



MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG

In unserer Studie erfahren sie, wie deutsche Unternehmen mit Wirtschaftskriminalität in der analogen und digitalen Welt umgehen und wie Compliance-Programme sich haftungsrechtlich auswirken.

Wirtschaftskriminalität 2018

Mehrwert von Compliance – forensische Erfahrungen



www.pwc.de/wirtschaftskriminalitaet_2018

Das digitale Zeitalter geht mit neuen Formen der Kriminalität einher: 47 % der Unternehmen sind bereits Opfer einer Cyber-Attacke geworden – oder haben den konkreten Verdacht.

IT-Sicherheit wird zum existenziellen Thema. Wie können sich Unternehmen gegen digitale Angriffe wappnen? Cyberrisiken dürfen nicht zum Hemmschuh für die Industrie 4.0 werden.

Mehrwert von Compliance – forensische Erfahrungen

Unsere neunte Studie zur Entwicklung der Wirtschaftskriminalität setzt ihre Schwerpunkte auf die weitere Entwicklung von Compliance-Programmen und der forensischen Praxis der von Wirtschaftskriminalität betroffenen Unternehmen.

Rasanter Anstieg der Fälle von Cybercrime

Im Unterschied zur rückläufigen Entwicklung der analogen Wirtschaftskriminalität (Abnahme um sechs Prozentpunkte) stellen wir einen rasanten Anstieg im Bereich Cybercrime fest. Fast jedes zweite Unternehmen (46 %) berichtete über mindestens einen Fall. Dies bedeutet gegenüber 2015 einen Anstieg um zwölf Prozentpunkte. Der Abstand zwischen analoger (49 %) und digitaler Kriminalität (46 %) ist somit weitgehend verschwunden.

Allerdings verursachten analoge Formen der Wirtschaftskriminalität im Durchschnitt gesehen weiterhin deutlich höhere Schäden als Cybercrime. Die durchschnittlichen Kosten infolge eines schweren Wirtschaftsdelikts bezifferten die betroffenen Unternehmen auf 7,23 Millionen Euro, während Fälle von Cybercrime durchschnittlich Schäden in Höhe von 183.000 Euro verursachten.

Risiko CEO-Fraud

Hohe Schäden entstanden auch durch CEO-Fraud. 40 % der befragten Unternehmen berichteten zwar nur über einen Versuch, aber bei 5 % der Unternehmen war der CEO-Fraud erfolgreich und verursachte in den schweren Fällen einen durchschnittlichen Schaden in Höhe von 4,4 Millionen Euro. Alarmierend sind auch Berichte über Angriffe in Form von Distributed Denial of Service (DDoS) und Verschlüsselungs- bzw. Erpressungstrojanern. 8 % der Unternehmen berichteten über leichte bis schwere DDoS-Fälle und 18 % über Trojaner. Einige Unternehmen berichteten sogar, das geforderte Lösegeld gezahlt zu haben.

Compliance-Programme weiterhin im Aufwind

Drei Viertel der mittelständischen Unternehmen und Großunternehmen verfügen über ein Compliance-Management-System (CMS) und bei weiteren 10 % befindet es sich in der Planung. Auch bei kleineren Mittelständlern mit 500 bis 999 Mitarbeitern ist heute ein CMS überwiegend selbstverständlich (60 %). Der Trend, Compliance-Programme auf zusätzliche Deliktsfelder auszuweiten, hält unvermindert an, wobei der Fokus auf der Prävention gegen Korruption (CMS 83 %), Kartellrechtsverletzungen (CMS 62 %) und Geldwäsche (CMS 65 %) liegt.

In unseren vertieften Interviews berichteten Unternehmen über noch bestehende Schwächen in der Umsetzung ihres CMS, denen sie sich verstärkt widmen wollen. Genannt wurden Kommunikationsprobleme, mangelnde Awareness und eine zu formale Ausgestaltung des CMS, eine mangelnde Konsistenz der Regelungen sowie eine unzureichende Integration in den Geschäftsprozessen, insbesondere bei global agierenden Unternehmen.

Klarer Trend: Aufstockung der Budgets für Personal- und Sachmittel des CMS

In den vergangenen fünf Jahren beobachteten nahezu alle Unternehmen eine leichte (34 %) oder starke Zunahme (59 %) der Anforderungen an ihr CMS, sodass jedes zweite die Personal- und Sachmittelausstattung hierfür leicht (33 %) oder deutlich (22 %) aufgestockt hat. Über eine allenfalls leichte Reduzierung berichteten nur 2 % der Unternehmen, bei 43 % der Unternehmen blieb das Budget unverändert.

Konkret zeigt sich dieser klare Trend bei der personellen Aufstockung des Compliance-Managements. Im Durchschnitt kommen heute rund 1.500 Mitarbeiter auf eine Compliance-Officer-Stelle, während es vor vier Jahren noch rund 2.400 waren. Die Relation ist bei fast zwei Dritteln der Unternehmen sogar deutlich besser. Bei einem Drittel (33 %) kommen sogar auf 500 Mitarbeiter bzw. bei 29 % der Unternehmen auf 500 bis 1.000 Mitarbeiter eine Compliance-Officer-Stelle.

Hinweisgebersysteme waren lange Zeit umstritten, mittlerweile entwickelten sie sich zum CMS-Standard.

Compliance-Vertragsklauseln werden in der Lieferkette immer üblicher

Aufgrund der wachsenden Erwartung im Markt und der Reputations- und Haftungsrisiken versuchen die meisten Unternehmen den Compliance-Risiken auch in ihrem geschäftlichen Umfeld konsequent zu begegnen. Einer deutlichen Mehrheit der Unternehmen (82 %) ist mittlerweile wichtig bzw. sehr wichtig, dass ihre Lieferanten und Dienstleister über ein CMS verfügen oder eines einführen. Viele Unternehmen berichteten, dass es inzwischen zur Routine gehöre, Compliance-Standards von ihren Lieferanten und Dienstleistern einzufordern. Dieser Erwartungsdruck in Richtung Geschäftspartner geht immer häufiger auch von mittelständischen Unternehmen aus.

Auch sie nutzen zunehmend ihren vertraglichen Gestaltungsspielraum. Verbreitet sind Compliance-Verpflichtungserklärungen, die Zusicherung eines Rechts auf anlassbezogene Prüfung und Compliance-Haftungsklauseln. Allerdings nehmen hierdurch auch Konflikte zwischen verschiedenen Compliance-Standards zu, die sich jedoch weitgehend vermeiden ließen, wenn Zertifizierungen selbstverständlicher werden würden. Nur knapp die Hälfte der befragten Unternehmen hat eine unabhängige Prüfung nach dem IDW PS 980 oder eine Zertifizierung gemäß ISO 19600 durchführen lassen (Abschnitt D6, 47 %), sodass in der Praxis eine Vielfalt an CMS herrscht, die eine gegenseitige Anerkennung erschwert.

Compliance beats corruption

Das Eis scheint gebrochen, alle von uns erhobenen Kennwerte deuten auf eine sinkende Korruptionsbelastung der deutschen Wirtschaft hin. Durch Korruption wurden nur 6 % der Unternehmen betroffen und gegenüber 2015 nahmen die Verdachtsfälle von 19 % auf 11 % ab. Auch der Anteil der Unternehmen, denen Geschäfte vermutlich infolge von Korruption eines Wettbewerbers entgangen sind, sinkt von 21 % auf 9 %. Diese Entwicklung dürfte vor allem auf die wachsende Zahl von Anti-Korruptionsprogrammen zurückzuführen sein, die zunehmend auch in mittelständischen Unternehmen implementiert wurden.¹ Über drei Viertel (77 %) der Unternehmen mit 1.000 bis 4.999 Mitarbeitern und fast zwei Drittel (60 %) der Unternehmen mit 500 bis 999 Mitarbeitern verfügen über ein entsprechendes CMS. Rechtlich wurde diese Entwicklung vermutlich auch durch die Erweiterung der strafrechtlichen Haftung nach § 299 StGB unterstützt, da nunmehr Bestechung und Bestechlichkeit auch außerhalb einer Wettbewerbssituation strafbar sind.

Schulungen und Hinweisgebersysteme werden zur Norm

Für die meisten Unternehmen sind im Rahmen ihres korruptionsrechtlichen CMS Classroom-Schulungsmaßnahmen (70 %) ein wesentlicher Bestandteil. Zunehmend werden jedoch auch digitale Trainingsformate eingesetzt, fast zwei Drittel der Schulungsmaßnahmen erfolgen durch webbasierte Lernprogramme und Schulungsfilme (61 %).

Hinweisgebersysteme waren lange Zeit umstritten, mittlerweile entwickelten sie sich zum CMS-Standard. Die Mehrheit der Unternehmen bietet nicht nur einen internen Ansprechpartner an, sondern auch eine telefonische Hotline (57 %), ein webbasiertes System (35 %) oder eine Ombudsperson (29 %). 86 % der Unternehmen sehen mindestens einen dieser Kommunikationskanäle vor. In unseren vertieften Interviews zeigten sich die Unternehmen ganz überwiegend vom Nutzen ihres Hinweisgebersystems überzeugt und wollen hierauf nicht mehr verzichten. Fälle von Missbrauch werden als Ausnahmen angesehen.

Hinweisgebersysteme sollten nicht auf unternehmensinterne Personen beschränkt sein, wie unsere Studien zur Bedeutung externer Hinweise zeigen. Zudem fordern die Richtlinien des Foreign Corrupt Practices Act (FCPA), dass solche Systeme außenstehenden Dritten zugänglich sind. Jedoch zeigen unsere Ergebnisse, dass nur knapp jedes dritte Hinweisgebersystem auch Geschäftspartnern und Subunternehmen (31 %) und jedes vierte allgemein der Öffentlichkeit (23 %) zugänglich ist. In dieser Hinsicht besteht bei vielen Unternehmen noch Handlungsbedarf.

¹ Bei Großunternehmen sind Anti-Korruptionsprogramme selbstverständlich (97 %).

Erste Erfolge im Kampf gegen Kartellrechtsverstöße

Nicht nur in der Bekämpfung der Korruption zeigt sich eine präventive Wirkung der Compliance-Programme, sondern auch bei den Kartellrechtsverstößen gibt es Anzeichen für einen Rückgang. Der Anteil der Unternehmen, die über einen Verdacht auf einen kartellrechtlichen Verstoß berichteten, sinkt auf 8%. Gleichzeitig halten es Unternehmen seltener für wahrscheinlich, ein Angebot zu einer wettbewerbswidrigen Absprache zu erhalten (4%). Allerdings sank nach den Angaben der befragten Unternehmen der Marktanteil (8%), der auf wettbewerbswidrigen Absprachen beruht, nur leicht. Wir führen diese Entwicklung auf die wachsende Verbreitung von Compliance-Programmen zurück (62%), und zwar auch im Mittelstand.

Marktwirtschaftlicher und rechtlicher Mehrwert von Compliance

Unsere Studie zeigt, dass sich aus Sicht der allermeisten Unternehmen ein CMS sowohl auf inländischen als auch ausländischen Märkten vorteilhaft auswirkt. Über ein Drittel (36%) beurteilt das eigene Compliance-Programm im Wettbewerb überwiegend als vorteilhaft und ein Viertel (24%) erkennt hierin sogar einen klaren Vorteil. Nur 9% berichteten über Wettbewerbsnachteile im deutschen Markt, davon nur 1% über klare Wettbewerbsnachteile.

Überdies können wir mit unserer Studie als Erste in Deutschland aufzeigen, dass sich ein CMS nicht nur in wirtschaftlicher Hinsicht als vorteilhaft erweist, sondern auch in haftungsrechtlicher. 21 Unternehmen berichteten über ihre Erfahrungen mit den Strafverfolgungsbehörden bei Verfahren nach § 130 Abs. 1 OWiG. Über ein Drittel (37%) der betroffenen Unternehmen gab an, dass die Tatsache, dass sie über ein CMS verfügten, die Höhe der Geldbuße positiv beeinflusst habe. Bei 43% der Unternehmen, die ein CMS implementiert hatten, beförderte dies die Einstellung des Verfahrens. Bei jedem dritten Unternehmen hat sich zudem die nachträgliche Zusage, ein CMS einzuführen bzw. Verbesserungen vorzunehmen, auf die Höhe der Geldbuße positiv ausgewirkt; bei fast jedem zweiten Unternehmen beförderte dies die Einstellung des Verfahrens.

Hoher Anteil statushoher interner Täter sowie der organisierten Kriminalität (OK)

Rund die Hälfte der gegen Unternehmen gerichteten Wirtschaftsstraftaten wird von Personen aus dem eigenen Unternehmen begangen. Dabei handelte es sich in jedem vierten Fall (25%) um eine Person aus der obersten Führungsebene. Empirisch gesehen sind folglich besondere Vorsicht und Sorgfalt bei der Auswahl und Überwachung von Personen in Führungs- und Vertrauenspositionen geboten. Betrachtet man die Gruppe der externen Täter, beunruhigt der relativ hohe Anteil derjenigen, die vermutlich aus dem Kreis der OK stammen (19%).

Interne Untersuchungen sind die Regel

In dieser Studie haben wir einen Schwerpunkt auf die forensische Praxis betroffener Unternehmen gelegt. Die Aufklärung bzw. Aufdeckung etwaiger Straftaten durch interne oder hiermit beauftragte externe Spezialisten ist für eine große Mehrheit der Unternehmen selbstverständlich (85%). Die Leitung oblag zumeist entweder der Internen Revision (38%) oder der Rechtsabteilung (31%) und aufgrund des häufig anderen Aufgabenprofils seltener der Compliance-Abteilung (24%).

Interne Untersuchungen haben vielfältige Gründe. Sie erfolgten, um arbeitsrechtliche (54%) und strafrechtliche (64%) Maßnahmen vorzubereiten sowie Schadensersatzforderungen durchzusetzen (63%) und gesellschaftsrechtliche Verpflichtungen zu erfüllen (61%). Oft wollen die betroffenen Unternehmen aus den Fällen lernen und nutzen interne Untersuchungen zur Verbesserung des internen Kontrollsystems (IKS 69%) und zur Optimierung des CMS (55%). Immerhin sehen fast zwei Drittel der Compliance-Programme spezielle Case Reports zur Evaluation des CMS vor (61%).

Bedeutung externer Ermittler

In der Praxis wurden in über der Hälfte der Fälle zusätzlich externe Ermittler mit den Untersuchungen beauftragt (57%). Ein Grund ist sicherlich, dass im Vergleich zur Ermittlungstätigkeit der Strafverfolgungsbehörden (sehr zufrieden: 24%) die Unternehmen mit der hauseigenen Aufklärungsarbeit (51%) und auch der Arbeit der hinzugezogenen externen Ermittler (46%) häufig sehr zufrieden waren.

Die Beauftragung externer Ermittler dürfte auf die sachliche und rechtliche Komplexität vieler Fälle zurückzuführen sein, sodass sie bereits beim ersten Verdacht (41%) oder im Laufe der internen Ermittlungen (43%) hinzugezogen werden. Aus diesem Grund gaben die betroffenen Unternehmen am häufigsten das Erfordernis entsprechender Qualifikation an (84%).

Als weitere Gründe nannten die betroffenen Unternehmen die höhere Objektivität externer Ermittler (56%) und Kapazitätsgründe (35%). Die Beauftragung externer Ermittler wurde seltener mit dem Druck von Stakeholdern (20%) oder der Presse (5%) begründet. Vermutlich wurden die wenigsten Fälle öffentlich bekannt. Anders wird die Lage im Falle einer skandalisierenden Presseberichterstattung zu beurteilen sein, hier dürfte sich die Beauftragung externer Ermittler empfehlen.

Sanktionspraxis bei Compliance-Verstößen

Die Sanktionspraxis vieler Unternehmen ist in den vergangenen Jahren konsequenter geworden. In aller Regel erfolgt bei gravierenden Compliance-Verstößen eine Kündigung (87%) und deutlich häufiger als vor sechs Jahren wurden zivilrechtliche Schritte eingeleitet (65%) und eine Strafanzeige erstattet (65%).

Die Strafanzeige erfolgte in jedem zweiten Fall nicht beim ersten Verdacht, sondern erst im Laufe (23%) oder nach Abschluss des Verfahrens (23%). Die Unternehmen begründeten dies mit der schnelleren Aufklärung durch interne Untersuchungen (64%), aber nur selten mit einer mangelnden fachlichen Kompetenz der staatlichen Ermittler (8%). Kritik an Polizei und Staatsanwaltschaft äußerten jedoch mehr als ein Viertel der Unternehmen aufgrund deren zu geringer Kenntnis über betriebswirtschaftliche Abläufe (29%).

An dieser Stelle möchten wir uns bei den befragten Unternehmen für ihre Bereitschaft zur Teilnahme an der vorliegenden Studie bedanken. Auch diesmal haben wir uns neuen Themen gewidmet, um über die Sicht der Wirtschaft auf zentrale Fragen der Compliance- und Haftungsentwicklung zu berichten und diese zu kommentieren.

Frankfurt am Main und Halle an der Saale im Februar 2018

Claudia Nestler

Steffen Salvenmoser

Prof. Dr. jur. Kai-D. Bussmann

Compliance-Verstöße werden zunehmend konsequenter von den Unternehmen sanktioniert. In 87 % aller Fälle erfolgte bei schwerwiegenden Verstößen eine Kündigung. In zwei Drittel der schwerwiegenden Verstöße wurde eine Strafanzeige gestellt.

Inhaltsverzeichnis

9	Abbildungsverzeichnis
12	Methodisches Vorgehen
14	Wachsende Risiken in der digitalen Wirtschaft
16	Leichter Rückgang in der analogen Wirtschaft
17	Rückgang der Verdachtsfälle
18	Wachsende Bedrohung der Wirtschaft durch Cybercrime
19	Spezial: CEO-Fraud und Erpressungsfälle keine Seltenheit
21	Hohe Einzelschäden durch Wirtschaftskriminalität
22	Compliance-Programme weiterhin im Aufwind
24	Ausweitung des Anwendungsbereichs von CMS
26	Wahrgenommene Schwächen im Compliance-Management
28	Gestiegene Anforderungen an Compliance-Programme
28	Compliance-Budgets
29	Erhöhung der Budgets für Personal- und Sachmittel
31	Personelle Aufstockung des CMS
32	Trend: Compliance in der Lieferkette
34	Compliance aus Sicht der Auftraggeber
35	Compliance-Vertragskonditionen
38	Compliance beats Corruption
40	Entwicklung der Korruptionsrisiken
41	Der Mittelstand holt auf
42	Verbreitung von Anti-Korruptionsmaßnahmen
42	Schulungen zunehmend auch digital
44	Trend: Hinweisgebersysteme
46	Evaluation des Compliance-Managements
48	Erste Erfolge im Kampf gegen Kartellrechtsverstöße
50	Abnahme der Kartellrechtsverstöße
51	Kartellrechtliche Compliance zunehmend im Mittelstand

52	<i>Mehrwert von Compliance</i>
54	Compliance als Wettbewerbsvorteil
56	Bonus für CMS in Verfahren nach § 130 OWiG
58	<i>Forensische Praxis betroffener Unternehmen</i>
60	Tätermerkmale – Risiko OK
61	Praxis interner Untersuchungen
62	Gründe interner Untersuchungen
63	Bedeutung externer Ermittler in der Praxis
64	Phase der Beauftragung externer Ermittler
64	Gründe für die Beauftragung externer Ermittler
65	Zufriedenheit mit der Arbeit externer und staatlicher Ermittler
66	<i>Sanktionspraxis bei Compliance-Verstößen</i>
68	Folgen für interne Täter
68	Praxis der Strafanzeige
69	Pro und Kontra einer Strafanzeige
70	<i>Ihre Ansprechpartner</i>
72	<i>Impressum</i>

Abbildungsverzeichnis

Abb. 1	Funktion der Interviewperson im Unternehmen	12
Abb. 2	Unternehmensgröße	13
Abb. 3	Entwicklung der Wirtschaftskriminalität 2009–2017	16
Abb. 4	Entwicklung der Verdachtsfälle 2011–2017	17
Abb. 5	Von Cybercrime betroffene Unternehmen – eindeutige Fälle 2015–2017	18
Abb. 6	Verdachtsfälle auf Cybercrime 2015–2017	19
Abb. 7	Von CEO-Fraud und Erpressungsfällen betroffene Unternehmen in den letzten zwei Jahren.....	20
Abb. 8	Hohe Schäden durch Wirtschaftskriminalität	21
Abb. 9	Status des CMS nach Deliktgruppen	25
Abb. 10	Entwicklung der Anforderungen an CMS	28
Abb. 11	Compliance-Budget nach Anzahl der Mitarbeiter	28
Abb. 12	Entwicklung der Personal- und Sachmittel für Compliance in den letzten zwei Jahren.....	29
Abb. 13	Entwicklung der Personal- und Sachmittel für Compliance nach Größe der Unternehmen	29
Abb. 14	Good Practice: Personelle Ausstattung der Compliance-Abteilung	31
Abb. 15	Bedeutung eines CMS aus Sicht der Auftraggeber	34
Abb. 16	Bedeutung eines CMS aus Sicht der Auftraggeber, nach Unternehmensgröße	35
Abb. 17	Verbreitung von Compliance-Vertragskonditionen	36

Abb. 18	Regelmäßige Compliance-Vertragskonditionen, nach Unternehmensgröße	37
Abb. 19	Entwicklung der Korruptionsrisiken 2005–2017	40
Abb. 20	Verbreitung von Anti-Korruptionsprogrammen 2013–2017, nach Unternehmensgröße	41
Abb. 21	Verbreitung der Anti-Korruptionsmaßnahmen 2013–2017	42
Abb. 22	Praxis der Schulungen 2013–2017	43
Abb. 23	Bewertung der Schulungen 2013–2017	43
Abb. 24	Hinweisgebersysteme 2013–2017	44
Abb. 25	Art der Evaluation des CMS	46
Abb. 26	Entwicklung des Risikos wettbewerbswidriger Absprachen 2011–2017	50
Abb. 27	Durch wettbewerbswidrige Absprachen erzielter Umsatzanteil in der eigenen Branche 2013–2017	51
Abb. 28	Verbreitung kartellrechtlicher Compliance-Maßnahmen, nach Unternehmensgröße	51
Abb. 29	Compliance im Wettbewerb	54
Abb. 30	Compliance im Wettbewerb, nach Unternehmensgrößen	55
Abb. 31	Auswirkungen von CMS auf das Ergebnis in Verfahren nach § 130 OWiG	57
Abb. 32	Beziehung der Täter zum geschädigten Unternehmen	60
Abb. 33	Position des internen/externen Haupttäters	60
Abb. 34	Leitung der internen Untersuchungen	61
Abb. 35	Gründe interner Ermittlungen	62

Abb. 36	Gründe interner Ermittlungen – Vergleich interne versus externe Täter.....	63
Abb. 37	Tatsächliche oder hypothetische Beauftragung externer Ermittler	63
Abb. 38	Phase der Beauftragung externer Ermittler.....	64
Abb. 39	Gründe für die Beauftragung externer Ermittler.....	64
Abb. 40	Zufriedenheit mit der Arbeit der Ermittler	65
Abb. 41	Konsequenzen gegenüber internen Haupttätern 2011–2017.....	68
Abb. 42	Strafanzeige in welcher Phase der internen Ermittlungen.....	68
Abb. 43	Pro und Contra Strafanzeige	69

Methodisches Vorgehen

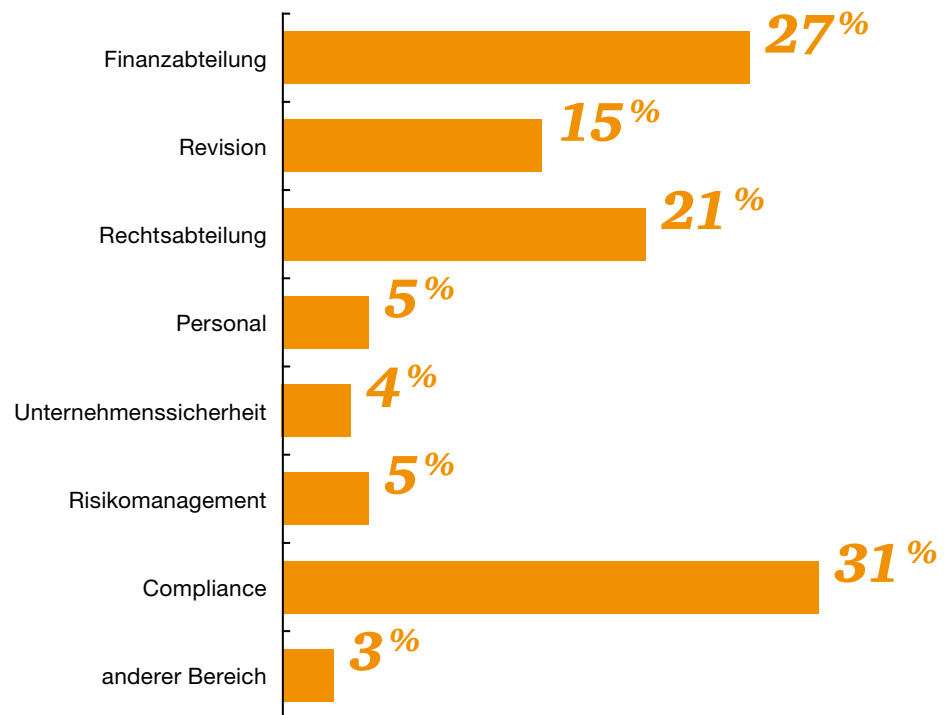
Die vorliegende, neunte Studie zur Wirtschaftskriminalität wurde im Auftrag von PwC und der Martin-Luther-Universität Halle-Wittenberg von Kantar EMNID durchgeführt. Von Anfang Juli bis Ende September 2017 wurden in Deutschland mithilfe eines standardisierten Fragebogens Verantwortliche aus 500 Unternehmen telefonisch interviewt, die sich in ihrem Unternehmen für den Themenbereich Kriminalitätsprävention und -aufklärung

zuständig erklärt hatten. Des Weiteren wurden mit 32 Unternehmen ergänzende vertiefte Interviews zu ausgewählten Fragen durchgeführt, um detailreichere Berichte und Einschätzungen zu erhalten.

Die Befragten stammten zu etwa einem Drittel (31 %) aus dem Bereich Compliance, 27 % der Befragten gehörten der Finanzabteilung an und 21 % der Rechtsabteilung.

Abb. 1 Funktion der Interviewperson im Unternehmen

Mehrfachnennungen waren möglich.



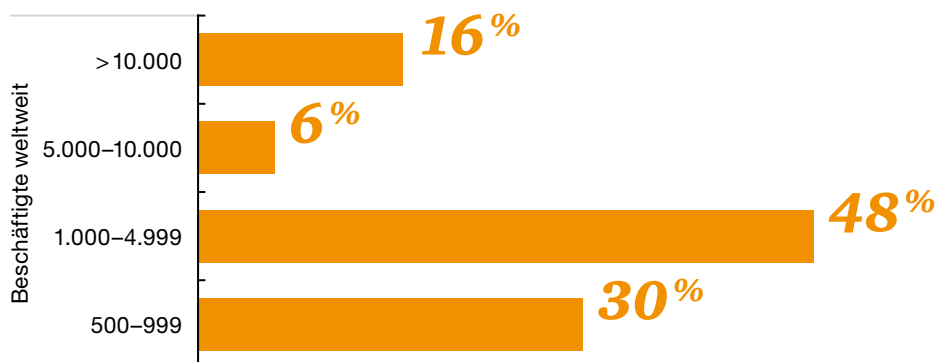
Die Antwortbereitschaft war auch dieses Mal hoch. Aufgrund der Art und des Umfangs der Stichprobenziehung handelt es sich um eine repräsentative Studie zur Sicherheitslage von Unternehmen mit mehr als 500 Mitarbeitern in Deutschland bzw. weltweit. Rund die Hälfte der Unternehmen verfügt über 1.000 bis 4.999 Mitarbeiter (48%). Jedes fünfte Unternehmen (21%) ist börsennotiert und 28% unterliegen dem US-amerikanischen FCPA, da sie

nach US-Recht gegründet wurden, ihren Geschäftssitz in den USA haben, an einer US-Börse notiert sind oder auf andere Weise in den USA geschäftlich tätig sind.

Fast jedes zweite Unternehmen (46%) verfügt über Auslandsvertretungen, mehr als jedes fünfte (19%) ist weltweit vertreten. Die folgende Abbildung zeigt die Größe der befragten Unternehmen nach Anzahl der weltweit beschäftigten Mitarbeiter.

