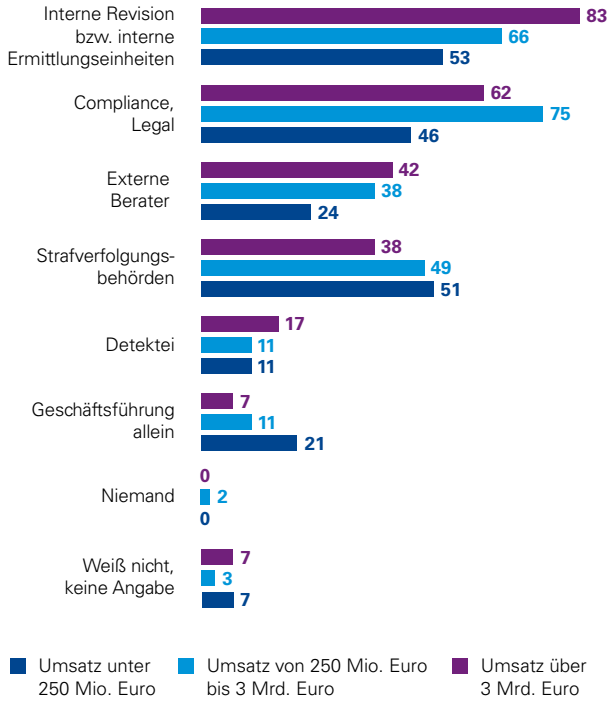
Abb. 20: Entdeckung der Handlung
Angaben in Prozent



Quelle: KPMG, 2016

Der schon 2014 beschriebene Trend, interne Abteilungen mit der Aufklärung von wirtschaftskriminellen Handlungen zu betrauen, hält an. So nennen jeweils knapp zwei Drittel der Betroffenen die Interne Revision bzw. interne Ermittlungseinheiten (65 Prozent) sowie den Bereich Compliance/Legal (63 Prozent) als zuständige Abteilungen für die operative Aufklärung (Abb. 21). Bei großen Unternehmen können die Interne Revision bzw. interne Ermittlungseinheiten schon fast als Standardorgan für die Aufklärung bezeichnet werden (83 Prozent). Dies spricht dafür, dass diese Einheiten bei großen Unternehmen mit den entsprechenden Ressourcen ausgestattet und entsprechend spezialisiert sind. Der Bereich Compliance/Legal ist in drei Viertel der mittleren Unternehmen mit der operativen Aufklärung betraut, jedoch in weniger als zwei Dritteln der großen Unternehmen für diese Aufgaben zuständig (62 Prozent).

Abb. 21: Operative Aufklärung
Angaben in Prozent



Quelle: KPMG, 2016

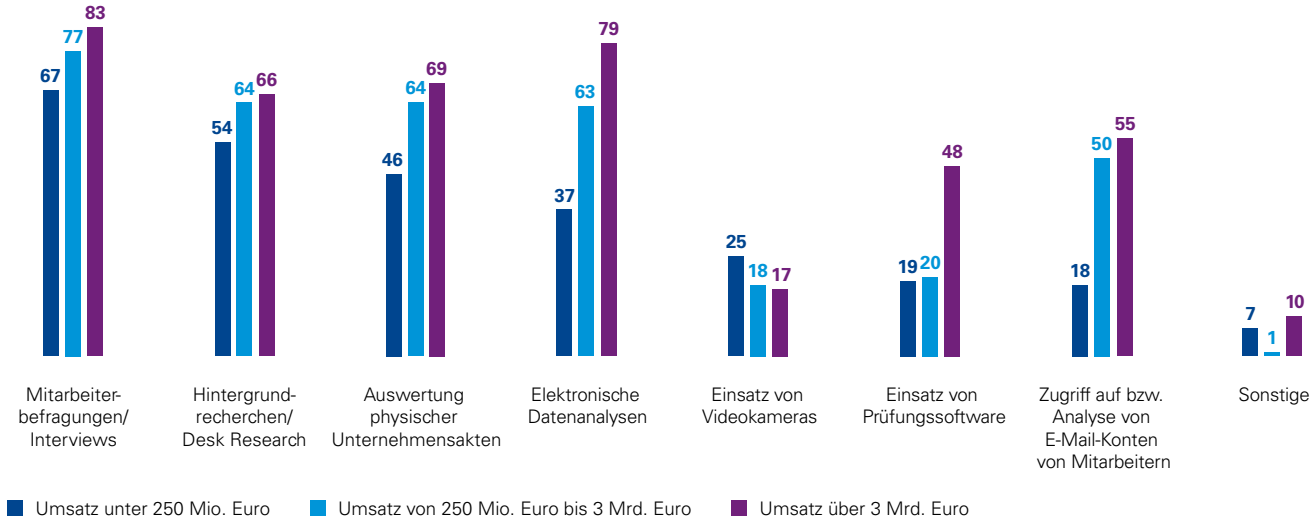
Strafverfolgungsbehörden befassen sich bei weniger als 50 Prozent der befragten Unternehmen mit der operativen Aufklärung wirtschaftskrimineller Sachverhalte – bei großen Unternehmen lag der Wert sogar bei nur 38 Prozent. Externe Berater wie Rechtsanwälte und Wirtschaftsprüfer werden in etwa einem Drittel der Fälle zur operativen Aufklärung herangezogen. Detekteien spielen, wie schon 2014, kaum eine Rolle bei der Aufklärung (zwölf Prozent).

