MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG

In unserer Studie erfahren sie, wie deutsche Unternehmen mit Wirtschaftskriminalität in der analogen und digitalen Welt umgehen und wie IT-Sicherheits- und Compliance-Maßnahmen zum jetzigen Zeitpunkt umgesetzt werden.

Wirtschaftskriminalität in der analogen und digitalen Wirtschaft 2016

pwc

www.pwc.de/wirtschaftskriminalitaet

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.

Wirtschaftskriminalität in der analogen und digitalen Wirtschaft

Unsere achte Studie zur Entwicklung der Wirtschaftskriminalität setzt ihren Schwerpunkt bei der Kriminalität in der digitalen Wirtschaft – der Bedrohung von Unternehmen durch E-Crime, auch „Cybercrime" genannt. Wir haben dieses Phänomen aus verschiedenen Blickwinkeln beleuchtet. Hierzu wurden von Anfang September bis Ende November 2015 720 Unternehmen befragt.

Risiken in der analogen Welt werden nicht geringer

Die Zeiten werden nicht ruhiger. Wir stellen – nach einem Rückgang der Wirtschaftskriminalität in unserer letzten Studie – einen erneuten, wenn auch nur leichten Anstieg auf das Niveau von 2011 fest. 51 % der Unternehmen waren von Wirtschaftskriminalität betroffen. Betrugsdelikte haben zugenommen. Ein Rückgang zeigt sich bei Verstößen gegen Patent- und Markenrechte sowie beim Diebstahl vertraulicher Kunden- und Unternehmensdaten.

Eine Fortsetzung des sinkenden Trends beobachten wir auch bei Korruptionsdelikten. Hingegen verharrt das Risiko wettbewerbswidriger Absprachen auf einem unverändert hohen Niveau. Angesichts der nach wie vor noch zu geringen Verbreitung kartellrechtlicher Compliance-Management-Systeme (CMS) müssen wir bei Kartelldelikten weiterhin von einem sehr großen Dunkelfeld ausgehen.

Wachsende Risiken in der digitalen Welt

Das digitale Zeitalter bringt neue Kriminalitätsformen mit sich. Am häufigsten sind Computerbetrug (13 %), Manipulation von Konto und Finanzdaten (11 %) und Ausspähen und Abfangen von Daten (9 %). Berücksichtigen wir auch die Anzahl der Verdachtsfälle, so sind die Risiken hinsichtlich des Ausspähens und Abfangens sicherheitsrelevanter Daten (18 %) sowie des Diebstahls vertraulicher Kunden- und Unternehmensdaten (15 %) doppelt bzw. dreimal so hoch.

Unter Einbeziehung von Verdachtsfällen waren insgesamt 57 % der Unternehmen durch klassische Wirtschaftskriminalität und 47 % durch E-Crime (vermutlich) betroffen. Unsere Studie zeigt ein wachsendes Bedrohungspotenzial durch E-Crime, vor dem auch das Bundeskriminalamt (BKA) warnt.

Hohe Schadensrisiken durch Organisierte Kriminalität (OK)

Die monetären Schäden infolge von E-Crime sind zwar im Vergleich zur herkömmlichen Wirtschaftskriminalität noch gering, aber nach den Ergebnissen unserer Studie müssen wir von einer wachsenden Bedrohung durch E-Crime-Angriffe aus dem Spektrum der OK ausgehen. Nach den Fallberichten der befragten Unternehmen sind vermutlich 30 % der externen Täter der OK zuzuordnen, wenn es um Angriffe auf Daten und Know-how des Unternehmens geht. Hinsichtlich anderer Wirtschaftsdelikte bewegt sich der Anteil in ähnlicher Höhe (27 %).

Die OK dürfte ihre Aktivitäten vermehrt auf die Informations- und Kommunikationstechnik von Unternehmen verlagern, wobei nach unseren Ergebnissen vor allem forschungsintensive Unternehmen gefährdet sind.

Das Bedrohungspotenzial durch E-Crime wächst: Gefährdet ist vor allem das geistige Eigentum des Unternehmens. Forschungsintensive Unternehmen sehen sich besonders gefährdet.

Cybercrime potenziert Risiken des Daten- und Wissensverlusts

Bemerkenswerterweise wurden die berichteten Fälle eines Daten- und Wissensverlusts vornehmlich durch Entwenden und Kopieren von Firmenunterlagen begangen (42 %). Viele Begehungsformen setzen jedoch auch an Schwachpunkten in der Informations- und Kommunikationstechnik an. Jeder fünfte Angriff auf stationäre und immerhin jeder zehnte auf mobile IT-Systeme geschah auf diese Weise. Unternehmen sehen sich heute einer doppelten Herausforderung gegenübergestellt: Sie dürfen keinesfalls die – insbesondere durch Social Engineering entstehenden – Risiken in den Bereichen Personal und Geschäftsablauf vernachlässigen und müssen sich zugleich den wachsenden Risiken der Cyberspionage stellen.

40 % der forschungsintensiven Unternehmen zögern aufgrund hoher E-Crime-Risiken beim Schritt in Richtung Industrie 4.0,[1] da mit der wachsenden digitalen Vernetzung zugleich das wahrgenommene Bedrohungspotenzial von E-Crime zunimmt. 70 % der forschungsintensiven Unternehmen sehen die vierte industrielle Revolution mit höheren E-Crime-Risiken verbunden. Diese befürchteten Risiken können zu Wettbewerbsnachteilen führen, wenn sie die technologische Innovationsbereitschaft von Unternehmen hemmen.

Zu selten Zertifizierung des IT-Risk-Managements

Viele Unternehmen wappnen sich gegen die wachsende Bedrohung durch Cyberangriffe. Nach Angaben der befragten Unternehmen verfügen drei Viertel über ein internes Sicherheitsmanagement zur Identifikation von IT-Sicherheitsvorfällen und 67 % führen interne Sicherheitsaudits durch. Aber nur eine Minderheit der Unternehmen lässt die eigenen Aktivitäten auch extern überprüfen: Nur 39 % haben eine Zertifizierung ihres IT-Sicherheitsmanagements durchführen lassen; bei 38 % ist diese nicht einmal vorgesehen. Wir befürchten, dass Unternehmen sich vielfach in trügerischer Sicherheit wähnen, da sie sich keiner unabhängigen Prüfung gestellt haben.

Überwiegende Zustimmung zum IT-Sicherheitsgesetz

Mit dem seit Juli 2015 geltenden IT-Sicherheitsgesetz will der Gesetzgeber dem wachsenden Bedrohungspotenzial für kritische Infrastrukturen begegnen. Dieses Gesetz stößt bei Unternehmen, die als Betreiber kritischer Infrastrukturen (KRITIS) gelten, überwiegend auf Zustimmung, obwohl es von ihnen die Einhaltung erhöhter IT-Sicherheitsstandards verlangt und eine Meldepflicht an das Bundesamt für Sicherheit in der Informationstechnik (BSI) vorsieht. Ermutigend ist auch, dass das IT-Risk-Management von Unternehmen, die ihrer Einschätzung nach zur KRITIS gehören, weiter fortgeschritten ist. Allerdings mangelt es auch hier bei über der Hälfte der Unternehmen an einer unabhängigen Prüfung: Nur 42 % haben ihr IT-Risk-Management zertifizieren lassen.

Um an Ergebnisse der Forschungs- und Entwicklungsarbeit zu gelangen, gehen Täter oft ganz konventionell vor: Sie kopieren Unterlagen – früher auf Papier, heute zunehmend auf dem Speicherstick.

[1] 13 % der forschungsintensiven Unternehmen beantworteten die entsprechende Frage mit „ja“und 27 % mit „teils, teils“.

Compliance-Druck in der Zulieferkette

Nur die wenigsten Unternehmen stufen die Haftungsrisiken innerhalb ihrer Branche nahe null ein. Das Thema Compliance ist wohl auch aus diesem Grund eine Selbstverständlichkeit. 76 % der befragten Unternehmen verfügen über ein CMS und bei weiteren 13 % befindet sich dieses in der Planung. Bei Großunternehmen mit mehr als 10.000 Mitarbeitern ist es schon die Regel: 96 % haben bereits ein CMS eingeführt.

Marktmechanismen haben hier das Regime übernommen. Den meisten Unternehmen ist es zunehmend wichtig geworden, dass auch ihre Lieferanten und Dienstleister über ein CMS verfügen. Jedes dritte Unternehmen gab sogar an, dass ihm dies sehr wichtig ist. Als unwichtig bezeichneten es nur 7 %.

Der Druck in der Zulieferkette geht vor allem von Großunternehmen aus. Diese sind dazu übergegangen, in ihre Verträge mit Lieferanten und Dienstleistern Haftungsklauseln aufzunehmen und sich Kontrollrechte einzuräumen. Neben Haftungsklauseln dominieren auch vertragliche Verpflichtungserklärungen. Außerdem sehen die Verträge häufig eine Verpflichtung des Lieferanten zur Zertifizierung seines CMS vor.

Werte-Management in den Anfängen

Es mehren sich die Anzeichen, dass Unternehmen ihre anfänglich vielfach eher auf Regelkonformität basierende Unternehmenskultur hin zu einer wertebasierten Kultur entwickeln. Viele Unternehmen nannten als Werte, die ihre Kultur am stärksten kennzeichnen, unter anderem Integrität, Verbindlichkeit, Vertrauen, Transparenz und offene Kommunikation.

Zudem zeigte sich, dass es Unternehmen auch in schwierigen Märkten wie China gelingen kann, ihr Compliance-Programm umzusetzen. Die Herausforderungen in diesen Märkten sind jedoch erheblich. Am häufigsten nannten Unternehmen hier als Gründe eine schlecht funktionierende Verwaltung (59 %) oder korrupte lokale Netzwerke (55 %).

Auch stellt für einen Teil der Unternehmen die Rekrutierung integrer Mitarbeiter ein Problem dar (39 %). Knapp zwei Drittel (61 %) verwiesen zudem auf die für Mitarbeiter nicht leicht zu überwindende Spannung zwischen den Compliance-Standards des Unternehmens und der „Korruptionskultur“ im Alltag der Auslandstochter.

Unternehmen mit CMS aufgeschlossen gegenüber Rechtsreformen

Vor allem Unternehmen mit einem entwickelten CMS[2] stehen einer Neuordnung der strafrechtlichen Unternehmenshaftung, die auch Anreize zur Implementierung von Compliance-Standards bietet, aufgeschlossen gegenüber. 37 % der befragten Unternehmen mit einem CMS halten eine gesetzliche Regelung, die Mindestaufsichts- bzw. Mindest-Compliance-Standards zur Schaffung von Rechtssicherheit formuliert, für sinnvoll und fast jedes zweite Unternehmen hält eine solche Regelung für überlegenswert (47 %).

Auch zeigen sich Unternehmen in dieser Gruppe deutlich häufiger an einer Regelung zur sanktionsausschließenden bzw. -mildernden Anrechnung eines CMS interessiert. 44 % bewerten dies als sinnvoll. Eine hohe Zustimmung erfährt ferner eine entsprechende „Bonusregelung“ bei Selbstanzeige und/oder Kooperation mit den Strafverfolgungsbehörden. Jedes zweite Unternehmen mit einem CMS beurteilt eine solche Regelung als sinnvoll (53 %) und weitere 36 % betrachten sie als überlegenswert.

[2] Zur Gruppe der Unternehmen mit einem entwickelten CMS gehören Unternehmen, die über ein CMS verfügen, dessen Aufbau aus ihrer Sicht bezogen auf mindestens zwei Deliktsfelder abgeschlossen ist. Hierzu zählen mehr als zwei Drittel der Unternehmen (68 %).

Viele Unternehmen haben IT-Sicherheitssysteme eingerichtet. Doch reichen diese aus? Nur wenige machen die Probe aufs Exempel und lassen ihr Programm auf Lücken überprüfen.

Auch dem im November 2015 neugefassten Straftatbestand zur Bekämpfung der Bestechlichkeit und Bestechung im geschäftlichen Verkehr steht die Mehrheit der befragten Unternehmen aufgeschlossen gegenüber. Durch die Reform des § 299 StGB[3] droht Mitarbeitern nicht nur bei Formen von Korruption in einer Wettbewerbssituation eine Strafverfolgung (sog. Wettbewerbsmodell), sondern auch dann, wenn sie gegen Compliance-Vorgaben ihres Unternehmens verstoßen (sog. Geschäftsherrenmodell). Vor allem in der Gruppe der Unternehmen, die über ein entwickeltes CMS verfügen, hält jedes vierte Unternehmen eine Reform für sinnvoll (23 %) und fast jedes zweite für überlegenswert (46 %).

Bei der Bekämpfung von Korruption im Gesundheitswesen zeigen die befragten Unternehmen in dieser Branche ebenfalls eine hohe Akzeptanz gegenüber einem umfassenden strafrechtlichen Schutz. Nach der Entscheidung des Bundesgerichtshofs (BGH) vom März 2012 ist hinsichtlich der Strafbarkeit niedergelassener Ärzte eine Strafbarkeitslücke entstanden, die durch die Einführung des neuen Straftatbestands § 299a StGB geschlossen werden soll. Eine deutliche Mehrheit (82 %) der Unternehmen im Gesundheitswesen sieht hierin ein wichtiges Signal zur Unterstützung ihres Verhaltenskodex und einen zusätzlichen Schutz vor „schwarzen Schafen“ (84 %).

Compliance-Audit noch nicht selbstverständlich

Die Studie zeigt eine klare Tendenz zur Bereitschaft, sich gegen Risiken von herkömmlicher Wirtschaftskriminalität und E-Crime zu wappnen. Compliance-Management- und auch IT-Risk-Management-Systeme gelten heute als Best Practice.

Es bedarf jedoch auch einer unabhängigen Bewertung der Qualität dieser Präventionsmaßnahmen. Hier besteht weiterhin erheblicher Nachholbedarf. Dies gilt sowohl für das IT-Risk-Management als auch für das CMS. Nur jedem zweiten Unternehmen ist der Prüfungsstandard 980 des Instituts der Wirtschaftsprüfer in Deutschland (IDW PS 980) für CMS bekannt (54 %) und von diesen hat sich bislang kaum mehr als jedes dritte Unternehmen nach diesem Standard zertifizieren lassen (39 %). Auch den internationalen Standard nach ISO 19600[4] kennt weniger als die Hälfte der Unternehmen (46 %).

Abschließend möchten wir uns bei den befragten Unternehmen für ihre Bereitschaft zur Teilnahme an der vorliegenden Studie bedanken. Auch diesmal haben wir wieder neue Themen aufgegriffen, 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 2016

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

[3] Strafgesetzbuch.
[4] International Organization for Standardization.

Inhaltsverzeichnis

9 *Abbildungsverzeichnis*

12 *Methodisches Vorgehen*

14 *Risiken bleiben auf hohem Niveau – analog und digital*
16 Kriminalität in der analogen Wirtschaft
18 Parallele Entwicklung bei den Verdachtsfällen
19 Erhebliche zusätzliche Risiken durch E-Crime
21 Unternehmensrisiko Korruption: leicht abnehmend
22 Unternehmensrisiko wettbewerbswidrige Absprachen: unverändert hoch
23 Aufdeckung wettbewerbsrechtlicher Verstöße

24 *Schäden*
26 Schäden durch klassische Kriminalität
27 Schäden durch E-Crime – Risiko OK wächst
30 Risiko Industrie 4.0 – E-Crime als Innovationshemmnis

32 *Hohes Risiko des Daten- und Wissensverlusts*
34 Typische Angriffsvektoren und Risiken des Daten- und Wissensverlusts
36 Vergleich von vermuteten und tatsächlichen Risiken
38 Bedrohung durch OK
40 Profil von Tätern im Bereich Daten- und Wissensverlust und bei anderen Wirtschaftsdelikten
41 Näher als man denkt – regionale Risiken
42 Erstentdeckung und Speak-up-Kultur

44 *Unternehmen der kritischen Infrastruktur*
46 Betroffenheit vom IT-Sicherheitsgesetz
48 Überwiegende Befürwortung des IT-Sicherheitsgesetzes
50 IT-Risk-Management

52 *Compliance unter dem Regime des Marktes*
54 Verbreitung von Compliance-Programmen
56 Status der Compliance-Programme nach Deliktsgruppen
57 Compliance in der Lieferkette aus Sicht der Auftragnehmer
59 Compliance in der Lieferkette aus Sicht der Auftraggeber
60 Compliance-Vertragskonditionen

62 ***Compliance und Wertekulturen***
64 Handlungsbedarf im Compliance-Management
66 Die stärksten Werte in den Unternehmen
68 Compliance in fremden Kulturen

70 ***Haftungsrisiken und Rechtsreformen***
72 Haftungsrisiken in der eigenen Branche
74 Befürwortung von Compliance-Anreizen in der Unternehmenshaftung
76 Aufgeschlossenheit gegenüber Reform des Korruptionsstrafrechts im privaten Sektor
77 Beurteilung eines Korruptionsstraftatbestands im Gesundheitswesen

78 ***Compliance-Audit***
80 Bedeutung des IDW PS 980 und der ISO 19600
81 Compliance-Audit noch nicht selbstverständlich

82 ***Ihre Ansprechpartner***

84 ***Impressum***

Abbildungsverzeichnis

Abb. 1 Funktion der Interviewperson im Unternehmen 12

Abb. 2 Unternehmensgröße – Anzahl der Beschäftigten (weltweit) 13

Abb. 3 Entwicklung der Wirtschaftskriminalität 2009–2015 17

Abb. 4 Entwicklung der Verdachtsfälle 2011–2015 18

Abb. 5 Von E-Crime betroffene Unternehmen 20

Abb. 6 Entwicklung der Korruptionsrisiken 2005–2015 21

Abb. 7 Entwicklung des Risikos wettbewerbswidriger Absprachen 2011–2015 22

Abb. 8 Durch wettbewerbswidrige Absprachen erzielter Umsatzanteil in der eigenen Branche 2013–2015 22

Abb. 9 Einschätzung der Effizienz von Maßnahmen zur Aufdeckung wettbewerbsrechtlicher Verstöße 23

Abb. 10 Das klassische Wirtschaftsdelikt mit dem höchsten direkten und indirekten Schaden 26

Abb. 11 Durchschnittliche Schäden durch Wirtschaftskriminalität nach Unternehmensgröße (in Mio. Euro) 26

Abb. 12 Durchschnittliche Schäden durch E-Crime nach Unternehmensgröße (in Mio. Euro) 28