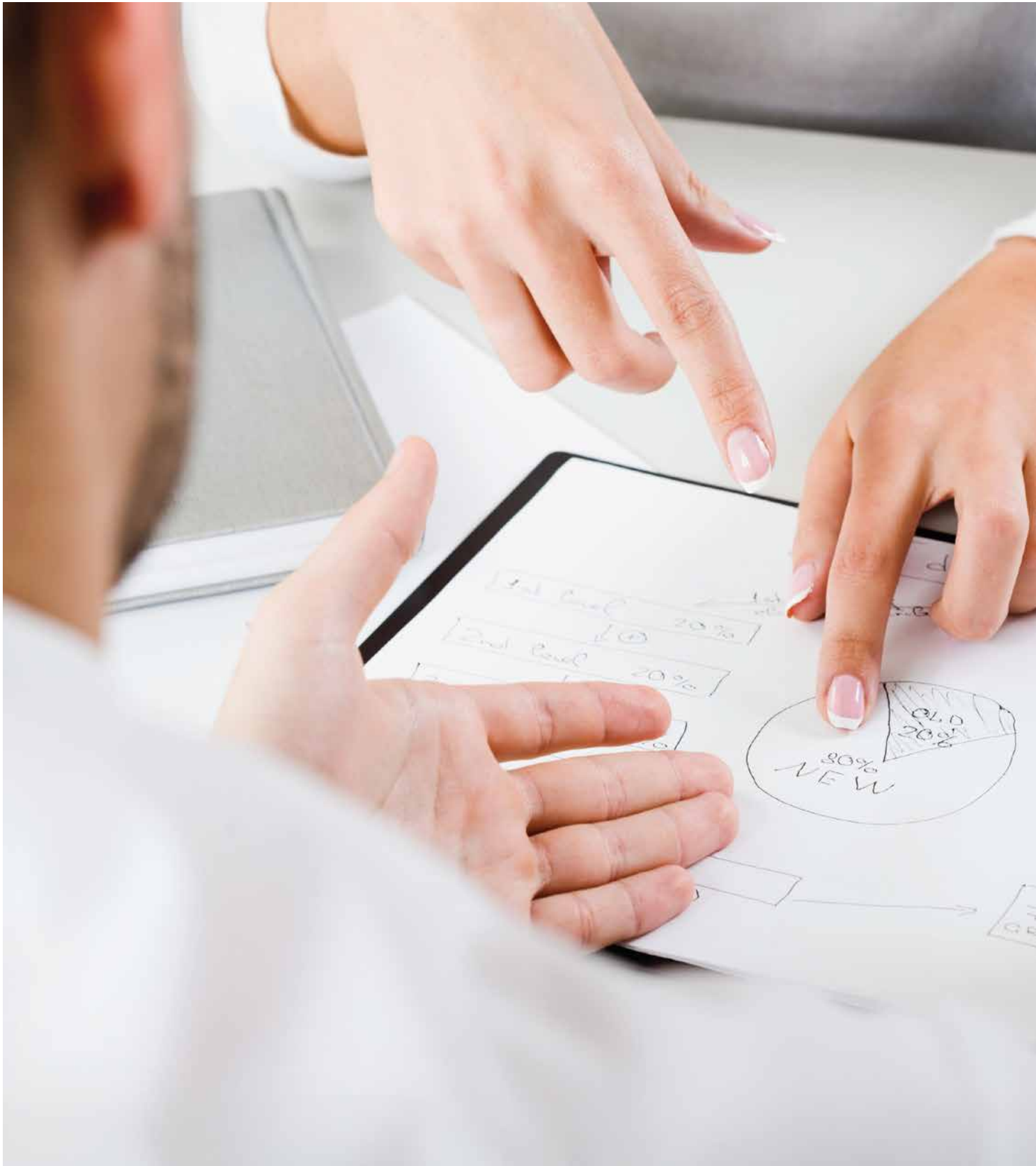
Ein Teil der Fragen ermöglicht einen direkten Vergleich mit unseren von 2005 bis 2017 zweijährlich durchgeführten Studien. Auch dieser Report enthält eine Fallstudie (siehe Seite 66 ff.). Diese ermöglicht insbesondere die Erhebung von Tätermerkmalen sowie des Umgangs mit konkreten Verdachtsfällen der betroffenen Unternehmen. 2017 berichteten die befragten Unternehmen von 212 gravierenden Schadensfällen, dabei handelte es sich bei jedem zweiten Fall (49%) um ein Vermögensdelikt, bei 16% um wettbewerbswidrige Absprachen und bei 9% um Korruption.

Abb. 2 Unternehmensgröße



In unseren zweijährigen Studien berichten wir seit 2001 kontinuierlich über die Erfahrungen von mittelständischen und Großunternehmen rund um das Risikofeld Wirtschaftskriminalität.

Wachsende Risiken in der digitalen Wirtschaft





Während die Belastung der Unternehmen durch die Risiken klassischer Wirtschaftskriminalität abnimmt, ist ein dramatischer Anstieg von Cybercrime-Fällen zu verzeichnen.

Leichter Rückgang in der analogen Wirtschaft

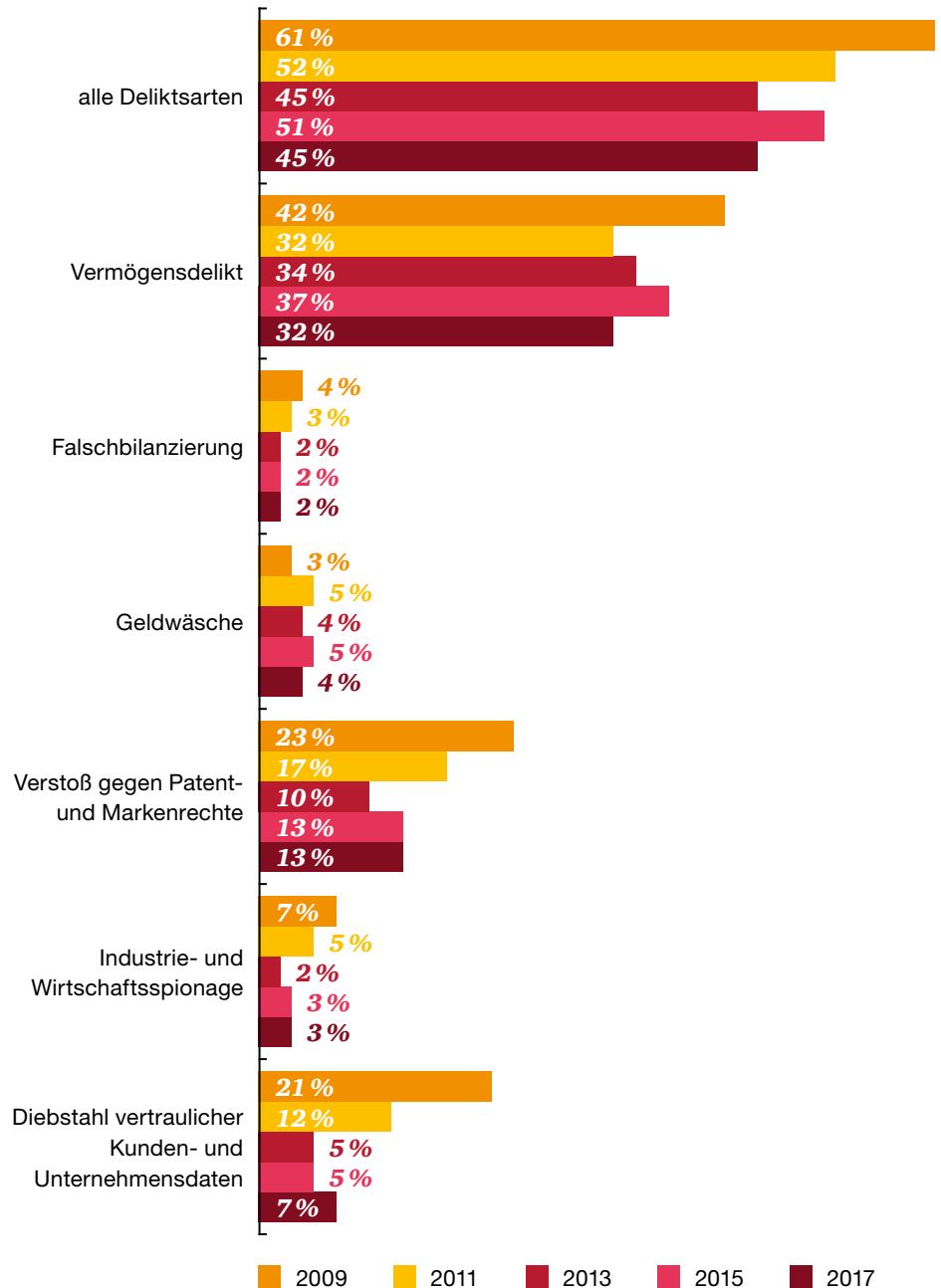
Im langfristigen Vergleich zeichnet sich in der deutschen Wirtschaft ein Rückgang in der Entwicklung der (analogen) Wirtschaftskriminalität ab. Gegenüber 2015 beobachten wir eine weitere Abnahme der Kriminalitätsbelastung um sechs Prozentpunkte auf das Niveau von 2013. Der Höchststand lag 2009 bei 61 % (alle Deliktsarten). Wir sehen daher unsere These bestätigt, dass sich die optimierten Compliance-Programme zunehmend präventiv auswirken.² Allerdings bleibt das Dunkelfeld groß, wie an den weiterhin berichteten Verdachtsfällen deutlich wird (siehe Seite 17).

Unsere Studie zeigt gegenüber 2015 und auch im langjährigen Vergleich, dass die Zahl der von Vermögensdelikten betroffenen Unternehmen zurückgeht. Gegenüber 2015 ist die Zahl der berichteten Verstöße gegen Patent- und Markenrechte zwar unverändert (13 %), aber seit 2009 (23 %) stark rückläufig. Dies dürfte auch auf das veränderte Marktumfeld zurückzuführen sein. Auch die Emerging Markets und insbesondere China zeigen ein eigenes Interesse am Schutz geistigen Eigentums. Vergleichsweise selten waren die befragten Unternehmen durch Industrie- und Wirtschaftsspionage betroffen (3 %). Allerdings wissen wir aus vorangegangenen Studien, dass forschungsintensive Unternehmen weiterhin sehr viel höheren Risiken ausgesetzt sind.³

Beim Diebstahl vertraulicher Kunden- und Unternehmensdaten beobachten wir langfristig ebenfalls eine positive Entwicklung (2009: 21 %); der geringe Anstieg auf 7 % gegenüber 2015 (5 %) sollte dabei nicht überinterpretiert werden.

Abb. 3 Entwicklung der Wirtschaftskriminalität 2009–2017

Mehrfachnennungen waren möglich.



² Vgl. PwC, Wirtschaftskriminalität in der analogen und digitalen Wirtschaft, 2016, S. 16 f.

³ Vgl. ebenda, S. 34 f.

Rückgang der Verdachtsfälle

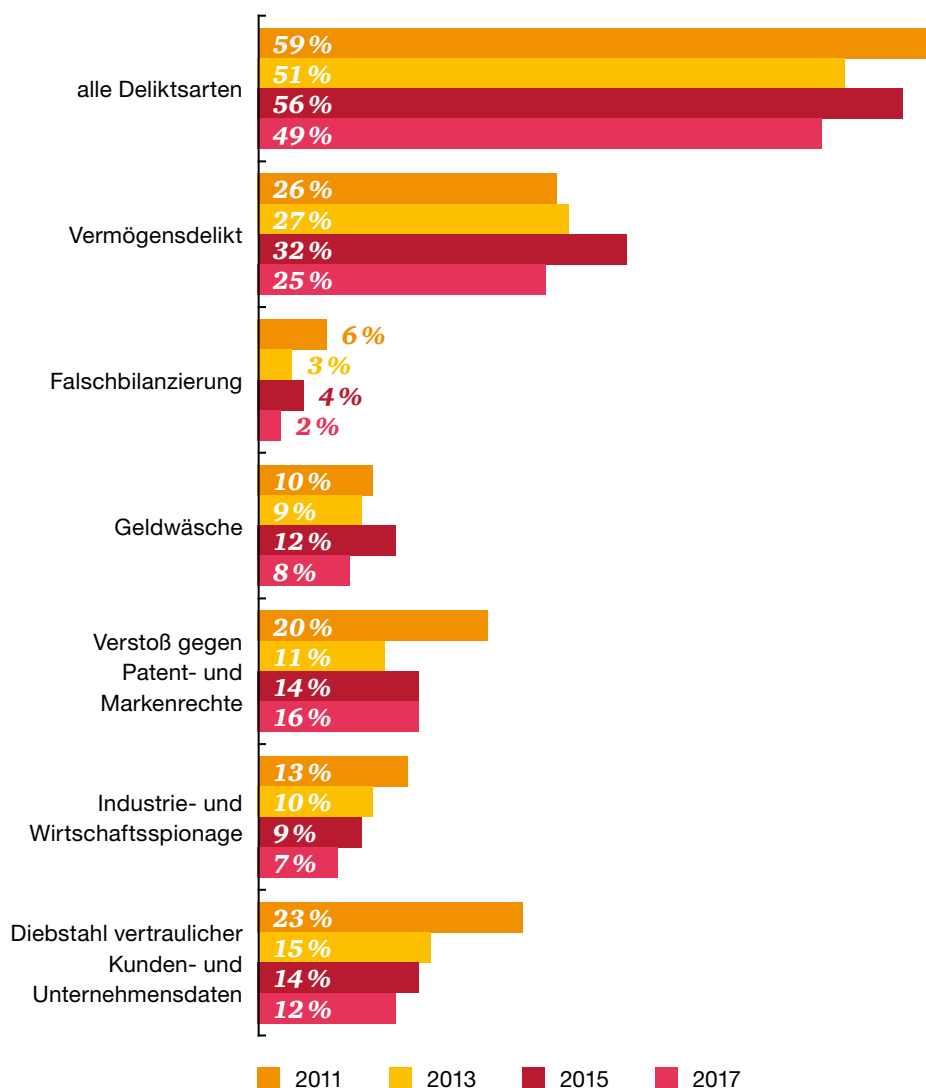
Gegenüber 2015 sinkt die Zahl der Unternehmen, die mindestens einen konkreten Verdacht auf eine Wirtschaftsstraftat berichtet haben, um sieben Prozentpunkte auf 49%. Auch im langfristigen Vergleich zeigt sich ein Rückgang der Verdachtsfälle⁴ – sowohl

insgesamt (2011: 59%) als auch bei den meisten Deliktsarten. Lediglich über einen Verdacht auf Patent- und Markenrechtsverletzungen berichteten Unternehmen häufiger als im Jahr 2013, jedoch seltener als 2011 (20%).

Im Vergleich zu den eindeutigen Fällen berichteten die Unternehmen mit Ausnahme der Falschbilanzierung häufiger über einen Verdacht auf Geldwäsche (8%), Verstöße gegen Patent- und Markenrechte (16%), Wirtschafts- und Industriespionage (7%) und Diebstahl vertraulicher Kunden- und Unternehmensdaten (12%). Das Dunkelfeld der Wirtschaftskriminalität bleibt somit groß.

Abb. 4 Entwicklung der Verdachtsfälle 2011–2017

Mehrfachnennungen waren möglich.



⁴ Durch den Begriff „konkreter Verdacht“ sollen vage Vermutungen ausgeschlossen werden. Eine Strafanzeige war jedoch nicht Voraussetzung.

Wachsende Bedrohung der Wirtschaft durch Cybercrime

Deutliche Zunahme der Cybercrime-Attacken

Auch diesmal haben wir untersucht, inwieweit die Unternehmen von Cybercrime betroffen waren.⁵ Deutlich

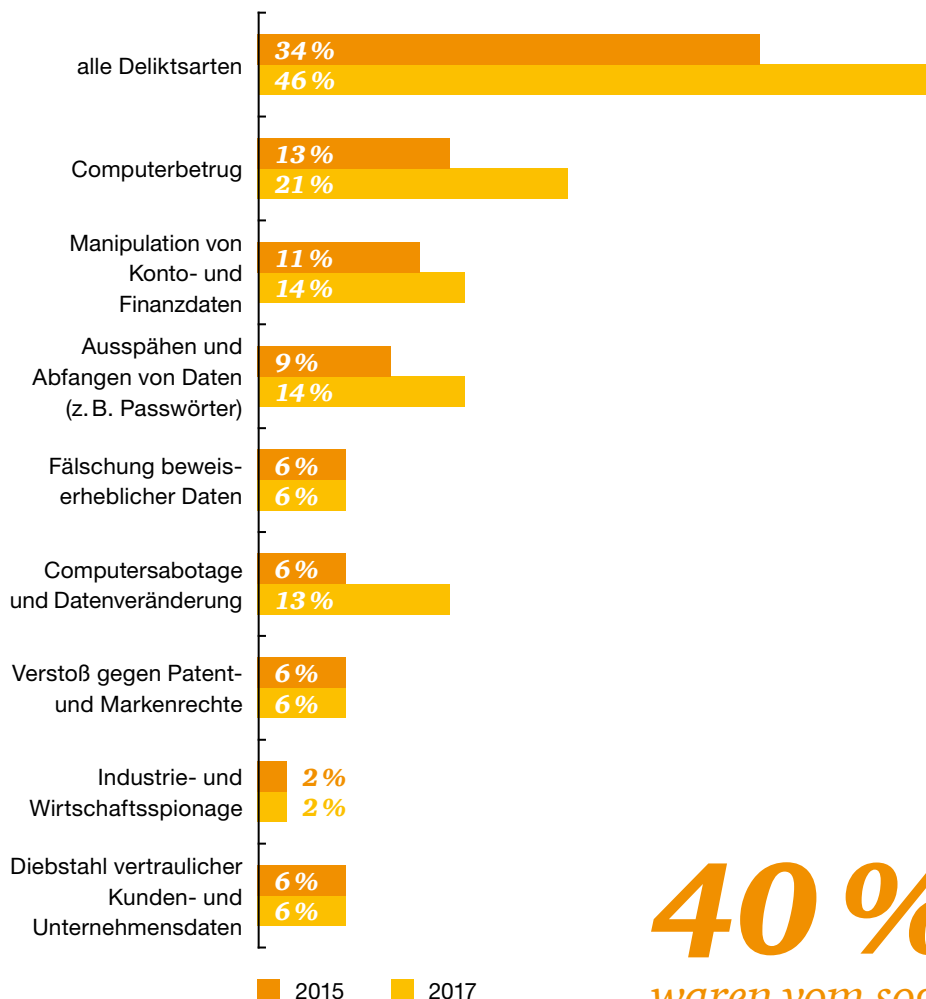
zugenommen haben vor allem Computerbetrug (21 %), Computersabotage und Datenveränderung (13 %) sowie das Ausspähen und Abfangen von Daten (14 %).

Stagnation bei Cybercrime-Verdachtsfällen

Bei den berichteten konkreten Verdachtsfällen (38 %; 2015: 39 %) ist keine vergleichbare Entwicklung zu beobachten. Hier stagniert die Betroffenheit der Unternehmen. Auch bei den einzelnen Formen von Cybercrime zeigt sich keine signifikante Entwicklung.

Abb. 5 Von Cybercrime betroffene Unternehmen – eindeutige Fälle 2015–2017

Mehrfachnennungen waren möglich.



Der starke Anstieg bei den eindeutigen Cybercrime-Fällen kann daher auch auf einer erhöhten Awareness und verbesserten IT-Sicherheitstechnik beruhen, sodass immer mehr Cybercrime-Attacken entdeckt werden. Die Cybercrime-Fälle aus dem Dunkelfeld gelangen möglicherweise verstärkt in das Hellfeld der Unternehmen. Dies beruhigt nur bedingt, denn die Cybercrime-Bedrohungslage ist somit erwiesenermaßen sehr viel ernster, als in Unternehmen angenommen wird.⁶

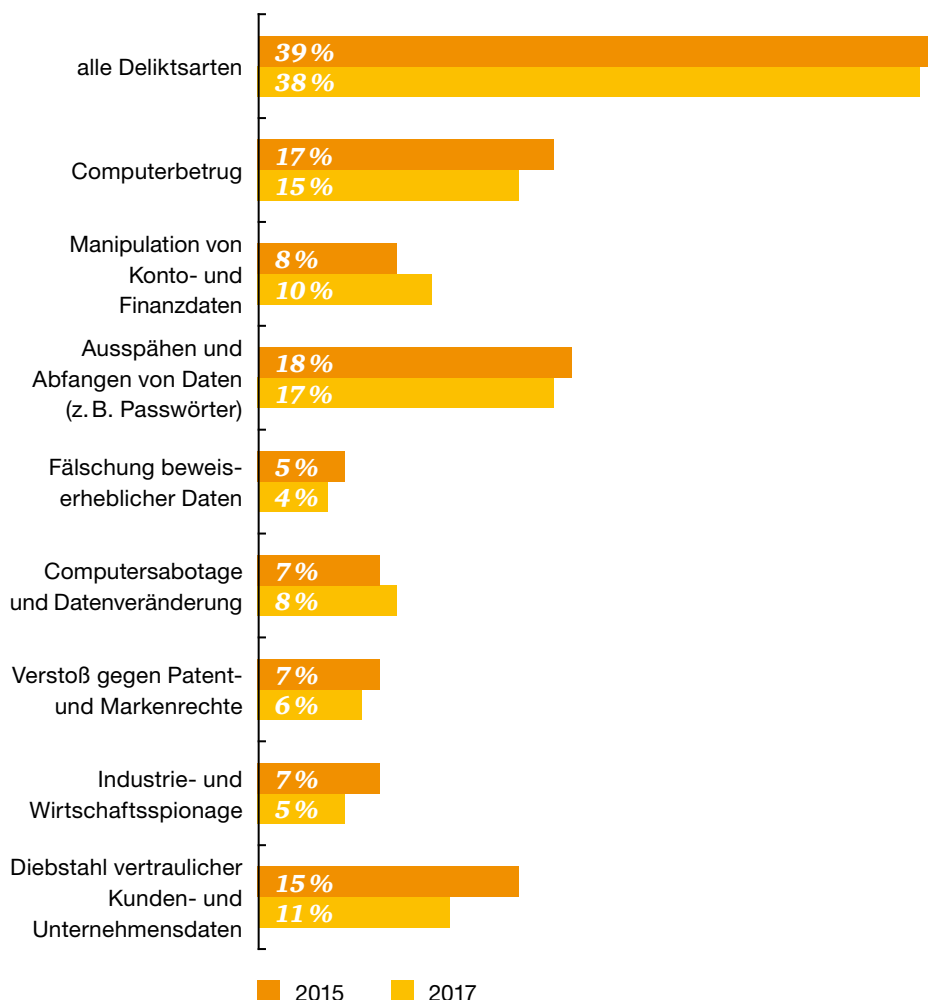
40 % der Unternehmen waren vom sogenannten CEO-Fraud betroffen. Bei 5 % der Unternehmen war der Angriff erfolgreich.

⁵ Bei Cybercrime handelt es sich um Delikte, die nicht nur durch bloße Nutzung, sondern durch gezielte Ausnutzung elektronischer Systeme und Kommunikationsmittel begangen wurden (auch: cyber-dependent crimes). Ausgeschlossen wurden Delikte, bei denen der Computer oder das Internet nur gewählt wurden, um beispielsweise einen Betrug einfacher begehen zu können.

⁶ Ausführlich zu Risiken des Daten- und Wissensverlusts: PwC, Wirtschaftskriminalität in der analogen und digitalen Wirtschaft, 2016, S. 32 ff.

Abb. 6 Verdachtsfälle auf Cybercrime 2015–2017

Mehrfachnennungen waren möglich.



Spezial: CEO-Fraud und Erpressungsfälle keine Seltenheit

In unserer Studie fragten wir nach Versuchen von CEO-Fraud, auch als „Fake President“-Fraud bezeichnet. Hierbei handelt es sich um eine Variante des Social Engineering, bei dem Mitarbeiter vorrangig aus dem Finanz- und Rechnungswesen vermeintlich im Auftrag des Topmanagements zur Überweisung eines größeren Geldbetrags auf ein ausländisches Konto veranlasst werden – meist durch einen Anruf oder eine E-Mail.⁷ Dabei werden die Mitarbeiter unter Druck gesetzt, den Transfer schnellstmöglich durchzuführen und Verschwiegenheit zu bewahren, da es sich um ein geheimes und vertrauliches Projekt handle.⁸

Die Täter, die überwiegend der OK zuzurechnen sind,⁹ sammeln zunächst Informationen aus Wirtschaftsberichten der Unternehmen, aus dem Handelsregister, von der Website und aus Werbebroschüren der Unternehmen oder durch direkte Anrufe, um die sich anschließende Kommunikation mit dem Mitarbeiter aus der Finanzabteilung glaubwürdig zu gestalten.¹⁰

BSI: „Social Engineering ist weiterhin eine vielfach genutzte Methode, um Cyber-Angriffe erfolgreich auszuführen oder zu unterstützen. Für Angreifer ist es einfacher, die Schwachstelle Mensch als oftmals schwächstes Glied der IT-Sicherheitskette zu überwinden, anstatt komplexe technische Sicherheitsmaßnahmen mit viel Aufwand zu umgehen.“¹¹

⁷ Vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2016, S. 23; BKA, Bundeslagebild Wirtschaftskriminalität 2016, S. 8.

⁸ Vgl. BSI, Pressemitteilung vom 10.07.2017.

⁹ Vgl. BKA, Bundeslagebild Wirtschaftskriminalität 2016, S. 8.

¹⁰ Vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2016, S. 23; BKA, Bundeslagebild Wirtschaftskriminalität 2016, S. 9.

¹¹ Vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2016, S. 22.

Die Zahl der Fälle hat dem Bundeskriminalamt (BKA) zufolge seit 2013 kontinuierlich zugenommen. Im Jahr 2013 wurden zwei versuchte und zwei vollendete Fälle von CEO-Fraud erfasst. Drei Jahre später registrierte das BKA dagegen bereits 51 vollendete und 291 versuchte Fälle und gelangte zu folgender Einschätzung der Sicherheitslage:

BKA: „Bei der Schadensentwicklung im Bereich des CEO-Fraud sind starke Anstiege zu verzeichnen. Seit 2014 verdreifachte sich der Schaden durch das betrügerische Handeln der Täter und lag im Berichtsjahr bei 75,2 Mio. Euro (2015: 46,7 Mio. Euro: +61 %).“¹²

Unsere Studie zeigt das Bedrohungspotenzial des CEO-Fraud: 40 % der befragten Unternehmen berichteten über einen derartigen Versuch, davon waren 5 % sogar erfolgreich. Der hohe Verbreitungsgrad, aber auch die Schadensrisiken sind beunruhigend. Als gravierendstes Wirtschaftsdelikt in den letzten Jahren nannten sieben Unternehmen einen CEO-Fraud, der im Durchschnitt einen Schaden in Höhe von 4,4 Millionen Euro verursachte. Im Bereich Cybercrime sind Fälle von CEO-Fraud daher die schadensträchtigsten Delikte.

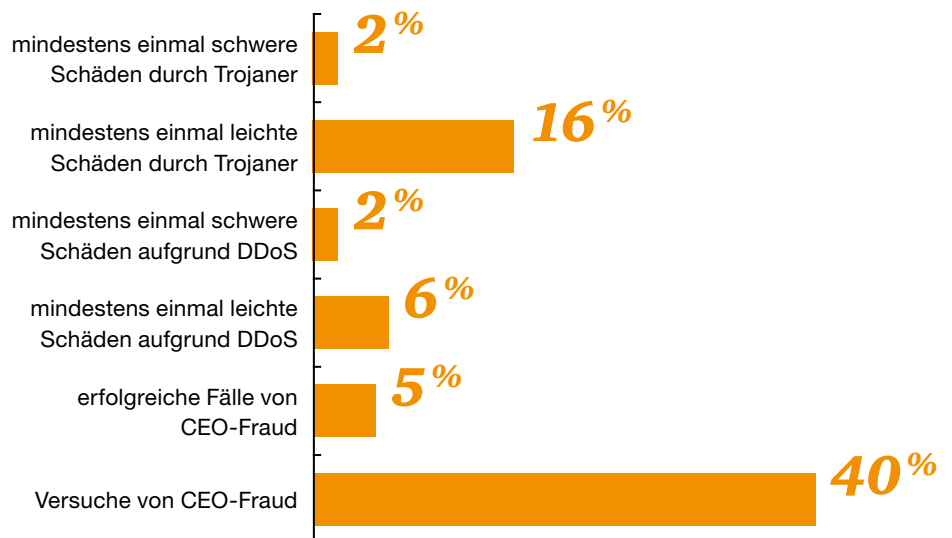
Alarmierend sind auch Berichte über Fälle von DDoS und Verschlüsselungs- bzw. Erpressungstrojanern, auch unter dem Oberbegriff „Ransomware“ zusammengefasst.¹³ In unserer Studie haben wir zwischen leichten und schweren Fällen unterschieden, um die Bedrohungslage besser evaluieren zu können. Ein leichter Fall mit geringen Schäden wird bei kurzzeitigen Systemausfällen ohne nennenswerte Beeinträchtigungen angenommen, bei denen nur einzelne Rechner betroffen sind und ein Back-up ohne großen Aufwand möglich ist. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt allerdings auch vor Trittbrettfahrern, die ohne tatsächliche DDoS-Angriffe darauf hoffen, dass der Empfänger zahlt.¹⁴

Als schwerer Fall mit erheblichen Schäden wird dagegen ein längerfristiger Systemausfall verstanden, der das Tagesgeschäft beeinträchtigt und mehrere Rechner oder sogar das gesamte Netzwerk betrifft. Ein schwerer Fall liegt auch dann vor, wenn Lösegeld gezahlt wird.