Gegenüber 2014 ist die Geschäftsführung seltener alleinig für die Aufklärung zuständig (13 Prozent). Anders bei kleinen Unternehmen: Hier wird die Geschäftsführung noch bei jedem fünften betroffenen Unternehmen ohne Unterstützung anderer Aufklärungsorgane aktiv (21 Prozent). Angesichts der Komplexität vieler wirtschaftskrimineller Sachverhalte, der Notwendigkeit einer zügigen Aufklärung und der hohen Anforderungen, die an eine (gerichtsverwertbare) Beweissicherung gestellt werden, sollte das Management dieser Unternehmen frühzeitig spezialisierte interne oder externe Fachleute einbeziehen.

Elektronische Aufklärungsmaßnahmen auf dem Vormarsch

Im Rahmen der Aufklärungsmaßnahmen (Abb. 22) dominieren nach wie vor die Mitarbeiterbefragung (75 Prozent), Hintergrundrecherchen (61 Prozent) sowie die Auswertung physischer Unternehmensakten (59 Prozent).

Abb. 22: Aufklärungsmaßnahmen
Angaben in Prozent

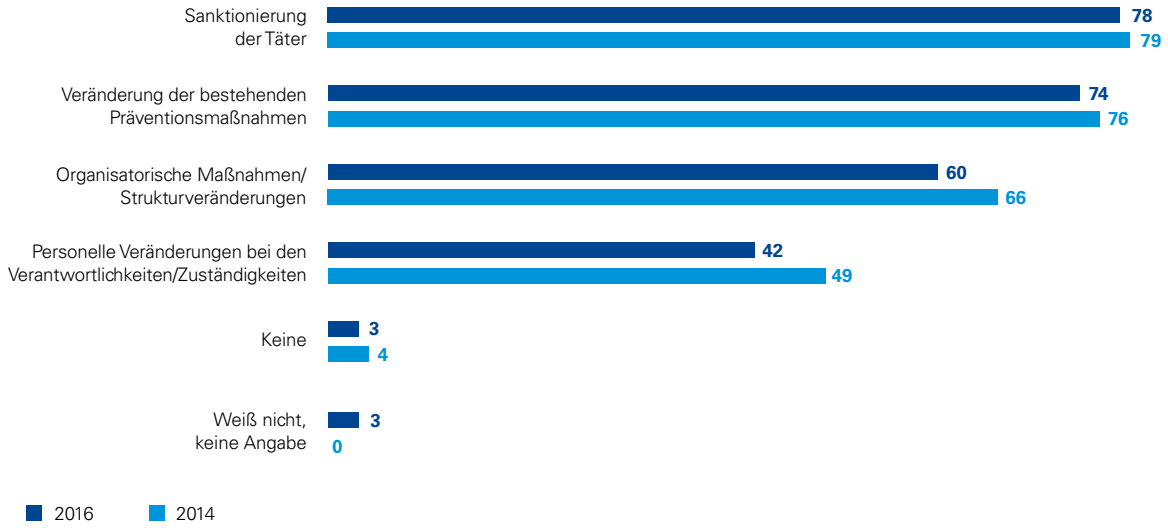


Quelle: KPMG, 2016

Neben diesen Maßnahmen setzt sich allerdings der Trend fort, elektronische Datenanalysen zur Aufklärung von Wirtschaftskriminalität einzusetzen (57 Prozent). Der Rohstoff „Daten" ist für die heutige Wirtschaft, aber auch im Rahmen der Wirtschaftskriminalität eminent wichtig geworden. Durch die zunehmende Digitalisierung der Geschäftswelt dürfte die elektronische Datenanalyse für die Aufklärung der meisten wirtschaftskriminellen Sachverhalte unerlässlich sein. Bei großen Unternehmen löst die elektronische Datenanalyse (79 Prozent) bereits heute die Auswertung von physischen Unternehmensakten (69 Prozent) als eine der wesentlichen Untersuchungsmethoden ab. Auch bei mittleren Unternehmen führen 63 Prozent der Betroffenen schon Datenanalysen durch; so häufig etwa wie die Auswertung der physischen Unternehmensakten (64 Prozent). Lediglich kleine Unternehmen setzen nach wie vor auf analoge Untersuchungsmethoden.