Abb. 13 Das E-Crime-Delikt mit dem höchsten direkten und indirekten Schaden 29

Abb. 14 Einschätzung des E-Crime-Risikos infolge von Industrie 4.0 30

Abb. 15 Auswirkung erhöhter E-Crime-Risiken auf Industrie 4.0 31

Abb. 16 Typische Angriffsvektoren und Risiken des Daten- und Wissensverlusts 35

Abb. 17 Vermutete und tatsächliche Risiken des Daten- und Wissensverlusts (alle Unternehmen) 37

Abb. 18 Beziehung der Täter zum geschädigten Unternehmen 39

Abb. 19 Profil der Täter von gravierenden Wirtschaftsdelikten im Vergleich 40

Abb. 20 Schadensschwerpunkt und Herkunft externer Täter tatsächlicher Fälle von Daten- und Wissensverlust 41

Abb. 21 Gründe für die Erstentdeckung von Delikten im Vergleich 43

Abb. 22 Sektoren der KRITIS 46

Abb. 23 Einschätzung der Zugehörigkeit zur KRITIS 47

Abb. 24 Gesetzliche Regelung von IT-Sicherheitsstandards für Betreiber der KRITIS in Abstimmung mit Branchenverbänden 48

Abb. 25 Beurteilung der gesetzlichen Meldepflicht von erheblichen IT-Sicherheitsvorfällen 49

Abb. 26 Verbreitung und Status von IT-Sicherheitsmaßnahmen 50

Abb. 27 Verbreitung von IT-Sicherheitsmaßnahmen nach KRITIS-Zugehörigkeit 51

Abb. 28 Verbreitung und Status von CMS nach Unternehmensgröße 54

Abb. 29 Verbreitung von Antikorruptionsprogrammen nach Unternehmensgröße 55

Abb. 30 Verbreitung kartellrechtlicher Compliance-Maßnahmen nach Unternehmensgröße 55

Abb. 31 Status des CMS nach Deliktsgruppen 56

Abb. 32 Compliance-Druck aus Sicht der Auftragnehmer 57

Abb. 33 Compliance-Druck aus Sicht der Auftragnehmer nach Unternehmensgröße 58

Abb. 34 Bedeutung eines CMS aus Sicht der Auftraggeber 59

Abb. 35 Bedeutung eines CMS aus Sicht der Auftraggeber nach Unternehmensgröße 59

Abb. 36 Verbreitung von Compliance-Vertragskonditionen 60

Abb. 37 Regelmäßige Compliance-Vertragskonditionen nach Unternehmensgröße 61

Abb. 38 Größerer Handlungsbedarf nach Status des CMS 65

Abb. 39 Die zehn stärksten Werte in Unternehmenskulturen 67

Abb. 40 Regionen und Länder mit den größten Hindernissen für Compliance aus Sicht weltweit operierender Unternehmen 68

Abb. 41 Compliance-Hindernisse in China 68

Abb. 42 Art der Compliance-Herausforderungen in fremden Regionen und Kulturen 69

Abb. 43 Einschätzung der Haftungsrisiken in der eigenen Branche 72

Abb. 44 Einschätzung der Haftungsrisiken nach Branchen 73

Abb. 45 Beurteilung gesetzlicher Regelungen im Falle einer Reform der Unternehmenshaftung 75

Abb. 46 Beurteilung der Reform des § 299 StGB im Sinne des Geschäftsherrenmodells 76

Abb. 47 Beurteilung eines Korruptionsstraftatbestands im Gesundheitswesen (§ 299a StGB) 77

Abb. 48 Kenntnis des IDW PS 980 und der ISO 19600 sowie Zertifizierung des CMS 80

Abb. 49 Kenntnis des IDW PS 980 und erfolgte Zertifizierung nach Unternehmensgröße 80

Abb. 50 Kenntnis der ISO 19600 und erfolgte Zertifizierung nach Unternehmensgröße 81

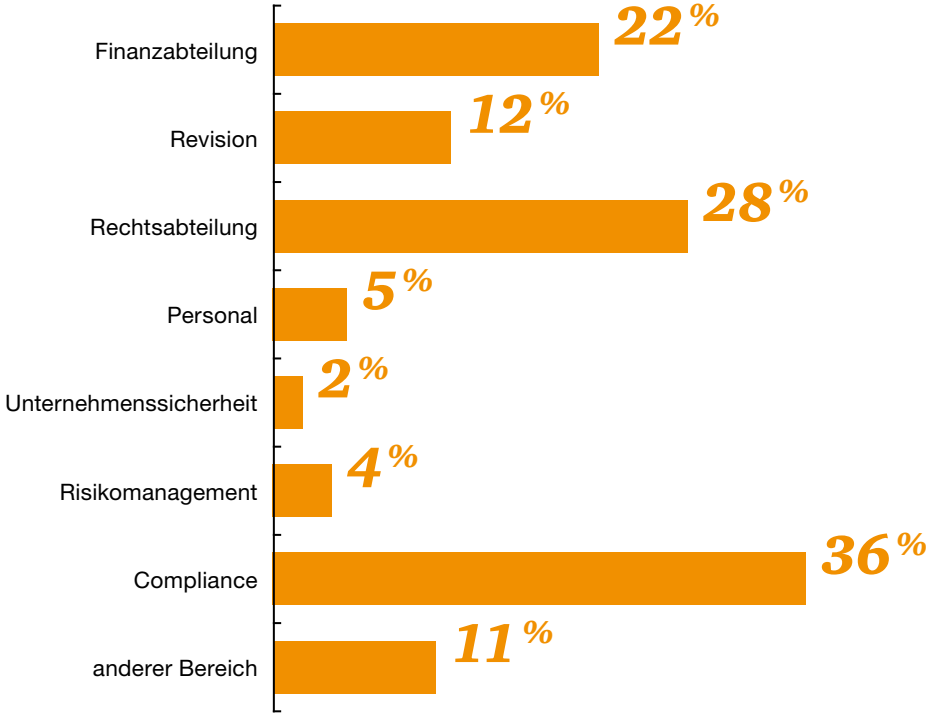
Abb. 51 Wahrscheinlichkeit einer Zertifizierung nach IDW PS 980 und ISO 19600 in den nächsten zwei Jahren 81

Methodisches Vorgehen

Die vorliegende, achte Studie zur Wirtschaftskriminalität wurde im Auftrag von PricewaterhouseCoopers und der Universität Halle-Wittenberg von TNS Emnid durchgeführt. Von Anfang September bis Ende November 2015 wurden in Deutschland mithilfe eines standardisierten Fragebogens Verantwortliche aus 720 Unternehmen telefonisch interviewt, die sich in ihrem Unternehmen für den Themenbereich Kriminalitätsprävention und -aufklärung zuständig erklärt haben. 28 % der Befragten gehören der Rechtsabteilung an und 22 % der Finanzabteilung. Entsprechend der wachsenden Bedeutung von Compliance für die Unternehmen übt jeder dritte Befragte (36 %) die Funktion eines Compliance-Beauftragten aus.

Abb. 1 Funktion der Interviewperson im Unternehmen

Mehrfachnennungen waren möglich.



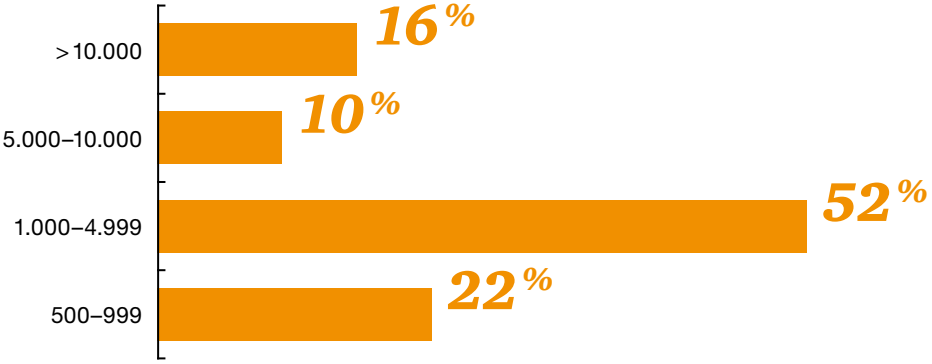
Experten aus 720 Unternehmen in Deutschland berichten, inwieweit ihre Unternehmen von Wirtschaftskriminalität betroffen waren: In den vergangenen zwei Jahren hatten sie 291 gravierende Schadensfälle zu verzeichnen.

Die Antwortbereitschaft war auch dieses Mal wieder hoch. Aufgrund der Art und des Umfangs der Stichprobenziehung handelt es sich um eine repräsentative Studie zur Sicherheitslage von Großunternehmen in Deutschland. Einbezogen wurden Unternehmen, die in Deutschland bzw. weltweit mindestens 500 Mitarbeiter haben, wobei über die Hälfte der Unternehmen 1.000 bis 4.999 Mitarbeiter beschäftigt (52 %).

Mehr als jedes dritte Unternehmen (37 %) betreibt eigenen Angaben zufolge viel Forschung und Entwicklung.

Über die Hälfte der Unternehmen (58 %) verfügt über Auslandsvertretungen, mehr als jedes vierte Unternehmen (29 %) ist weltweit vertreten. Die folgende Grafik zeigt die Größe der befragten Unternehmen nach Anzahl der weltweit beschäftigten Mitarbeiter.

Abb. 2 Unternehmensgröße – Anzahl der Beschäftigten (weltweit)

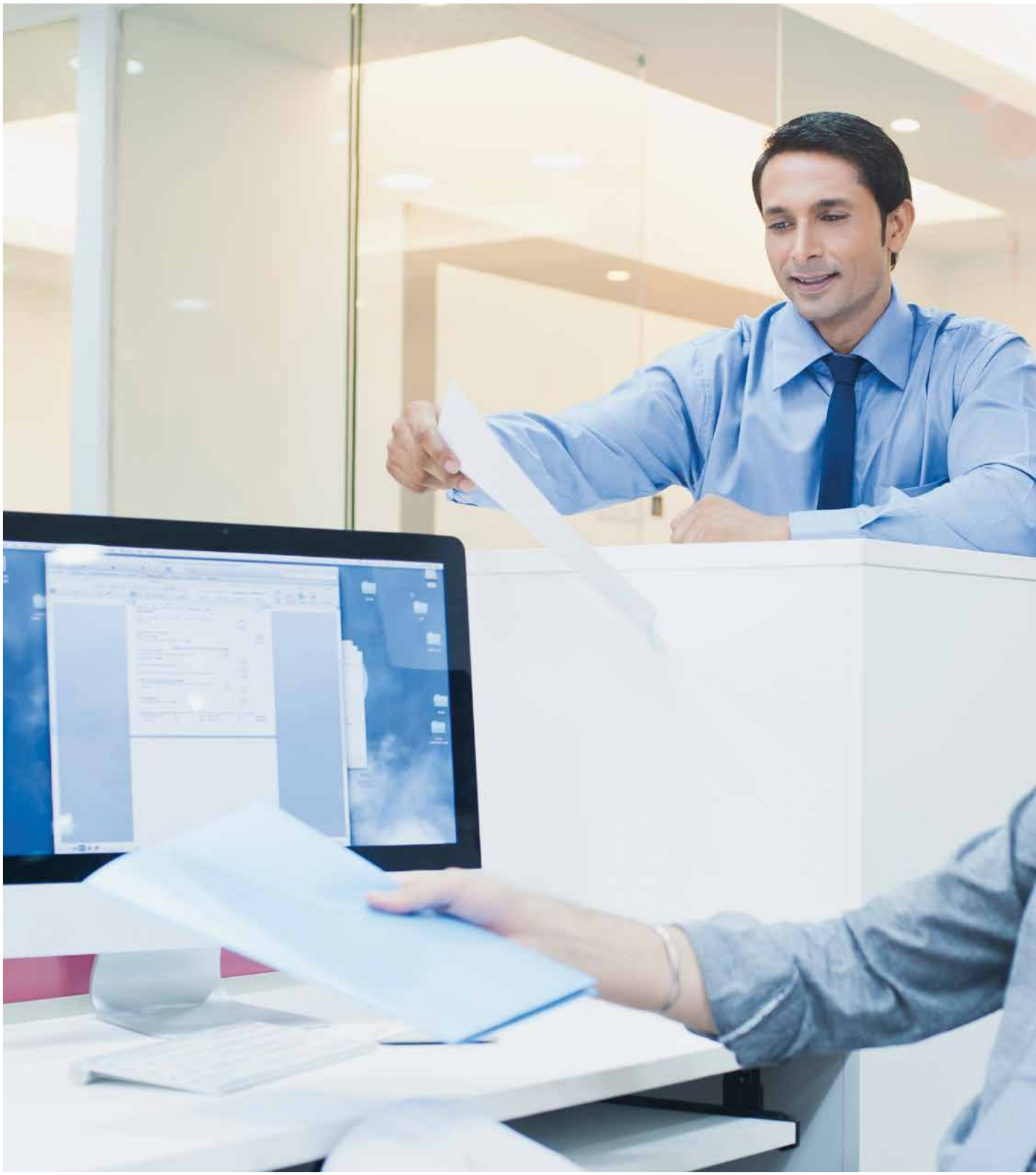


Ein Teil der Fragen ermöglicht einen direkten Vergleich mit unseren von 2005 bis 2013 zweijährlich durchgeführten Studien.[5]

Auch dieser Report enthält eine Fallstudie (siehe Seite 36 ff.). Diese ermöglicht insbesondere die Erstellung von Täterprofilen sowie die Analyse der Aufdeckungsart. 2015 berichteten die befragten Unternehmen von 291 gravierenden Schadensfällen, dabei handelte es sich bei 40 % der genannten Fälle um Daten- und Wissensverlust infolge von Industrie- und Wirtschaftsspionage oder Diebstahl vertraulicher Kunden- und Unternehmensdaten (n = 115, analog oder digital).

[5] Da ab 2009 nur noch Unternehmen mit mehr als 500 Beschäftigten befragt wurden, kann die Vergleichbarkeit der Ergebnisse mit denen früherer Veröffentlichungen eingeschränkt sein.

Risiken bleiben auf hohem Niveau – analog und digital



Computerbetrug, Datenspionage oder die Manipulation von Kontodaten: Mit der digitalen Vernetzung von Unternehmen steigt auch das Risiko von Attacken aus dem Internet. In den vergangenen zwei Jahren sind 34 % der deutschen Unternehmen Opfer von E-Crime geworden. Konkrete Verdachtsfälle inbegriffen, beläuft sich dieser Anteil sogar auf 47 %.

Die Zahl der Unternehmen, die von klassischer Wirtschaftskriminalität betroffen sind, ist nach wie vor hoch. Jedes zweite der befragten Unternehmen (51 %) hat solche Delikte zu verzeichnen. Das sind sechs Prozentpunkte mehr als in der Vorgänger-Studie von 2013.

Dieser Anstieg beruht vor allem auf der Zunahme der Vermögensdelikte. Sie bilden mit 37 % die größte Gruppe, gefolgt von Verstößen gegen Patent- und Markenrechte (13 %), Diebstahl vertraulicher Kunden- und Unternehmensdaten sowie Korruptionsdelikte (5 %).

Bei den digitalen Risiken berichten Unternehmen am häufigsten über Computerbetrug (13 %), Manipulation von Konto- und Finanzdaten (11 %) und das Ausspähen und Abfangen wichtiger Daten wie Passwörter (9 %).

Kriminalität in der analogen Wirtschaft

In unserer letzten Studie aus dem Jahr 2013 wagten wir die optimistische Einschätzung, dass die deutsche Wirtschaft in die Präventionsphase eingetreten ist, in der Compliance-Maßnahmen zu greifen beginnen und zumindest ein weiterer Anstieg der Wirtschaftskriminalität verhindert und sogar ein Rückgang erreicht wird. Aktuell beobachten wir jedoch gegenüber 2013 einen Anstieg der Kriminalitätsbelastung um 6 Prozentpunkte nahezu auf das Niveau von 2011 (52 %), ohne jedoch den Höchststand von 2009 (61 %) zu erreichen (alle Deliktsarten).

Über einen längeren Zeitraum gesehen gehen wir daher davon aus, dass die deutsche Wirtschaft trotz des beobachteten leichten Anstiegs, der vor allem auf einer Zunahme bei den Betrugsdelikten beruht, sich in einer Phase des allmählichen Rückgangs befindet.[6]

Die Formen klassischer Wirtschaftskriminalität überwiegen nach wie vor. Doch E-Crime-Fälle haben eine beachtliche Größenordnung erreicht.

Insgesamt gesehen ist die beobachtete Entwicklung kein Anlass zur Entwarnung, das Dunkelfeld ist weiterhin sehr groß, wie auch die ebenfalls leicht angestiegene Zahl der Verdachtsfälle zeigt. Hierzu lässt sich festhalten, dass sich die Zahl der Verdachtsfälle parallel zur Zahl der eindeutigen Fälle entwickelt hat, wobei wir hier allerdings nur bis in das Jahr 2011 zurückschauen können (siehe Seite 18).

Seit 2009 stellen wir einen fast ungebrochenen Rückgang bei Verstößen gegen Patent- und Markenrechte sowie beim Diebstahl vertraulicher Kunden- und Unternehmensdaten fest. Allerdings betrafen von den berichteten 291 gravierenden Schadensfällen allein 85 Fälle gravierende Diebstähle von Kunden- und Unternehmensdaten (29 %).[7]

Wenige Fälle können somit durchaus zu schwerwiegenden Folgen führen. Den Rückgang beim Datendiebstahl führen wir auf die erzielten Fortschritte im IT-Risk-Management (siehe Seite 50 f.) und auf die Selbstverständlichkeit zurück, mit der entsprechende CMS mittlerweise eingesetzt werden (89 %, siehe Seite 56).