In unserer Studie berichteten insgesamt 8 % der Unternehmen über leichte und schwere DDoS-Fälle und 18 % über Trojaner. Zwar waren die Schäden zumeist eher geringer, aber jeweils 2 % wurden schwer geschädigt. In unserer Stichprobe von 500 Unternehmen berichteten sogar vier, sie hätten das geforderte Lösegeld gezahlt.

Abb. 7 Von CEO-Fraud und Erpressungsfällen betroffene Unternehmen in den letzten zwei Jahren

Mehrfachnennungen waren möglich.



¹² Vgl. BKA, Bundeslagebild Wirtschaftskriminalität 2016, S. 10.

¹³ Vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2016, S. 20 und 29.

¹⁴ Vgl. ebenda, S. 29.

Einzelschäden können unkalkulierbare Ausmaße annehmen, in einem unserer berichteten Fälle über 10 Millionen Euro.

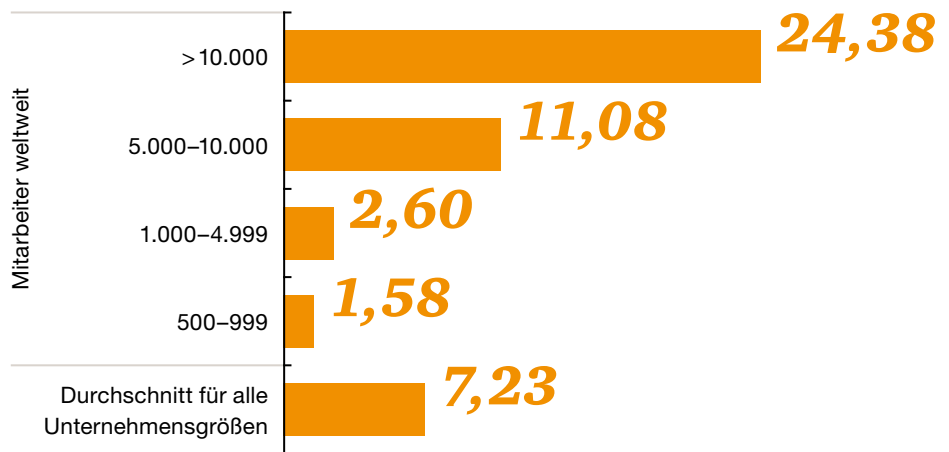
Hohe Einzelschäden durch Wirtschaftskriminalität

Die finanziellen Folgen von Wirtschaftskriminalität lassen sich nur bedingt beziffern, insbesondere wenn man auch die zahlreichen indirekten Konsequenzen wie Schadensersatzforderungen, straf- bzw. bußgeldrechtliche Haftungsrisiken, Kosten für Rechtsverfahren, Stakeholdermanagement und Reputationschäden zu berücksichtigen hat. Der durchschnittliche Schaden sinkt von 1,55 Millionen Euro im Jahr 2015 auf 723.000 Euro je Unternehmen, wobei größere Unternehmen wiederum über deutlich höhere Schäden berichteten. Die geringeren Schadensfolgen könnten auf verbesserte Compliance-Programme zurückzuführen sein. Die weitere Entwicklung wird jedoch abzuwarten sein.

Einzelne gravierende Wirtschaftsdelikte führten allerdings zu deutlich höheren finanziellen Verlusten. In unserer Studie bezifferten 212 Unternehmen¹⁵ die durchschnittlichen Kosten aufgrund eines schweren Wirtschaftsdelikts auf 7,23 Millionen Euro, wobei die Höhe des Schadens stark von der Größe der Unternehmen abhängt. Unternehmen mit mehr als 10.000 Mitarbeitern schätzten den Gesamtschaden des schwersten Wirtschaftsdelikts durchschnittlich auf 24,38 Millionen Euro.

Abb. 8 Hohe Schäden durch Wirtschaftskriminalität¹

durchschnittliche Schäden je Delikt in Mio. €



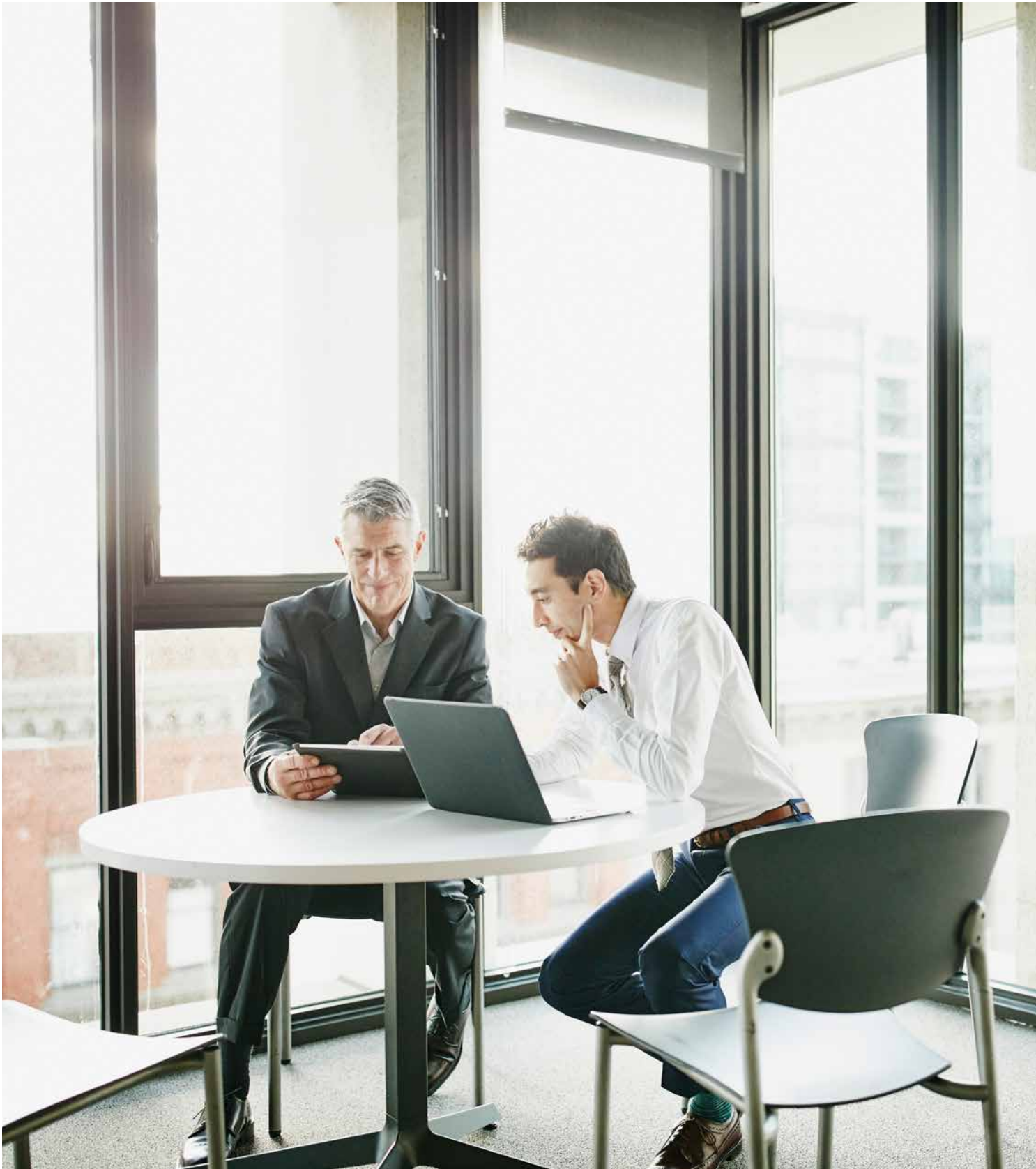
¹ Differenzierung: betrifft nur die 212 Unternehmen, die Aussagen bzgl. schwerer Wirtschaftsdelikte getroffen haben.

Die von den Unternehmen bezifferten Schäden aufgrund von Cybercrime fallen im Vergleich zu denen aufgrund analoger Kriminalität auch 2017 deutlich geringer aus. Die betroffenen Unternehmen schätzten die durch Cybercrime verursachten Schäden auf durchschnittlich 183.000 Euro.

Allerdings waren sie auch hier in Einzelfällen deutlich höher. 6% berichteten über Schadensfolgen in Höhe von 500.000 bis 2 Millionen Euro. In einem Fall stieg die Schadensbilanz auf beachtliche 10 bis 50 Millionen Euro. Auch kann es durch CEO-Fraud zu erheblichen Verlusten kommen, wie wir bereits berichtet haben (siehe Seite 19 f.).

¹⁵ Bei 49% der schwersten Fälle handelte es sich um ein Vermögensdelikt, bei 16% um wettbewerbswidrige Absprachen und bei 9% um Korruption.

Compliance-Programme weiterhin im Aufwind





Compliance und Compliance-Management-Systeme sind zur Selbstverständlichkeit geworden. Compliance wird als klarer Wettbewerbsvorteil empfunden und nicht mehr als „Geschäftsverhinderung“.

Ausweitung des Anwendungsbereichs von CMS

Compliance-Programme haben sich in der deutschen Wirtschaft etabliert. Drei Viertel der Unternehmen (75 %) mit mehr als 500 Mitarbeitern verfügen über ein CMS und bei weiteren 10 % befindet sich eines in der Planung. Nahezu alle Großunternehmen mit mehr als 10.000 Mitarbeitern verfügen über ein CMS (97 %), während von den Unternehmen mit 500 bis 999 Mitarbeitern nur knapp zwei Drittel (60 %) Compliance-Programme implementiert haben. Wir beobachten weiterhin eine Top-down-Entwicklung, die insbesondere auf den höheren rechtlichen und öffentlichen Druck auf größere Unternehmen zurückzuführen ist.¹⁶ Größere Unternehmen operieren häufiger international, unterliegen daher vermehrt der Aufsicht der US-amerikanischen Behörden und dem strikten Reglement des FCPA.¹⁷ Diesen Druck geben die Unternehmen an wirtschaftlich mit ihnen verbundene kleinere Unternehmen weiter.¹⁸

Ferner setzt sich der Trend zu einer Ausweitung der Compliance-Programme auf zusätzliche Deliktsfelder fort. Unternehmen richten ihren Compliance-Fokus verstärkt auf die Zurückdrängung von Korruption (83 %) und Kartellrechtsverletzungen (62 %). Auch den Risiken der Geldwäsche widmet sich eine wachsende Zahl von Compliance-Programmen, zwei Drittel (65 %) erstrecken sich hierauf. Dies könnte insbesondere auf die Ausweitung des Geltungsbereichs des Geldwäschegesetzes (GwG) im Zuge der Umsetzung der 4. EU-Geldwäscherichtlinie zurückzuführen sein. Bei börsennotierten Unternehmen¹⁹ erhält die Prävention gegen Insidertransaktionen (§ 38 WpHG) einen höheren Stellenwert, drei Viertel verfügen über ein derart ausgerichtetes CMS (76 %).

Nahezu alle Großunternehmen mit mehr als 10.000 Mitarbeitern verfügen über ein CMS (97 %).

¹⁶ Vgl. PwC, Wirtschaftskriminalität in der analogen und digitalen Wirtschaft, 2016, S. 52 ff.

¹⁷ 28 % der befragten Unternehmen unterliegen dem US-amerikanischen FCPA.

¹⁸ Vgl. Bussmann/Salvenmoser/Jeker, Compliance ist im Markt, aber noch nicht im Recht – Ergebnisse aus einer Unternehmensbefragung, in: CCZ 5/2016, S. 236–240.

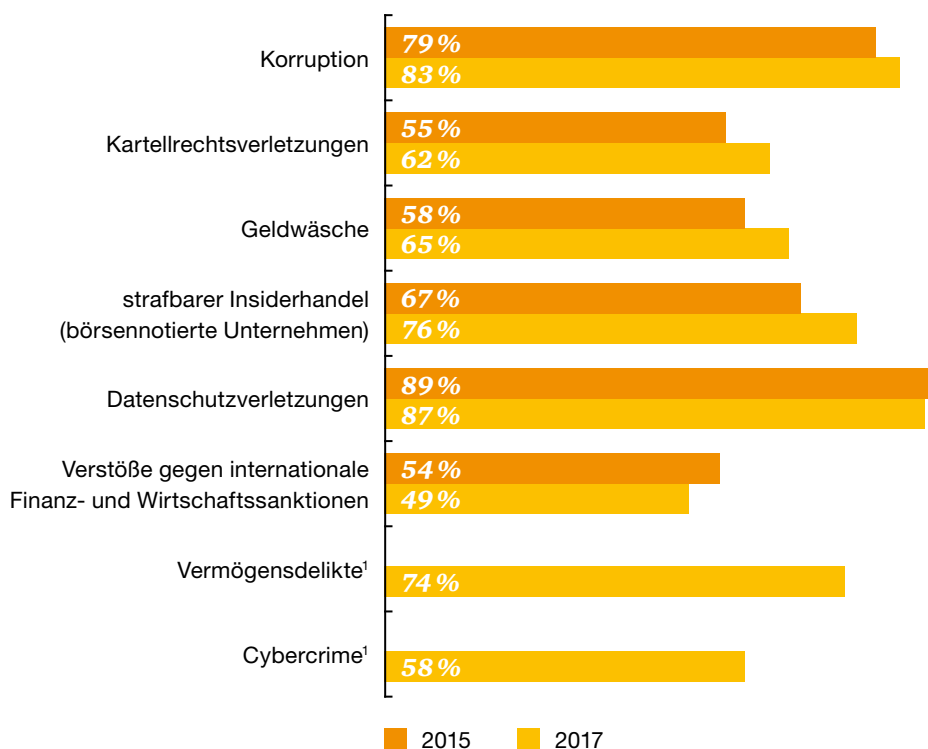
¹⁹ Die entsprechende Frage wurde nach der Börsennotierung gefiltert. In der Stichprobe sind 21 % der Unternehmen börsennotiert.

65 % der CMS widmen sich den Risiken der Geldwäsche. Die Ausweitung des Geltungsbereichs des GWG dürfte die Erklärung für den deutlichen Anstieg (7 Prozentpunkte) sein.

In die diesjährige Studie haben wir auch die Prävention gegen Betrug und andere Vermögensdelikte sowie gegen Cybercrime aufgenommen. Gegen Vermögenskriminalität wappnen sich drei Viertel der Unternehmen durch ein entsprechendes CMS (74%). Demgegenüber ist der Schutz vor Cybercrime weiterhin eher unterentwickelt (58%), wie auch unsere vorangegangene Studie ergab.²⁰

Auch zur Vermeidung von Verstößen gegen internationale Finanz- und Wirtschaftssanktionen besteht weiterhin Handlungsbedarf bei der Compliance-Entwicklung, 49% der befragten Unternehmen verfügen über ein entsprechendes CMS, obwohl von diesen internationalen Sanktionen nicht nur Unternehmen des Finanzsektors tangiert sind, sondern Unternehmen fast aller Branchen.

Abb. 9 Status des CMS nach Deliktgruppen



Basis: Unternehmen mit CMS

¹ Keine Daten für 2015.

²⁰ Vgl. PwC, Wirtschaftskriminalität in der analogen und digitalen Wirtschaft, 2016, S. 32 ff.

Wahrgenommene Schwächen im Compliance-Management

Viele Unternehmen dehnen ihr CMS nicht nur auf weitere Rechtsgebiete aus, sondern arbeiten auch an ihren

Schwachpunkten, wie wir anhand einiger Statements aus unseren vertieften Interviews zeigen können:

Kommunikationsprobleme

„Kommunikation ist definitiv der Schwachpunkt – dass nicht immer alles da ankommt, wo es ankommen soll, und vielleicht auch nicht in der Form ankommt, wie es ankommen soll.“

Strategie: „An der Art der Vermittlung müssen wir ganz stark arbeiten, also daran, wie wir es besser in den Arbeitsalltag integriert bekommen, ohne immer Tausende von Checklisten ausfüllen zu müssen, sondern dass wir auch wirklich sichergehen können, dass verstanden wurde, was

in welchem Arbeitsumfeld wichtig ist zu wissen.“ (Pharma und Gesundheitswesen, mehr als 10.000 Mitarbeiter weltweit)

„Informationsdurchlässigkeit. Das heißt, wir sind ein stark diversifiziertes Unternehmen und haben das Problem, dass Informationen, die in einem Unternehmensteil gut verbreitet sind, in einem anderen Unternehmensteil eher noch nicht verankert sind. Also es ist im Prinzip ein Kommunikationsproblem.“

Strategie: „Wir sind dabei, in unserem eigenen hausinternen Netzwerk ein internes Informationssystem aufzubauen, um dort mit gängigen Suchmaschinen die Begrifflichkeiten finden zu können. Also im Prinzip eine Holschuld für die Organisationseinheiten, indem sie sich darüber informieren müssen, welche Neuigkeiten existieren.“ (Pharma und Gesundheitswesen, mehr als 10.000 Mitarbeiter weltweit)

Mangelnde Konsistenz der Regelungen

„Eine Schwäche besteht in der Integration der verschiedenen Compliance-relevanten Instrumente. Wenn Sie das innerbetriebliche Kontrollsystem nehmen, wie es mit dem Richtlinien-Management-System verbunden ist und wie diese beiden wiederum verbunden sind mit unserem Geschäftsprozess-Management-System und mit unserem IT-Fachverfahren-Management-System: An dieser Integration [...] müssen wir noch arbeiten, dass diese ganzen Teilsysteme

zu einem gesamten konsistenten, vor allen Dingen in ihren Bezügen stets aktuellen Gesamtsystem werden.“

Strategie: „Wir sind dabei, eine integrierte Software einzuführen, die ebendiese Querbezüge zwischen den Teilinstrumenten überwacht bzw. erlaubt zu überwachen und uns aktiv auf Inkonsistenzen hinweist.“ (Versicherungswirtschaft, mehr als 10.000 Mitarbeiter weltweit)

Mangelnde Integration in Geschäftsprozesse

„Also ich glaube, das Problem bei Compliance-Systemen insgesamt ist immer, sie am Ende in die letzte Verästelung des Konzerns zu tragen. Und das kann man nicht dadurch machen, dass man irgendwelche Themen wiederholt.“

Strategie: „Schulungen sind natürlich auch Mittel, aber im Grunde funktioniert das am Ende nur, wenn man in die Geschäftsprozesse geht. Je besser die Prozesse sind und je besser die Prozesse selbst Kontrollen beinhalten, umso besser wird man auch Compliance in den Alltag integrieren können. Wenn man es immer nur auf der ‚Ich-denke-mal-dran-da-war-doch-noch-Compliance‘-Ebene belässt, dann wird das immer dazu führen, dass im Zweifel jemand nicht daran denkt.“ (Handel und Konsum, mehr als 10.000 Mitarbeiter weltweit)

Die qualitativen Interviews zeigen, dass die Umsetzung des CMS im Alltag häufig noch auf Hindernisse stößt.

Umsetzung in einem global agierenden Unternehmen

„Wenn Sie im Dax oder MDax gelistet sind und global operieren, ist es schwierig, in jeder letzten Einheit in Timbuktu ein Compliance-Management-System zu haben, insbesondere was das Berichtswesen angeht, das genauso gut funktioniert wie in Deutschland – weil die Wege einfach weiter sind.“

Strategie: „Ich glaube, alles, was global ist, lässt sich nur IT-basiert beheben, indem man sagt, man braucht IT-basierte Lösungen für das Berichtswesen beispielsweise und IT-basierte Lösungen für die Information von Mitarbeitern, und das personenunabhängig gestaltet.“ (Automobilindustrie, mehr als 10.000 Mitarbeiter weltweit)

„Ich glaube, das Wichtigste, was uns noch ein bisschen fehlt, ist die Compliance aus einem Guss, also als ein multinationales Unternehmen mit

Produktions- und Vertriebsstandorten in so ziemlich jedem Land der Erde – ich glaube, in über 170 Ländern. Weil die Compliance-Organisation in dieser jetzigen Form noch nicht sehr alt ist und auch noch keine absolute Homogenität im Wissensstand der Kollegen, die Compliance in den Ländern oder an den Standorten betreiben, vorhanden ist, fehlt es noch ein bisschen an dem einheitlichen Guss, an der gemeinsamen Schlagkraft.“

Strategie: „Es soll jetzt nicht bedeuten, dass die Kollegen deswegen nicht motiviert oder nicht kompetent sind, aber es fehlt so ein bisschen dieser einheitliche Auftritt und auch die einheitliche Sprache, weil doch für viele Themen, die wir lokal lösen, da nicht immer eine Einheitlichkeit gewährt ist [...]“ (Technologiewirtschaft, 5.000 bis 10.000 Mitarbeiter weltweit)

Zu formales CMS

„Das Problem ist vielleicht anders als bei Rechnungslegungssystemen – da hat man Zahlen –, weil es eben qualitativer Art ist. Und die Frage ist natürlich: Wie kriege ich qualitative Dinge in Daten? Das ist schon ein bisschen ein Problem. Und ich sehe da auch die riesen-große Gefahr des Compliance-Management-Systems, dass man sich dann auf Zahlen stützt und weniger die Inhalte hinterfragt. Das ist ein Spannungsfeld, das noch zu lösen ist.“

Strategie: „Es bleibt nichts anderes übrig, als noch intensiver die Zahlen zu hinterfragen, vielleicht auch mit Revisionsarbeit – und das ist natürlich auch aufwendig, zu hinterfragen und die Dinge abzufragen. Das ist ein großes Problem.“ (Industrielle Produktion, mehr als 10.000 Mitarbeiter weltweit)

Mangelnde Awareness

„[...] und überhaupt ein Gefühl dafür zu bekommen, dass Handlungsbedarf vorhanden ist und dass man da was tun muss und dass es, wie es in mancher Beziehung bisher gelaufen ist, so nicht weitergehen kann.“

Strategie: „Wir haben jetzt ein Vormittagsseminar in Planung, das wir gemeinsam mit einem Juristen, also hausintern, organisieren, an dem sich Führungskräfte beteiligen können, aber auch Mitarbeiter, und wir werden Kurzschulungen anbieten und das Ganze noch mal ein bisschen auf die Agenda packen.“ (Industrielle Produktion, 1.000 bis 4.999 Mitarbeiter weltweit)

„[...] und manche Situationen sind noch nicht hundertprozentig in den Köpfen.“

Strategie: „Wir machen im Gegensatz zu früher in dem Bereich wesentlich mehr webbasierte Schulungen, webbasierte Anwendungen, webbasierte Geschichten, zum Teil mit Verpflichtungscharakter.“ (Technologiewirtschaft, 1.000 bis 4.999 Mitarbeiter weltweit)

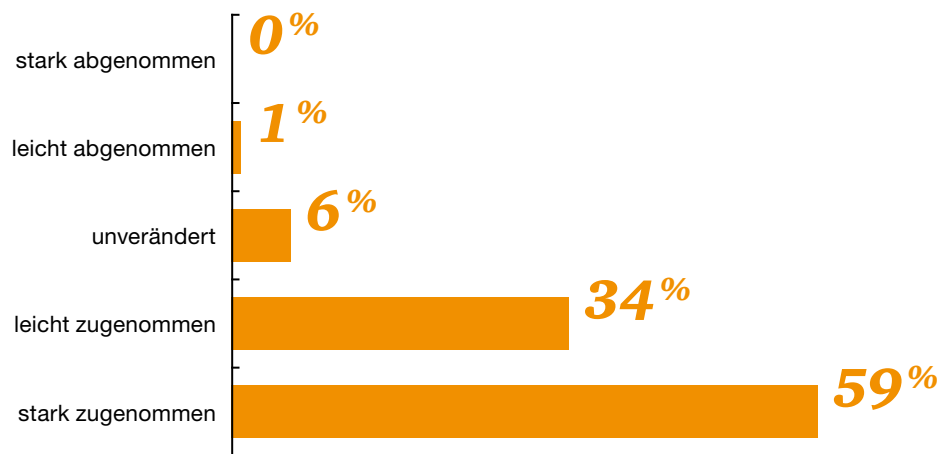
Gestiegene Anforderungen an Compliance-Programme

Auch im deutschen (Neben-)Strafrecht sind die Anforderungen an ein CMS höher geworden. So hat die Rechtsprechung entschieden, dass Aufsichtsmaßnahmen im Sinne des § 130 Abs. 1 OWiG nicht nur innerhalb eines Unternehmens sicherzustellen sind, sondern sogar im Einzelfall konzernweite Aufsichtspflichten bestehen.²¹ Für viele Muttergesellschaften dürfte die konzernweite Sicherstellung der Einhaltung strafrechtlicher Vorschriften eine große Herausforderung darstellen.

Des Weiteren können nach der höchstrichterlichen Rechtsprechung des Bundesgerichtshofs (BGH) Compliance-Maßnahmen im Rahmen der Strafzumessung bei einer Verbandssanktionierung im Sinne des § 30 OWiG berücksichtigt werden.²² Nach einem Rechtsverstoß kommt es für die Strafzumessung trotz eines bereits implementierten Compliance-Programms auch darauf an, entsprechende Compliance-Maßnahmen so zu optimieren, „dass vergleichbare Normverletzungen zukünftig jedenfalls deutlich erschwert werden“²³. Dies bedeutet, es besteht auch eine Rechtspflicht zur stetigen Evaluierung und Anpassung der bereits vorhandenen Compliance-Maßnahmen.

Das rechtliche Umfeld hat sich vor allem durch die höchstrichterliche Rechtsprechung mittlerweile stark verändert. Ein Drittel der befragten Unternehmen (34%) stellt daher zu Recht eine Zunahme der Anforderungen in den vergangenen fünf Jahren fest, 59% gehen sogar von einer starken Zunahme aus. Nur 6% können keine Veränderungen erkennen.

Abb. 10 Entwicklung der Anforderungen an CMS



Basis: alle befragten Unternehmen

Compliance-Budgets

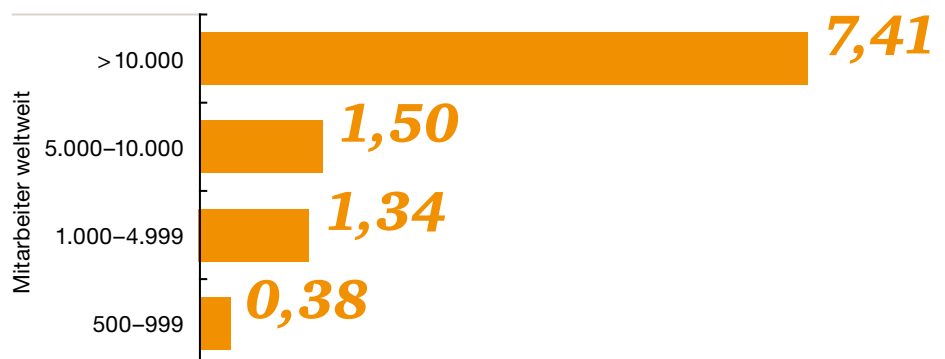
Viele Unternehmen statten mittlerweile ihre Compliance-Programme mit einem beachtlichen Budget aus.