Neben der elektronischen Datenanalyse bietet auch die Analyse von E-Mail-Konten und sonstigen unstrukturierten Daten Möglichkeiten der IT-gestützten Aufklärung. Große und mittlere sind auch hier wesentlich aktiver als kleine Unternehmen. Etwa die Hälfte der großen und mittleren Unternehmen wertet E-Mail-Konten aus (55 bzw. 50 Prozent). Gleiches gilt bei großen Unternehmen für den Einsatz von Prüfungssoftware (48 Prozent). Bei kleinen Unternehmen werden beide Instrumente derzeit nur von etwa jedem fünften betroffenen Unternehmen eingesetzt. Mit Blick auf eine Effizienzsteigerung und Professionalisierung der Aufklärungsmaßnahmen bieten IT-gestützte Aufklärungsinstrumente hier also erhebliche Potenziale, insbesondere bei kleinen Unternehmen. Dabei gilt stets, dass Unternehmen die einschlägigen Datenschutzregelungen beachten müssen.

Abb. 23: Maßnahmen nach der Aufklärung
Angaben in Prozent



Quelle: KPMG, 2016

Eine wesentliche Maßnahme nach der Aufklärung von wirtschaftskriminellen Sachverhalten ist die Sanktionierung der Täter, die bei 78 Prozent der Unternehmen erfolgt. Obgleich dies einen hohen Wert darstellt, bedeutet es im Umkehrschluss, dass die Täter in 22 Prozent der betroffenen Unternehmen nicht sanktioniert werden. Dabei bieten Sanktionen wirkungsvolle Instrumente zur nachhaltigen Abschreckung. Insofern ist es bemerkenswert, dass jedes fünfte Unternehmen von einer Sanktionierung absieht.

Neben der Sanktionierung der Täter leiten viele Unternehmen nach wirtschaftskriminellen Vorfällen im Sinne eines Lerneffekts und zur Erlangung eines besseren Schutzes insbesondere zukunftsorientierte Maßnahmen ein (Abb. 23). Hierzu gehören Veränderungen der bestehenden Präventionsmaßnahmen (74 Prozent) sowie Strukturveränderungen im Unternehmen (60 Prozent).

4. Über die Studie

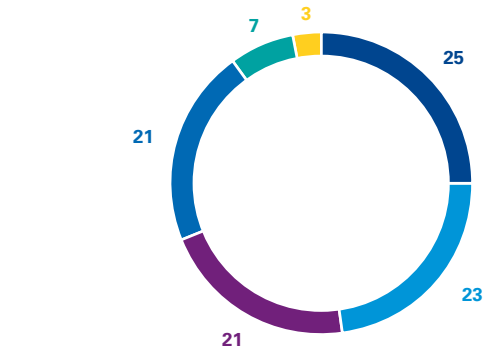
In der diesjährigen Studie wurden 500 repräsentativ nach Branche, Mitarbeiterzahl und Umsatz ausgewählte Unternehmen zu ihren Erfahrungen im Bereich Wirtschaftskriminalität befragt.

Wie in den vorherigen Studien zur Wirtschaftskriminalität in Deutschland wurde das Sozialforschungsinstitut TNS Emnid in Bielefeld mit den telefonischen Interviews durch speziell geschulte Mitarbeiter beauftragt. Die Erfahrung hat gezeigt, dass aufgrund der Komplexität des Themas die Teilnehmer der Studie eine persönliche Befragung wünschen. Die Interviews wurden im März/April 2016 durchgeführt. Die konkreten Gesprächspartner und deren jeweilige Antworten sind KPMG nicht bekannt.

Der standardisierte Fragebogen orientiert sich an der Struktur der Vorgängerstudie mit Anpassungen bezüglich der diesjährigen Schwerpunkte der Studie. Außerdem sollte auch die vorliegende Studie wie schon die Vorgängerstudien mit der von KPMG veröffentlichten „e-Crime-Studie" vergleichbar sein.