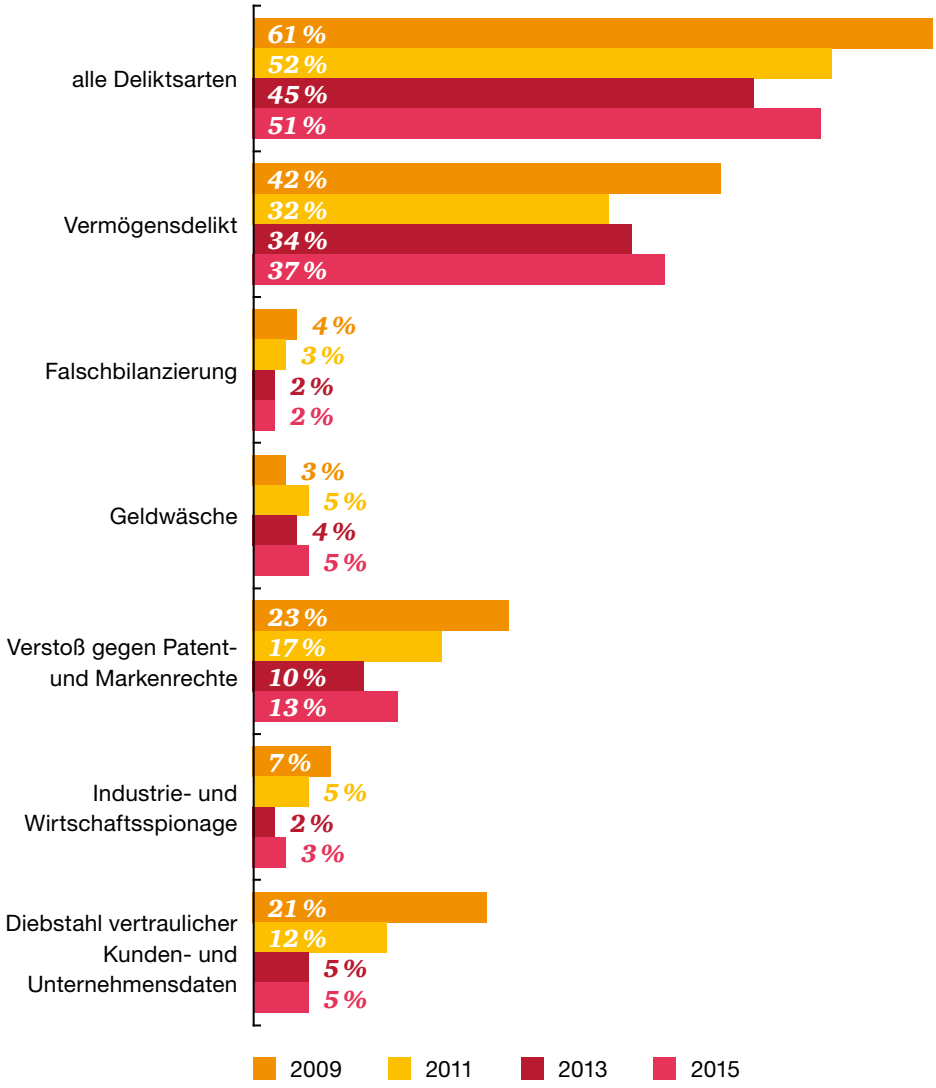
[6] In der allgemeinen polizeilichen Kriminalstatistik 2014 des BKA zeigt sich ebenfalls ein Rückgang der Wirtschaftskriminalität. Allerdings führt das BKA diesen – abweichend von unserem Ergebnis – auf eine Abnahme der Betrugsdelikte zurück. BKA, Polizeiliche Kriminalstatistik 2014, S. 8 und 10; vgl. auch BKA, Bundeslagebild Wirtschaftskriminalität 2014, S. 3 f.

[7] Es wurden von den Unternehmen 291 gravierende Schadensfälle genannt, dabei handelte es sich bei 40 % der Fälle um Daten- und Wissensverlust infolge von Industrie- und Wirtschaftsspionage oder Diebstahl vertraulicher Kunden- und Unternehmensdaten (n = 115, analog oder digital).

Beziehen wir das Umfeld der Unternehmen mit ein, so kann der Rückgang bei Verstößen gegen Patent- und Markenrechte auch auf eine weltweit festzustellende Tendenz zurückzuführen sein: Inzwischen haben vor allem auch die Emerging Markets – allen voran China – selbst ein Interesse am Schutz ihres geistigen Eigentums entwickelt.

Abb. 3 Entwicklung der Wirtschaftskriminalität 2009–2015

Mehrfachnennungen waren möglich.



Auch die Zahl der Verdachtsfälle ist im Vergleich zu 2013 leicht gestiegen. Das Dunkelfeld der Wirtschaftskriminalität ist beachtlich.

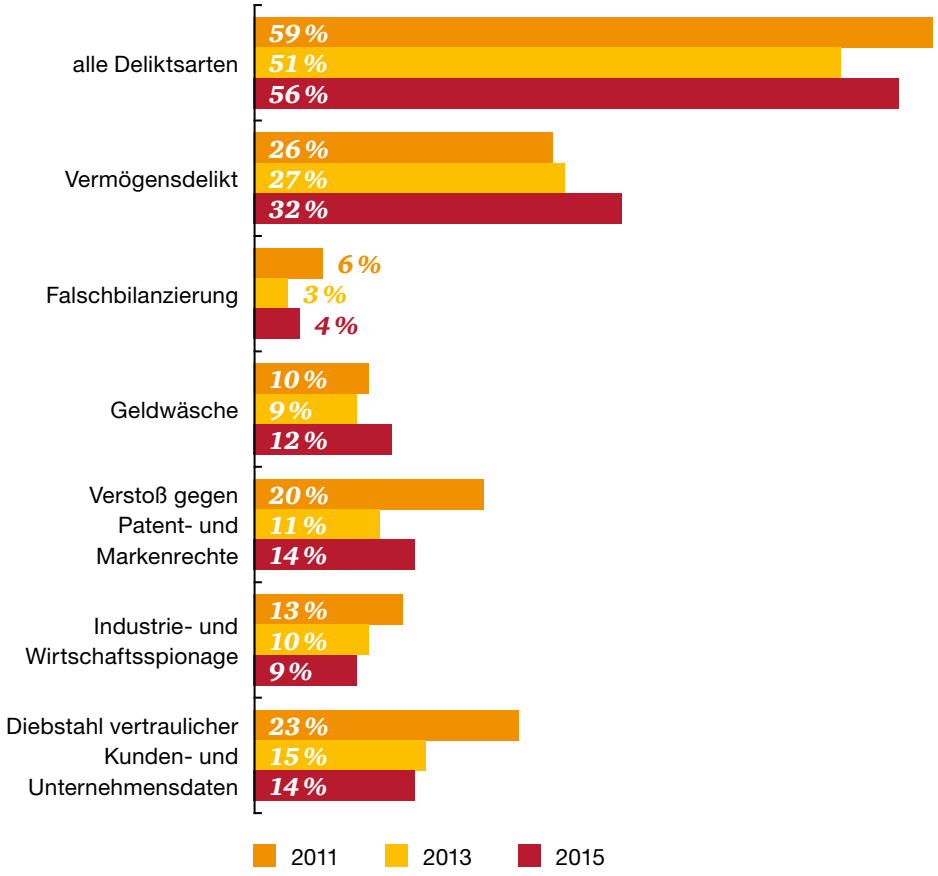
Parallele Entwicklung bei den Verdachtsfällen

Wie wir gesehen haben, ist die Zahl der berichteten eindeutigen Fälle seit unserer letzten Erhebung angestiegen und entspricht in etwa dem Niveau von 2011. Auch die Zahl der berichteten konkreten Verdachtsfälle[8] ist seit 2013 angestiegen, und zwar auf 56 % (alle Deliktsarten). Zudem wird beinahe das Niveau von 2011 erreicht. Dies ist vor allem auf die wachsende Zahl von Vermögensdelikten zurückzuführen; 32 % der Unternehmen berichteten über mindestens einen Fall. Wir werden diesen seit 2011 bemerkbaren leichten Anstieg sowohl bei den eindeutigen Fällen wie auch den Verdachtsfällen weiter beobachten.

Gegenüber der letzten Erhebung 2013 berichteten die Unternehmen bei fast allen Deliktsarten mit Ausnahme der Vermögensdelikte etwa genauso häufig oder seltener über Verdachtsfälle. In der aktuellen Studie zeigt sich allerdings, dass die Zahl der von Verdachtsfällen betroffenen Unternehmen die Zahl der Unternehmen mit eindeutigen Fällen teilweise erheblich übersteigt. So ist die Zahl der Verdachtsfälle in den Bereichen Wirtschafts- und Industriespionage (9 %) und Diebstahl vertraulicher Kunden- und Unternehmensdaten (14 %) im Vergleich zu den berichteten eindeutigen Fällen dreimal so hoch (siehe Abb. 3 und 4). Das Dunkelfeld der Wirtschaftskriminalität ist somit beachtlich.

Abb. 4 Entwicklung der Verdachtsfälle 2011–2015

Mehrfachnennungen waren möglich.



[8] Mithilfe der Erhebung konkreter Verdachtsfälle können wir die Größe des Dunkelfelds besser einschätzen. Durch den Begriff „konkreter Verdacht“ sollten bloße vage Vermutungen ausgeschlossen werden. Eine Strafanzeige war jedoch nicht Voraussetzung zur Einordnung als „konkreter Verdacht“.

Erhebliche zusätzliche Risiken durch E-Crime

Mit jeder technischen Innovation eröffnen sich neue Missbrauchsmöglichkeiten. Das digitale Zeitalter brachte neue Kriminalitätsformen mit sich – „E-Crime“ oder auch „Cybercrime“ genannt –, die für Unternehmen zu vollkommen neuen Risiken führten. Allerdings handelt es sich nicht bei jedem Delikt, bei dem der Täter sich beispielsweise eines digitalen Speichermediums bedient, um E-Crime. Auch in der Vergangenheit konnten vertrauliche Dokumente durch Abfotografieren oder Kopieren „entwendet“ werden. Mit der Digitalisierung von Informationen sind der Zugriff wie die Verfügbarkeit jedoch deutlich erleichtert worden.

Eine neue Kriminalitätsform wie ein Hackerangriff von außen entstand erst durch neue technische Möglichkeiten. Diebstahl hat damit ein vollkommen neues Gesicht bekommen und ist in dieser Form viel schwerer zu entdecken. Nahezu alle Buchungen und Abrechnungsprozesse in Unternehmen erfolgen elektronisch, aber nicht jede digitale Begehungsform sollte als E-Crime eingeordnet werden, wenn man das Ausmaß der Risiken bestimmen will, die mit neuen Informations- und Kommunikationstechniken einhergehen. Zur Abgrenzung verwenden wir folgende Begriffsdefinition:

> Bei E-Crime oder 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).[9]

Ausgeschlossen werden somit Delikte, bei denen der Computer oder das Internet beiläufig gewählt wurden, um beispielsweise die Begehung von Betrug zu vereinfachen. Berücksichtigt werden dagegen solche Delikte, bei denen Informations- und Kommunikationstechnik als wesentliches Element der Tatausführung zur Verwirklichung der Wirtschaftsstraftat eingesetzt wird, wie Computerbetrug oder das Ausspähen und Abfangen elektronischer Daten.

34 % *oder jedes dritte Unternehmen wurde Opfer von E-Crime. Datendiebstahl bekommt durch Hackerangriffe ein völlig neues Gesicht, die Taten sind viel schwerer zu entdecken.*

[9] Vgl. McGuire/Dowling, online abrufbar unter: www.gov.uk → Publications → Contains: Cyber crime → Cyber crime: a review of the evidence (7 Oct. 2013, Department: Home Office, publication type: Research and Analysis) → Chapter 1: Cyber-dependent crimes, S. 4.

Unsere Befragung zeigt, dass jedes zweite (51 %) der befragten Unternehmen innerhalb von zwei Jahren durch analoge Formen von Wirtschaftskriminalität geschädigt wurde, während jedes dritte (34 %) von E-Crime betroffen war.[10] Berücksichtigen wir zusätzlich die Berichte der Unternehmen über konkrete Verdachtsfälle, so waren 57 % von klassischer Wirtschaftskriminalität betroffen, während fast jedes zweite Unternehmen (47 %) von E-Crime (vermutlich) betroffen war. Unter Berücksichtigung der Verdachtsfälle nähern sich die Risiken beider Deliktsgruppen somit weiter an.

Das Risiko für Unternehmen, von klassischer Wirtschaftskriminalität betroffen zu werden, ist zwar weiterhin höher, aber E-Crime-Risiken haben bereits eine beachtliche Größenordnung erreicht. Zudem dürften E-Crime-Risiken nach den Ergebnissen unserer Studie weiter ansteigen, so auch die Einschätzung des BKA:

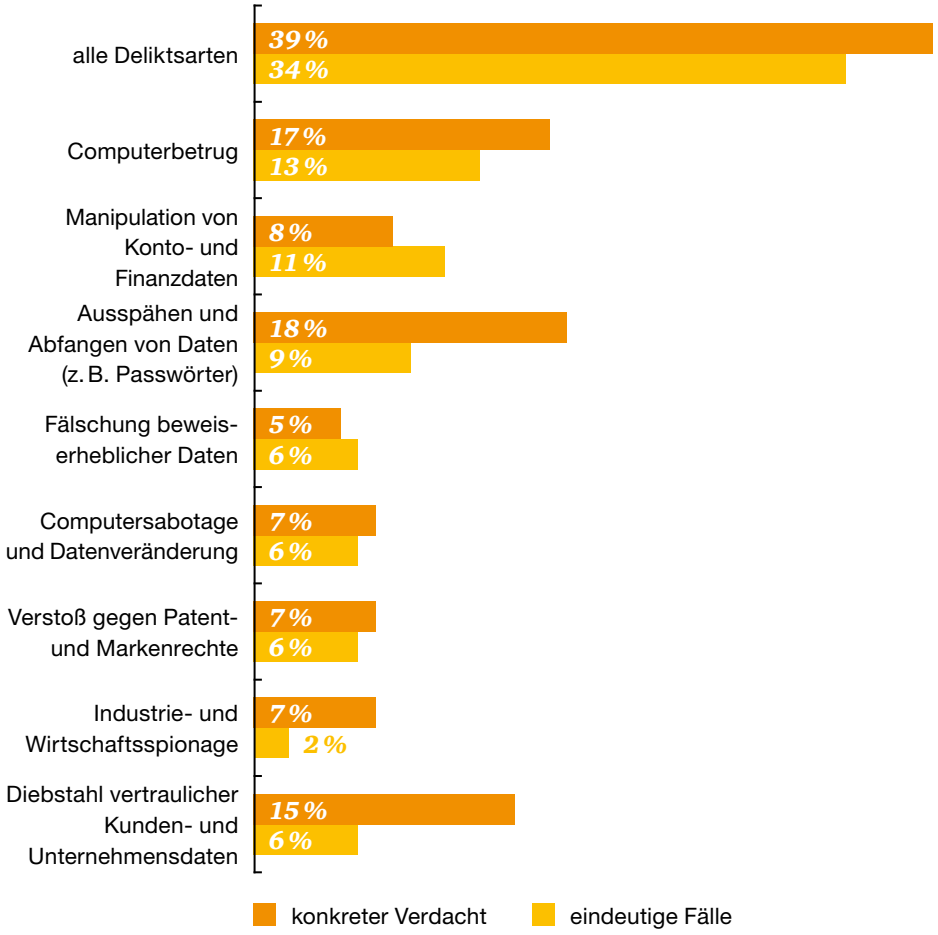
> *„Zusammenfassend ist davon auszugehen, dass die von den verschiedenen Facetten des Phänomens Cybercrime ausgehenden Gefahren in ihrem Ausmaß und in ihren Ausprägungen weiter zunehmen werden, wobei aktuelle Entwicklungen wie z. B. das „Internet der Dinge“, „Industrie 4.0“ oder auch die weiterhin ansteigende Nutzung des Internets durch den Privatanwender einen wesentlichen Einfluss haben dürften.“*[11]

Am häufigsten waren Unternehmen von Computerbetrug (13 %), Manipulation von Konto und Finanzdaten (11 %) sowie Ausspähen und Abfangen von Daten (9 %) betroffen.

Berücksichtigen wir zusätzlich die berichteten konkreten Verdachtsfälle, so verdoppelt sich die Zahl der Unternehmen, die vom Ausspähen und Abfangen sicherheitsrelevanter Daten (18 %) sowie vom Diebstahl vertraulicher Kunden- und Unternehmensdaten (15 %) vermutlich betroffen sind. Daraus entnehmen wir, dass E-Crime schwer zu entdecken und nachzuweisen ist. Die teilweise hohe Zahl der Verdachtsfälle lässt auf ein sehr hohes Dunkelfeld schließen.

Abb. 5 Von E-Crime betroffene Unternehmen

Mehrfachnennungen waren möglich.



[10] In der Befragung wurde der Anteil der analog und digital begangenen wirtschaftskriminellen Taten in zwei getrennten Fragen erhoben, um zwischen den beiden Risiken zuverlässiger trennen zu können. Beide Anteile bilden daher eine unechte Teilmenge.
[11] Vgl. BKA, Bundeslagebild Cybercrime 2014, S. 14.