Das durchschnittliche Budget für die Personal- und Sachmittel einer Compliance-Abteilung beläuft sich unabhängig von der organisatorischen Zuordnung auf 1,9 Millionen Euro,

allerdings hängt der Durchschnittswert wesentlich von der Größe des Unternehmens ab. Die Spannweite der durchschnittlichen Budgets reicht von 380.000 Euro bei Unternehmen mit 500 bis 999 Mitarbeitern bis zu 7,41 Millionen Euro bei Großunternehmen mit mehr als 10.000 Mitarbeitern.

Abb. 11 Compliance-Budget nach Anzahl der Mitarbeiter

Budget in Mio. Euro (Mittelwert)



²¹ Vgl. OLG München, Beschluss vom 23.09.2014 – 3 Ws 599, 600/14, BB 2015, 2004.

²² Vgl. BGH, Urteil vom 09.05.2017 – 1 StR 265/16.

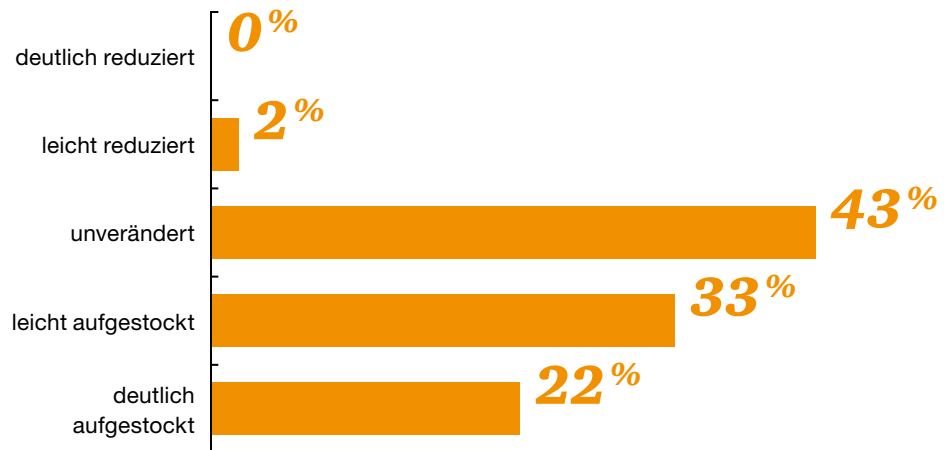
²³ BGH, Urteil vom 09.05.2017 – 1 StR 265/16.

Erhöhung der Budgets für Personal- und Sachmittel

Die Einschätzung, dass die Anforderungen an CMS stetig wachsen, spiegelt sich auch in der verbesserten Personal- und Sachmittelausstattung des CMS vieler Unternehmen wider. Mehr als jedes zweite Unternehmen hat sein Budget hierfür in den letzten zwei Jahren leicht (33 %) oder gar deutlich aufgestockt (22 %). Bei 43 % der Unternehmen blieb das Budget unverändert, nur 2 % berichteten über eine leichte Reduzierung.

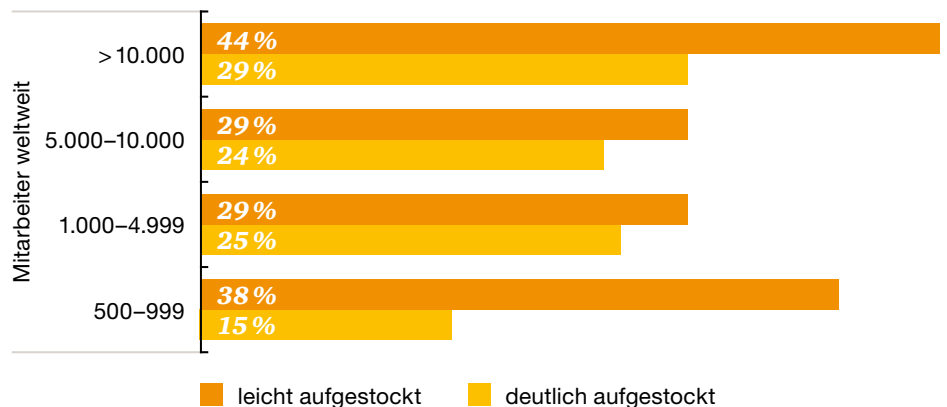
Eine Tendenz zur deutlichen Aufstockung des Budgets für die Personal- und Sachmittelausstattung des CMS besteht in Unternehmen aller Größen, am deutlichsten jedoch bei Großunternehmen mit mehr als 10.000 Mitarbeitern (29 %), am schwächsten bei mittelständischen Unternehmen mit 500 bis 999 Mitarbeitern (15 %). Über eine leichte Erhöhung des Etats berichteten jedoch beide Unternehmensgrößen nahezu gleichermaßen (44 % bzw. 38 %).

Abb. 12 Entwicklung der Personal- und Sachmittel für Compliance in den letzten zwei Jahren



Basis: alle befragten Unternehmen

Abb. 13 Entwicklung der Personal- und Sachmittel für Compliance nach Größe der Unternehmen



Basis: alle befragten Unternehmen

Die Ergebnisse unserer Studie lassen vermuten, dass die Budgets für den Ausbau der Compliance-Organisation in den nächsten Jahren sowohl bei Großunternehmen als auch mittelständischen Unternehmen weiter steigen werden. Zwar wurde in unseren vertieften Interviews vereinzelt vermutet, dass der große Compliance-Hype vorbei ist:

„Ich glaube, dass ein gewisses Verständnis und auch eine gewisse Sättigung dafür inzwischen am Markt ist [...]. Und der große Hype oder die große Umsetzungsphase ist, glaube ich, schon vorbei.“
(Automobilindustrie, 1.000 bis 4.999 Mitarbeiter weltweit)

Gegen diese Einschätzung spricht zurzeit jedoch, dass über 90 % der Unternehmen eine (starke) Zunahme der Anforderungen an CMS in den vergangenen fünf Jahren beobachteten (siehe Seite 28), die vielfach einen weiteren Ausbau des Compliance-Bereichs erfordern. Auch führt die Implementierung eines CMS in den Unternehmen weiterhin zu einer Sensibilisierung für Compliance-Risiken und organisatorische Schwachstellen, auf die Unternehmen zu reagieren haben. Zudem dürfte die Entwicklung auch aufgrund des Generationswechsels auf der Führungsebene kaum an Schwung verlieren; Manager der nachfolgenden Generation dürften im Allgemeinen offener für den „Compliance-Wandel“ sein und diesen eher forcieren.

Jedenfalls fanden sich auch in unseren vertieften Interviews noch keine Hinweise auf eine überwiegende Stagnation oder gar rückläufige Entwicklung der Budgetierung (siehe auch Seite 31). Vielmehr bestehen bei vielen Unternehmen Überlegungen, das Budget für die Personal- und Sachmittelausstattung des CMS eher aufzustocken. Hierzu einige Statements:

„Es wird immer wichtiger. Und es wird ein höherer Kostenblock werden. Wir sitzen jetzt in Budgetgesprächen und wir stocken die Budgets enorm auf, was Compliance betrifft.“ (sonstige Branche, mehr als 10.000 Mitarbeiter weltweit)

„Ich glaube, dass man langfristig ohne nicht mehr überleben kann als Unternehmen, insbesondere in unserer Branche. Ich sehe da eher einen weiteren Ausbau, also ich sehe da noch keine Stagnation.“
(Automobilindustrie, mehr als 10.000 Mitarbeiter weltweit)

„Compliance wird weiter an Bedeutung gewinnen und auch mehr an Akzeptanz. Das merkt man auch – also gerade jetzt. Wir haben ein neues Management bekommen und die ersten Rückfragen an Legal oder Compliance sind immer: Was haben wir? Wie arbeitet ihr?“
(Industrielle Produktion, 1.000 bis 4.999 Mitarbeiter weltweit)

Allerdings suchen alle Unternehmen nach einer angemessenen Balance zwischen Aufwand und Nutzen, hierzu ein Statement eines mittelständischen Unternehmens:

„Insgesamt, denke ich, wird man da den Kompromiss finden müssen zwischen Bürokratie und dem damit verbundenen Aufwand und der Sinnhaftigkeit der Regelungen. Natürlich muss Compliance sein, und je sensibler die Bereiche sind, in denen Compliance-Raum greift und angewendet werden will, umso dringender ist es [...]. Aber man muss auch immer den Aufwand für die Wirtschaft im Kopf behalten.“
(Maschinenbau und Metallindustrie, 500 bis 999 Mitarbeiter weltweit)

Die eigentlich kritische Frage ist jedoch, ob eine schlechtere unternehmerische oder volkswirtschaftliche Lage zu einer Reduzierung des CMS-Budgets führen würde. Hierauf fanden wir in unseren vertieften Interviews keine belastbare Antwort und es gab nur wenige kritische Einschätzungen:

„Compliance-Organisationen sind sehr viel selbstverständlicher geworden. Sie unterliegen in vielen Unternehmen mittlerweile den gleichen Mechanismen wie andere Organisationen. Das heißt, wenn Sie Budget oder Personal ansprechen, dann unterliegen sie prinzipiell den gleichen Entwicklungen – geht es dem Unternehmen schlecht, wird auch überlegt werden müssen, bei Compliance einzusparen. Das ist kein per se ausgeschlossener Bereich mehr.“ (Handel und Konsum, mehr als 10.000 Mitarbeiter weltweit)

„Sollte der internationale Wettbewerb mal wieder härter werden und Deutschland vielleicht nicht mehr so weit vorn liegen, dann wird auch an entsprechenden Stellen mehr auf Kosten geachtet werden müssen und dann muss man, glaube ich, schon besser darauf aufpassen, dass man nicht zu ausufernd Compliance betreibt, also nicht mit Kanonen auf Spatzen schießt.“ (Maschinenbau und Metallindustrie, 500 bis 999 Mitarbeiter weltweit)

Das Thema „wirtschaftliche Performance und Compliance“ werden wir in unseren Studien weiterverfolgen, meinen jedoch, dass Compliance nicht nur als Kosten-, sondern auch als Produktivfaktor gesehen werden sollte. Zu den internationalen Wettbewerbsvorteilen von Compliance aus Sicht der Unternehmen erfahren Sie mehr auf Seite 54 f.

Personelle Aufstockung des CMS

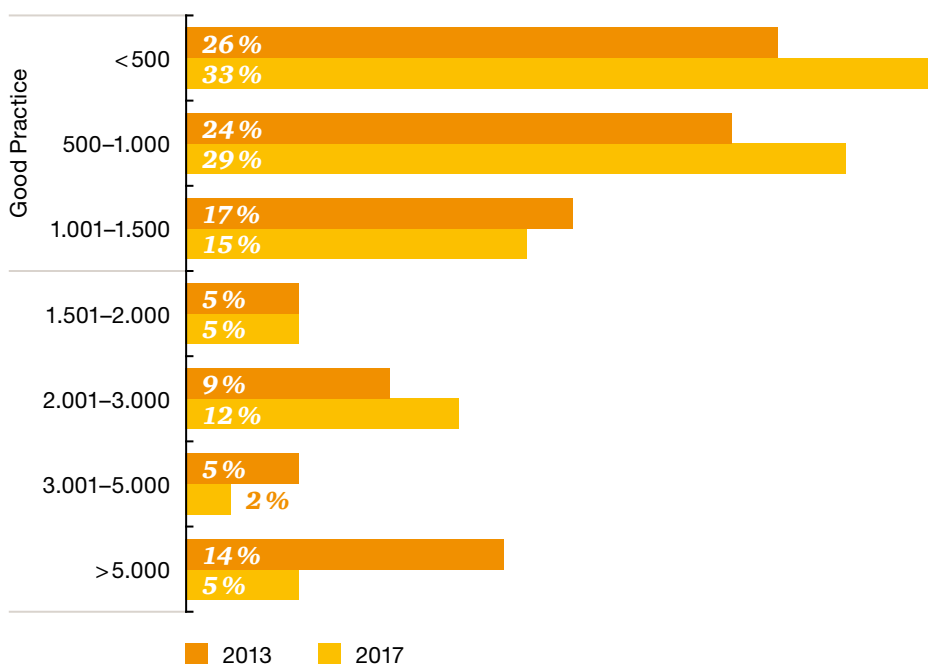
Konkret zeigt sich dieser positive Trend auch bei der Personalausstattung der Compliance-Programme. Zwar haben einige Großunternehmen die Personalausstattung nach dem Abschluss nationaler und internationaler Strafverfahren zurückgefahren, aber dies lässt sich nicht verallgemeinern. Unsere Studie zeigt vielmehr im Vergleich zu den Ergebnissen von 2013 eine klare Tendenz zur personellen Aufstockung.²⁴

Im Durchschnitt kommen heute rund 1.500 Mitarbeiter auf eine volle bzw. zwei halbe Compliance-Officer-Stellen,²⁵ während es in Deutschland vor vier Jahren noch rund 2.400 Mitarbeiter waren.²⁶ Als neuer Orientierungswert für eine personelle Good Practice kann daher gelten, im Durchschnitt eine Compliance-Officer-Stelle für etwa 1.500 Mitarbeiter vorzusehen.

Die Mehrheit der Unternehmen sieht zudem eine deutlich bessere Relation vor. So kommt bei einem Drittel der Unternehmen (33%) auf 500 Mitarbeiter und bei weiteren 29% auf 500 bis 1.000 Mitarbeiter eine Compliance-Officer-Stelle.

Abb. 14 Good Practice: Personelle Ausstattung der Compliance-Abteilung

Anteil der Unternehmen nach Anzahl der Mitarbeiter je Compliance-Officer



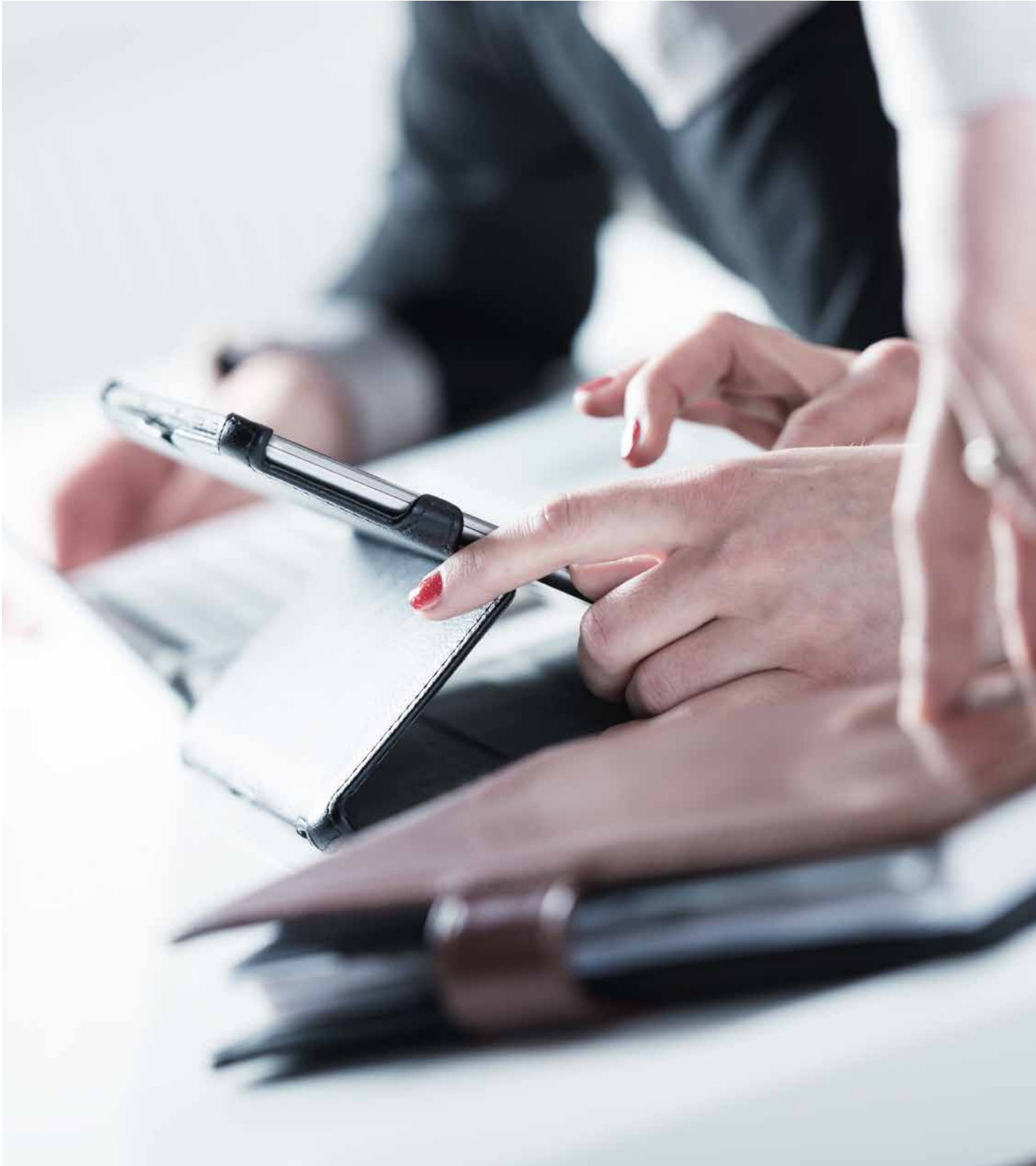
Im Durchschnitt kommen heute rund 1.500 Mitarbeiter auf eine volle bzw. zwei halbe Compliance-Officer-Stellen, während es vor vier Jahren noch rund 2.400 Mitarbeiter waren.

²⁴ Vgl. PwC, Wirtschaftskriminalität und Unternehmenskultur, 2013, S. 29 f.

²⁵ In unsere Berechnung sind Teilzeitstellen mit 0,5 eingegangen.

²⁶ In international operierenden Unternehmen kommen auf eine Compliance-Officer-Stelle weltweit 2.100 Mitarbeiter (2013: 2.200 Mitarbeiter weltweit).

Trend: Compliance in der Lieferkette





Einer deutlichen Mehrheit der Unternehmen (82%) ist mittlerweile wichtig bzw. sehr wichtig, dass ihre Lieferanten und Dienstleister über ein CMS verfügen oder eines einführen.

Viele Unternehmen berichteten, dass es inzwischen zur Routine gehöre, Compliance-Standards von ihren Lieferanten und Dienstleistern einzufordern.

Compliance aus Sicht der Auftraggeber

Bereits in unserer vorangegangenen Studie zeigte sich, dass Compliance auch durch den Markt vorangetrieben wird.²⁷ Die meisten Unternehmen versuchen den Compliance-Risiken auch in ihrem geschäftlichen Umfeld konsequent zu begegnen. In unseren vertieften Interviews wurde dies vor allem mit der wachsenden Erwartung im Markt und etwaigen Reputations- und Haftungsrisiken begründet:

„[...] die Verantwortung geht heute eben ein bisschen weiter als nur bis zum Nächsten, sondern sie sind schon in der Kette für uns verantwortlich. Verantwortung greift eben heute tiefer.“ (Industrielle Produktion, mehr als 10.000 Mitarbeiter weltweit)

„Das ist zum einen ja ein Reputationsanspruch, den man verfolgt. Zum anderen hat das natürlich auch massive rechtliche Aspekte. Sie haften eben auch für alle Handlungen Ihrer Geschäftspartner. – Ja, das sind die Hauptaspekte.“ (Automobilindustrie, mehr als 10.000 Mitarbeiter weltweit)

„Und das andere Thema ist, dass natürlich auch viele Kunden wiederum von uns erwarten, dass wir die Zusagen, die wir unseren Kunden machen, an unsere Lieferanten entsprechend weitergeben.“ (Automobilindustrie, 1.000 bis 4.999 Mitarbeiter weltweit)

Diese Statements spiegeln die Ergebnisse unserer repräsentativen Befragung wider, 82 % der Unternehmen gaben an, ihnen sei sehr wichtig bzw. wichtig, dass ihre Lieferanten und Dienstleister über ein CMS verfügen oder eines einführen wollen. Dies bedeutet gegenüber

unserer Studie von 2015 (72 %) eine Zunahme um zehn Prozentpunkte. Viele Unternehmen berichteten in unseren vertieften Interviews darüber, dass es mittlerweile Routine sei, Compliance-Standards von ihren Lieferanten und Dienstleistern einzufordern.

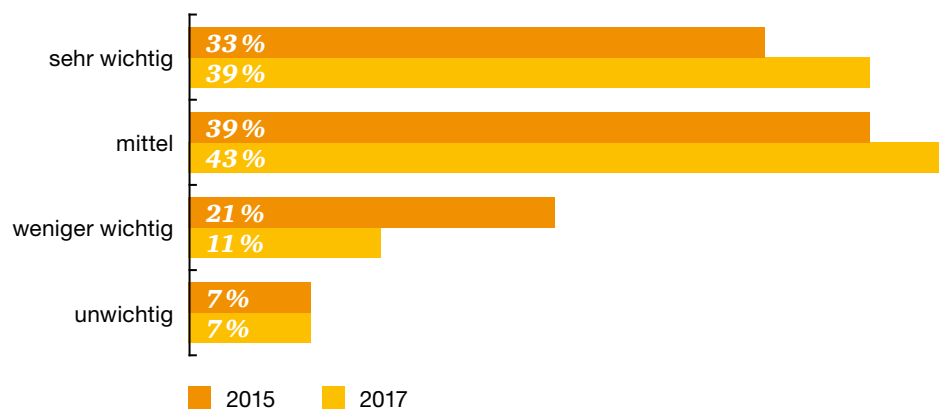
„Die Unternehmen haben natürlich verschiedene Levels eines Compliance-Managements, aber mir sind keine Probleme dahin gehend bekannt, dass sich jemand dem komplett verweigern würde.“ (Industrielle Produktion, 1.000 bis 4.999 Mitarbeiter weltweit)

„Ein oder zwei Lieferanten sind mir jetzt in der Vergangenheit bekannt gewesen, die sich etwas dagegen

gewehrt haben, aber mittlerweile auch darauf eingestiegen sind.“ (Pharma und Gesundheitswesen, mehr als 10.000 Mitarbeiter weltweit)

„Viele Lieferanten, die wir haben, sehen das Thema auch positiv und sind offen für die Diskussion.“ (Handel und Konsum, mehr als 10.000 Mitarbeiter weltweit)

Abb. 15 Bedeutung eines CMS aus Sicht der Auftraggeber



Basis: Unternehmen mit CMS

Über die Hälfte der Großunternehmen mit mehr als 10.000 Mitarbeitern erwartet von ihren Lieferanten und Dienstleistern, dass sie über ein CMS verfügen (55 %). Dieser Druck geht zunehmend auch von mittelständischen

Unternehmen aus. Als sehr wichtig bezeichneten dies über ein Drittel der Unternehmen mit 1.000 bis 4.999 Mitarbeitern (36 %) und über ein Viertel der Unternehmen mit 500 bis 999 Mitarbeitern (28 %).

²⁷ Vgl. Bussmann/Salvenmoser/Jeker, Compliance ist im Markt, aber noch nicht im Recht – Ergebnisse aus einer Unternehmensbefragung, in: CCZ 5/2016, S. 236–240.

In unseren vertieften Interviews berichteten einige Unternehmen allerdings über gelegentlich noch auftretende Probleme mit kleineren und mittelständischen Unternehmen:

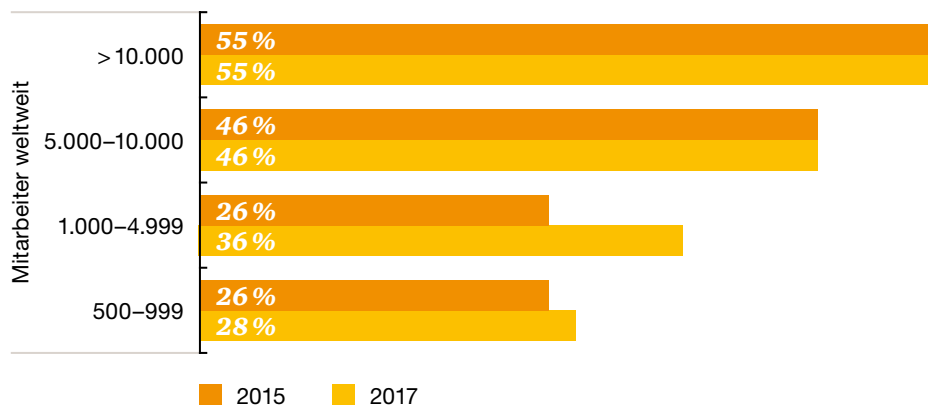
„Das Problem, das wir häufig antreffen, ist die Größe des Lieferanten – dass Sie besonders kleine Betriebe haben, die sich mit der Umsetzung eines Compliance-Management-Systems verständlicherweise schwertun [...]“. (Maschinenbau und Metallindustrie, 500 bis 999 Mitarbeiter weltweit)

„Ich glaube, das kommt natürlich auf die Größe des Zulieferers oder des Vertragspartners an. Die Größeren, die sich auch in einer Konzernstruktur befinden, haben damit weniger ein Problem, die kennen das, die haben ähnliche Systeme. Kleinere, insbesondere Mittelständler und Einzelkämpfer, haben natürlich ganz erhebliche Probleme – das ist auch zu verstehen.“ (sonstige Branche, mehr als 10.000 Mitarbeiter weltweit)

„Also ich habe auch das Gefühl, dass bei kleineren Unternehmen, insbesondere Mittelständlern und Einzelkämpfern, das Verständnis nicht da ist – man unterzeichnet die Dokumente, aber hält sich oft nicht daran.“ (sonstige Branche, mehr als 10.000 Mitarbeiter weltweit)

Abb. 16 Bedeutung eines CMS aus Sicht der Auftraggeber, nach Unternehmensgröße

Einschätzung der Bedeutung: sehr wichtig



Basis: Unternehmen mit CMS

Compliance-Vertragskonditionen

Für ein Drittel der Unternehmen gehört es mittlerweile zur alltäglichen Gestaltung ihrer Geschäftsbeziehung mit Lieferanten und Dienstleistern, sich die Einhaltung eines Code of Conduct vertraglich zusichern zu lassen (allgemeine Verpflichtungserklärung, 33 %):

„Unseren Lieferanten übermitteln wir eine sogenannte Lieferanten-Charta und nach anfänglichen Widerständen läuft das eigentlich in den letzten wenigen Jahren nach meiner Beobachtung problemlos. Wer bei uns aufs Lieferantenpanel möchte, muss das gegenzeichnen, und das funktioniert auch.“ (Transport und Logistik, mehr als 10.000 Mitarbeiter weltweit)

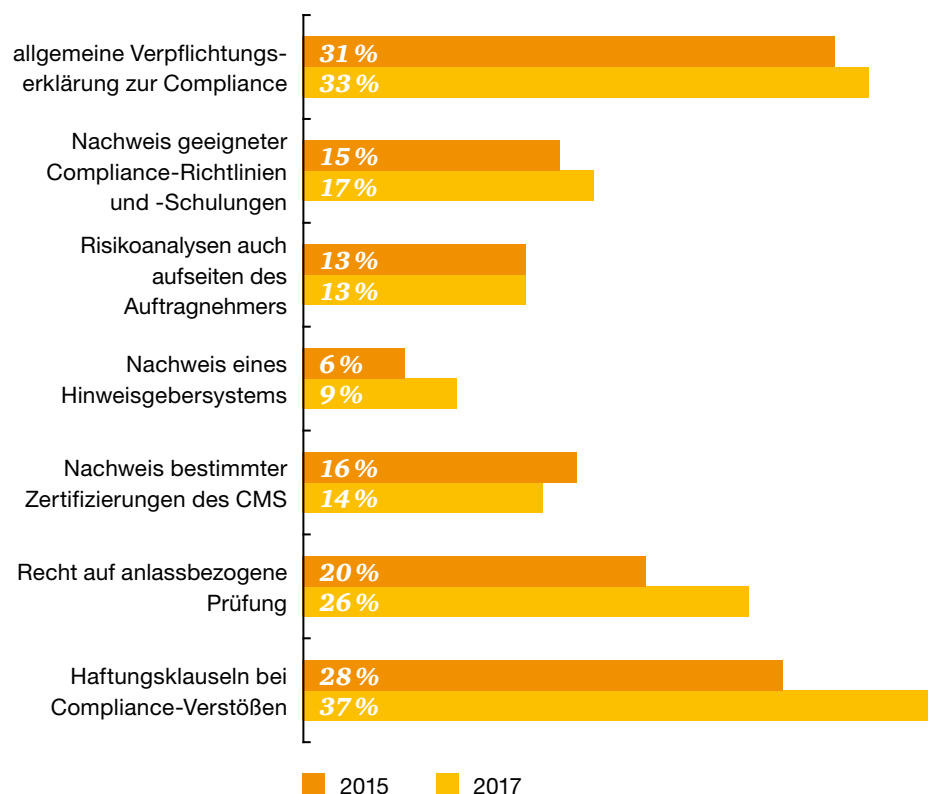
„Wir haben ja einen Code of Conduct für Lieferanten. Den lassen wir grundsätzlich bei Aufnahme einer neuen Geschäftsbeziehung immer erst mal bestätigen, und zwar schriftlich. Das erfolgt meines Wissens auch ohne nennenswerte Probleme.“ (Energiewirtschaft, 1.000 bis 4.999 Mitarbeiter weltweit)

Im Vergleich zu unserer Studie 2015 zeigt sich allerdings eine Tendenz, nunmehr auch über Haftungsklauseln die Umsetzung eines CMS bei Lieferanten und Dienstleistern durchzusetzen (37%). Darüber hinaus lassen sich Unternehmen in ihren Verträgen häufiger ein Recht auf anlassbezogene Prüfungen zusichern, bei einem Viertel der Unternehmen gehört diese sogenannte Audit Clause zur gängigen Praxis (26%). Ferner werden Nachweise über Compliance-Richtlinien und entsprechende Schulungen verlangt (17%). Mehr als jedes zehnte Unternehmen sieht in seinen Verträgen des Weiteren einen Nachweis bestimmter CMS-Zertifizierungen (14%) und Risikoanalysen auch aufseiten des Auftragnehmers vor (13%).