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

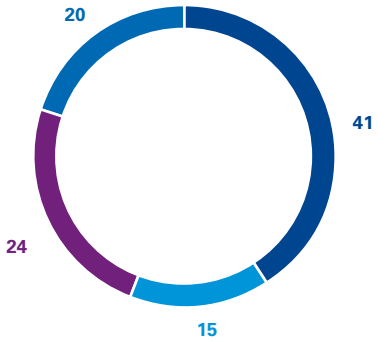
Abb. 24: Funktion des Ansprechpartners
Angaben in Prozent



- Compliance-Officer
- Mitglieder Vorstand/Geschäftsführung
- Leiter/-in Controlling/Rechnungswesen
- Leiter/-in Recht
- Leiter/-in Interne Revision
- Leiter/in Risikomanagement

Quelle: KPMG, 2016

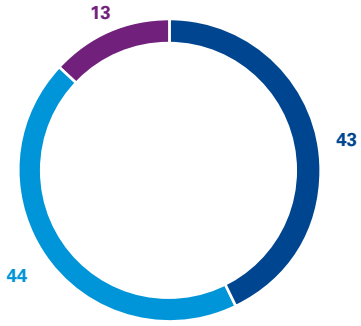
Abb. 25: Befragte nach Branche
Angaben in Prozent



- Verarbeitendes Gewerbe (Automobilindustrie, Chemie und Pharma, Energie und Rohstoffe, Industrielle Produktion, Technologie)
- Handel (Handel und Konsumgüter)
- Andere Dienstleister (Gesundheitswirtschaft, Medien und Telekommunikation, Öffentlicher Sektor)
- Finanzdienstleister (Kreditinstitute, Versicherungen)

Quelle: KPMG, 2016

Abb. 26: Befragte nach Umsatz
Angaben in Prozent



- Umsatz unter 250 Mio. Euro
- Umsatz von 250 Mio. Euro bis 3 Mrd. Euro
- Umsatz über 3 Mrd. Euro

Quelle: KPMG, 2016

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 Fachleute 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 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 analysieren wir umfangreiche Unternehmensdaten.

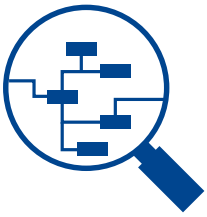
Forensic Due Diligence
Im Rahmen von Transaktionen unterstützen unsere Spezialisten bei der Identifizierung von Fraud-Risiken, Compliance-Schwachstellen und der Aufarbeitung konkreter Vorfälle beim Kaufobjekt. Dabei werden wir sowohl auf Käufer- als auch auf Verkäuferseite tätig. Auf Basis der Erkenntnisse aus der 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-Management-Systems, 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 Monitoring-Maßnahmen.

Fraud Risk Management
Unsere Spezialisten unterstützen bei der Implementierung von Maßnahmen zu 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 Fachleute Integrity Due Diligences (IDD) anhand 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.

Cyber Insurance Service
Unsere Beratungsleistungen begleiten den gesamten Lebenszyklus von Cyber-Versicherungen von der Produktentwicklung, Pre- und Post-Binding über Krisenreaktion und forensische Aufklärung bis hin zu Remediation im Nachgang von Cyber-Vorfällen und Benchmarking von Versicherungskennzahlen. Zu unseren Leistungen für Versicherungen und Makler zählen dabei unter anderem Empfehlungen zur Praxistauglichkeit von Bedingungswerken und Reaktionsverfahren im Ernstfall, die Risikobeurteilung von potenziellen Versicherungsnehmern durch ein standardisiertes Assessment, den sogenannten „KPMG CyberSAFE“, sowie die Einrichtung einer individuellen deutschen und internationalen Hotline mit garantierten Reaktionszeiten zur Erstmeldung von Vorfällen.



Forensic Data Center
Um Unternehmen oder Behörden bestmöglich unterstützen und Untersuchungshandlungen unabhängig durchführen zu können, betreibt Forensic Technology ein hochgesichertes Forensic Data Center (FDC). Über 50 Server mit skalierbarem Speicherplatz sorgen für 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 Kunden bewertet und entsprechend nachverfolgt. Mit über 80 Spezialisten stehen wir unseren Mandanten bundesweit zur Verfügung.

Platz für Ihre Notizen

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft

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

An dieser Studie haben mitgewirkt:
Zhen Cai und Marc Oliver Scheben

www.kpmg.de/forensic

www.kpmg.de/socialmedia