Unternehmensrisiko Korruption: leicht abnehmend

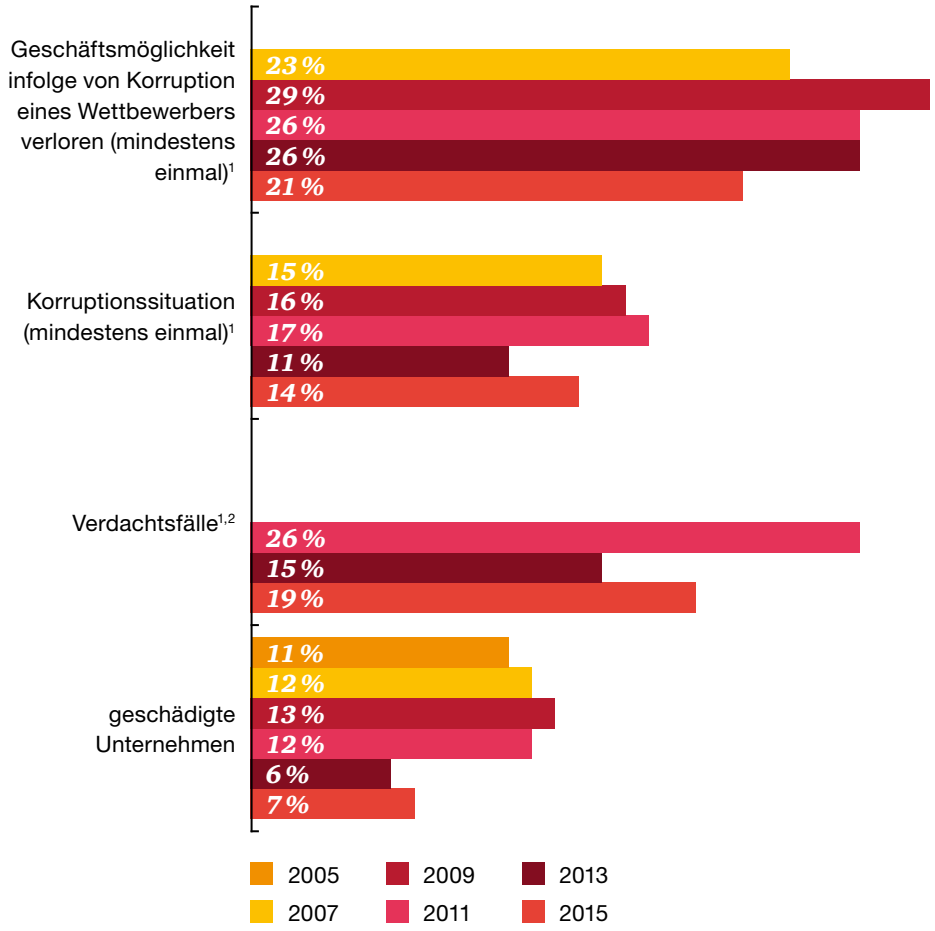
Die Zahl der von Korruption betroffenen Unternehmen ist gegenüber unserer Studie im Jahr 2013 (6 %) mit 7 % nahezu unverändert. Wir verzeichnen aber einen leichten Anstieg der Verdachtsfälle von 15 % auf 19 % und der Zahl der berichteten Korruptionssituationen von 11 % auf 14 %. Der Anteil der Unternehmen, die Geschäftsmöglichkeiten vermutlich infolge von Korruption verloren haben, sinkt von 26 % auf 21 %. Der Anteil der geschädigten Unternehmen, die über mindestens einen Korruptionsfall berichten, liegt mit 7 % deutlich unterhalb des Niveaus der Jahre 2005 bis 2011 (11 % bis 13 %).

Trotz des uneinheitlichen Bildes gehen wir von keiner Zunahme der Korruptionsbelastung, sondern eher von einem langsamen Rückgang aus. Denn letztlich ist das gesamte Umfeld der Unternehmen zu berücksichtigen. Das wachsende Problembewusstsein und der zunehmende Ausbau von CMS in der öffentlichen Verwaltung dürften die positive Entwicklung maßgeblich unterstützen.[12]

Die Zunahme bei den Verdachtsfällen führen wir auf die wachsende Verbreitung von korruptionsrechtlichen CMS zurück. In unserer Studie 2013 verfügte etwa die Hälfte der Unternehmen über ein entsprechendes CMS (52 %), 2015 waren es knapp vier Fünftel (79 %). Hierdurch steigen die Sensibilität, die Entdeckungswahrscheinlichkeit und die Zahl der Verdachtsfälle in den Unternehmen.

Nicht eindeutig ist, wie sich die Erweiterung der Strafbarkeit der Korruption im privaten Sektor durch den reformierten § 299 StGB auf die weitere Entwicklung auswirken wird (siehe Seite 76). Mit der Einführung des Geschäftsherrenmodells können Bestechung und Bestechlichkeit auch außerhalb einer Wettbewerbssituation strafrechtlich verfolgt werden. In der Folge könnte die Zahl der Fälle künftig zunehmen. Dabei wird das Anzeigeverhalten der Unternehmen einen maßgeblichen Einfluss auf die weitere Entwicklung der Zahlen haben. Bei den befragten Unternehmen besteht eine relativ hohe Akzeptanz der Reform des § 299 StGB (siehe Seite 76), sodass insgesamt gesehen eine wachsende Anzahl von Strafanzeigen zu erwarten ist. Für Unternehmen mit einem CMS dürfte eine Strafanzeige in der Regel geboten sein, um ihre Glaubwürdigkeit zu erhalten. Zugleich kann von der Ausdehnung der Strafbarkeit ein Abschreckungseffekt ausgehen, sodass es – auch angesichts des hohen Verbreitungsgrads von Antikorruptionsprogrammen – auch zu einer signifikanten Zurückdrängung korrupter Verhaltensweisen kommen kann. Die weitere Entwicklung bleibt somit abzuwarten.

Abb. 6 Entwicklung der Korruptionsrisiken 2005–2015



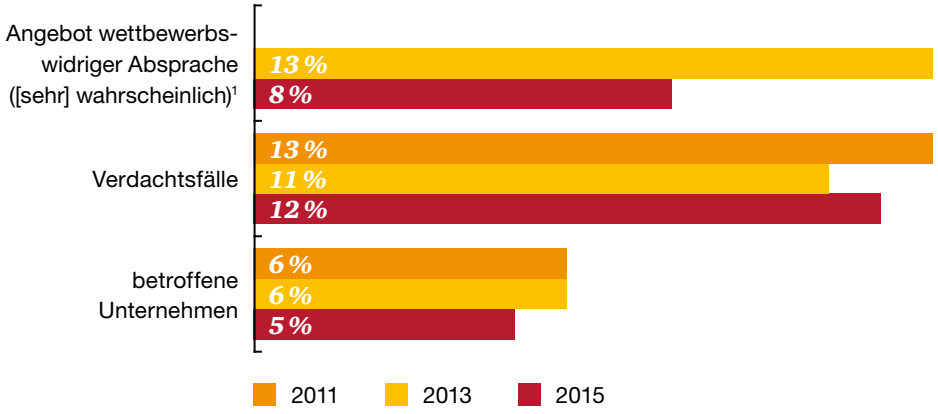
[1] Keine Daten für 2005.
[2] Keine Daten für 2007 und 2009.

[12] Vgl. auch die Beiträge in Stober/Ohrtmann (Hrsg.), Compliance: Handbuch für die öffentliche Verwaltung, 2015.

Unternehmensrisiko wettbewerbswidrige Absprachen: unverändert hoch

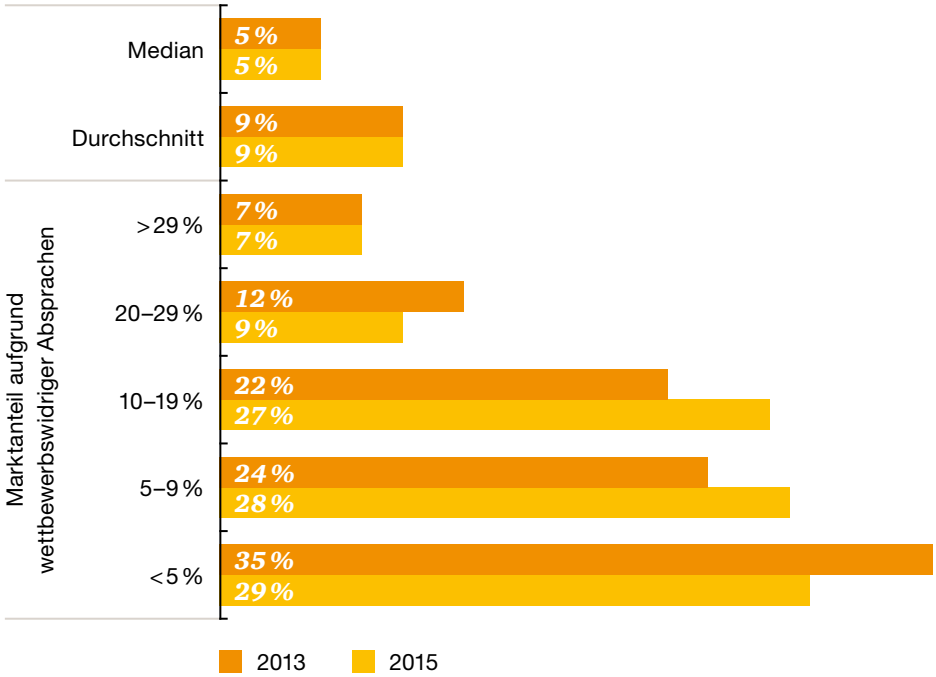
Im Unterschied zur Korruptionsbelastung erkennen wir bei wettbewerbswidrigen Absprachen keine Anzeichen für eine abnehmende Tendenz. Der Anteil der betroffenen Unternehmen ist im Vergleich zu 2013 nahezu unverändert. Gleiches gilt hinsichtlich der berichteten Verdachtsfälle. Allerdings halten es Unternehmen seltener für wahrscheinlich, ein Angebot für eine wettbewerbswidrige Absprache zu erhalten (8 %). Diese Zuversicht könnte auf die wachsende Verbreitung kartellrechtlicher Compliance-Maßnahmen zurückzuführen sein, die insgesamt jedoch weiterhin zu gering ist (55 %, siehe Seite 56).

Abb. 7 Entwicklung des Risikos wettbewerbswidriger Absprachen 2011–2015



[1] Keine Daten für 2011.

Abb. 8 Durch wettbewerbswidrige Absprachen erzielter Umsatzanteil in der eigenen Branche 2013–2015



Wir gehen aus zwei Gründen weiterhin von einem sehr großen Dunkelfeld aus: Zum einen ist, wie bereits erwähnt, die Verbreitung kartellrechtlicher Compliance-Maßnahmen nach wie vor zu gering.

Zum anderen wird der Umsatzanteil in der eigenen Branche, der auf wettbewerbswidrigen Absprachen beruht, gemessen am Mittelwert unverändert hoch eingeschätzt. Über ein Viertel der Unternehmen schätzen diesen Umsatzanteil auf über 10 % bis 19 %, und 16 % gehen von einem Umsatzanteil von mehr als 20 % aus.

Aufdeckung wettbewerbsrechtlicher Verstöße

Angesichts des weiterhin großen Dunkelfelds im Bereich wettbewerbswidriger Absprachen sollten Unternehmen geeignete Maßnahmen zu ihrer Aufdeckung ergreifen. Bemerkenswerterweise beurteilen Unternehmen, die über eine in der Entwicklung abgeschlossene kartellrechtliche Compliance verfügen,[13] die Wirksamkeit vieler Maßnahmen positiver als Unternehmen ohne entsprechende Compliance (siehe Abb. 9). Hierin drückt sich ihre vielfach auf Erfahrung beruhende Überzeugung aus, dass Unternehmen durchaus sehr wirkungsvolle Maßnahmen zur Aufdeckung von Kartelldelikten zur Verfügung stehen. Sie stufen die Effizienz vieler Maßnahmen daher höher ein.

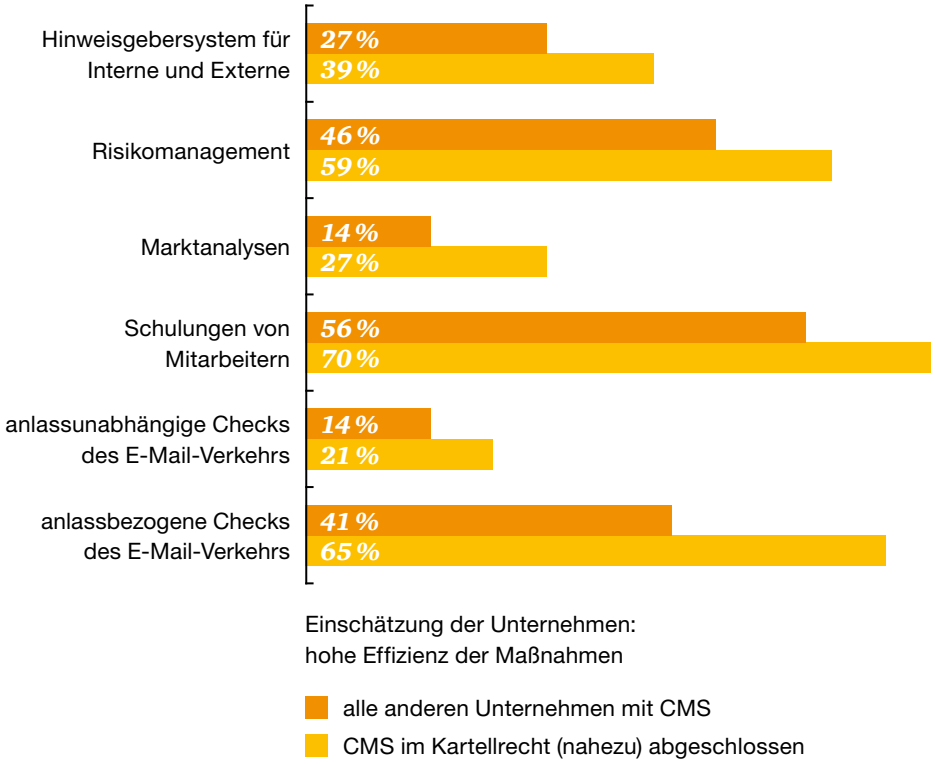
Zur Analyse von Schwachstellen und zur Aufdeckung von Kartelldelikten eignet sich ein Risikomanagement, das 59 % der Unternehmen mit kartellrechtlichen Compliance-Maßnahmen als hocheffizient einstufen.

Eine ähnliche Strategie stellt die Analyse von Marktkonstellationen dar. Dabei wird gezielt auf Indizien geachtet, die die Wahrscheinlichkeit von Wettbewerbsdelikten erhöhen, wie etwa eine geringe Anzahl an Wettbewerbern mit einer hohen Konzentration am Markt, ein geringes Potenzial für Produktinnovationen bzw. Nachfrageentwicklungen, relativ homogene Güter und eine hohe Abhängigkeit von einzelnen Produkten oder Dienstleistungen.[14] Allerdings wurden derartige Marktanalysen nur von jedem vierten Unternehmen mit Compliance-Maßnahmen zur Aufdeckung von Kartellrechtsverstößen als effizient bewertet (27 %). Wir meinen jedoch, dass ihre Effizienz damit unterbewertet wird.

Auch sollte die Eignung von Schulungen zur Aufdeckung nicht unterschätzt werden, da Mitarbeiter über die Vermittlung kartellrechtlicher Kenntnisse für mögliche Kartellrechtsverstöße sensibilisiert werden. Über zwei Drittel der Unternehmen mit einer kartellrechtlichen Compliance messen Schulungen einen hohen Wirkungsgrad nicht nur für die reine Wissensvermittlung und Sensibilisierung, sondern auch für die Aufdeckung von Verstößen bei.

Anlassunabhängige Checks des E-Mail-Verkehrs, die in der Regel rechtlich unzulässig sein dürften oder zumindest erheblichen rechtlichen Hürden ausgesetzt sind, werden seltener für effizient gehalten. Hingegen empfehlen zwei Drittel (65 %) der Unternehmen mit kartellrechtlicher Compliance anlassbezogene E-Mail-Checks. Außerdem beurteilen Unternehmen mit kartellrechtlicher Compliance den Nutzen von Hinweisgebersystemen häufiger höher (39 %).

Abb. 9 Einschätzung der Effizienz von Maßnahmen zur Aufdeckung wettbewerbsrechtlicher Verstöße



Basis: Unternehmen mit CMS

[13] Zur Gruppe der Unternehmen mit einem entwickelten kartellrechtlichen CMS gehören 55 % der Unternehmen, siehe Seite 56.
[14] Vgl. PwC, Wirtschaftskriminalität und Unternehmenskultur 2013, S. 61.

Schäden

Der finanzielle Schaden, den Wirtschaftskriminalität in den befragten Unternehmen verursacht hat, beläuft sich durchschnittlich auf 1,55 Millionen Euro. Doch im Einzelfall kann es sich um viel größere Summen handeln. So ist bei Unternehmen mit mehr als 10.000 Mitarbeitern der durchschnittliche Schaden mit 4,44 Millionen Euro fast drei Mal so hoch.

Vergleichsweise niedrig erscheinen dagegen Schäden, die durch Cyber-Kriminalität entstehen: Sie sind mit durchschnittlich 337.000 Euro deutlich geringer. Doch auch hier kann das im Einzelfall drastisch abweichen: Bei 5 % der Unternehmen, die Opfer einer Attacke aus dem Internet wurden, lag der Schaden bei mehr als einer Million Euro.

Hinzu kommt: Viele Schäden sind nicht quantifizierbar. Es ist kaum abzuschätzen, wie weitreichend die Folgen für ein Unternehmen sind, wenn vertrauliche Daten in falsche Hände gelangen. Das kostet Kundenvertrauen und kann die Reputation über Jahre hinweg beeinträchtigen.

Schäden durch klassische Kriminalität

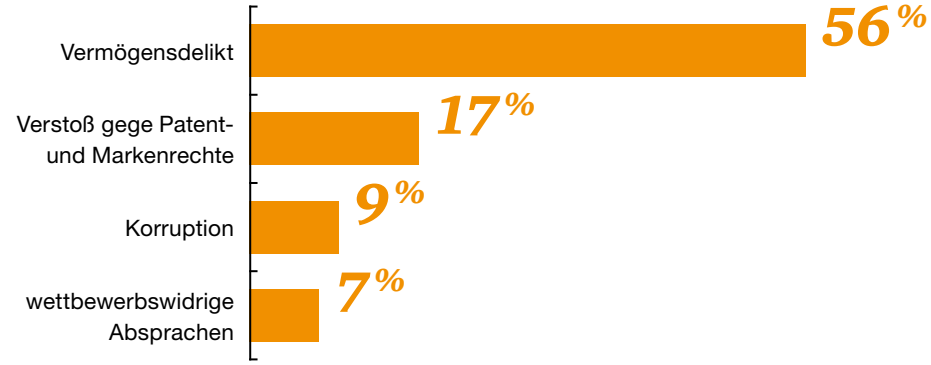
Für die betroffenen Unternehmen sind die Folgen von Wirtschaftskriminalität keinesfalls nur direkter finanzieller Art, vielmehr sind zahlreiche indirekte Konsequenzen wie Schadensersatzforderungen, straf- bzw. bußgeldrechtliche Haftungsrisiken oder Reputationsschäden zu berücksichtigen, die sich jedoch nur sehr schwer beziffern lassen.

Gleichwohl haben wir auch in der vorliegenden Studie wiederum den finanziellen Verlust aufgrund von Wirtschaftskriminalität erhoben, wobei auch die indirekten Kosten wie Managementkosten, Ausgaben für Untersuchungen und Rechtsverfahren sowie Stakeholdermanagement berücksichtigt wurden.

Im Einzelfall kann jede Deliktsart zu erheblichen Schäden führen. Nach den Erfahrungen der betroffenen Unternehmen verursachen Vermögensdelikte allerdings den höchsten direkten und indirekten Schaden.