Für ein Drittel der Unternehmen gehört es mittlerweile zur alltäglichen Gestaltung ihrer Geschäftsbeziehung mit Lieferanten und Dienstleistern, sich die Einhaltung eines Code of Conduct vertraglich zusichern zu lassen.

Abb. 17 Verbreitung von Compliance-Vertragskonditionen

Einschätzung der Verbreitung: regelmäßig



Basis: Unternehmen mit CMS

Insbesondere Großunternehmen mit mindestens 5.000 Mitarbeitern nutzen ihren vertraglichen Gestaltungsspielraum. Deutlich häufiger als noch in unserer vorangegangenen Befragung sehen Verträge von Großunternehmen mit über 10.000 Mitarbeitern eine Compliance-Verpflichtungserklärung vor, bei mehr als der Hälfte ist dies üblich (59 %). Auch Klauseln, die eine anlassbezogene Prüfung ermöglichen, werden bei Großunternehmen mit über 5.000 Mitarbeitern immer gebräuchlicher (45 % bzw. 39 %). Außerdem sehen vor allem Großunternehmen bei ihren Lieferanten und Dienstleistern entsprechende Compliance-Haftungsklauseln vor (60 % bzw. 41 %).

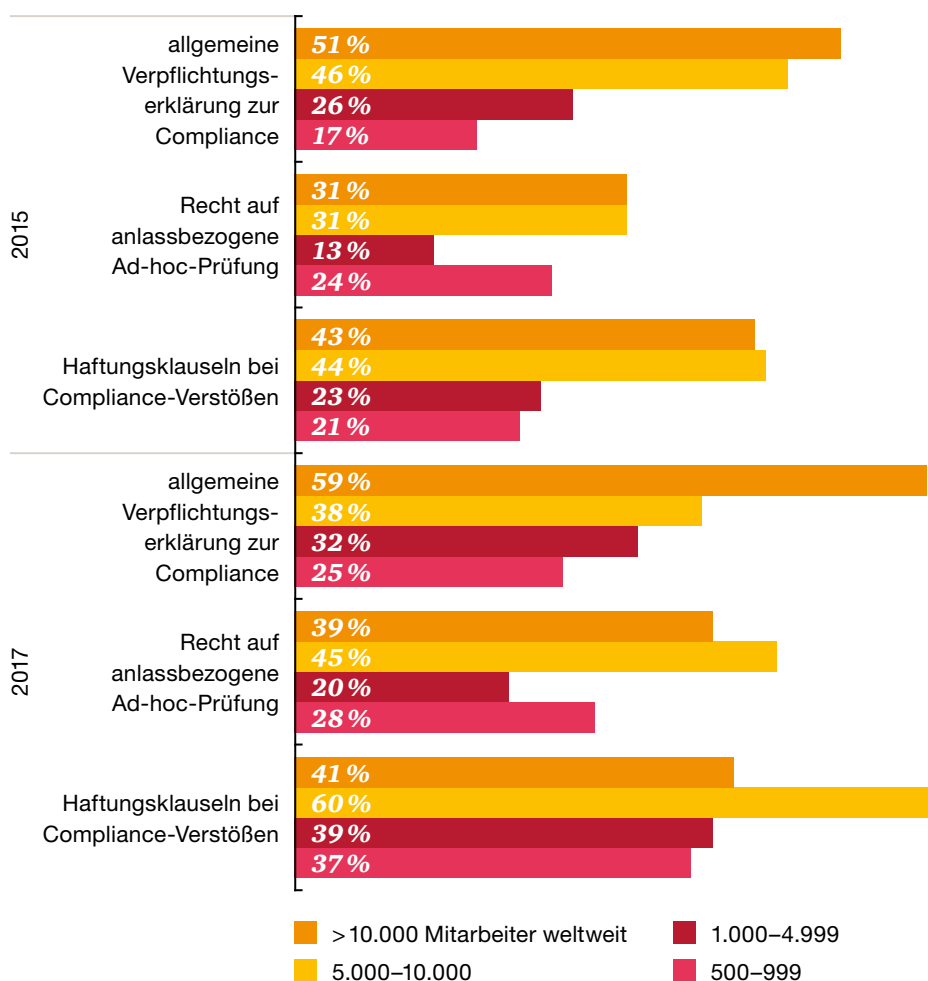
In den letzten zwei Jahren ist auch bei mittelständischen Unternehmen eine ähnliche Entwicklung festzustellen. So enthalten ihre Verträge mit Lieferanten und Dienstleistern gegenüber 2015 sehr viel häufiger Compliance-Haftungsklauseln, ein Anstieg um 16 Prozentpunkte (37 % bzw. 53 %). Über die Vertragsgestaltung üben somit nicht nur Großunternehmen einen Compliance-Druck auf Lieferanten und Dienstleister aus, sondern auch mittelständische Unternehmen.

Im Zuge des allgemeinen Trends, sich in Verträgen Compliance zusichern zu lassen, zeichnen sich allerdings nunmehr Konflikte zwischen verschiedenen Compliance-Standards ab. Hier einige Statements aus unseren vertieften Interviews:

Konflikte zwischen CMS-Standards

„Wir haben die meisten Probleme und Widerstände dort, wo wir natürlich unsere Vorgaben vereinbart haben wollen, wie zum Beispiel Code of Conduct oder Mindestlohnzusagen, und die Lieferanten dann immer das gleiche Problem haben – die haben einen eigenen Code of Conduct, und wir kommen dann an das Thema: Ja, grundsätzlich sind wir mit dem einverstanden, aber wir können das jetzt nicht genauso zusagen, wie ihr das wollt, weil wir das sonst für jeden Kunden separat machen müssen.“ (Automobilindustrie, 1.000 bis 4.999 Mitarbeiter weltweit)

Abb. 18 Regelmäßige Compliance-Vertragskonditionen, nach Unternehmensgröße



Basis: Unternehmen mit CMS

Darüber hinaus sehen sich Unternehmen mit der zunehmenden Verbreitung von Compliance-Vertragskonditionen

einer wachsenden Regelungs-unübersichtlichkeit ausgesetzt:

Neue Unübersichtlichkeit

„Was wir heute erleben, ist, dass Kunden, aber auch Lieferanten versuchen, uns ihre jeweiligen Verhaltenskodizes quasi unterzujubeln, indem sie uns bitten, diese schriftlich anzuerkennen. Und wir versuchen, das in der Regel abzuwenden, indem wir auf unsere eigenen Compliance-Richtlinien verweisen, weil wir sonst anfangen, Tausende von Verhaltenskodizes anderer Firmen zu unterschreiben [...].“ (Technologiewirtschaft, 5.000 bis 10.000 Mitarbeiter weltweit)

„Also mittlerweile ist es so, dass es meiner Meinung nach auch ein bisschen überhandnimmt, dass beispielsweise große Kunden ihren Lieferanten vorschreiben, ihren Verhaltenskodex zu übernehmen. Und das kann natürlich niemand machen – dann hat man sich nachher einverstanden erklärt mit hundert verschiedenen Verhaltenskodexen. Also das sehe ich grundsätzlich schon als Problem an.“ (Industrielle Produktion, 1.000 bis 4.999 Mitarbeiter weltweit)

Diese Probleme ließen sich weitgehend vermeiden, wenn die Unternehmen ihr CMS unabhängig überprüfen und/oder zertifizieren lassen würden, um eine gemeinsame Verständnisgrundlage zu fördern und die gegenseitige Anerkennung der vorhandenen Compliance-Programme zu erleichtern. Allerdings hat bislang nur knapp die Hälfte der befragten Unternehmen eine unabhängige Prüfung nach dem IDW Prüfungsstandard 980 oder eine Zertifizierung gemäß ISO 19600 durchführen lassen (siehe Seite 46 f., 47%). Der Verzicht darauf führt zwangsläufig zu einem Wildwuchs von Compliance-Standards und entsprechender Vertragskonditionen. Auch setzen sich Unternehmen der Marktmacht größerer Kunden aus, wie folgende Aussage illustriert:

„Wir versuchen jetzt eher auf Themen wie gegenseitige Anerkennung zu gehen, dass wir sagen: Ihr erkennt unseren Code of Conduct an, wir erkennen euren Code of Conduct an – und müssen dann nicht immer wieder Details aus diesen Regelungen bei unseren Lieferanten neu verhandeln. Das wäre die beste Vorgehensweise. Aber das klappt leider nicht immer. Vor allem große Kunden mit entsprechender Verhandlungsmacht bestehen einfach darauf, dass ihre Sachen so akzeptiert werden, wie sie sind.“ (Automobilindustrie, 1.000 bis 4.999 Mitarbeiter weltweit)

Compliance beats Corruption





Das Eis scheint gebrochen, alle von uns erhobenen Kennwerte deuten auf eine sinkende Korruptionsbelastung der deutschen Wirtschaft hin.

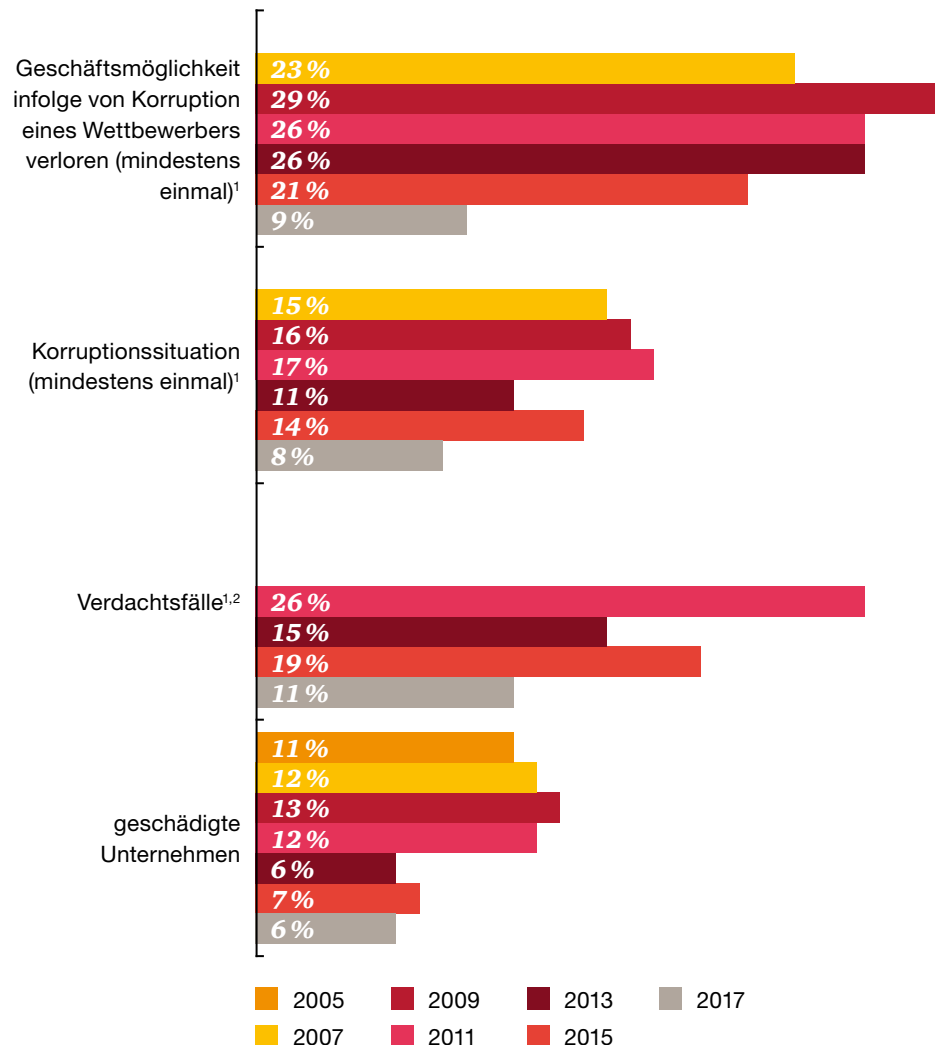
Durch Korruption wurden nur 6 % der Unternehmen betroffen und gegenüber 2015 nahmen die Verdachtsfälle von 19 % auf 11 % ab.

Entwicklung der Korruptionsrisiken

Bereits in unserer vorangegangenen Studie vermuteten wir eine allmähliche Abnahme der Korruption. Die Ergebnisse dieser Studie bestätigen diese Einschätzung. Alle Kennwerte dieser Studie deuten auf eine sinkende Korruptionsbelastung der deutschen Wirtschaft hin. Die Zahl der von Korruption betroffenen Unternehmen stagniert seit 2013 auf einem niedrigen Niveau von 6 %, wird aber nunmehr von einem deutlichen Rückgang anderer Kennwerte begleitet. Gegenüber 2015 nahmen die Verdachtsfälle von 19 % auf 11 % ab. Auch der Anteil der Unternehmen, denen Geschäfte vermutlich infolge von Korruption eines Wettbewerbers entgangen sind, sinkt von 21 % auf 9 %. Ebenfalls rückläufig ist der Anteil der Unternehmen, die angaben, sich mindestens einmal in einer Korruptionssituation befunden zu haben (8 %).

Diese positive Entwicklung dürfte auf mehrere Faktoren zurückzuführen sein. Zum einen wurden korruptionsrechtliche Compliance-Programme optimiert und in immer mehr Unternehmen implementiert (siehe Abb. 19), begleitet von einem wachsenden Problembewusstsein auch in der öffentlichen Verwaltung. Zum anderen dürfte auch der Gesetzgeber mit der Reform des § 299 StGB in Richtung eines Geschäftsherrnmodells eine wichtige Signal- und Abschreckungswirkung erzielt haben, da nunmehr Bestechung und Bestechlichkeit auch außerhalb einer Wettbewerbssituation strafrechtlich verfolgt werden können. Diese innerhalb und außerhalb der Unternehmen erfolgten regulatorischen Maßnahmen dürften für eine signifikante Zurückdrängung der Korruption verantwortlich sein.

Abb. 19 Entwicklung der Korruptionsrisiken 2005–2017



¹ Keine Daten für 2005.

² Keine Daten für 2007 und 2009.

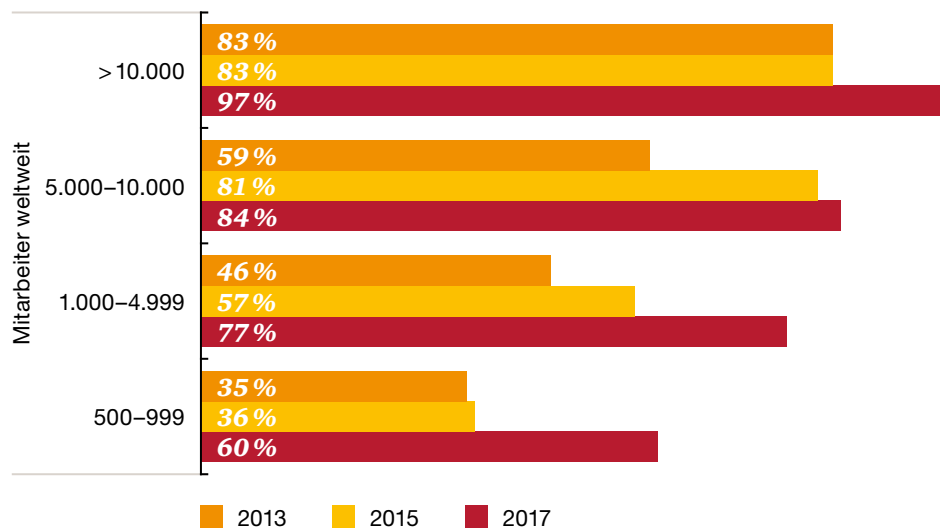
Bei Großunternehmen sind Anti-Korruptionsprogramme selbstverständlich (97%), aber auch mittelständische Unternehmen haben erheblich nachgezogen.

Der Mittelstand holt auf

Compliance-Programme erstrecken sich heute in der Regel auch auf Korruptionsprävention (83 %). Bei weiteren 10 % der Unternehmen befindet sich dies gerade im Aufbau bzw. in der Planung. Unabhängig von der Größe der Unternehmen wurde der Ausbau eines CMS zur Korruptionsprävention vorangetrieben.

Bei Großunternehmen sind Anti-Korruptionsprogramme selbstverständlich (97 %), aber auch mittelständische Unternehmen haben erheblich nachgezogen. 2015 verfügte nur ein gutes Drittel der Unternehmen mit 500 bis 999 Mitarbeitern über ein entsprechendes CMS, 2017 sind es bereits fast zwei Drittel (60 %). Deutlich aufgeholt haben auch Unternehmen mit 1.000 bis 4.999 Mitarbeitern, über drei Viertel (77 %) verfügen über ein Anti-Korruptionsprogramm; die größenabhängigen Unterschiede schwinden.

Abb. 20 Verbreitung von Anti-Korruptionsprogrammen 2013–2017, nach Unternehmensgröße



Basis: Unternehmen mit CMS

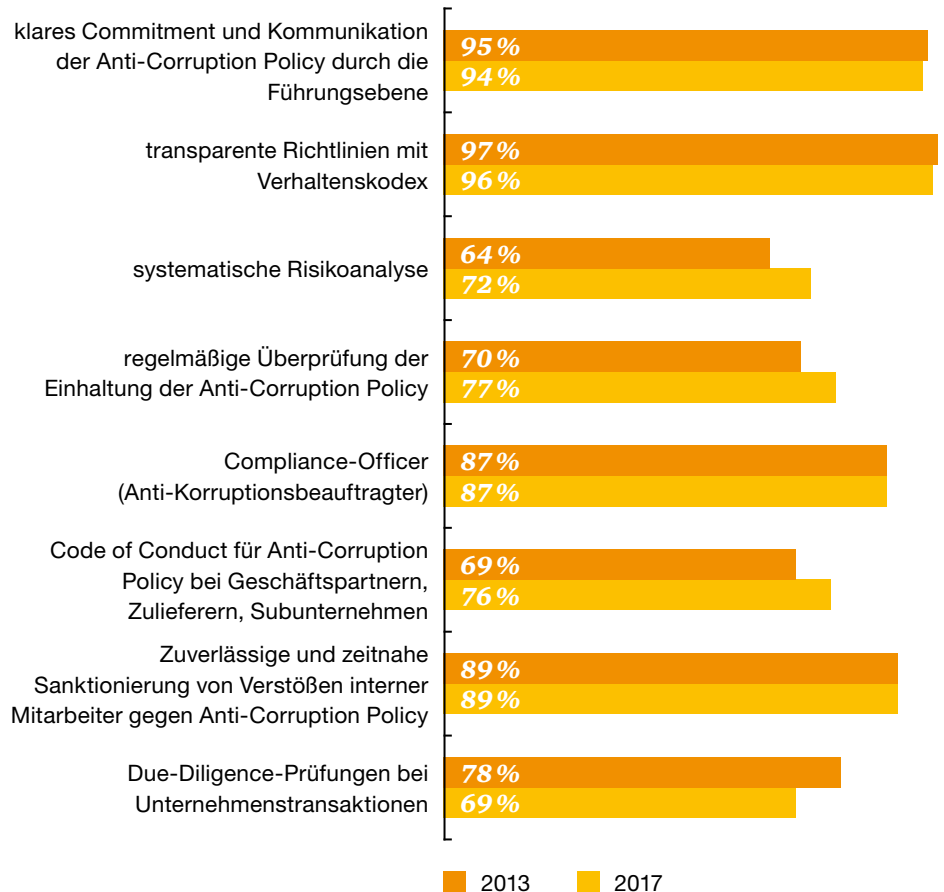
Verbreitung von Anti-Korruptionsmaßnahmen

Für ein wirksames korruptionsrechtliches CMS sind ein von der Führungsebene klar kommuniziertes Commitment und ein entsprechender Verhaltenskodex unerlässlich, fast alle Compliance-Programme sehen dies vor (94% bzw. 96%). Konsequenterweise werden Compliance-Verstöße interner Mitarbeiter zeitnah sanktioniert (89%). Selbstverständlich ist ebenfalls die Funktion eines Compliance-Officers (87%).

Unsere aktuelle Studie zeigt, dass Unternehmen ihr CMS weiter ausbauen und optimieren. Eine systematische Risikoanalyse und regelmäßige Überprüfung der Einhaltung der Compliance-Regeln sind mittlerweile Bestandteil von rund drei Vierteln der Anti-Korruptionsprogramme (72% bzw. 77%). Bei einer wachsenden Zahl der Unternehmen richtet sich der Blick auf Geschäftspartner, Zulieferer und Subunternehmen. Ein Viertel verlangt einen Code of Conduct (76%). Im Rahmen von Unternehmenstransaktionen haben allerdings entsprechende Compliance-Due-Diligence-Prüfungen leicht an Bedeutung verloren (69%). Dies sehen wir kritisch. Zwar sind Compliance-Programme zur Korruptionsprävention zunehmend selbstverständlich geworden, dennoch empfiehlt sich bei Mergers & Acquisitions weiterhin eine gewissenhafte Prüfung des jeweiligen CMS.

Abb. 21 Verbreitung der Anti-Korruptionsmaßnahmen 2013–2017

Mehrfachnennungen waren möglich.



Basis: Unternehmen mit CMS

Schulungen zunehmend auch digital

Schulungs- und Informationsangebote zum Umgang mit Korruptionssituationen sind das Herzstück eines CMS. Gemessen hieran sind sie noch nicht so selbstverständlich, wie sie sein sollten. Nur 79 % der Compliance-Programme sehen Schulungsmaßnahmen vor, etwas weniger als im Vergleich zu unserer Studie vor vier Jahren (82%).²⁸ Wesentlicher Bestandteil sind weiterhin Face-to-Face- und Classroom-Schulungsmaßnahmen (70 %). Den persönlichen

Kontakt zu ihren Mitarbeitern hält somit die Mehrheit der Unternehmen für sehr wertvoll. Ergänzend werden zunehmend auch digitale Trainingsformate eingesetzt. Fast zwei Drittel der Schulungsmaßnahmen erfolgen auch durch webbasierte Lernprogramme und Schulungsfilme (61 %), ein Format, das im Jahr 2013 noch deutlich weniger verbreitet war (39 %). Zur Vertiefung der Inhalte dienen Workshops mit fallpraktischen Übungen, Dilemmaszenarien und Verhaltenstraining (49 %).

²⁸ Vgl. PwC, Wirtschaftskriminalität und Unternehmenskultur, 2013, S. 39 f.

Fast zwei Drittel (64%) der Compliance-Programme erreichten mit ihren Schulungen alle relevanten Funktionsträger (100%). Im Durchschnitt betrug der Schulungsgrad in Unternehmen mit einem CMS mittlerweile 88%. Trotz Personalfuktuation wurden die meisten korruptionsgefährdeten Funktionsträger erreicht (2017: 78%; 2013: 60%).²⁹

Unternehmen haben die Qualität ihrer Schulungsmaßnahmen seit 2013 insgesamt gesehen weiter verbessert. Nach Einschätzung von 90% der befragten Unternehmen fühlen sich die Teilnehmer durch ihre Schulungen ausreichend über die rechtlichen Aspekte von Korruption informiert und 81% der Unternehmen meinen, dass ihre Schulungsteilnehmer sich hiernach auch ausreichend auf den Umgang mit Dilemmasituationen vorbereitet sehen. Allerdings stieg der Anteil der Unternehmen, deren Teilnehmer beklagten, dass die Informationen aus den Schulungen in der täglichen Praxis wieder verloren gehen, um fünf Prozentpunkte (20%).

Abb. 22 Praxis der Schulungen 2013–2017

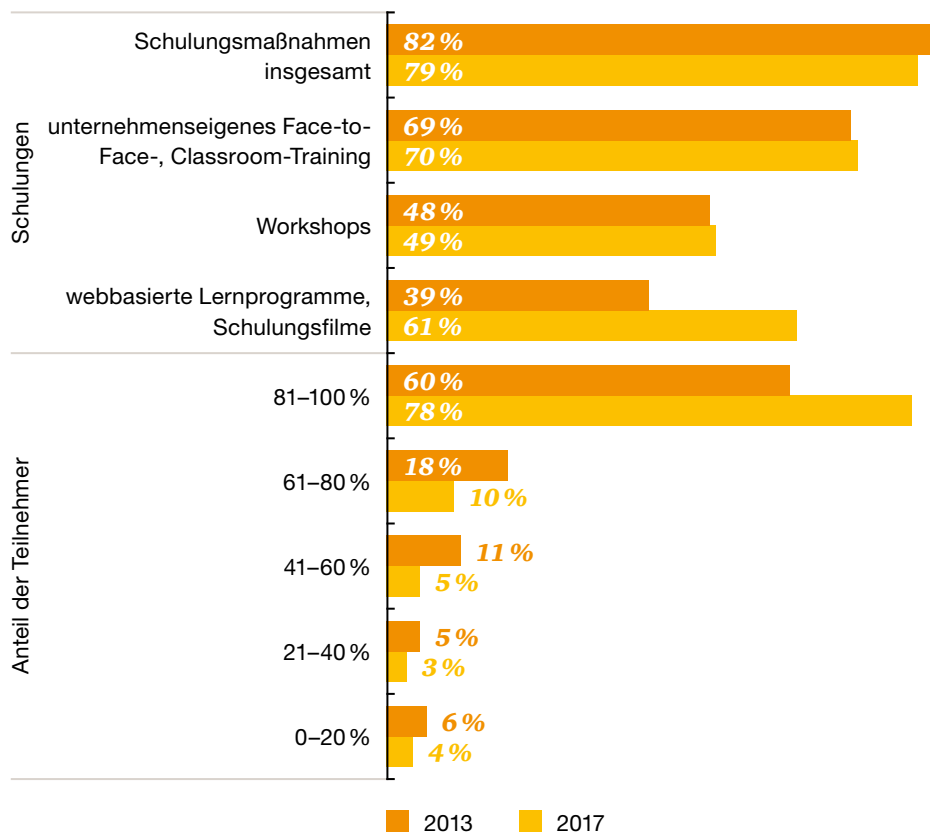
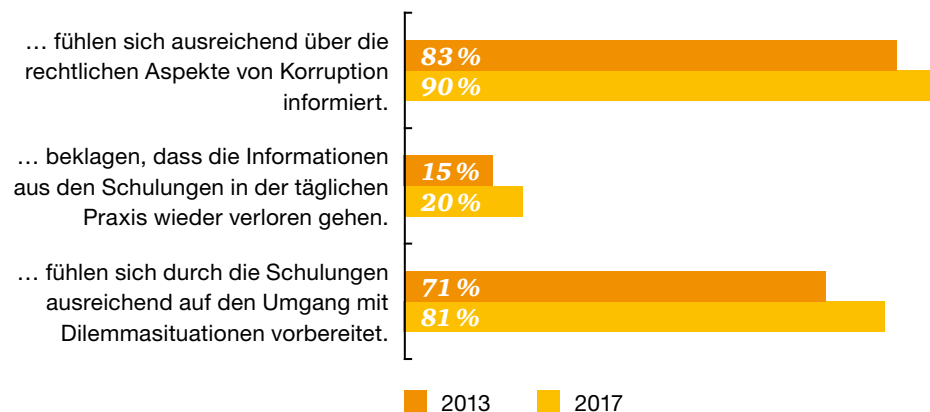


Abb. 23 Bewertung der Schulungen 2013–2017

„Trifft zu“: Die meisten Kollegen ...