Abb. 10 Das klassische Wirtschaftsdelikt mit dem höchsten direkten und indirekten Schaden

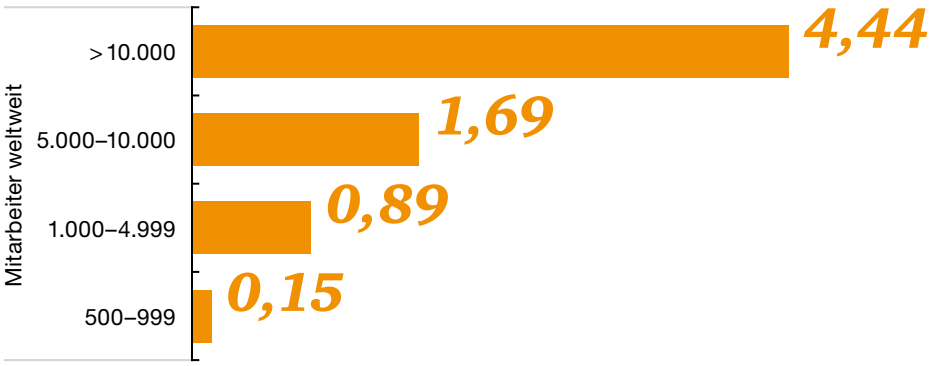
alle Delikte über 5 % der Nennungen



Basis: alle betroffenen Unternehmen

Der durchschnittliche Schaden beläuft sich auf 1,55 Millionen Euro je Unternehmen. Hierbei dürfte es sich jedoch vor allem aufgrund der schwer bestimmbaren indirekten Schäden um eine zu niedrige Schätzung handeln. Außerdem hängt die durchschnittliche Schadenshöhe stark von der Größe der Unternehmen ab, wie die nachfolgende Abbildung veranschaulicht:

Abb. 11 Durchschnittliche Schäden durch Wirtschaftskriminalität nach Unternehmensgröße (in Mio. Euro)



Höhe der durchschnittlichen direkten und indirekten Schäden (Mittelwert)
Basis: alle von Wirtschaftskriminalität betroffenen Unternehmen

Im Fall von Daten- und Wissensverlust deuten die Spuren nach Einschätzung der Betroffenen in 30 % der Fälle direkt auf OK hin.

Schäden durch E-Crime – Risiko OK wächst

Laut dem United Nations Office on Drugs and Crime (UNODC) sind über 80 % der Cyberangriffe organisiert und werden strukturiert und zielorientiert durchgeführt.[15] Aufgrund der fortschreitenden Digitalisierung von Gesellschaft und Wirtschaft verlagert mittlerweile auch die OK ihre Aktivitäten vermehrt in die digitale Welt und wird somit zu einer zunehmenden Bedrohung für die Privatwirtschaft. In der digitalen Wirtschaft liegen leichter zugängliche Felder für kriminelle Aktivitäten, da diese von nahezu jedem Ort der Welt ausgeführt werden können.

Hinzu kommt, dass wir uns von der Vorstellung, es handele sich bei OK-Strukturen um hierarchische Gebilde, lösen müssen. Vielmehr breiten sich lose netzwerkförmige Strukturen aus. Solche loseren Netzwerkstrukturen können sich Veränderungen des Umfelds flexibler und schneller anpassen.[16] Auch kennen sich Netzwerkmitglieder untereinander häufig nicht, wodurch die Wahrscheinlichkeit einer effektiven Strafverfolgung sinkt.

Immer handelt es sich dabei um Akteure, die nach ähnlichen Prinzipien wie legale Unternehmen handeln, sich an den gleichen Gesetzen des Angebots und der Nachfrage am Markt orientieren und somit vergleichbaren Marktmechanismen ausgesetzt sind.[17] Sie kennen daher auch Einheiten zur Forschung und Entwicklung.

Nach den Ergebnissen unserer Studie müssen wir von einem sehr hohen Bedrohungspotenzial durch OK ausgehen. 30 % der Fälle von Daten- und Wissensverlust werden von den betroffenen Unternehmen auf OK zurückgeführt (siehe Seite 38 f.).

Damit steht fest: Die Erfolgsrezepte in der legalen Marktwirtschaft werden auch in der illegalen eingesetzt. Dies macht OK für Staat und Wirtschaft so gefährlich. Zu dieser Einschätzung kommt auch das BSI in seinem Lagebericht 2015:

„Die Teilnehmer der Cyber-Sicherheitsumfrage 2015 der Allianz für Cyber-Sicherheit benennen weiterhin OK und Wirtschaftskriminalität als Angreifergruppe mit dem höchsten Bedrohungspotenzial in den kommenden Jahren.

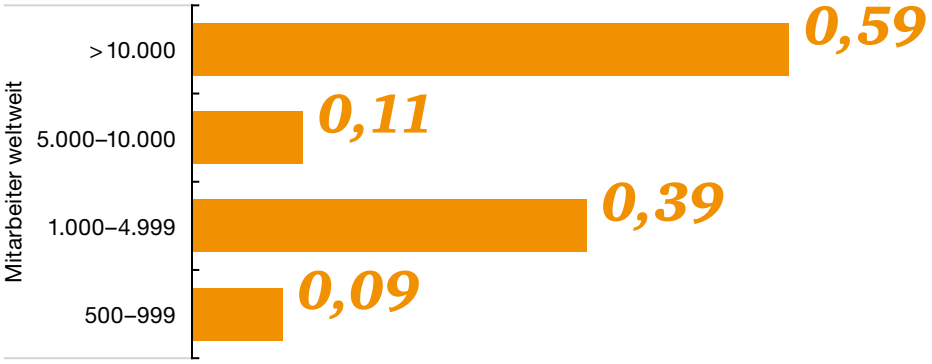
Der bestehende Markt, auf dem die Schwachstellen, Angriffsmethoden oder die Durchführung von Cyber-Angriffen offeriert werden, sorgt dafür, dass die Gefährdungslage unübersichtlicher wird. So bieten Organisationen ihre Fähigkeiten und Leistungen auch anderen interessierten Kreisen im Rahmen von Auftragsarbeiten an („Cybercrime-as-a-Service“). Damit werden hochwertige Angriffe auch für Organisationen und Staaten verfügbar, die diese Expertise bisher nicht eigenständig bzw. aufgrund mangelnder Fähigkeiten grundsätzlich nicht ausbauen können.“[18]

[15] Vgl. UNODC, online abrufbar unter: http://www.unodc.org/ → Topics: Organized Crime → Emerging Crimes → Comprehensive study on cybercrime → S. 45 ff.
[16] Vgl. Mastrofski/Potter, Controlling Organized Crime: A Critique of Law Enforcement Policy, in: Criminal Justice Policy Review, 1987 vol. 2, no. 3, S. 269 ff.
[17] Zum Ganzen vgl. Kleemans, Theoretical perspectives on organized crime, in: Handbook of Organized Crime, 2014, S. 32 f.
[18] Vgl. BSI, Die Lage der IT-Sicherheit in Deutschland, S. 36.

Die Bedrohung ist daher sehr viel größer, als es sich aus den derzeit berichteten Schäden ablesen lässt. Der durchschnittliche Schaden betrug je Unternehmen 337.000 Euro. Die höchsten Schäden weisen Unternehmen mit mehr als 10.000 Mitarbeitern auf. Berücksichtigen wir hingegen den Median, so bewegt sich die typische Schadenssumme in der Größenordnung von 30.000 Euro. E-Crime Vorfälle führen somit bisher überwiegend zu eher geringen finanziellen Schäden.

Dies kann sich künftig drastisch ändern. Schon jetzt betrug der Schaden bei 5 % der betroffenen Unternehmen mehr als eine Million Euro. Auch dürften viele Unternehmen das wahre Ausmaß des Schadens infolge eines E-Crime-Angriffs nicht zu quantifizieren vermocht haben. Dies gilt insbesondere für Reputations- und Vertrauensschäden.

Abb. 12 Durchschnittliche Schäden durch E-Crime nach Unternehmensgröße (in Mio. Euro)



Höhe der durchschnittlichen direkten und indirekten Schäden (Mittelwert)
Basis: alle von E-Crime betroffenen Unternehmen

Die durchschnittlichen finanziellen Schäden, die durch E-Crime entstehen, muten vergleichsweise gering an. Doch im Einzelfall können die Verluste um ein Vielfaches höher sein.

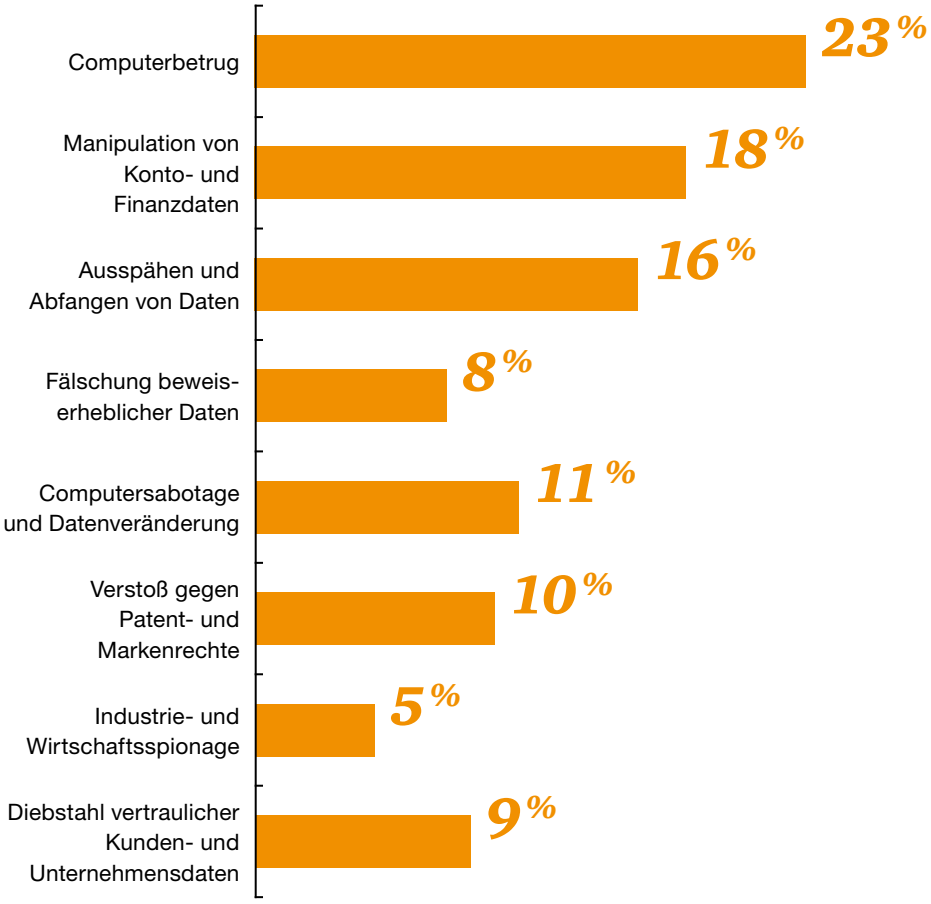
Die häufigsten Wirtschaftsdelikte sind Vermögensdelikte – bei E-Crime wie auch der klassischen Wirtschaftskriminalität.

Im Unterschied zur herkömmlichen Wirtschaftskriminalität werden die höchsten finanziellen Schäden bei E-Crime nicht primär durch eine Deliktsart verursacht, sondern durch eine Vielzahl von Angriffen auf die Informations- und Kommunikationstechnik.

Drei Delikte bestimmen das Schadensbild: Die befragten Unternehmen nannten am häufigsten Computerbetrug (23 %), die Manipulation von Konto und Finanzdaten (18 %) sowie das Ausspähen und Abfangen von Daten (16 %). Hiervon zielen jedoch mindestens zwei auf das Vermögen des Unternehmens ab, sodass es sich wiederum um Vermögensdelikte handelt, die auch bei den E-Crime-Delikten die höchsten Schäden verursachen.

Abb. 13 Das E-Crime-Delikt mit dem höchsten direkten und indirekten Schaden

alle Delikte über 5 % der Nennungen



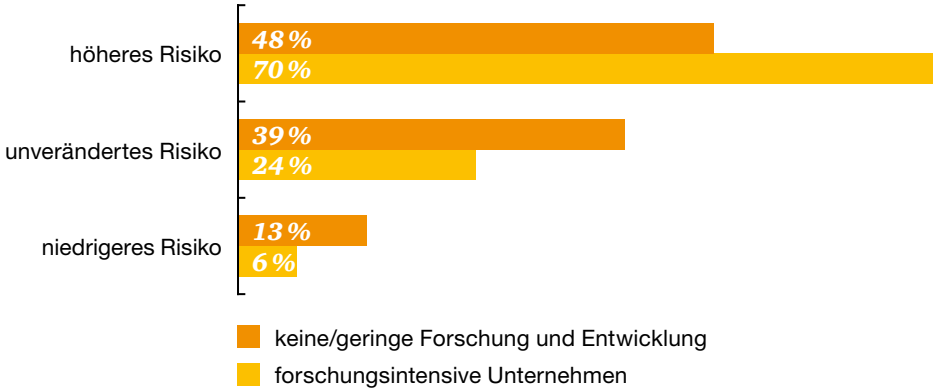
Basis: alle betroffenen Unternehmen

Risiko Industrie 4.0 – E-Crime als Innovationshemmnis

Die E-Crime-Schadensrisiken werden auch aufgrund der weiteren technischen Entwicklung zwangsläufig deutlich zunehmen. Die vierte industrielle Revolution – auch Industrie 4.0 genannt – zielt vor allem auf selbstoptimierende Verfahren und eine stärkere Verzahnung von Produktionsschritten und -technologien ab. Mit der wachsenden digitalen Vernetzung wächst zugleich das Bedrohungspotenzial durch E-Crime, wenn dieser Gefahr nicht durch geeignete IT-Sicherheitsmaßnahmen entschieden begegnet wird.

Viele der befragten Unternehmen erkennen diese mit Industrie 4.0 verbundenen neuen Risiken. Man muss sich auf höhere Risiken einstellen, antworteten sinngemäß vor allem forschungsintensive Unternehmen. Rund drei Viertel dieser Unternehmen (70 %) sehen in der vierten industriellen Revolution ein erhöhtes Risiko für E-Crime.

Abb. 14 Einschätzung des E-Crime-Risikos infolge von Industrie 4.0



Basis: alle befragten Unternehmen

Die hohe Risikobewertung vieler Unternehmen, insbesondere der forschungsintensiven Unternehmen, deckt sich mit dem Risikoszenario des BKA, das in seinem Lagebild zu Cybercrime – auch mit Blick auf (digitale) Erpressungsrisiken – ebenfalls zu einer alarmierenden Risikobeurteilung gelangt:

> *„ […] Die zunehmende Vernetzung, die Abhängigkeit vernetzter, sich selbst steuernder Produktionsprozesse und Logistikketten von der Verfügbarkeit der Netze und die Problematik der Trennung/Abschottung dieser Netze zum Internet, stellen dabei eine große Herausforderung dar. […] Eine Schädigung der IT-Infrastruktur von Unternehmen kann mittlerweile nicht mehr nur zur Störung der Kommunikation führen, sondern vielmehr auch zum kompletten Produktionsstillstand, was enorme Verluste für Unternehmen nach sich ziehen würde. Insbesondere die Gefahr der digitalen Erpressung von Unternehmen steigt dadurch.“*[19]

[19] Vgl. BKA, Bundeslagebild Cybercrime 2014, S. 13.

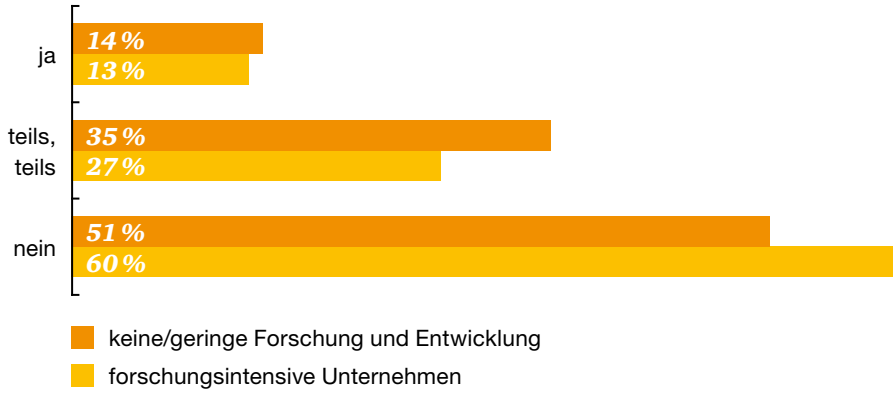
60 % *der forschungsintensiven Unternehmen lassen sich hinsichtlich Industrie 4.0 nicht durch damit verbundene E-Crime-Risiken abschrecken.*

Diese Bedenken lassen etwa die Hälfte der befragten Unternehmen, die für sich ein hohes Risiko sehen, zögern, Schritte in Richtung Industrie 4.0 zu gehen. Die Haltung eines Teils der forschungsintensiven Unternehmen zeigt jedoch, dass IT-Risiken gegen Wettbewerbschancen abzuwägen sind und auch als bewältigbar gesehen werden können. Vor allem forschungsintensive Unternehmen sind zu stark von technologischen Innovationen abhängig, als dass sie sich von damit verbundenen E-Crime-Risiken von der Nutzung abhalten ließen (60 %).

Allerdings zeigen unsere Ergebnisse auch, dass 40 % der forschungsintensiven Unternehmen aufgrund höherer E-Crime Risiken das Tempo in Richtung Industrie 4.0 zumindest drosseln. Dies ist angesichts der Herausforderungen im internationalen Wettbewerb kritisch zu sehen. Unsere Ergebnisse zeigen vielmehr, dass die Vorteile von Industrie 4.0 durch entsprechende Investitionen in die IT-Sicherheit abgesichert werden müssen (siehe Seite 50 f.).

Abb. 15 Auswirkung erhöhter E-Crime-Risiken auf Industrie 4.0

Lassen höhere E-Crime-Risiken Ihr Unternehmen zögern, Schritte in Richtung Industrie 4.0 zu gehen?



Basis: Unternehmen, die von einem höheren Risiko infolge von Industrie 4.0 ausgehen

Hohes Risiko des Daten- und Wissensverlusts

Cybercrime steht derzeit im Zentrum der Aufmerksamkeit. Es ist jedoch gar nicht so einfach, eine realistische Einschätzung von der tatsächlichen Bedrohung zu entwickeln.