²⁹ Vgl. ebenda S. 41.

Trend: Hinweisgebersysteme

Hinweisgebersysteme sind zunehmend Normalität. Am verbreitetsten ist mit 79 % ein interner Ansprechpartner, zum Beispiel in der Rechtsabteilung. Allerdings bietet diese Form zumeist nur eine eingeschränkte Anonymität, sodass wir sie nicht als Hinweisgebersystem im engeren Sinne ansehen. Über eine telefonische Hotline (57 %), ein webbasiertes System (35 %) oder eine Ombudsperson (29 %) verfügen jedoch mittlerweile insgesamt 86 % der Unternehmen mit einem Anti-Korruptionsprogramm, somit deutlich mehr als 2013 (72 %).

Ihr Nutzen zur Aufdeckung insbesondere schwerer Compliance-Verstöße wird kaum noch bezweifelt. Bisher ist die Einrichtung von Hinweisgebersystemen für deutsche Unternehmen – abgesehen für Kredit- bzw. Finanzdienstleistungsunternehmen gemäß § 25a Abs. 1 Satz 6 Nr. 3 KWG – nicht gesetzlich verpflichtend.³⁰ Eine rechtliche Verpflichtung erwächst jedoch den Unternehmen, die dem FCPA oder UK Bribery Act unterliegen.³¹ Beide verlangen die Einrichtung solcher Hinweisgebersysteme.³²

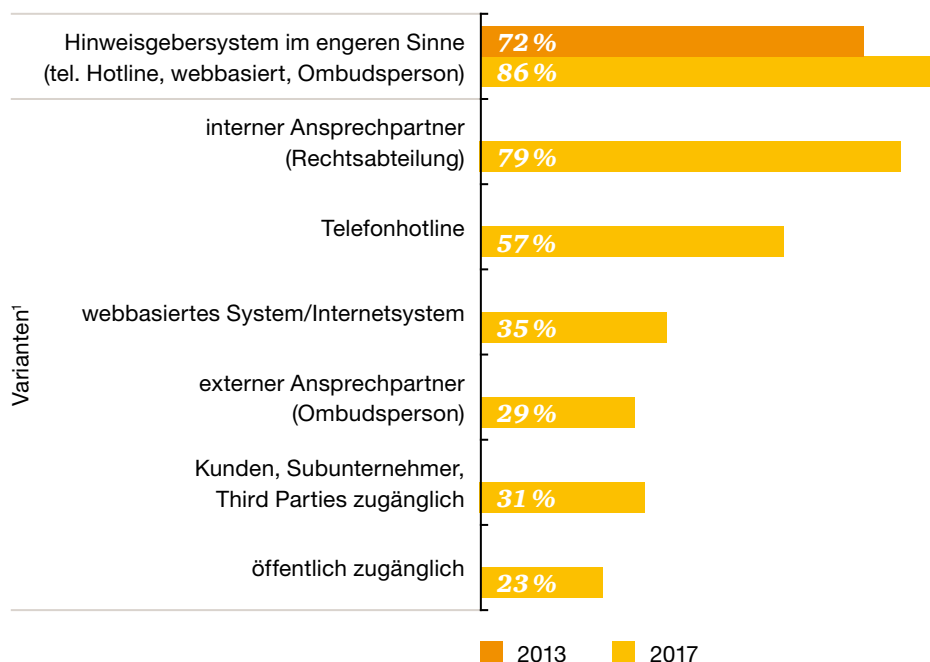
Frankreich hat jüngst mit dem Sapin-II-Gesetz eine Regelung erlassen, welche die Implementierung eines Hinweisgebersystems für Unternehmen unter anderem mit mehr als 500 Arbeitnehmern und einem Umsatz von über 100 Millionen Euro verpflichtend regelt und damit auf die

vielen in den USA ergangenen FCPA-Entscheidungen gegen europäische Unternehmen reagiert.³³ Ähnliche Gesetzesvorschläge verschiedener Fraktionen und Parteien, gerade zum Schutz von Hinweisgebern, sind in Deutschland bisher gescheitert. Eine Änderung der bestehenden Rechtslage scheint derzeit in Deutschland nur durch eine Verordnung der Europäischen Union denkbar. Aktuell gibt es allerdings keinen entsprechenden Gesetzentwurf auf europäischer Ebene. In naher Zukunft könnte jedoch ein EU-Gesetz zum Schutz von Hinweisgebern erlassen werden.³⁴

Handlungsbedarf besteht derzeit noch hinsichtlich der Öffnung von Hinweisgebersystemen, sie sollten nicht auf interne Tippgeber beschränkt sein, wie auch die Richtlinien des FCPA fordern.³⁵ Auch unsere Studien zeigen, dass rund ein Fünftel der Hinweise von externen Tippgebern kommen.³⁶ Nur knapp jedes dritte Hinweisgebersystem ist auch Geschäftspartnern und Subunternehmen zugänglich (31 %) und jedes vierte allgemein der Öffentlichkeit (23 %). In dieser Hinsicht ist daher die Effizienz vieler Hinweisgebersysteme verbesserungswürdig.

Abb. 24 Hinweisgebersysteme 2013–2017

Mehrfachnennungen waren möglich.



Basis: Unternehmen mit CMS

¹ Keine differenzierten Daten für 2013.

³⁰ Für die Implementierung eines Hinweisgebersystems plädieren: Schemmel/Ruhmannseder/Witzigmann, Hinweisgebersysteme, S. 315, Rn. 3 ff. m. w. N.

³¹ In unserer Studie 2017 unterliegen über ein Viertel (28 %) der befragten Unternehmen dem FCPA, da sie nach US-Recht gegründet wurden, ihren Geschäftssitz in den USA haben, an einer US-Börse notiert sind oder auf andere Weise in den USA geschäftlich tätig sind.

³² Vgl. Guidance FCPA, S. 61, online abrufbar unter: www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf; Guidance UK Bribery Act, S. 29 f., online abrufbar unter: www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf.

³³ Vgl. www.schulte-lawyers.com/schulteblog/1632017 (zuletzt abgerufen am 30.10.2017).

³⁴ Vgl. www.heise.de/newsticker/meldung/Europaeischer-Parlamentsausschuss-fordert-gesetzlichen-Whistleblower-Schutz-3822362.html (zuletzt abgerufen am 30.10.2017).

³⁵ Richtlinie zum FCPA; im Abschnitt „Confidential Reporting and Internal Investigation“ (S. 61) wird ein *mechanism for employees and others to report suspected or actual misconduct or violations* verlangt.

³⁶ Vgl. zum Beispiel PwC, Wirtschaftskriminalität und Unternehmenskultur, 2013, S. 83.

Unsere vertieften Interviews ergaben, dass in einzelnen Fällen die Geschäftsleitung erst von den Vorteilen eines Hinweisgebersystems überzeugt werden musste:

„Es hat ein bisschen gedauert, auch die Geschäftsführung zu überzeugen, dass das etwas Gutes ist, was uns nützt, was die Fehlerkultur im Unternehmen verbessern kann.“ (Pharma und Gesundheitswesen, mehr als 10.000 Mitarbeiter weltweit)

Die meisten Unternehmen zeigten sich jedoch vom Nutzen ihres Hinweisgebersystems überzeugt und wollen hierauf nicht mehr verzichten:

„Es sind Themen aufgekommen, die mit Sicherheit so nicht gekommen wären, weil natürlich jeder Mitarbeiter Angst hat, seinen Chef oder Vorgesetzten ‚anzuschwärzen‘, und dann nicht genau weiß, an wen er sich wenden soll, wem er vertrauen kann. Da ist ein anonymes Postfach oder eine Eingabemaske im Internet doch deutlich einfacher und ziel-führender.“ (Automobilindustrie, 1.000 bis 4.999 Mitarbeiter weltweit)

„Es bringt auf jeden Fall zusätzliche Erkenntnisse über Fälle, die sonst nicht an uns herangetragen würden. Und zwar auch für durchaus wichtige Fälle, nicht nur für Beschwerden übers Kantinenessen.“ (Technologiewirtschaft, 5.000 bis 10.000 Mitarbeiter weltweit)

Wie auch in einer unserer früheren Studien bestätigen die Interviews, dass sich Hinweise zum Teil als unzutreffend oder nicht nachweisbar herausstellen, aber nicht offensichtlich missbräuchlich gegeben wurden:³⁷

„Jede Meldung ist wichtig und ernst zu nehmen – die Relevanz oder Irrelevanz der Meldung stellt sich erst im Nachhinein heraus.“ (Maschinenbau und Metallindustrie, 5.000 bis 10.000 Mitarbeiter weltweit)

„Es ist das etablierte Medium, wie Kontakt über Compliance-Verstöße aufgenommen wird. Wir haben keine Hinweise auf Denunziation – das ist ein ganz großer Vorteil, den wir darin sehen. Wir haben eine permanente Erreichbarkeit über das System.“ (Pharma und Gesundheitswesen, 1.000 bis 4.999 Mitarbeiter weltweit)

„Das Wichtigste dabei ist, dass es genutzt wird und dabei bisher kein einziges Mal ein Missbrauch stattgefunden hat.“ (Handel und Konsum, 5.000 bis 10.000 Mitarbeiter weltweit)

Zudem trägt ein Hinweisgebersystem nicht allein zur Aufdeckung von Compliance-Verstößen bei, sondern auch zur weiteren Verbesserung des CMS, wie einige Unternehmen betonen:

„Ein gut vermarktetes Hinweisgebersystem gibt immer Hinweise auf konkrete Fälle, aber auch Anhaltspunkte für die Verbesserung eines Systems insgesamt.“ (Handel und Konsum, mehr als 10.000 Mitarbeiter weltweit)

Allerdings zeigt unsere Studie auch, dass der Nutzen der Hinweisgebersysteme sehr von ihrer Anonymität und Zugänglichkeit abhängt:

„Null – es kommt nichts rein. [...] Vielleicht ist es nicht gut installiert – es ist eine reine E-Mail-Adresse, die man erst einmal suchen muss.“ (Transport und Logistik, mehr als 10.000 Mitarbeiter weltweit)

**Hinweisgebersysteme sind
inzwischen die Regel (86 %).**

³⁷ Vgl. PwC, Compliance und Unternehmenskultur, 2010, S. 35.

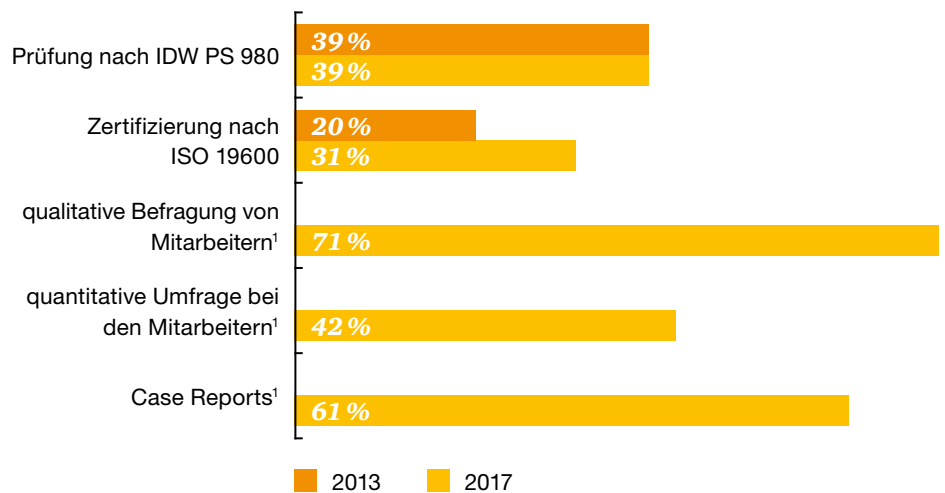
Evaluation des Compliance-Managements

Compliance-Programme sind in der deutschen Wirtschaft weitgehend selbstverständlich geworden. Gleichwohl scheut ein noch zu hoher Anteil der Unternehmen eine unabhängige Evaluation ihres CMS. Jedes zweite führte keine unabhängige Prüfung durch (47%), weder nach dem IDW Prüfungsstandard 980 noch dem internationalen Standard ISO 19600.³⁸ Der Anteil der Unternehmen, die ihr CMS nach IDW Prüfungsstandard 980 evaluiert haben, blieb unverändert bei 39%. Der Anteil der Evaluationen nach dem internationalen Standard ISO 19600 stieg um elf Prozentpunkte auf 31%.

Fast zwei Drittel der Compliance-Programme sehen Case Reports vor (61%), die eine ungetrübte Fallanalyse ermöglichen und daher unverzichtbar sind. Ihr Nachteil ist allerdings, dass

sie sich auf die entdeckten Fälle beschränken, somit auf das sogenannte Hellfeld. Demgegenüber erlauben Mitarbeiterbefragungen einen tieferen Blick in das sogenannte Dunkelfeld. Fast drei Viertel der Unternehmen wählten für die Evaluation die Methode einer qualitativen Befragung von Mitarbeitern (71%). Im Unterschied zu einer quantitativen Befragung kann jedoch mit persönlichen Interviews die Anonymität kaum gewährleistet werden. Auch können nur kleine Fallzahlen erreicht werden, sodass eine repräsentative Aussage nur bedingt möglich ist.³⁹ Qualitative Befragungen vermitteln somit einen guten ersten Eindruck, der anhand einer quantitativen Befragung repräsentativ abgesichert werden sollte. Eine solche gehört jedoch nur bei 42% der Compliance-Programme zur Evaluation.

Abb. 25 Art der Evaluation des CMS



Basis: alle befragten Unternehmen

¹ Keine Daten für 2013.

³⁸ Eine Prüfung nach IDW Prüfungsstandard 980 oder Zertifizierung nach ISO 19600 erfolgte bei 53 % der befragten Unternehmen.

³⁹ Vgl. ausführlich zu Methoden auch DICO e. V., Leitlinie 07: Hinweise und Kriterien zur Messung einer Unternehmenskultur, 2016, S. 9 ff., online abrufbar unter: www.dico-ev.de/wp-content/uploads/2017/06/L07_Unternehmenskultur_12S_2016_WEB.pdf.

Wir meinen, dass eine Evaluation aus verschiedenen Blickwinkeln erfolgen und daher neben Case Reports auch unabhängige Prüfungen und Mitarbeiterbefragungen umfassen sollte. In unseren vertieften Interviews zeigte sich, dass die meisten Unternehmen in ihren Evaluationsmaßnahmen einen Mehrwert zur weiteren Optimierung ihres CMS sehen. Hier einige Stimmen:

Mehrwert zur weiteren CMS-Optimierung

„Wir haben ein aus meiner Sicht sehr gutes Reportingsystem zum Thema Compliance installiert, auch eine regelmäßige Berichterstattung dazu aufgesetzt, sodass wir eigentlich einen fachlich guten, regelmäßigen Überblick über Compliance-relevante Sachverhalte haben.“ (Technologiewirtschaft, 5.000 bis 10.000 Mitarbeiter weltweit)

„Es ist nicht so, dass wir Richtlinien und Regeln nur ausgeben, sondern wir hinterfragen mit diesem System natürlich, wie das in Gesellschaften gelebt wird. Und ich glaube, der Kern ist eigentlich die Information und Kommunikation und letztendlich der Dialog.“ (Industrielle Produktion, mehr als 10.000 Mitarbeiter weltweit)

Einige Unternehmen sehen jedoch Herausforderungen in der Entwicklung von Benchmarks und Key Performance Indicators (KPIs) zur Messung der Wirksamkeit ihrer Compliance-Programme:

Benchmarks und KPIs

„Das grundsätzliche Problem ist, dass es keine vernünftigen Benchmarks für Compliance gibt. Solange Sie keine Kennzahlen haben und keine vernünftigen Kennzahlen entwickeln können, können die auch nichts aussagen über die Frage: Wie misst man Compliance?“ (Pharma und Gesundheitswesen, mehr als 10.000 Mitarbeiter weltweit)

„Wenn man sich eine externe Prüfung anguckt, dann kann die aussagekräftig sein; wenn man intern KPIs benutzt, können die auch sehr aussagekräftig sein – wenn man sie stringent verwendet und daraus auch Maßnahmen ableitet.“ (Handel und Konsum, mehr als 10.000 Mitarbeiter weltweit)

Unternehmen versuchen zunehmend, die Wirksamkeit ihres CMS anhand von Benchmarks und KPIs zu messen.

Erste Erfolge im Kampf gegen Kartellrechtsverstöße





Der Anteil der Unternehmen, die über einen Verdacht auf einen kartellrechtlichen Verstoß berichteten, sinkt auf 8 %.

Abnahme der Kartellrechtsverstöße

In dieser Studie finden sich die ersten Hinweise auf einen Rückgang wettbewerbsrechtlicher Verstöße. Gegenüber den vorangegangenen Studien sinkt der Anteil der Unternehmen, die über einen Verdacht auf einen kartellrechtlichen Verstoß berichteten, um drei bis fünf Prozentpunkte auf 8 %. Gleichzeitig halten es Unternehmen seltener für wahrscheinlich, ein Angebot zu einer wettbewerbswidrigen Absprache zu erhalten (4 %).

Wir führen diese sich abzeichnende positive Entwicklung auch auf die wachsende Zahl der kartellrechtlichen Compliance-Programme zurück, ihr Anteil stieg im gleichen Zeitraum um sieben Prozentpunkte auf 62 % (2013: 55 %; siehe Seite 24 f.).

Überdies dürfte die Kronzeugenregelung des Bundeskartellamts und auch der Europäischen Kommission einen abschreckenden Effekt besitzen. Die sogenannte Bonusregelung bietet mit dem vollständigen Erlass des Bußgelds einen sehr attraktiven Ausstieg aus einem Kartell an, sodass Kartellabsprachen instabiler geworden sind. Zeitlich nachfolgend gestellte Bonusanträge können die Geldbuße nur um maximal 50 % mindern.⁴⁰

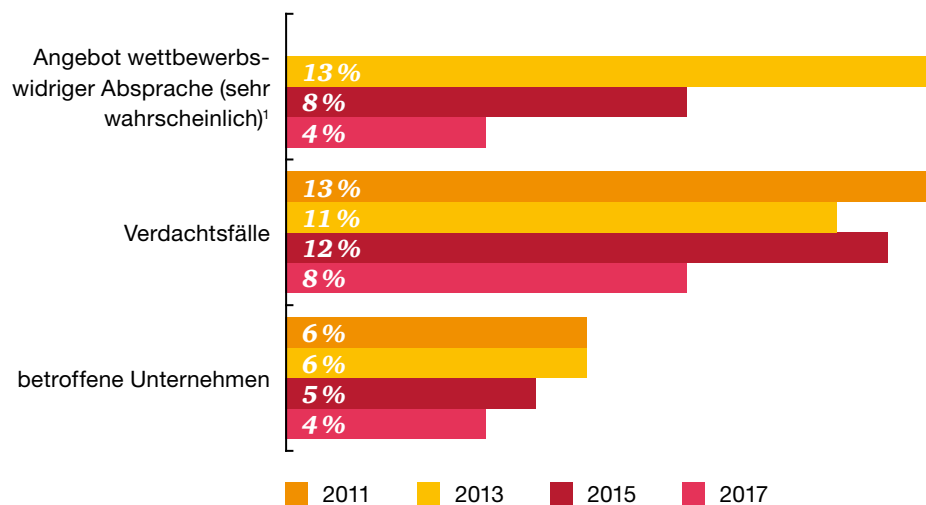
Seit ihrer Einführung im März 2006 hat sich die neue Bonusregelung als zentrales Ermittlungsinstrument bei der Aufdeckung von Kartellen bewiesen. Seit 2013 bewegt sich die Anzahl der Bonusanträge beim Bundeskartellamt auf konstant hohem Niveau.

Im Jahr 2013 wurden 66 gestellt, 2014 und 2015 waren es 72 bzw. 76 und schließlich im Jahr 2016 immerhin noch 59 Anträge.⁴¹ 2016 schloss das Bundeskartellamt vier Kartellverfahren ab. Zudem wurden 2016 insgesamt Bußgelder in Höhe von 124,5 Millionen Euro verhängt.⁴²

Die befragten Unternehmen gehen allerdings weiterhin von einem nahezu unveränderten Anteil wettbewerbswidriger Absprachen aus. So sank nach den Angaben der befragten Unternehmen der Umsatzanteil, der auf wettbewerbswidrigen Absprachen beruht, nur leicht um einen Prozentpunkt auf 8 %. Der am häufigsten genannte Umsatzanteil (Median) lag unverändert bei 5 %. Auch schätzten 27 % der Unternehmen den Anteil des Umsatzes, der auf wettbewerbswidrigen Absprachen basiert, auf über 29 %, deutlich mehr als noch 2015 (7 %).

Trotz einer sinkenden Zahl von Unternehmen, die in den letzten zwei Jahren von wettbewerbswidrigen Absprachen betroffen wurden (Abb. 26), gehen die befragten Unternehmen folglich von einem gleichbleibenden oder teilweise sogar höheren Anteil von Kartellrechtsverletzungen aus. Letzteres dürfte jedoch bei einem Teil der Unternehmen auf eine wachsende Awareness zurückzuführen sein, für einen tatsächlichen Anstieg im Dunkelfeld finden sich keine Belege; eher haben wir von einer rückläufigen Tendenz auszugehen.

Abb. 26 Entwicklung des Risikos wettbewerbswidriger Absprachen 2011–2017



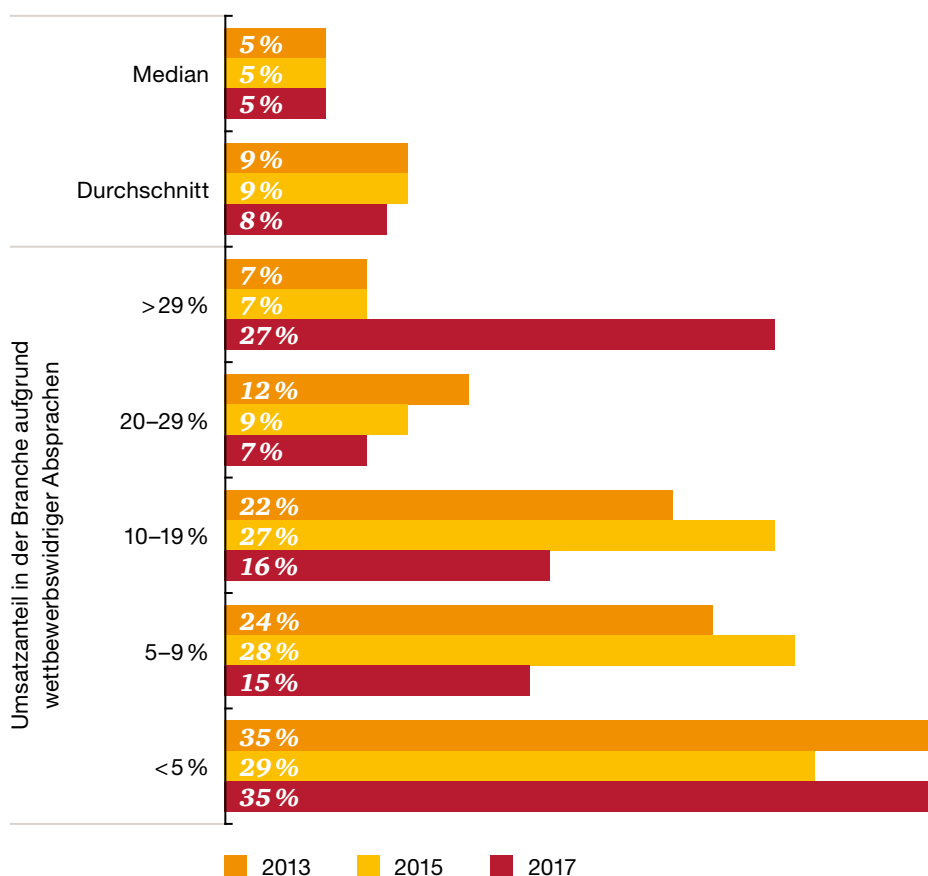
¹ Keine Daten für 2011.

⁴⁰ Vgl. Bundeskartellamt, Erfolgreiche Kartellverfolgung, S. 21, online abrufbar unter: www.bundeskartellamt.de/SharedDocs/Publikation/DE/Broschueren/Informationsbrosch%C3%BCre%20-%20Erfolgreiche%20Kartellverfolgung.pdf?__blob=publicationFile&v=12.

⁴¹ Vgl. Bundeskartellamt, Erfolgreiche Kartellverfolgung, S. 20 f., online abrufbar unter: www.bundeskartellamt.de/SharedDocs/Publikation/DE/Broschueren/Informationsbrosch%C3%BCre%20-%20Erfolgreiche%20Kartellverfolgung.pdf?__blob=publicationFile&v=12.

⁴² Auskunft des Bundeskartellamts, online abrufbar unter: www.bundeskartellamt.de/DE/Kartellverbot/kartellverbot_node.html.

Abb. 27 Durch wettbewerbswidrige Absprachen erzielter Umsatzanteil in der eigenen Branche 2013–2017

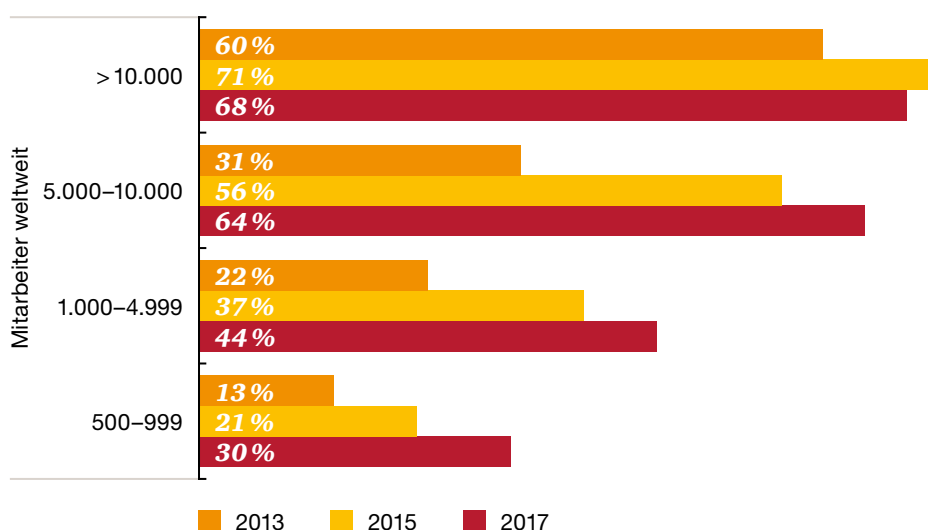


Kartellrechtliche Compliance zunehmend im Mittelstand

Insgesamt stieg der Anteil der Compliance-Programme, die auch kartellrechtliche Risiken berücksichtigen, auf 62 % (siehe Seite 24 f.). Bei Großunternehmen mit über 10.000 Mitarbeitern verharrt der Anteil auf dem Niveau von 2015.⁴³

Hingegen zeigt sich bei den Unternehmen mit 500 bis 10.000 Mitarbeitern eine eindrucksvolle Entwicklung. Rund zwei Drittel (64 %) der Unternehmen mit 5.000 bis 10.000 Mitarbeitern haben ein kartellrechtliches CMS implementiert. Stark aufgeholt haben auch Unternehmen mit 1.000 bis 4.999 bzw. 500 bis 999 Mitarbeitern, über eine Kartellrechts-Compliance verfügen 44 % bzw. 30 %. Gegenüber 2013 bedeutet dies einen Anstieg um 22 bzw. 17 Prozentpunkte. Compliance wird zunehmend unabhängig von der Unternehmensgröße, der Top-down-Prozess erreicht verstärkt auch mittelständische Unternehmen.

Abb. 28 Verbreitung kartellrechtlicher Compliance-Maßnahmen, nach Unternehmensgröße



Basis: alle befragten Unternehmen

⁴³ Bei Großunternehmen ist der leichte Rückgang um 3 % gegenüber 2015 aufgrund der zu geringen Fallzahl nicht interpretierbar.

Mehrwert von Compliance





Über ein Drittel (37 %) der betroffenen Unternehmen gab an, dass die Tatsache, dass sie über ein CMS verfügten, die Höhe der Geldbuße positiv beeinflusst habe. Bei 43 % der Unternehmen, die ein CMS implementiert hatten, beförderte dies die Einstellung des Verfahrens.