Anhand von 115 gravierenden Fällen des Diebstahls vertraulicher Kunden- und Unternehmensdaten, von denen uns die befragten Unternehmen berichteten, können wir die vermuteten und tatsächlichen Risiken miteinander vergleichen. Das Ergebnis: Die Gefahr einer Cyber-Attacke wird eher überbewertet. Denn der Vergleich zeigt: Das konventionelle Kopieren und Entwenden von Firmenunterlagen kommt viel häufiger vor.

Es sind nicht nur Hacker, die von einem beliebigen Ort auf der Welt ins Firmennetzwerk eindringen, sondern weitaus häufiger die eigenen Mitarbeiter, durch die Daten in unbefugte Hände gelangen. Unternehmen sehen sich heute also einer doppelten Herausforderung gegenüber: Sie dürfen keinesfalls konventionelle Risiken vernachlässigen und müssen sich zusätzlich der wachsenden Gefahr der Cyberspionage stellen.

Typische Angriffsvektoren und Risiken des Daten- und Wissensverlusts

Moderne Informationstechnologien erlauben es, Geschäftsprozesse heute mit sehr viel höherer Effizienz abzuwickeln, allerdings nutzen auch Straftäter ihre Vorteile. Cyberspionage gehört zu unserer Realität. Staaten wie auch Wettbewerber suchen auf allen ihnen zur Verfügung stehenden Wegen nach dem Informationsvorteil und auch die OK hat Cybercrime als einträgliches Geschäftsfeld für sich entdeckt, wie auch das BSI in seinem Lagebericht 2015 betont.[20]

Unternehmen mit intensiver Forschungs- und Entwicklungsarbeit schätzen die Risiken, von einem Diebstahl vertraulicher Kunden- und Unternehmensdaten sowie Industrie- und Wirtschaftsspionage betroffen zu werden, verständlicherweise deutlich höher ein als andere Unternehmen.[21] Sie sehen etwa doppelt so häufig mittlere bis hohe Risiken für gezielte Mitarbeiterbeeinflussung auf Messen (58 % vs. 30 %), Angriffe auf die Cloud (40 % vs. 21 %), Abhören von Telefonen, Abfangen von E-Mails (44 % vs. 24 %) und Abhören von Besprechungen und Geschäftsräumen (16 % vs. 8 %).

Die höchsten Risiken erblicken beide Unternehmensgruppen in Angriffen auf mobile IT-Systeme wie Mobiltelefone (71 % vs. 47 %) und im Abwerben von Mitarbeitern (68 % vs. 49 %). Demgegenüber wird das Risiko von Angriffen auf stationäre IT-Geräte deutlich geringer eingeschätzt (42 % vs. 33 %).

Die Risikobewertungen der Unternehmen zeigen auch, dass neben den Risiken infolge von Angriffen auf digitale Informations- und Kommunikationstechnologien auch herkömmliche Risiken nicht unterschätzt werden sollten, wie gezielte Beeinflussung von Mitarbeitern auf Messen oder Tagungen und gezielte Abwerbung. Auch sehen Unternehmen Risiken im Publizieren von Forschungsergebnissen und anderen sensiblen Geschäftsinformationen in öffentlich zugänglichen Quellen wie Verbands- und Fachzeitschriften oder auch in Social Media.

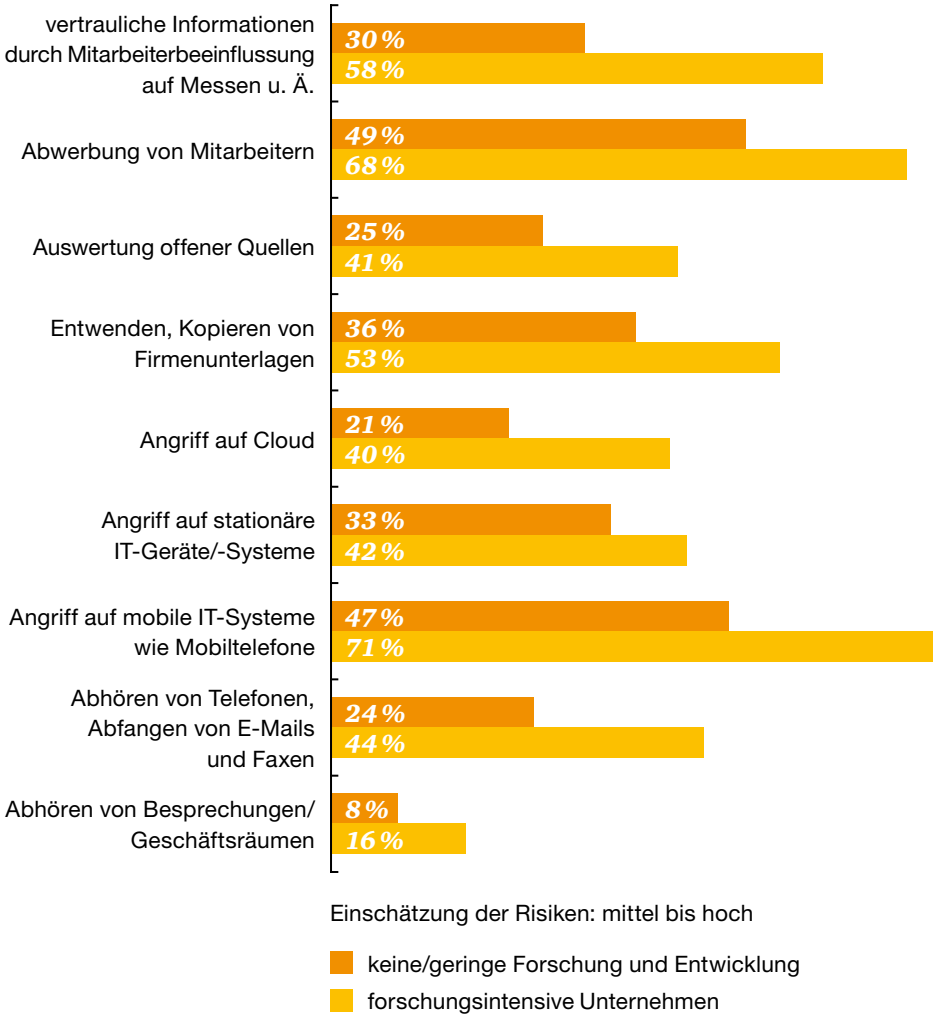
Wir meinen, Unternehmen werden ihre Mitarbeiter nachhaltig dafür sensibilisieren müssen, dass generell jede Kommunikation das Risiko eines Daten- und Wissensverlusts erhöht. Informationen sind immer schneller und leichter verfügbar. Offenheit und Transparenz finden sich als Werte in vielen Unternehmensleitbildern.

Es wird daher eine der wesentlichen Aufgaben für Unternehmen sein, die richtige Balance zwischen einer offenen Kommunikationskultur und dem berechtigten Interesse am Schutz des geistigen Eigentums zu finden und diese den Mitarbeitern zu vermitteln.

[20] Vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2015, S. 36.
[21] In der Studie gaben 37 % der Unternehmen an, dass sie viel Forschung und Entwicklung betreiben.

Abb. 16 Typische Angriffsvektoren und Risiken des Daten- und Wissensverlusts

Mehrfachnennungen waren möglich.



Basis: alle befragten Unternehmen

Kaum überraschend: Forschungsintensive Unternehmen schätzen die Risiken, von einem Diebstahl vertraulicher Kunden- und Unternehmensdaten sowie Industrie- und Wirtschaftsspionage betroffen zu werden, deutlich höher ein als andere Unternehmen.

Vergleich von vermuteten und tatsächlichen Risiken

Im Rahmen unserer Studie haben wir des Weiteren untersucht, wie sich die vermuteten zu den tatsächlichen Risiken verhalten. Anhand von 115 berichteten gravierenden Fällen eines Diebstahls vertraulicher Kunden- und Unternehmensdaten bzw. von Industrie- und Wirtschaftsspionage können wir die eingeschätzten mit den tatsächlichen Risiken vergleichen.[22]

Es zeigt sich, dass sowohl forschungsintensive Unternehmen als auch Unternehmen mit keiner oder geringer Forschung und Entwicklung die tatsächlichen Risiken teilweise nicht zutreffend einschätzen. Die berichteten Fälle eines Daten- und Wissensverlusts erfolgten entgegen der Risikoeinschätzung vornehmlich durch Entwenden und Kopieren von Firmenunterlagen (42 %).[23]

Generell offenbart der Vergleich, dass herkömmliche Begehungsformen weiterhin ein nennenswertes Risiko darstellen. Etwa jeder zehnte Fall von Daten- und Wissensverlust beruht auf einem Wechsel von Mitarbeitern zu anderen Unternehmen oder auf einer gezielten vertraulichen Mitarbeiterbeeinflussung auf Messen etc.

Neben diesen eher klassisch zu nennenden Risiken sind Unternehmen verschiedenen Formen der Cyberspionage ausgesetzt. Allerdings erfolgten die Angriffe entgegen der Einschätzung der befragten Unternehmen tatsächlich seltener als angenommen. 20 % der berichteten Fälle richteten sich auf stationäre und noch seltener auf mobile IT-Systeme (10 %). Und nur 2 % der Unternehmen berichteten über Angriffe auf die Cloud.[24]

Diese Ergebnisse rechtfertigen keine Vernachlässigung des Schutzes vor Angriffen auf die Kommunikations- und Informationstechnologien. Vielmehr sehen sich Unternehmen heute einer doppelten Herausforderung gegenübergestellt: Sie dürfen keinesfalls die konventionellen Risiken in den Bereichen Personal und Geschäftsablauf vernachlässigen und müssen sich aufgrund der sich verändernden Geschäftswelt zugleich den wachsenden Risiken der Cyberspionage stellen.

Die folgende Abbildung gibt neben den tatsächlichen Risiken auf Basis der berichteten Fälle auch die vermuteten Risiken aller befragten Unternehmen (Risikoeinschätzung) wieder:

[22] Insgesamt wurden von den Unternehmen 291 gravierende Schadensfälle genannt.

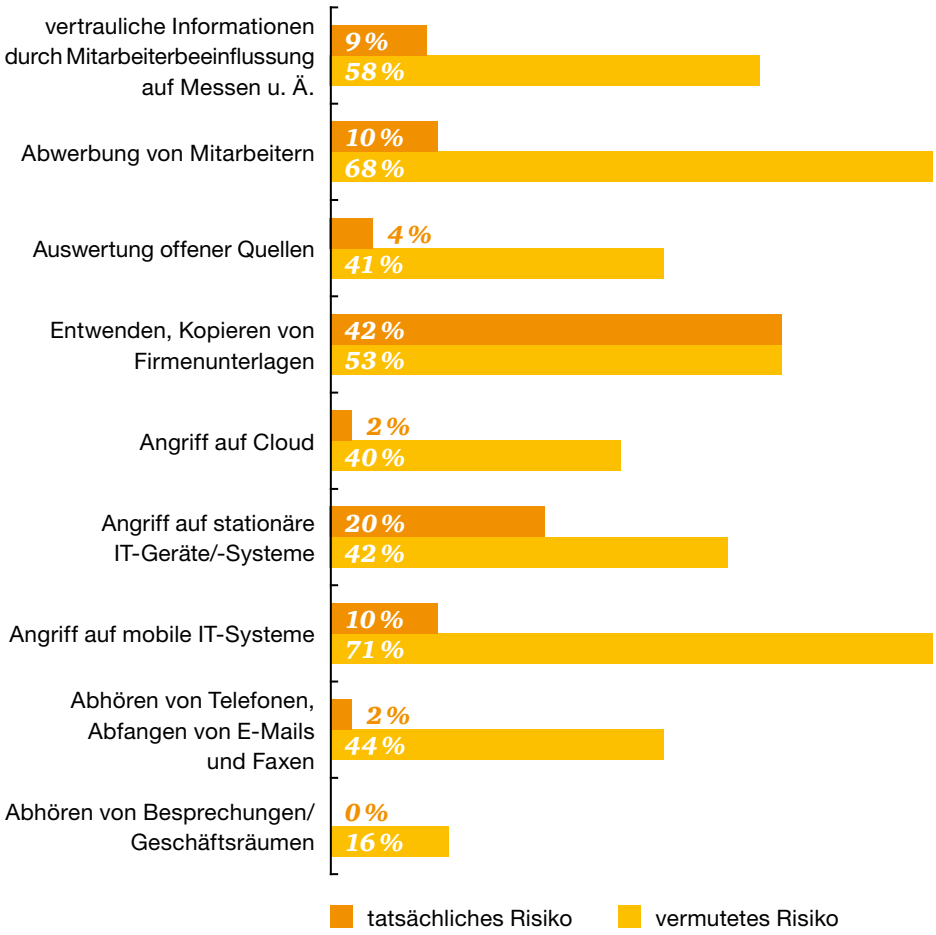
[23] Unerlaubte digitale Kopien können auch mittels USB-Sticks oder anderer Datenträger gezogen werden. Es handelt sich hierbei allerdings nicht um Fälle von Cybercrime, da das Kopieren auf digitale Datenträger nur durch bloße Nutzung und nicht durch gezielte Ausnutzung elektronischer Systeme erfolgt (zur Definition S. 19).

[24] Den Risiken des Cloud Computing haben wir uns bereits in der Studie von 2013 ausführlicher gewidmet, vgl. PwC, Wirtschaftskriminalität und Unternehmenskultur 2013, S. 19 ff.

Mobile IT-Systeme gelten als größte Schwachstelle im Hinblick auf das Risiko von Daten- und Wissensverlust. Doch tatsächlich kommt es viel häufiger vor, dass Firmenunterlagen einfach entwendet werden.

Abb. 17 Vermutete und tatsächliche Risiken des Daten- und Wissensverlusts (alle Unternehmen)

Mehrfachnennungen waren möglich.



Basis „vermutetes Risiko“: alle Unternehmen
Basis „tatsächliches Risiko“: alle berichteten Fälle von Daten- und Wissensverlust

Bei Cyber-Attacken haben es Unternehmen oft mit OK zu tun.

Bedrohung durch OK

Grundsätzlich wird Wirtschaftskriminalität eher von internen Tätern begangen (51 %), teilweise zusammen mit externen (12 %). Dies gilt grundsätzlich auch für Fälle von Industrie- und Wirtschaftsspionage oder Diebstahl vertraulicher Kunden- und Unternehmensdaten (Daten- und Wissensverlust),[25] aber der Anteil externer Täter ist hier deutlich höher (40 %). Bei diesen Deliktsgruppen liegt eine ausgeglichene Verteilung zwischen internen und externen Tätern vor. Für Unternehmen bedeutet dies, dass die Risiken eines Daten- und Wissensverlusts nicht primär von außen kommen, sondern von innen und außen gleichermaßen.

Innerhalb der Gruppe der externen Täter drohen Unternehmen seltener von Kunden (7 %) Angriffe auf ihr Know-how und ihre sensiblen Daten. Die größten Risiken gehen von den externen Tätern ohne Geschäftsbeziehung zum Unternehmen (63 %) aus.

Bemerkenswert ist des Weiteren, dass ein relativ hoher Anteil der Delikte von den betroffenen Unternehmen auf Aktivitäten der OK zurückgeführt wird. Diese Bedrohung besteht nach den Erfahrungen der Unternehmen mit Blick auf Daten- und Wissensverlust wie auch für alle anderen Wirtschaftsdelikte gleichermaßen (30 % bzw. 27 %). Diese Ergebnisse decken sich mit unserer Analyse des OK-Bedrohungspotenzials (siehe hierzu ausführlich Seite 27). Das BKA warnt in seinem Bundeslagebild ebenfalls vor der Bedrohung der Wirtschaft durch OK:

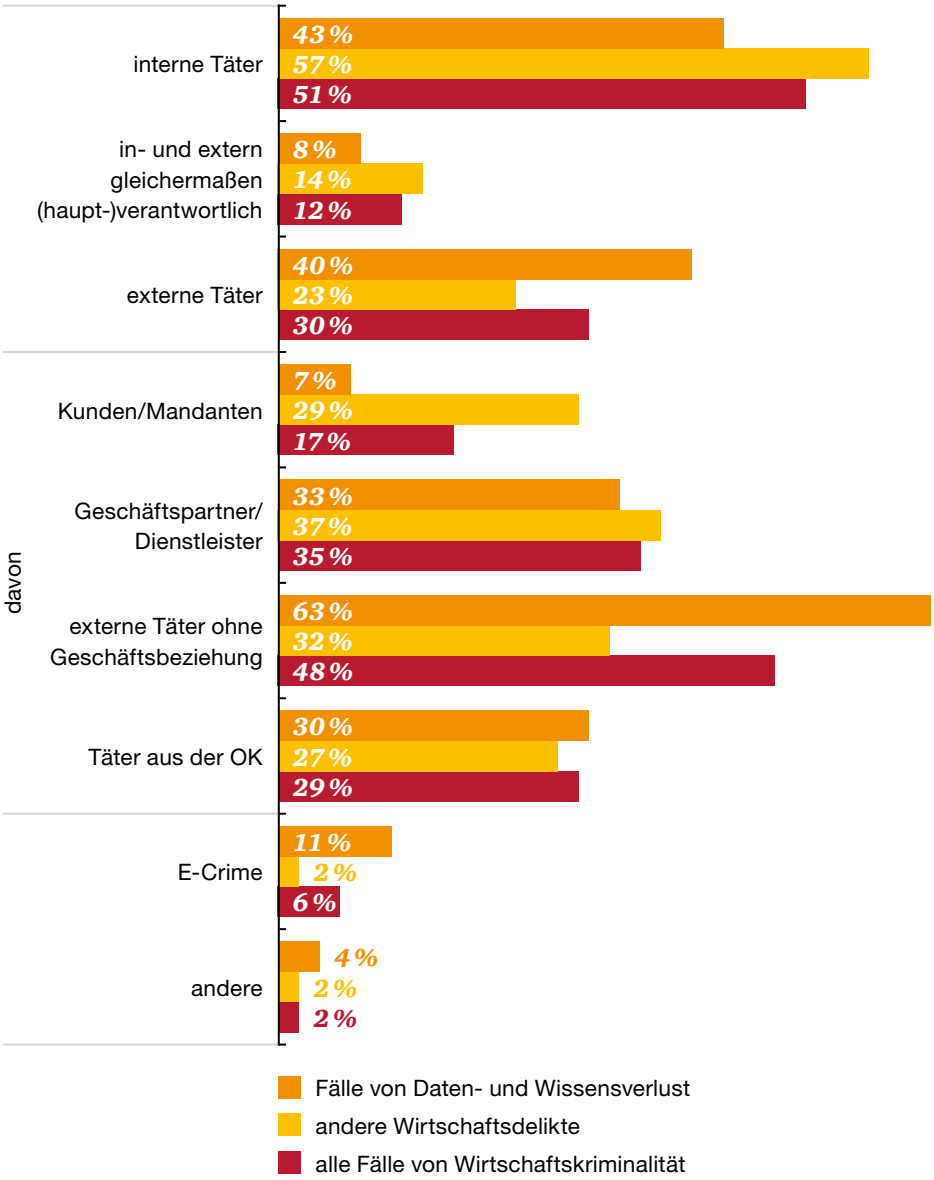
„Bezüglich der Kriminalität i. Z. m. dem Wirtschaftsleben wurden im Berichtsjahr 73 OK-Verfahren geführt (2013: 76). Somit nahm der Bereich unter den Hauptaktivitätsfeldern der OK weiterhin den dritten Rang ein. […] Gemessen an der Gesamtschadenssumme aller OK-Verfahren war der durch Wirtschaftskriminalität verursachte Schaden sehr hoch.“[26]

[25] Von den Unternehmen wurden 291 gravierende Schadensfälle genannt, dabei handelte es sich bei 40 % der Fälle um Daten- und Wissensverlust infolge von Industrie- und Wirtschaftsspionage oder Diebstahl vertraulicher Kunden- und Unternehmensdaten (n = 115, analog oder digital).

[26] Vgl. BKA, Bundeslagebild Organisierte Kriminalität, 2014, S. 25.

Abb. 18 Beziehung der Täter zum geschädigten Unternehmen

Mehrfachnennungen waren möglich.



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

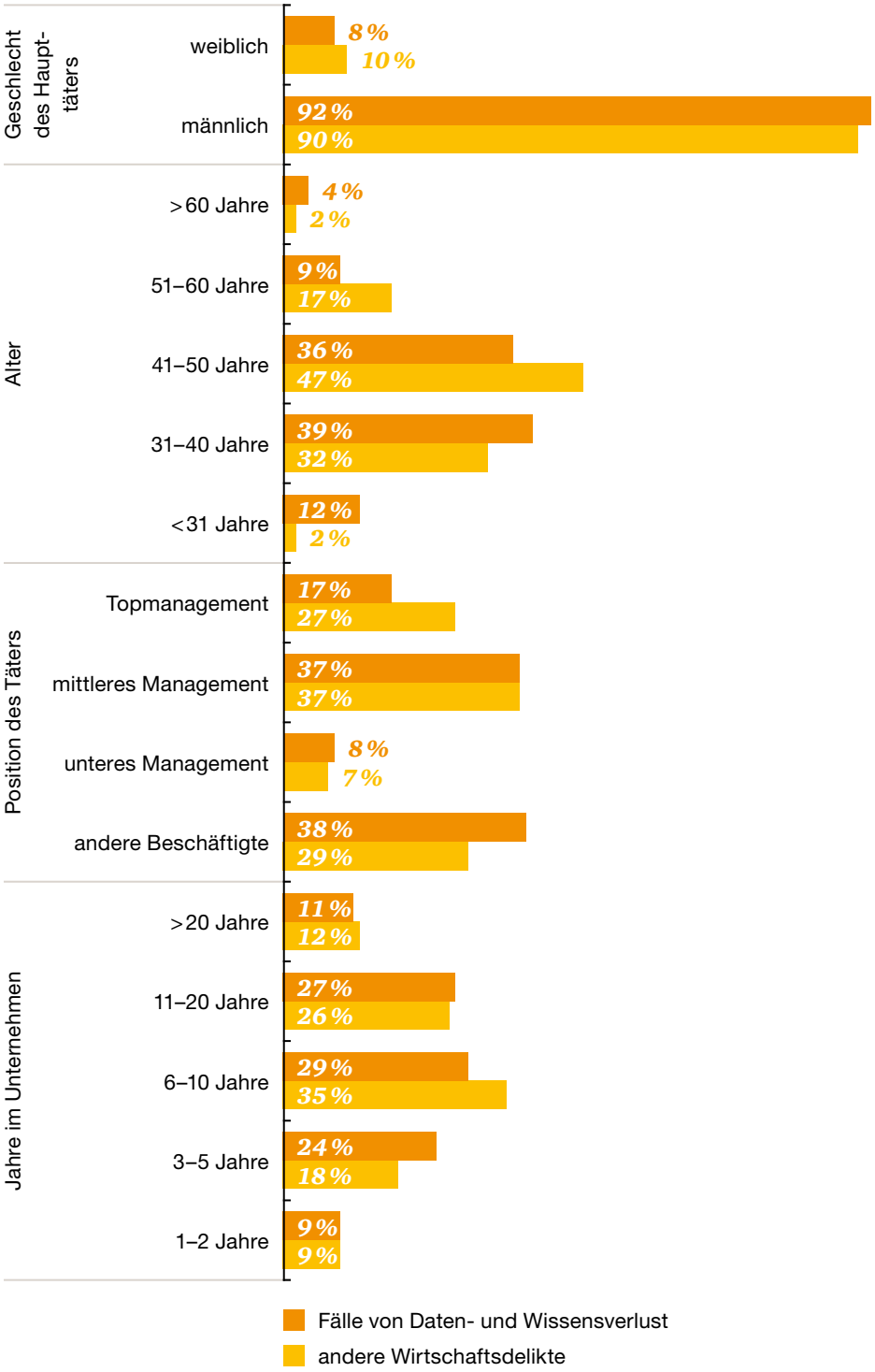
Profil von Tätern im Bereich Daten- und Wissensverlust und bei anderen Wirtschaftsdelikten

Vergleichen wir die Täterprofile bei Fällen von Daten- und Wissensverlust und anderen Wirtschaftsdelikten, so zeigen sich Parallelen: Die Täter sind überwiegend männlich, eher mittleren Alters und weisen einen relativ hohen Anteil an Senior- und Topmanagern (17 % bzw. 27%) sowie Managern aus dem mittleren Management (37 %) auf. In der Regel sind sie schon seit einigen Jahren im Unternehmen beschäftigt.

Allerdings gehören Täter von Straftaten, die zu Daten- und Wissensverlust führen, etwas häufiger jüngeren Altersgruppen an als Täter im Bereich anderer Wirtschaftsdelikte; hinsichtlich ihres Durchschnittsalters ähneln sich beide Gruppen wiederum (45 bzw. 43 Jahre). Die Profile beider Gruppen unterscheiden sich somit kaum.

Für den Schutz von sensiblen Daten und Know-how bedeuten unsere Ergebnisse, dass es keinen Grund für einen besonderen Vertrauensbonus etwa aufgrund der Position oder langjährigen Betriebszugehörigkeit gibt. Maßnahmen zur Prävention gegen Daten- und Wissensverlust haben sich grundsätzlich auf alle Mitarbeiter- und Managerebenen zu erstrecken.

Abb. 19 Profil der Täter von gravierenden Wirtschaftsdelikten im Vergleich



Basis: Anteil an den berichteten Fällen

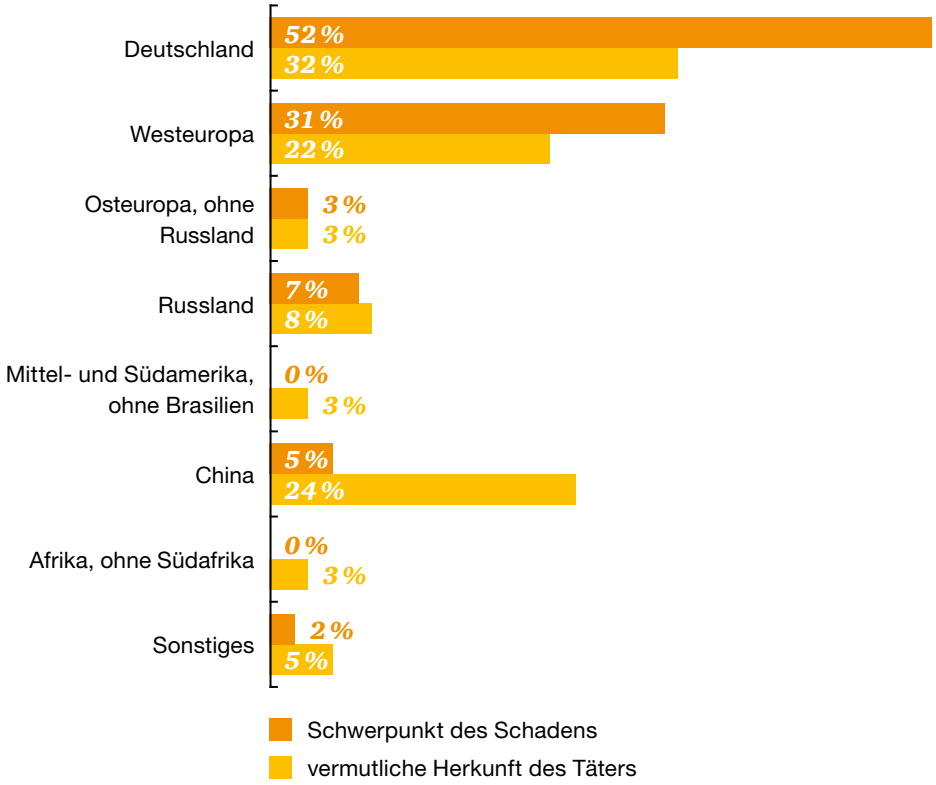
Näher als man denkt – regionale Risiken

Aus den Berichten von Unternehmen mit Auslandsvertretungen über tatsächliche Fälle eines Daten- und Wissensverlusts ergibt sich, dass der Schwerpunkt des Schadens in Deutschland (52 %) und in den Niederlassungen bzw. den Hauptsitzen[27] in Westeuropa (31 %) lag. Die höchsten Risiken eines Daten- und Wissensverlusts drohen Unternehmen somit primär im Heimatland. Eine Erklärung hierfür ist, dass Forschung und Entwicklung weniger in den Emerging Markets betrieben wird als vielmehr in den westlichen Industrieländern. Die „intellektuellen Kronjuwelen" der Unternehmen liegen hier.

Betrachtet man das Täterprofil, so stammt rund die Hälfte der externen Täter (vermutlich) aus Deutschland oder Westeuropa (zusammen 54 %). Etwa ein Viertel der externen Täter war chinesischer Herkunft (24 %) und die verbleibenden kamen aus Russland und anderen Ländern bzw. Regionen. Allerdings ist einschränkend anzumerken, dass viele Unternehmen den Ursprung eines Angriffs nicht kennen, sodass unsere Ergebnisse hinsichtlich der Tätermerkmale nur eine Annäherung an die Wirklichkeit darstellen.

Unsere Ergebnisse decken sich weitgehend mit den Erkenntnissen des BKA zur OK im Zusammenhang mit dem Wirtschaftsleben, so die Bezeichnung des BKA. Laut der Behörde handelt es sich nicht – wie vielfach fälschlicherweise angenommen – überwiegend um ausländische Täter, sondern bei jedem zweiten um einen deutschen Staatsangehörigen.[28] Die OK-Risiken mögen außerhalb Deutschlands sehr viel höher sein, sollten aber auch in Deutschland nicht unterschätzt werden. Dies gilt insbesondere für die Aktivitäten der OK im Bereich Cybercrime, wie wir oben bereits erläutert haben (siehe Seite 27).

Abb. 20 Schadensschwerpunkt und Herkunft externer Täter tatsächlicher Fälle von Daten- und Wissensverlust



Basis: alle berichteten Fälle von Daten- und Wissensverlust von Unternehmen mit Auslandsvertretungen (nur externe Täter)

[27] Die Studie beschränkt sich zwar auf Unternehmen in Deutschland, dies schließt aber auch ausländische Tochtergesellschaften mit ein, die ihren Hauptsitz außerhalb Deutschlands haben.
[28] Vgl. BKA, Bundeslagebild Organisierte Kriminalität, 2014, S. 25.

Erstentdeckung und Speak-up-Kultur

Wie sehr die Kriminalprävention von der Bereitschaft zur informellen Sozialkontrolle abhängt, zeigt unsere Studie sowohl für Fälle von Daten- und Wissensverlust als auch für andere Wirtschaftsdelikte. Bei mehr als jedem dritten Fall erfolgte die Erstaufdeckung durch einen internen Hinweis (35 % bzw. 39 %). Externe Hinweise sind die zweithäufigste Quelle von Informationen, die zur Aufdeckung führen.

Die informelle Sozialkontrolle besitzt in Unternehmen wie auch allgemein in der Gesellschaft eine zentrale kriminalpräventive Funktion.[29] In Studien zum Unternehmensalltag zeigte sich außerdem, dass die stärkste Abschreckungswirkung von der Erwartung informeller Sanktionen durch die Arbeitsgruppenmitglieder ausgeht. Demnach hängt die Gesetzes- und Richtlinientreue zu einem großen Teil von der Missbilligung der Mitarbeiter und ihrer informellen Sozialkontrolle ab.[30]

Durch eine integritätsförderliche Unternehmenskultur kann die Bereitschaft der Mitarbeiter erhöht werden, Kollegen auf mögliches Fehlverhalten und Compliance-Verstöße anzusprechen und dem Unternehmen gegebenenfalls einen Hinweis zu geben. Eine Speak-up-Kultur ist für den Erfolg des Compliance-Managements essenziell.[31]

Eine weitere wichtige Quelle für Informationen sind Hinweisgebersysteme, die zwar noch von relativ geringer Bedeutung sind, aber im Vergleich etwa zur internen Revision kaum seltener zur Aufdeckung beitragen und vor allem für gravierende Compliance-Verstöße von Bedeutung sind. Ihre Relevanz lässt sich daher nur bedingt an ihrer selteneren Inanspruchnahme ablesen. Zur Erhöhung ihres Beitrags zur Aufklärung bedürfen diese Systeme einer positiven Hinweisgeberkultur, in der potenzielle Hinweisgeber keine beruflichen und sozialen Nachteile befürchten müssen.

Den eigenen Mitarbeitern kommt bei der Kriminalprävention eine entscheidende Rolle zu: Mindestens jede dritte Tat wird durch einen internen Hinweis aufgedeckt.

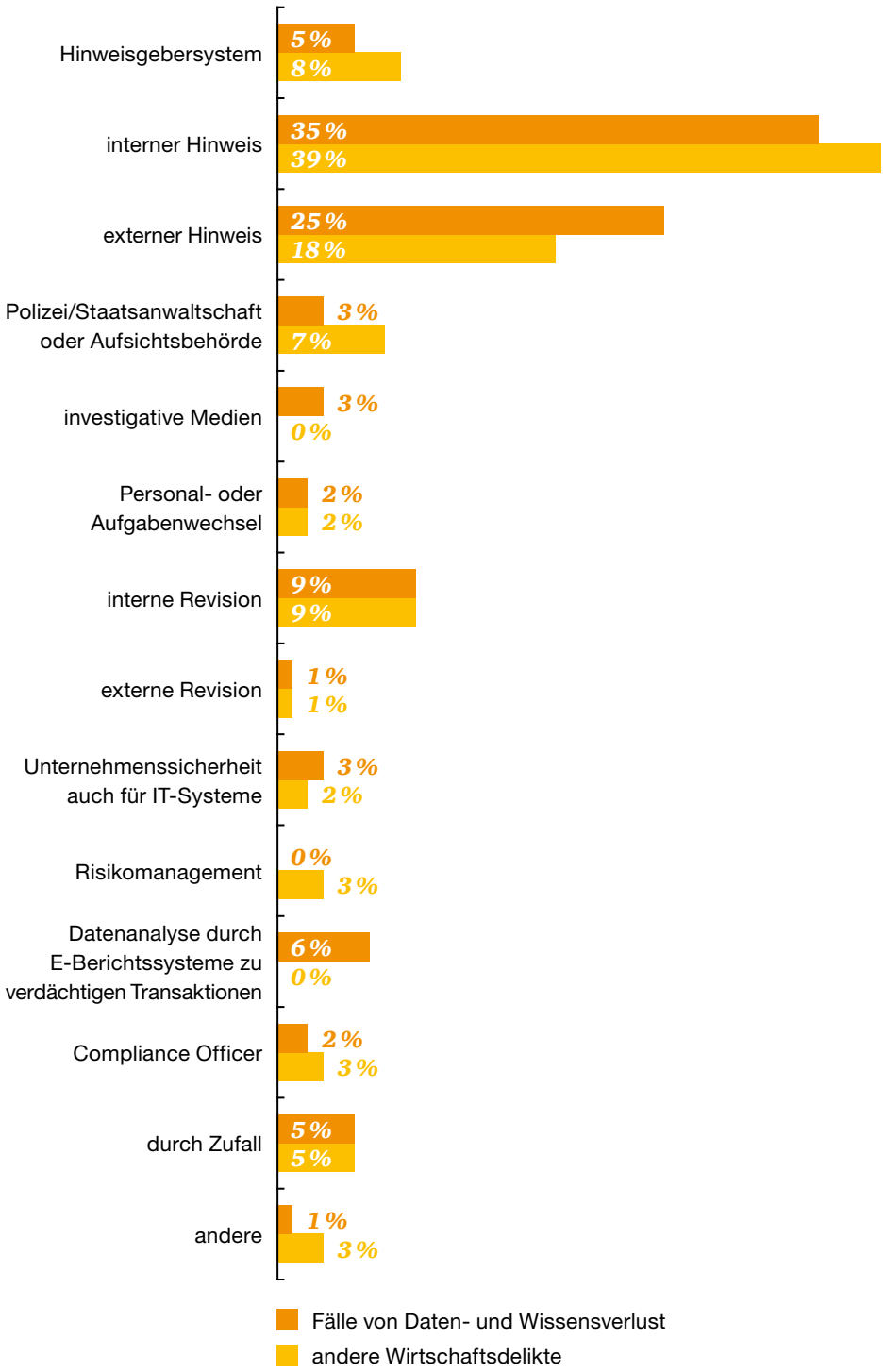
[29] Zur informellen Sozialkontrolle ausführlich Bussmann, Wirtschaftskriminologie Band I, 2015, Rn. 941 ff.
[30] Vgl. Trevino, The Social Effects of Punishment in Organizations. A Justice Perspective. Academy of Management Review, Vol. 17 (1992), 647–676 (652 f.).
[31] Vgl. Bussmann, Integrität durch nachhaltiges Compliance-Management. Über Risiken, Werte und Unternehmenskultur, in: CCZ 2/2016, 50–57.