Compliance als Wettbewerbsvorteil

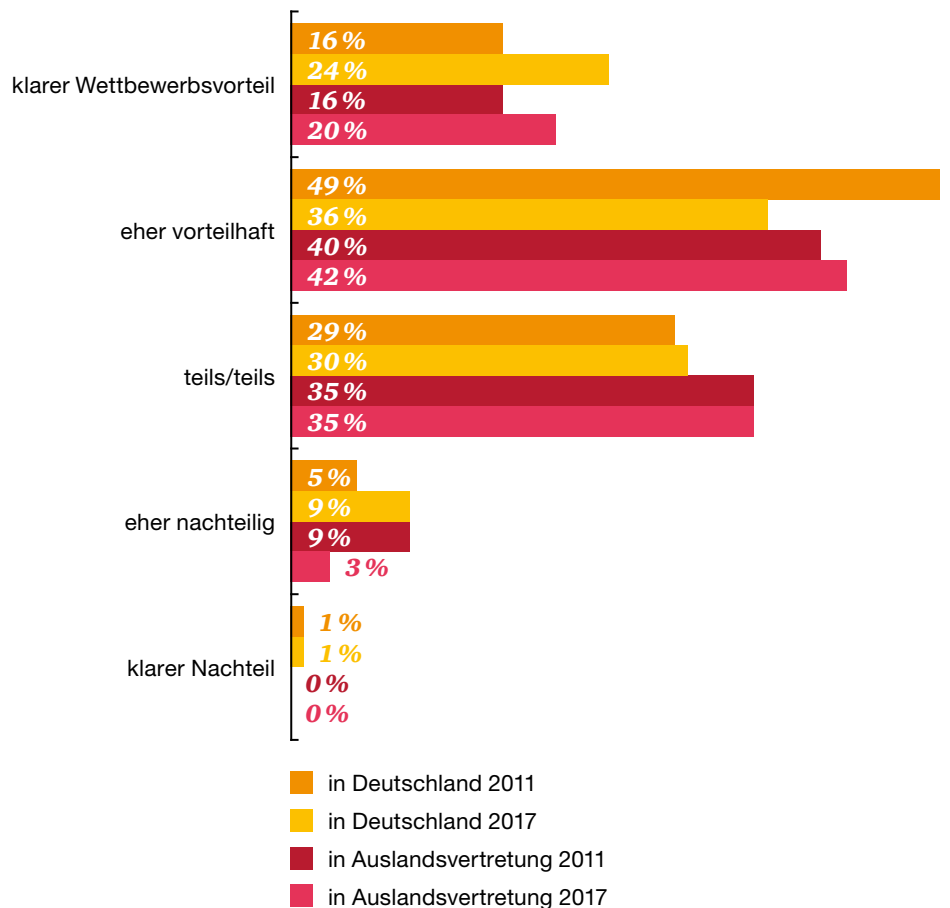
Die meisten Unternehmen verfügen nunmehr über mehrjährige Erfahrungen mit ihrem CMS und dessen Auswirkungen auf ihre Wettbewerbschancen. Das überwiegende Ergebnis ist positiv. Nur 9 % der befragten Unternehmen berichteten über Wettbewerbsnachteile im deutschen Markt, davon nur 1 % über einen klaren Wettbewerbsnachteil. Demgegenüber beurteilt über ein Drittel (36 %) das eigene Compliance-Programm im Wettbewerb überwiegend als vorteilhaft und ein Viertel (24 %) erkennt hierin sogar einen klaren Vorteil.

Im Vergleich zu den Einschätzungen vor sechs Jahren hat der Anteil der Unternehmen, die über klare Wettbewerbsvorteile im deutschen Markt berichteten (24 %), sogar um acht Prozentpunkte zugenommen (2011: 16 %).⁴⁴ Immer mehr Unternehmen scheint es zu gelingen, ihr CMS im Wettbewerb vorteilhaft zu vermarkten. Allerdings hat sich auch die Gruppe der Skeptiker etwas vergrößert, und zwar um vier Prozentpunkte auf nunmehr 9 %.

Bemerkenswert ist, dass die befragten Unternehmen auch in ihren Auslandsvertretungen über überwiegend gute Erfahrungen berichteten, wenn auch in etwas geringerem Maße. 20 % sehen in ihrem CMS auf ausländischen Märkten klare und 42 % überwiegende Wettbewerbsvorteile. Das ist für eine Wirtschaft, die im besonderen Maße vom Export abhängt und international erfolgreich operiert, ein wichtiges Ergebnis. Auch internationale Märkte belohnen zunehmend Compliance.

Abb. 29 Compliance im Wettbewerb

Anteil der befragten Unternehmen



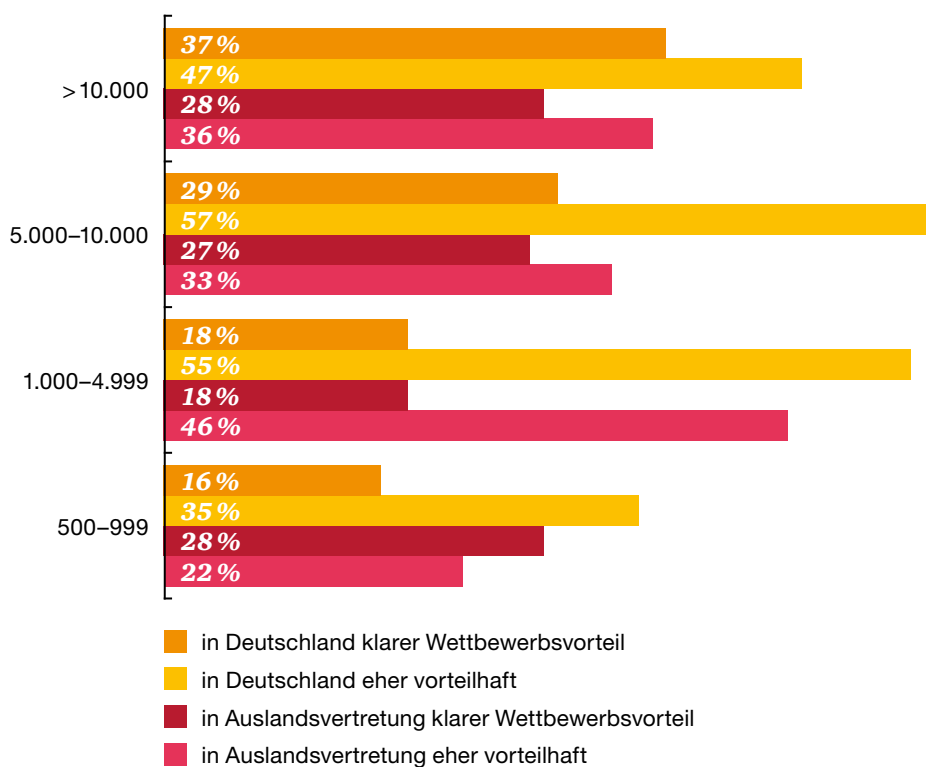
Über **ein Drittel** (36 %) der Unternehmen beurteilen das eigene Compliance-Programm im Wettbewerb überwiegend als vorteilhaft und ein Viertel (24 %) erkennt hierin sogar einen klaren Vorteil.

⁴⁴ Vgl. PwC, Wirtschaftskriminalität 2011, S. 48.

Es überrascht allerdings nicht, dass es größeren Unternehmen leichterfällt, mit einem CMS erfolgreich im Wettbewerb zu operieren. 37% der Großunternehmen mit mehr als 10.000 Mitarbeitern berichteten über klare Wettbewerbsvorteile, während diese positive Erfahrung mit sinkender Unternehmensgröße kontinuierlich abnimmt, vermutlich aufgrund ihrer geringeren Marktmacht. Die Vorteile überwiegen jedoch weiterhin. So berichteten nur 18% der Unternehmen mit 1.000 bis 4.999 Mitarbeitern über klare und 55% über leichte Wettbewerbsvorteile.

Am schwersten fällt es Unternehmen mit 500 bis 999 Mitarbeitern, ihr CMS als Wettbewerbsvorteil zu nutzen. 16% von ihnen berichteten über klare und 35% über eher vorteilhafte Auswirkungen. Dies bedeutet aber auch, dass zusammengekommen die Hälfte dieser kleineren Unternehmen ihr CMS eher als Wettbewerbsvorteil wahrnimmt, während 44% andere Erfahrungen gemacht haben und nur 5% ihr CMS als leichten Wettbewerbsnachteil einstufen.⁴⁵

Abb. 30 Compliance im Wettbewerb, nach Unternehmensgrößen



⁴⁵ Negative Ausprägungen sind in der Abbildung nicht enthalten.

Ein CMS bringt nicht nur Vorteile im Wettbewerb mit sich, sondern kann sich auch positiv auf Verfahren gegen das Unternehmen nach § 130 OWiG auswirken.

Bonus für CMS in Verfahren nach § 130 OWiG

Ein Verfahren nach § 130 Abs. 1 OWiG kommt in Betracht, wenn einem Unternehmensmitarbeiter eine betriebsbezogene Straftat nachgewiesen werden kann und diese durch Ausübung der gehörigen Aufsicht verhindert oder wesentlich erschwert worden wäre. Die Entscheidungen in den Verfahren nach dem Ordnungswidrigkeitenrecht werden anders als diejenigen nach dem allgemeinen Strafgesetzbuch (StGB) kaum publiziert, sodass weitgehend Unklarheit über die Auswirkungen eines CMS auf den Ausgang des Verfahrens besteht.⁴⁶

Das Gesetz nennt zwar in § 130 Abs. 1 Satz 2 OWiG die Bestellung, sorgfältige Auswahl und Überwachung von Aufsichtspersonen als erforderliche Aufsichtsmaßnahmen, lässt aber eine ausdrückliche Berücksichtigung von Compliance-Programmen auf der Rechtsfolgende offen.⁴⁷ Zwar hat die höchstrichterliche Rechtsprechung jüngst entschieden, dass Compliance-Maßnahmen bei der Strafzumessung des Verbands nach § 30 OWiG berücksichtigt werden können, jedoch ohne Leitlinien für solche Compliance-Maßnahmen zu formulieren.⁴⁸

In unseren vertieften Interviews wurde daher teilweise die Ansicht vertreten, dass anders als bei US-Behörden „das [CMS in Deutschland] nicht strafmildernd berücksichtigt wird, weil das als selbstverständlich vorausgesetzt wird“ (Automobilindustrie, mehr als 10.000 Mitarbeiter weltweit).

Wir sind in unserer Studie der Frage nachgegangen, wie betroffene Unternehmen die gegenwärtige Justizpraxis einschätzen. Von Ermittlungen in Zusammenhang mit einem Wirtschaftsdelikt nach § 130 OWiG berichteten 21 Unternehmen. Über ein Drittel (37%) der betroffenen Unternehmen gab an, dass ihr CMS die Höhe der Geldbuße positiv beeinflusst hat. Auch beförderte bei 43% der Unternehmen das Vorhandensein eines CMS die Einstellung des Verfahrens. Die oben wiedergegebene skeptische Einschätzung lässt sich daher nicht verallgemeinern.

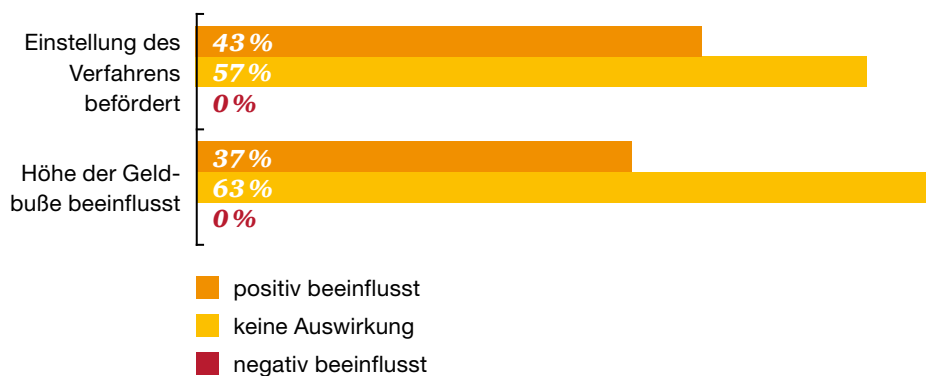
⁴⁶ Vgl. Bussmann/Matschke, Die Zukunft der unternehmerischen Haftung bei Compliance-Verstößen, in: CCZ 2/2009, S. 132–138.

⁴⁷ Vgl. für eine Berücksichtigung von CMS in der Literatur: Rübenstahl/Skoupil, Anforderungen der US-Behörden an Compliance-Programme nach dem FCPA und deren Auswirkungen auf die Strafverfolgung von Unternehmen – Modell für Deutschland, in: wistra 6/2013, S. 209–216; van Vormizeele, Kartellrechtliche Compliance-Programme im Rahmen der Bußgeldbemessung de lege lata und de lege ferenda, in: CCZ 2/2009, S. 41–48; Rosinus, Haftungsvermeidung und -minimierung bei Aufsichtspflichtverletzung und Verbandsgeldbuße durch Compliance in der Praxis, 2016, S. 127.

⁴⁸ Vgl. BGH, Urteil vom 09.05.2017 – 1 StR 265/16.

Abb. 31 Auswirkungen von CMS auf das Ergebnis in Verfahren nach § 130 OWiG

Beurteilung der Unternehmen



Basis: alle befragten Unternehmen

Des Weiteren wurde die nachträgliche Zusage, ein CMS einzuführen bzw. Verbesserungen vorzunehmen, bei einem Teil der betroffenen Unternehmen als positives Nachtatverhalten bewertet. Dies hat sich bei jedem dritten Unternehmen auf die Höhe der Geldbuße positiv ausgewirkt und beförderte bei fast jedem zweiten die Einstellung des Verfahrens.

In unseren zusätzlich durchgeführten vertieften Interviews nannten einige Unternehmen die Gründe für die positiven Auswirkungen ihres CMS auf ihr Verfahren:

„[...] positives Feedback der Staatsanwaltschaft, weil sie einen professionellen Ansprechpartner haben [...].“ (Pharma und Gesundheitswesen, mehr als 10.000 Mitarbeiter weltweit)

„Weil wir es frühzeitig erkannt und zur Aufdeckung intensiv beigetragen haben. Wir haben solche Dinge sofort untersucht und durch Gegenmaßnahmen sofort abgestellt.“

(Maschinenbau und Metallindustrie, 1.000 bis 4.999 Mitarbeiter weltweit)

„[...] dass das Compliance-System auch in den Fällen, wo es letztlich zu Sanktionen gekommen ist, positive Auswirkungen hatte, zumindest in der Aufarbeitung des Vorfalls und vielleicht auch als Beitrag dafür, dass nicht alles noch viel schlimmer war.“ (Handel und Konsum, mehr als 10.000 Mitarbeiter weltweit)

Forensische Praxis betroffener Unternehmen





Die Aufklärung bzw. Aufdeckung etwaiger Straftaten durch interne oder hiermit beauftragte externe Spezialisten ist für eine große Mehrheit der Unternehmen selbstverständlich (85 %).

Tätermerkmale – Risiko OK

Es handelt sich mittlerweile um Basiswissen unserer wirtschaftskriminologischen Studien: Rund die Hälfte der Wirtschaftsstraftaten gegen Unternehmen begehen Täter aus dem eigenen Unternehmen. 46% der Fälle wurden von internen Tätern begangen und bei 12% handelten die internen Täter zusammen mit externen.

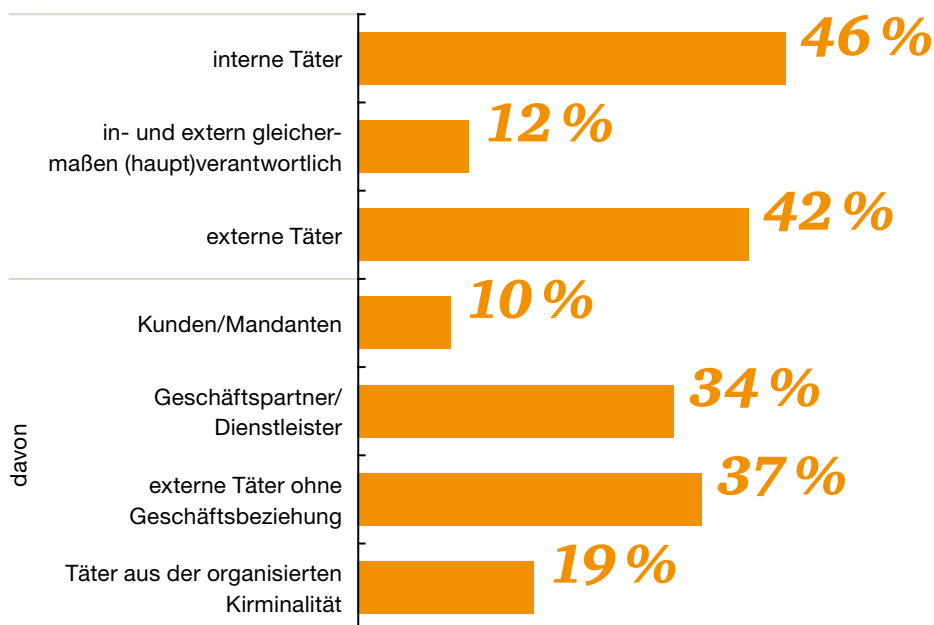
Auch die externen Täter waren den betroffenen Unternehmen vielfach bekannt. Rund ein Drittel (34%) der Wirtschaftsdelikte begingen Geschäftspartner und Dienstleister und weitere 10% wurden von Kunden verübt. Hoch ist weiterhin der Anteil der Täter, die vermutlich aus dem Kreis der OK stammen. Bei etwa jeder fünften Wirtschaftsstraftat (19%) gehen die betroffenen Unternehmen hiervon aus.

Wirtschaftsdelikte, die von außen begangen werden, sind in jedem zweiten Fall (49%) von einem Täter auf der Führungsebene des schädigenden Unternehmens zu verantworten. Dies überrascht nicht.

Beunruhigend ist, dass es sich in jedem vierten Fall (25%), der von internen Tätern begangen wurde, beim Haupttäter um eine Person aus der obersten Führungsebene handelte; das ist gemessen am geringen Anteil der obersten Führungskräfte an der gesamten Mitarbeiterschaft ein überdurchschnittlicher Wert. Je höher die Position, desto leichter und attraktiver sind die Möglichkeiten, eine Wirtschaftsstraftat zu begehen. Empirisch gesehen sind folglich besondere Vorsicht und Sorgfalt bei der Auswahl und Überwachung von Personen in Führungs- und Vertrauenspositionen geboten, wie auch unsere früheren Studien belegen.⁴⁹

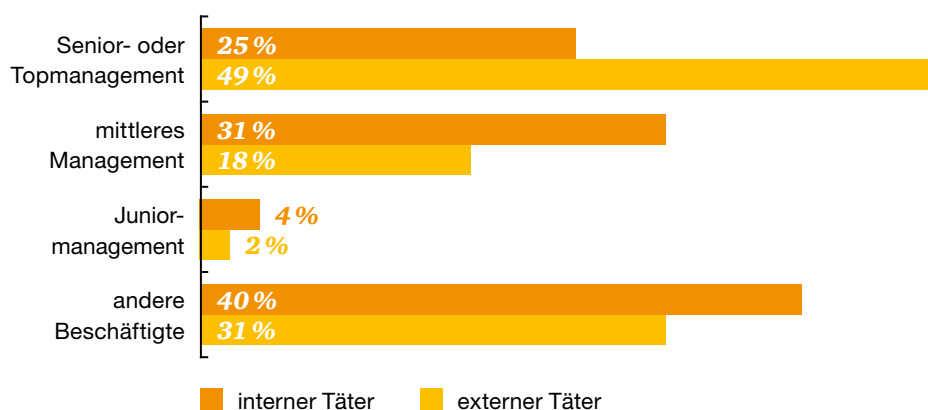
Abb. 32 Beziehung der Täter zum geschädigten Unternehmen

Mehrfachnennungen innerhalb externer Tätergruppen möglich.



Basis: Anteil an den berichteten Fällen mit internen und externen Tätern

Abb. 33 Position des internen/externen Haupttäters



⁴⁹ Vgl. PwC, Wirtschaftskriminalität und Unternehmenskultur, 2013, S. 82.

Praxis interner Untersuchungen

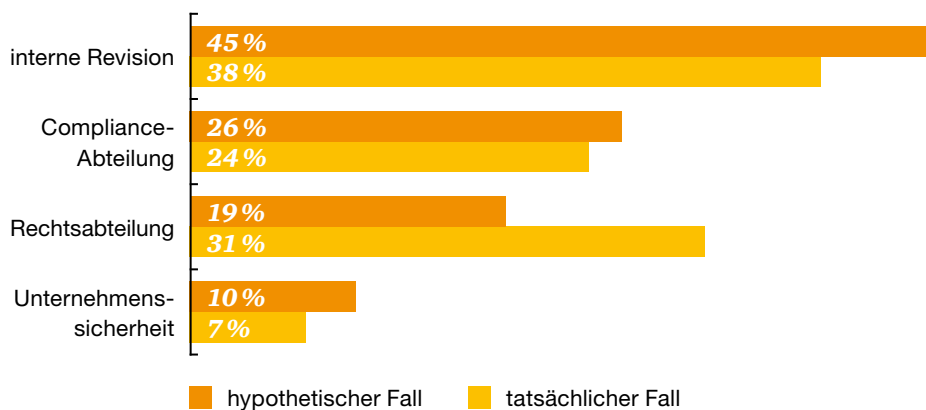
Für die Mehrheit der Unternehmen ist es im Falle eines Compliance-Verstoßes selbstverständlich, sich um Aufklärung zu bemühen und hiermit entweder interne oder externe Spezialisten zu beauftragen. 85 % der Unternehmen, die in unserer Studie über ein gravierendes Wirtschaftsdelikt berichteten, leiteten eigene interne Untersuchungen ein.⁵⁰ In der Gruppe der nicht betroffenen Unternehmen würden ebenfalls 86 % entsprechende Ermittlungen aufnehmen (ohne Abbildung).

Die Untersuchungen wurden zu 38 % von der Internen Revision und nahezu ebenso häufig von der Rechtsabteilung geleitet (31 %). Der Schwerpunkt der Compliance-Abteilung liegt typischerweise eher auf dem

Aspekt der Prävention, sodass nur in rund einem Viertel der Fälle (24 %) die internen Ermittlungen von der Compliance-Abteilung geleitet wurden.

Auch unsere hypothetische Frage an die Gruppe der nicht betroffenen Unternehmen ergab keine nennenswert größere Bedeutung der Compliance-Abteilung (26 %). Allerdings meinten die nicht betroffenen Unternehmen, sie würden eher der Internen Revision (45 %) die Leitung der internen Untersuchungen übertragen und seltener der Rechtsabteilung (19 %). Vermutlich bedarf es in der forensischen Praxis häufiger der Prüfung rechtlicher Fragen, sodass die tatsächliche forensische Bedeutung der Rechtsabteilung eher unterschätzt wird.

Abb. 34 Leitung der internen Untersuchungen



85 % der Unternehmen, die in unserer Studie über ein gravierendes Wirtschaftsdelikt berichteten, leiteten eigene interne Untersuchungen ein.

⁵⁰ 59 % der Unternehmen berichteten über einen gravierenden Fall in den letzten Jahren (n=212).

Gründe interner Untersuchungen

Die Einleitung interner Untersuchungen kann verschiedene Gründe haben. Im Vergleich zwischen den Gründen in einem tatsächlichen Fall und den von den befragten Unternehmen genannten hypothetischen Gründen zeigen sich gravierende Unterschiede. In der Realität erfolgen interne Untersuchungen sehr viel häufiger als angenommen auch zur Vorbereitung arbeitsrechtlicher Maßnahmen (54 %) und eines strafrechtlichen Verfahrens (64 %), wobei gegenüber internen Tätern diese Gründe noch häufiger eine Rolle gespielt haben (Abb. 36). Hypothetisch gefragt, geben nur 6 % bzw. 10 % an, aus diesen Gründen interne Untersuchungen einzuleiten. Offenbar rückt in den tatsächlichen Fällen der Aspekt der Sanktionierung des Täters in den Vordergrund.

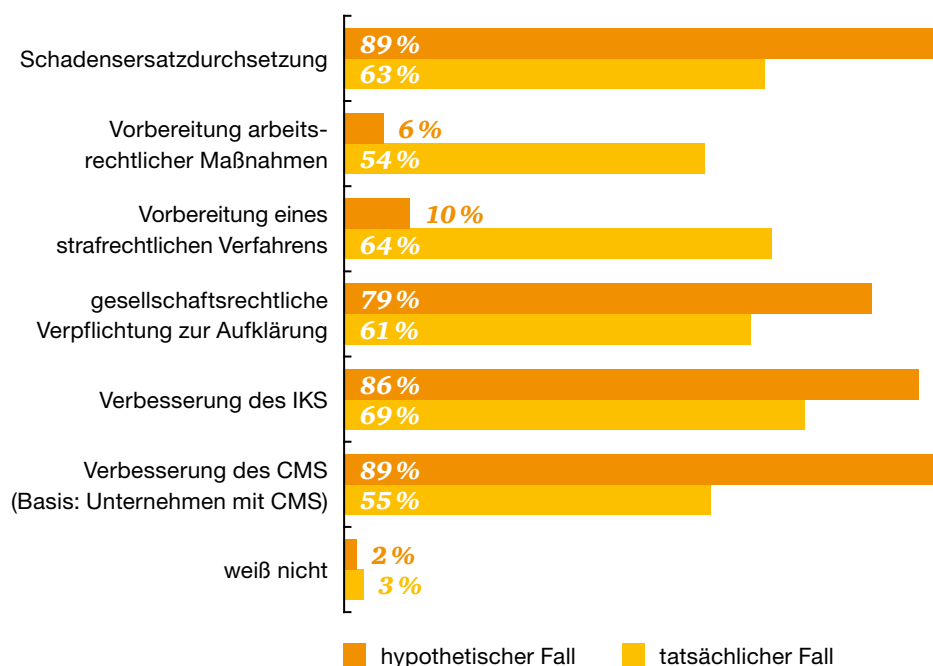
Unsere Studie zeigt die Vielfalt der Gründe, aus denen tatsächlich in der forensischen Praxis der betroffenen Unternehmen interne Untersuchungen erfolgten. In knapp zwei Dritteln der Fälle sollten sie der Durchsetzung von Schadensersatzansprüchen (63 %) und der Verbesserung des IKS (69 %) dienen, etwas seltener der Optimierung des CMS (55 %). Immerhin sehen fast zwei Drittel der Compliance-Programme spezielle Case Reports zur Evaluation des CMS vor (61 %; Seite 46 f.).

Auch spielten in knapp zwei Dritteln der Fälle gesellschaftsrechtliche Verpflichtungen eine Rolle (61 %). Mehrheitlich wird für den Vorstand einer Aktiengesellschaft aus §§ 76 Abs. 1, 93 Abs. 1 AktG eine Pflicht zu internen Untersuchungen angenommen, wenn ein Verdacht auf Gesetzesverstöße besteht.⁵¹ Das Gleiche gilt für die Geschäftsführung einer GmbH, das heißt, die Geschäftsführer müssen gemäß § 43 Abs. 1 GmbHG bei Verdacht auf einen Gesetzesverstoß Untersuchungen zur Aufklärung des Sachverhalts durchführen.

Unternehmen, die nur für den hypothetischen Fall antworteten, verbinden im Vergleich zur Gruppe der tatsächlich Betroffenen die Aufnahme interner Ermittlungen mit deutlich anders gewichteten Erwartungen. 79 % gaben an, sie würden zur Durchsetzung von Schadensersatzansprüchen (89 %), wegen gesellschaftsrechtlicher Verpflichtungen und zur Verbesserung des IKS (86 %) und des CMS (89 %) interne Untersuchungen einleiten. Offenbar sieht die Realität viel nüchterner aus.

Abb. 35 Gründe interner Ermittlungen

Mehrfachnennungen waren möglich.



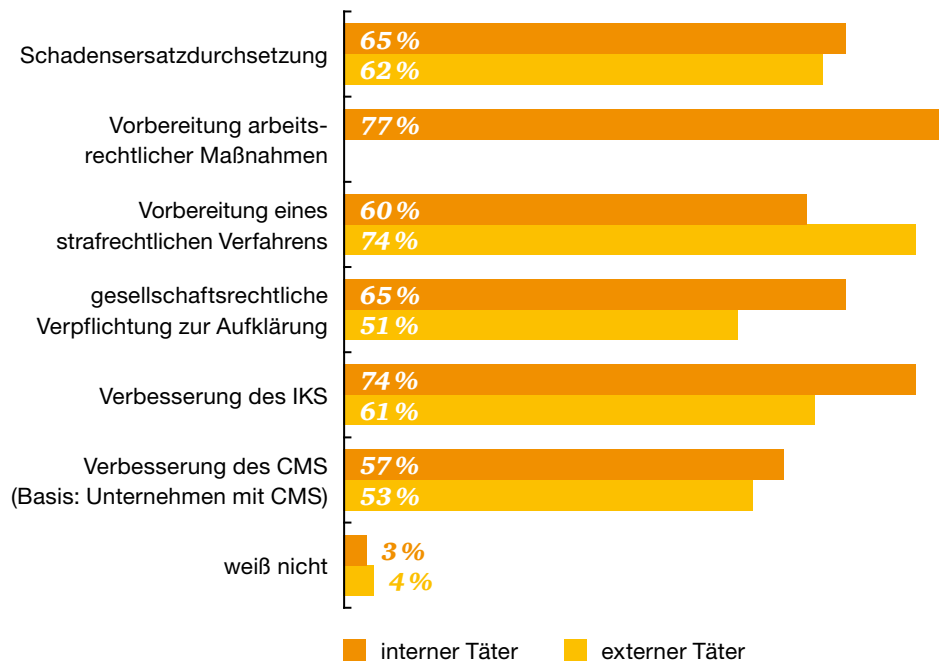
⁵¹ Vgl. Potinecke/Gottschalk, Die Rolle des Aufsichtsrates bei der betrieblichen Aufklärung von Compliance-Verstößen, in: CB 12/2015, S. 444–448; Arnold, Verantwortung und Zusammenwirken des Vorstandes und Aufsichtsrates bei Compliance-Untersuchungen, in: ZGR 1/2014, S. 76–106.

Differenzieren wir bei den genannten gravierenden Wirtschaftsdelikten zwischen internen und externen Tätern, so stellt sich heraus, dass interne Untersuchungen in beiden Fällen gleichermaßen der Durchsetzung von Schadensersatzansprüchen dienen (65 % versus 62 %). Hingegen erfolgen sie bei internen Tätern seltener zur Vorbereitung eines strafrechtlichen Verfahrens (60 %; externe Täter: 74 %), aber in über drei Vierteln der Fälle zur Vorbereitung arbeitsrechtlicher Schritte (77 %).

Eigene Ermittlungen werden bei internen Tätern auch häufiger mit der Verbesserung des IKS (74 %; externe Täter: 61 %) und des CMS begründet (57 %; externe Täter: 53 %). Ebenfalls häufiger erfolgen bei internen Tätern interne Untersuchungen aufgrund gesellschaftsrechtlicher Verpflichtungen (65 %; externe Täter 51 %).

Abb. 36 Gründe interner Ermittlungen – Vergleich interne versus externe Täter

Mehrfachnennungen waren möglich.

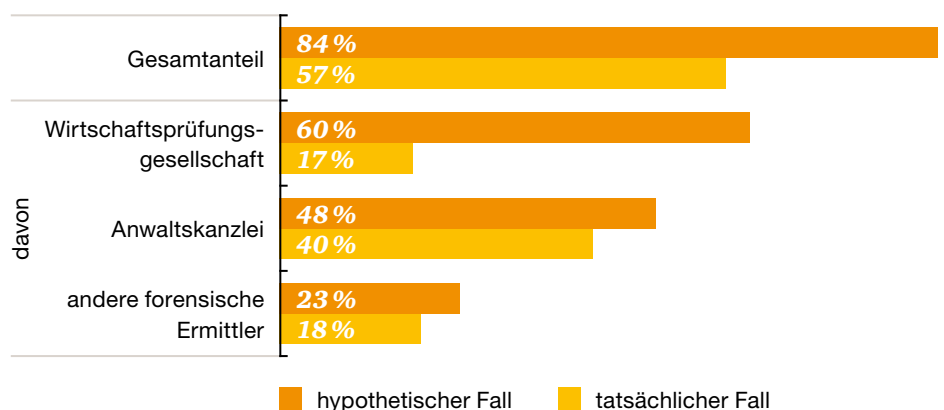


Bedeutung externer Ermittler in der Praxis

Die Mehrheit der befragten Unternehmen gab an, dass sie ihre Untersuchungen auch mit Unterstützung externer Ermittler durchführen würden (die Gruppe der nicht betroffenen Unternehmen sogar zu 84 %). Tatsächlich wurden nur in 57 % der Fälle zusätzlich externe Ermittler mit den Untersuchungen beauftragt. Am häufigsten handelte es sich um Anwaltskanzleien (40 %). Die forensische Expertise von Wirtschaftsprüfungsgesellschaften (17 %) und anderen privaten Ermittlern (18 %) wurde deutlich seltener in Anspruch genommen. Allerdings meinten fast zwei Drittel der Unternehmen, die nur hypothetisch gefragt werden konnten, dass sie die forensischen Dienste einer Wirtschaftsprüfungsgesellschaft bevorzugen würden (60 %).

Abb. 37 Tatsächliche oder hypothetische Beauftragung externer Ermittler

Mehrfachnennungen waren möglich.



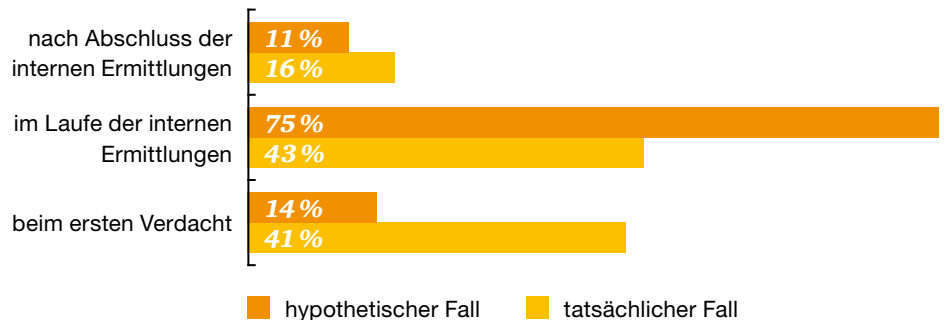
Phase der Beauftragung externer Ermittler

Es empfiehlt sich, möglichst bereits beim ersten Verdacht externe Ermittler zu beauftragen. Hingegen meinten drei Viertel der hypothetisch befragten Unternehmen, dass sie erst im Laufe der internen Ermittlungen externe Spezialisten hinzuziehen würden (75%). Die Praxis zeigt jedoch, dass tatsächlich häufiger bereits beim ersten Verdacht externe Ermittler beauftragt wurden (41 %) und im Laufe der internen Ermittlungen nur 43 % der Unternehmen diesen Schritt vollzogen. Wir führen die häufige

frühe Beauftragung externer Ermittler auf die sachliche und rechtliche Komplexität vieler Fälle zurück, die sich bereits in der sehr frühen Phase (beim ersten Verdacht) zeigt. So erfolgte

die Beauftragung externer Ermittler aus Sicht von 84 % der betroffenen Unternehmen vor allem aufgrund der erforderlichen zusätzlichen Qualifikation (siehe Abb. 39).

Abb. 38 Phase der Beauftragung externer Ermittler



Gründe für die Beauftragung externer Ermittler

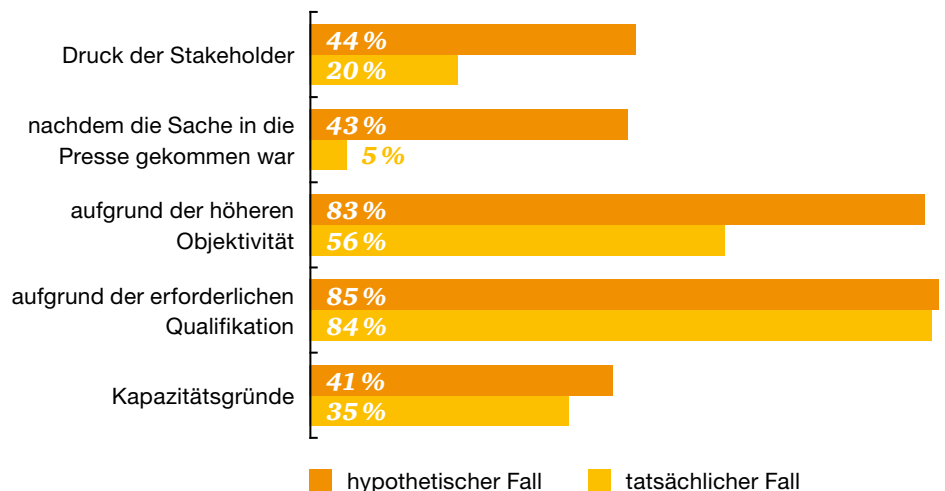
Externe Ermittlungskompetenz wird überwiegend aufgrund der erforderlichen Qualifikation hinzugezogen (84 %). Die höhere Objektivität spielt hingegen eine geringere Rolle als vielfach angenommen (83 %), nur in etwa jedem zweiten Fall war dies tatsächlich ein Grund (56 %). In jedem dritten Fall waren Kapazitätsgründe von Bedeutung (35 %). Dem Druck der Stakeholder kommt in der forensischen Praxis ein geringeres Gewicht zu (20 %) als vermutet (44 %).

Eine relativ große Relevanz wird der Presse zugemessen (43 %), aber in der Realität wurde in der Presse vermutlich über die wenigsten Fälle berichtet, sodass diese kaum als Grund für die

Beauftragung externer Ermittler genannt wurde (5 %). Insbesondere im Falle einer skandalisierenden Presseberichterstattung empfiehlt sich die Beauftragung externer Ermittler.

Abb. 39 Gründe für die Beauftragung externer Ermittler

Mehrfachnennungen waren möglich.



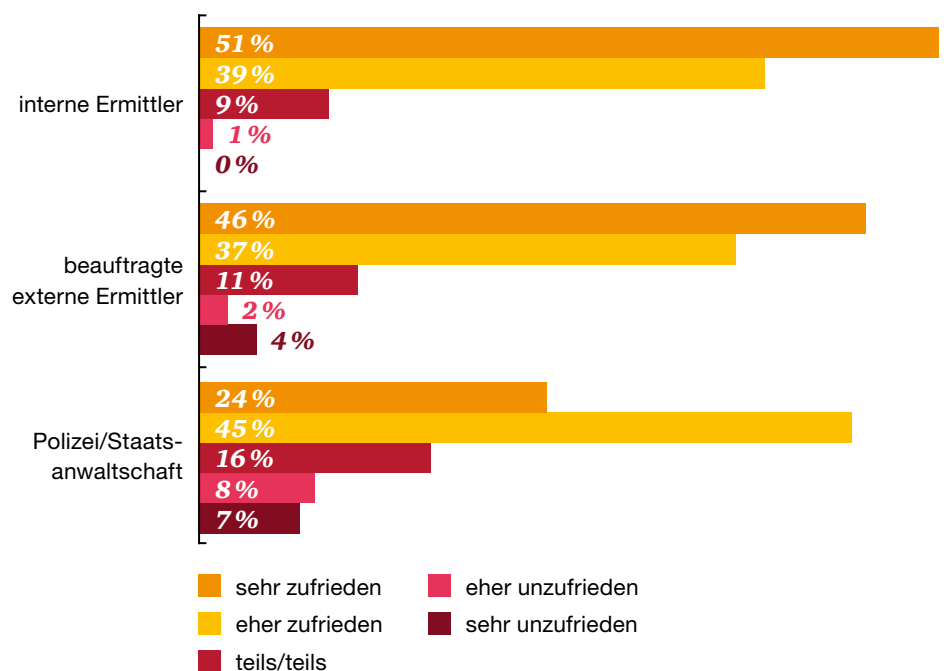
Nur jedes vierte Unternehmen beurteilte die Arbeit der behördlichen Ermittler als sehr zufriedenstellend (24 %). Deutlich weniger (schlechter) als bei internen oder externen Ermittlern.

Zufriedenheit mit der Arbeit externer und staatlicher Ermittler

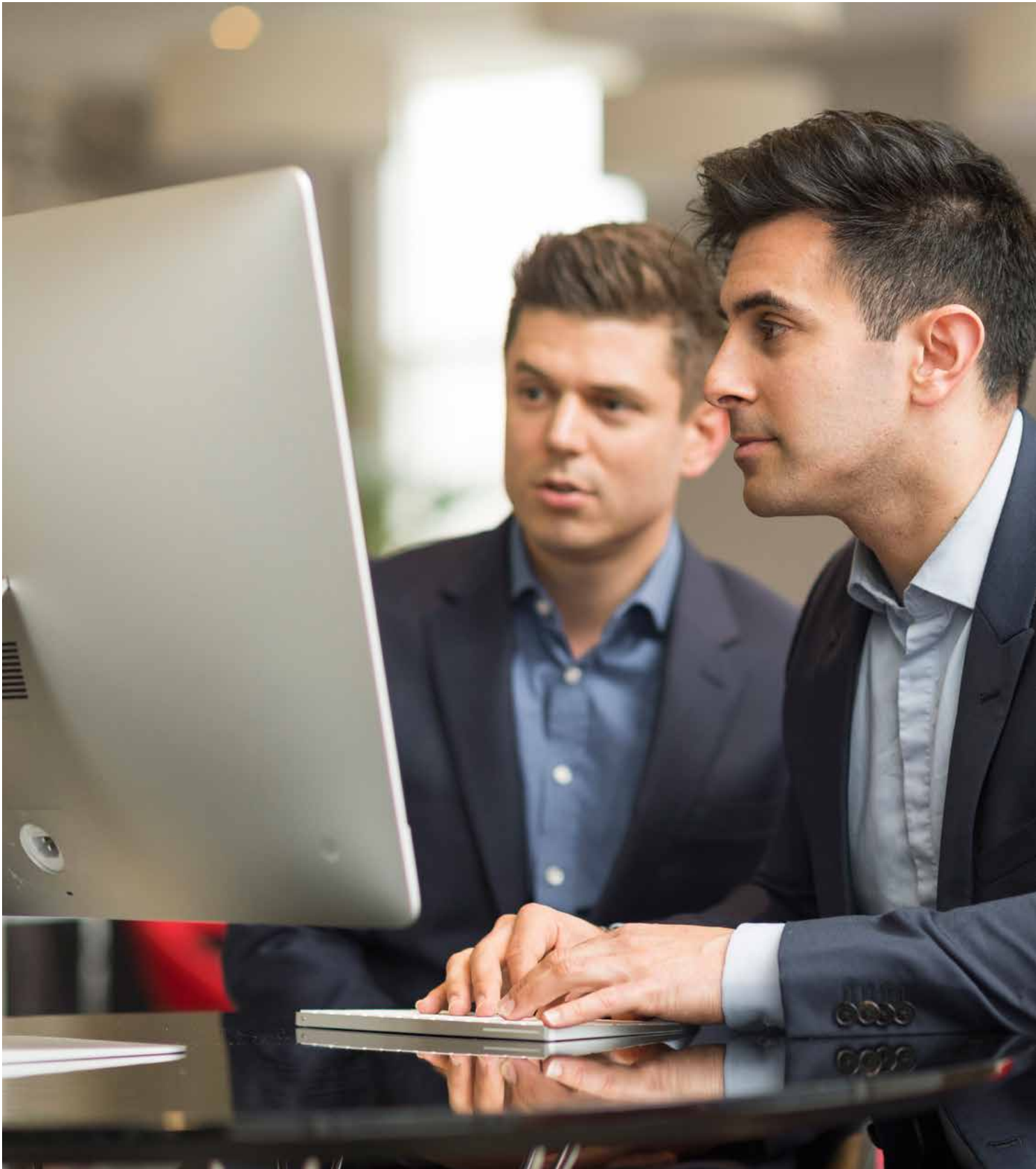
In unserem Vergleich zeigt sich, dass Unternehmen, soweit sie externe Ermittler hinzugezogen haben, mit nur geringen Abstrichen mit der Arbeit der Externen genauso zufrieden waren wie mit der hauseigenen Aufklärungsarbeit. Mit der internen Untersuchung waren 51 % der befragten Unternehmen sehr zufrieden, mit der Arbeit der externen Ermittler 46 %.

Deutlich kritischer wurde jedoch die Ermittlungstätigkeit der Strafverfolgungsbehörden gesehen. Nur jedes vierte Unternehmen beurteilte die Arbeit der behördlichen Ermittler als sehr zufriedenstellend (24 %). Eher ambivalent („teils/teils“) wurde ihre Arbeit von 16 % der Unternehmen bewertet und 15 % waren (sehr) unzufrieden. Im Vergleich hierzu wurden die forensischen Dienste der beauftragten externen Ermittler allein von 11 % als gemischt beurteilt („teils/teils“) und nur 6 % waren (sehr) unzufrieden.

Abb. 40 Zufriedenheit mit der Arbeit der Ermittler



Sanktionspraxis bei Compliance-Verstößen





Die Sanktionspraxis vieler Unternehmen ist in den vergangenen Jahren konsequenter geworden.

In aller Regel erfolgt bei gravierenden Compliance-Verstößen eine Kündigung (87 %) und deutlich häufiger als vor sechs Jahren wurden zivilrechtliche Schritte eingeleitet (65 %) und eine Strafanzeige erstattet (65 %).

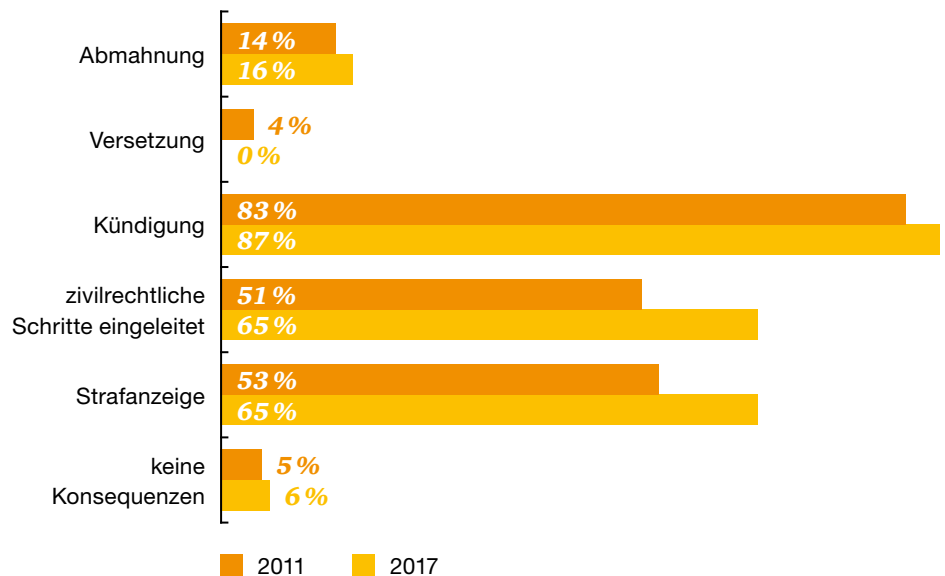
Folgen für interne Täter

Jedes Compliance-Management hat aus den Elementen Prevention, Detection und Response zu bestehen. Um die Glaubwürdigkeit der Compliance-Regeln zu gewährleisten, bedarf es immer einer Reaktion, auch um an der Geltung der betroffenen Compliance-Regel keinen Zweifel zu lassen.

Gemäß den Angaben der von uns befragten Unternehmen erfolgt in aller Regel bei gravierenden Compliance-Verstößen eine Kündigung (87%). Diese wird heute kaum häufiger als vor sechs Jahren ausgesprochen, wie unser Vergleich zeigt (83%). Allerdings werden heute deutlich häufiger als vor sechs Jahren zivilrechtliche Schritte eingeleitet (65%; 2011: 51%) und eine Strafanzeige gestellt (65%; 2011: 53%). Compliance-Verstöße werden somit konsequenter geahndet, sowohl zivilrechtlich als auch strafrechtlich.

Abb. 41 Konsequenzen gegenüber internen Haupttätern 2011–2017

Mehrfachnennungen waren möglich.



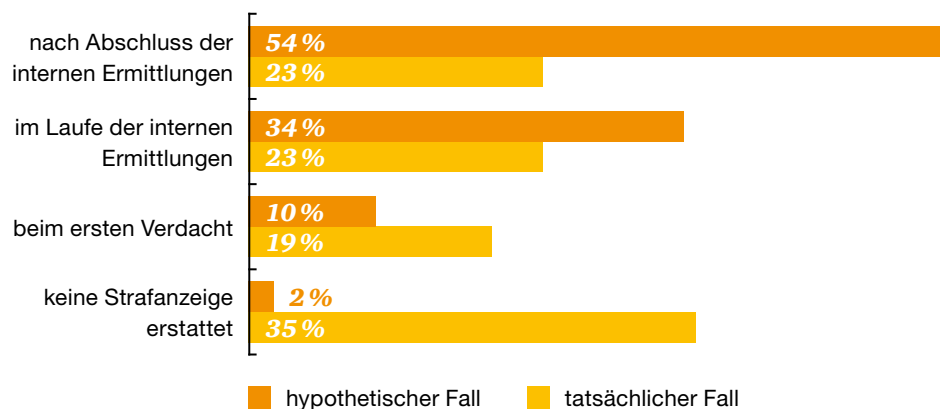
Praxis der Strafanzeige

Die Erfahrungen der betroffenen Unternehmen mit der Ermittlungstätigkeit von Polizei und Staatsanwaltschaft fallen gemischer aus als die Erfahrungen mit internen Untersuchungen (siehe Seite 64). Hierdurch erklärt sich vermutlich auch, dass in der forensischen Praxis jedes dritte (35%) Unternehmen keine Strafanzeige erstattet hat und nur in jedem fünften Fall (19%) bereits beim ersten Verdacht. Fast die Hälfte der Unternehmen erstattete Strafanzeige erst nach Abschluss (23%) oder im Laufe der internen Ermittlungen (23%).

Im Vergleich hierzu ist die Bereitschaft zur Strafanzeige bei Unternehmen, die diese Frage hypothetisch beantwortet haben, deutlich höher: 98% würden eine Strafanzeige erstatten. In der forensischen Praxis reagieren die

betroffenen Unternehmen somit sehr viel zurückhaltender. Allerdings würde jedes zweite Unternehmen vor der Erstattung einer Anzeige erst den Abschluss der internen Ermittlungen abwarten (54%).

Abb. 42 Strafanzeige in welcher Phase der internen Ermittlungen



Pro und Kontra einer Strafanzeige

Die meisten Unternehmen erstatten eine Strafanzeige nicht beim ersten Verdacht, sondern erst im Laufe oder nach Abschluss des Verfahrens. Die Gründe hierfür sind vielfältig. Am häufigsten äußerten die betroffenen Unternehmen, dass sie sich von der eigenen internen Untersuchung eine schnellere Aufklärung versprechen (64%) und Unruhe im Unternehmen vermeiden wollen (55%). Eher nachrangig sind andere Gründe wie der Verlust der Kontrolle über die eigene Ermittlungstätigkeit (32%) und die Sorge vor Publizitätsrisiken (36%).

Grundsätzliche Zweifel an der fachlichen Kompetenz der staatlichen Ermittlungsbehörden nannten nur 8% der betroffenen Unternehmen als Grund für eine erst nachgeordnet erfolgte Strafanzeige. Auch äußerten nur wenige Unternehmen ein geringes gegenseitiges Vertrauen (14%). Allerdings lag für über ein Viertel (29%) der Unternehmen ein Grund in der geringen Kenntnis der Polizei und Staatsanwaltschaft über betriebswirtschaftliche Abläufe. Es fehlt den Ermittlungsbehörden somit aus Sicht einiger Unternehmen durchaus am betriebswirtschaftlichen Fachwissen, sodass diese nicht beim ersten Verdacht eine Strafanzeige erstatten.

Der Verzicht auf eine Strafanzeige wurde ebenfalls kaum mit unzureichenden fachlichen Kompetenzen der staatlichen Ermittler (2%) oder zu geringen betriebswirtschaftlichen Kompetenzen begründet (4%). Es fehlt auch nur sehr selten am gegenseitigen Vertrauen (5%). Die Sorge vor einem Gegenschlag des Beschuldigten kann durchaus ein Grund für das Unterlassen einer Strafanzeige sein, allerdings nur selten (8%). Auch ein Verlust der Kontrolle über die eigene Ermittlungstätigkeit wurde selten angeführt (15%).

Hingegen wurden als Gründe, die gegen eine Strafanzeige sprachen, am häufigsten genannt: eine schnellere Aufklärung im Rahmen einer internen Untersuchung durch eigene bzw. externe Ermittler (37%), Publizitätsrisiken aufgrund mangelnder Vertraulichkeit (32%) und die Vermeidung von Unruhe im Unternehmen (27%).

Abb. 43 Pro und Contra Strafanzeige

Einschätzung der Unternehmen: „völlig“ bis „eher zutreffend“



¹ Entfällt bei „Strafanzeige im Laufe oder nach Abschluss des Verfahrens gestellt“.

Ihre Ansprechpartner

PwC

Friedrich-Ebert-Anlage 35–37
60327 Frankfurt am Main



Claudia Nestler
Partnerin
Forensic Services
Tel.: +49 69 9585-5552
claudia.nestler@pwc.com



Steffen Salvenmoser
Partner
Forensic Services
Tel.: +49 69 9585-5555
steffen.salvenmoser@pwc.com

Über uns

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expertennetzwerks in 158 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC. Mehr als 10.600 engagierte Menschen an 21 Standorten. 2,09 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.

Forensic Services

Trotz alarmierender Studien werden die Risikofaktoren Wirtschaftskriminalität und Wirtschaftskonflikte vielfach unterschätzt. Ihnen frühzeitig entgegenzusteuern ist heute wichtiger denn je. Wir begleiten Sie von der Prävention über die lückenlose Aufklärung aller Fälle – auf Wunsch in Zusammenarbeit mit den Ermittlungsbehörden – bis zur konkreten Umsetzung von Verbesserungsmaßnahmen. Als Berater oder Gutachter helfen wir Ihnen, Schäden aus Wirtschaftskonflikten geltend zu machen und die Interessen Ihres Unternehmens durchzusetzen. Auch als Schiedsgutachter, Schiedsrichter oder Konfliktmoderator stehen wir Ihnen gern zur Verfügung.

Martin-Luther-Universität Halle-Wittenberg

Universitätsplatz 6
06108 Halle (Saale)



Prof. Dr. jur. Kai-D. Bussmann

Lehrstuhl für Strafrecht und Kriminologie
Juristische und Wirtschaftswissenschaftliche
Fakultät
Tel.: +49 345 55-23116
kai.bussmann@jura.uni-halle.de

Impressum

Wirtschaftskriminalität 2018

Herausgegeben von der PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft und der Martin-Luther-Universität Halle-Wittenberg

Von Prof. Dr. jur. Kai-D. Bussmann, Claudia Nestler, Steffen Salvenmoser

Unter Mitarbeit von Dipl.-Jurist Tobias Günther, Dr. phil. Anja Niemeczek (Dipl.-Psych.), Ass. jur. Nicole Selzer und Dipl.-Kulturwirtin Nadja M. Wolf

Durchführung der Befragung durch Oliver Krieg, Senior Director Kantar EMNID, Kantar Deutschland GmbH, München

Februar 2018, 74 Seiten, 43 Abbildungen, Softcover

Alle Rechte vorbehalten. Vervielfältigungen, Mikroverfilmung, die Einspeicherung und Verarbeitung in elektronischen Medien sind ohne Zustimmung des Herausgebers nicht gestattet.

Die Inhalte dieser Publikation sind zur Information unserer Mandanten bestimmt. Sie entsprechen dem Kenntnisstand der Autoren zum Zeitpunkt der Veröffentlichung. Für die Lösung einschlägiger Probleme greifen Sie bitte auf die in der Publikation angegebenen Quellen zurück oder wenden sich an die genannten Ansprechpartner. Meinungsbeiträge geben die Auffassung der einzelnen Autoren wieder. In den Grafiken kann es zu Rundungsdifferenzen kommen.

Die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft bekennt sich zu den PwC-Ethikgrundsätzen (zugänglich in deutscher Sprache über www.pwc.de/de/ethikcode) und zu den Zehn Prinzipien des UN Global Compact (zugänglich in deutscher und englischer Sprache über www.globalcompact.de).

© Februar 2018 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft. Alle Rechte vorbehalten.
„PwC“ bezeichnet in diesem Dokument die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, die eine Mitgliedsgesellschaft der PricewaterhouseCoopers International Limited (PwCIL) ist. Jede der Mitgliedsgesellschaften der PwCIL ist eine rechtlich selbstständige Gesellschaft.