Eine Speak-up-Kultur ist essenziell für den Erfolg des Compliance-Managements. Das bedeutet Kolleginnen und Kollegen auf Verstöße anzusprechen und gegebenenfalls das Unternehmen zu informieren.

Alle internen Kontrollmaßnahmen zusammen gesehen tragen ebenfalls maßgeblich zur Aufdeckung von Daten- und Wissensverlust bei. Etwa jeder fünfte dieser Fälle wurde durch die interne Revision, die Unternehmenssicherheit (auch für IT-Systeme) sowie durch elektronische Datenanalysen und Berichtssysteme aufgedeckt (insgesamt 18 %). In anderen Fällen von Wirtschaftskriminalität erfolgte die Aufdeckung in etwa jedem zehnten Fall durch die genannten internen Kontrollmaßnahmen.

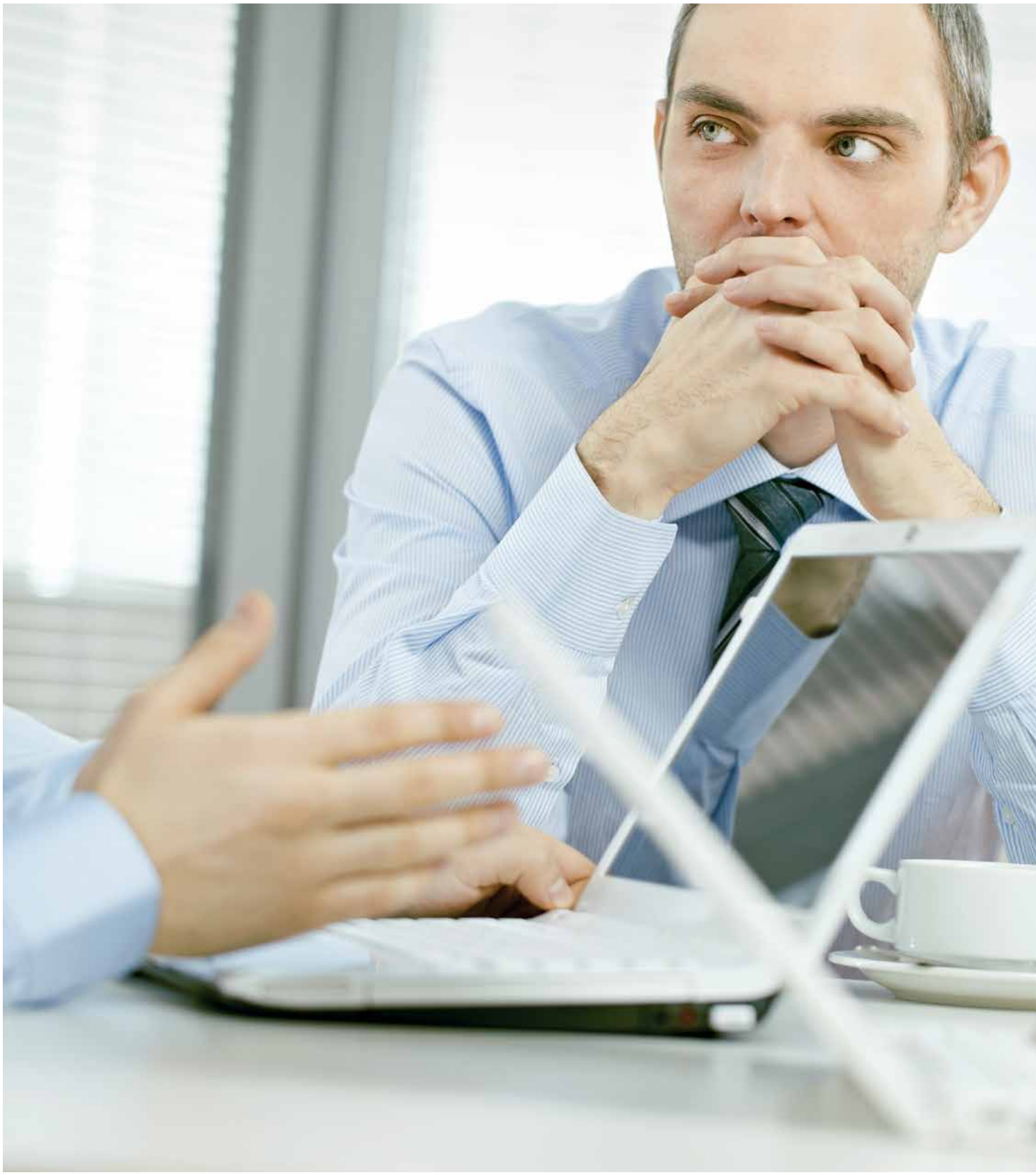
Investigative Medien und Strafverfolgungsbehörden sind demgegenüber von nachrangiger Bedeutung, wobei wir darauf hinweisen, dass gerade spektakuläre Fälle durch diese Instanzen aufgedeckt werden – aus unserer Sicht ein starkes Argument für die Einführung eines Hinweisgebersystems im Unternehmen.

Abb. 21 Gründe für die Erstentdeckung von Delikten im Vergleich



Basis: Anteil an den berichteten Fällen

Unternehmen der kritischen Infrastruktur



Seit Juli 2015 gilt für Unternehmen der kritischen Infrastruktur das IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) zur Aufrechterhaltung der öffentlichen Versorgung und Sicherheit. Es verpflichtet diese Unternehmen zu Sicherheitsstandards und trifft trotz des damit verbundenen administrativen Aufwands auf breite Zustimmung. Auch Unternehmen, die davon nicht betroffen sind, schätzen die gesetzlichen Vorgaben als Orientierung.

Inzwischen verfügen bereits drei Viertel der Unternehmen, die nach eigener Einschätzung unter das IT-Sicherheitsgesetz fallen, über ein internes Sicherheitsmanagement. Ein Penetration-Testing ist mit 53 % weit verbreitet. Doch nur eine Minderheit lässt das IT-Risk-Management im Rahmen einer Zertifizierung von externen Fachleuten überprüfen. Das birgt die Gefahr, dass Unternehmen Schwachstellen übersehen und sich in trügerischer Sicherheit wiegen.

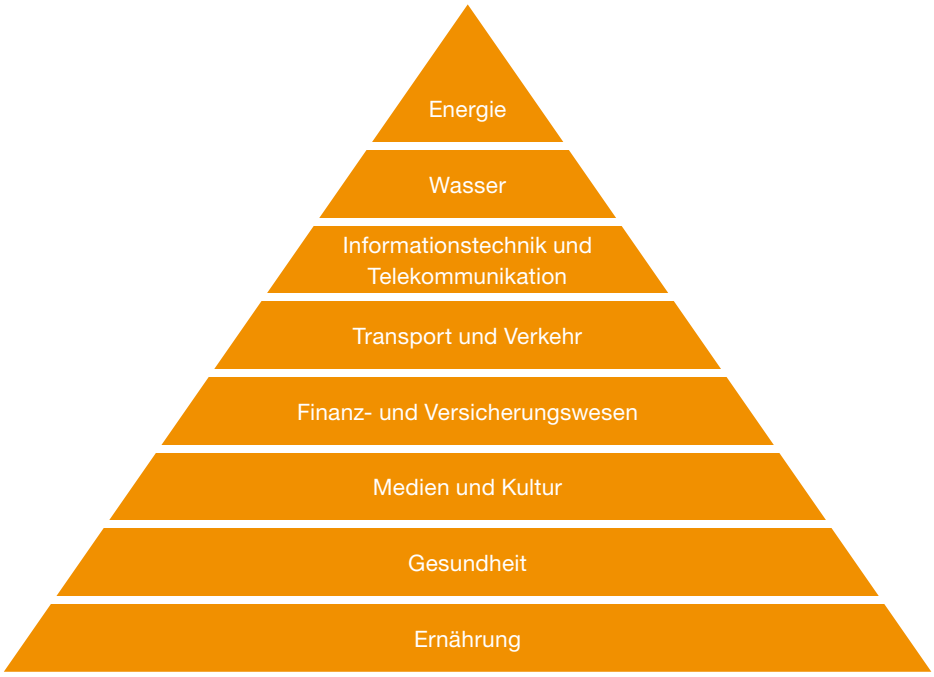
Hochkomplexe Industrienationen sind im Besonderen auf eine funktionierende Informations- und Kommunikationstechnik angewiesen. Unternehmen dieser Branchen müssen sich besonders vorsehen.

Betroffenheit vom IT-Sicherheitsgesetz

Nach dem seit Juli 2015 geltenden *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme* – kurz: IT-Sicherheitsgesetz – gehören Unternehmen zur kritischen Infrastruktur (KRITIS), wenn durch Ausfall oder Beeinträchtigung der von ihnen eingesetzten Informations- und Kommunikationstechnik erhebliche Versorgungsengpässe oder Gefährdungen der öffentlichen Sicherheit eintreten würden. Infolge der Finanz- und Warenströme zwischen den einzelnen Wirtschaftssektoren und Unternehmen beispielsweise in der Lieferkette besitzt ein erfolgreicher Angriff auf ein Unternehmen der KRITIS ein exponentielles Schadenspotenzial für Wirtschaft und Gesellschaft, das weit über das direkt betroffene Unternehmen hinausgeht.[32]

Für das Funktionieren hochkomplexer Industrienationen ist daher der Schutz der Informations- und Kommunikationstechnik auch von privaten Unternehmen, soweit sie zur KRITIS zu zählen sind, von besonderer Wichtigkeit. Zur KRITIS gehören gemäß § 2 Abs. 10 Nr. 1 BSIG[33] folgende Sektoren:

Abb. 22 Sektoren der KRITIS

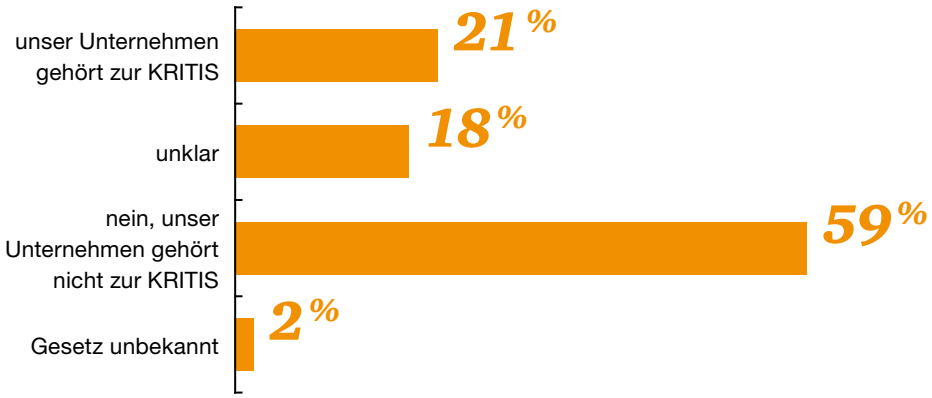


[32] Vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2015, Bonn, S. 40 ff.
[33] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik.

In einer Rechtsverordnung sollen der Anwendungsbereich präzisiert und die Betreiber kritischer Infrastrukturen benannt werden. Wir haben erhoben, welche Unternehmen nach eigener Einschätzung vom IT-Sicherheitsgesetz betroffen sein werden und wie sie das Gesetz beurteilen.

Das IT-Sicherheitsgesetz war nahezu allen Befragten bekannt (98 %) und jedes fünfte Unternehmen geht davon aus, dass es selbst zur KRITIS im Sinne des Gesetzes zu zählen ist (21 %). 18 % der Unternehmen sind sich unsicher, ob sie dem Gesetz unterliegen. Dies dürfte auch darauf beruhen, dass der Kreis der betroffenen Unternehmen erst noch in einer Rechtsverordnung bestimmt werden soll (§ 10 Abs. 1 BSIG).

Abb. 23 Einschätzung der Zugehörigkeit zur KRITIS



Beurteilung der Unternehmen
Basis: alle befragten Unternehmen

98 % *der befragten Unternehmen ist das IT-Sicherheitsgesetz bekannt, jedes fünfte (21 %) zählt sich zu den Unternehmen der KRITIS.*

Überwiegende Befürwortung des IT-Sicherheitsgesetzes

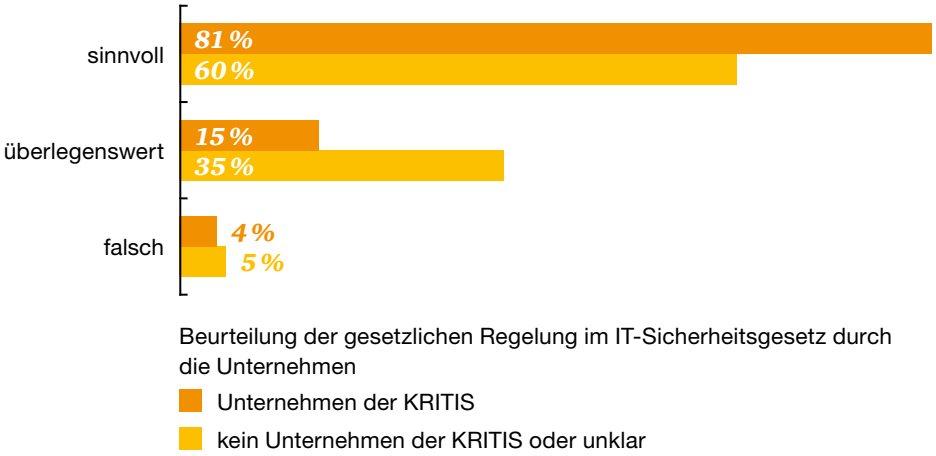
Das IT-Sicherheitsgesetz sieht weitreichende Kompetenzen für das zuständige Bundesamt – das BSI – vor. Betreiber kritischer Infrastrukturen müssen dem BSI mindestens alle zwei Jahre insbesondere die Einhaltung der IT-Sicherheit nach dem Stand der Technik nachweisen (§ 8a Abs. 1 und § 3 BSIG). Das BSI kann im Falle von Sicherheitsmängeln im Einvernehmen mit Aufsichtsbehörden ihre Beseitigung anordnen (§ 8a Abs. 3 BSIG).

Die Rechtsreform verfolgt dabei einen kooperativen Ansatz: Die Branchenverbände können dem BSI branchenspezifische Sicherheitsstandards vorschlagen (§ 8a Abs. 2 BSIG). Das Gesetz sieht somit vor, dass Betreiber kritischer Infrastrukturen ein mit Branchenverbänden abgestimmtes Mindestniveau an IT-Sicherheit einzuhalten haben.

Angesichts der bisher überwiegend kritischen öffentlichen Diskussion haben wir eine geringe Zustimmung zum IT-Sicherheitsgesetz erwartet. Immerhin wird durch die Erweiterung der Rechtsbefugnisse für das BSI in die Privatautonomie von Unternehmen eingegriffen.

Unsere Studie zeigt jedoch, dass die Regelung vor allem von den voraussichtlich vom Gesetz betroffenen Unternehmen, die sich zur KRITIS zählen, angesichts der wachsenden Cybercrime-Bedrohung für sinnvoll erachtet wird (81 %). Nur 4 % lehnen die Reform ab. Man hat wohl überwiegend verstanden, dass Stör- und Ausfälle bei Betreibern kritischer Infrastrukturen aufgrund ihrer Verzahnung etwa in Lieferketten ein erhebliches Bedrohungspotenzial für alle Unternehmen bergen.

Abb. 24 Gesetzliche Regelung von IT-Sicherheitsstandards für Betreiber der KRITIS in Abstimmung mit Branchenverbänden



Vier von fünf Unternehmen der KRITIS halten das IT-Sicherheitsgesetz für sinnvoll, nur 4 % lehnen die Reform ab.

Das IT-Sicherheitsgesetz verpflichtet Betreiber kritischer Infrastrukturen, dem BSI erhebliche Störungen ihrer informationstechnischen Systeme zu melden (§ 8b Abs. 4 BSIG). Eine Unternehmensbefragung der Industrie- und Handelskammer Nord im Jahr 2013 ergab, dass nur etwa 13 % der betroffenen Unternehmen Cyberattacken an Strafverfolgungs- und Aufsichtsbehörden melden, da Zweifel an Ermittlungserfolgen bestehen und der bürokratische Meldeaufwand als zu hoch empfunden wird.[34] Die Bereitschaft, IT-Sicherheitsvorfälle zu melden, ist bei Unternehmen im Allgemeinen eher gering, da sie auch Reputationsschäden und Wettbewerbsnachteile befürchten.

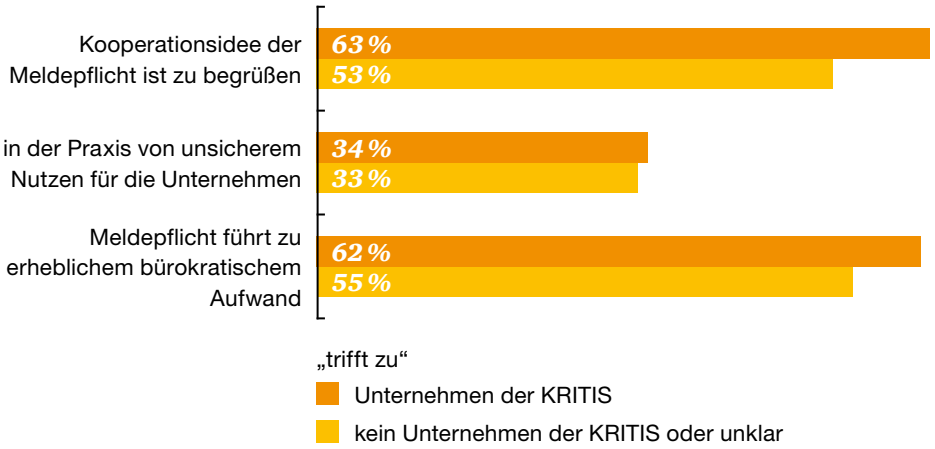
Das IT-Sicherheitsgesetz beschränkt sich nicht nur auf eine gesetzliche Meldepflicht, sondern bietet zugleich einen Anreiz zur Meldung von IT-Sicherheitsvorfällen. Das BSI sammelt und bewertet die aus den Vorfällen stammenden relevanten Informationen und leitet diese auch an die Betreiber kritischer Infrastrukturen weiter. Auf diese Weise können Erkenntnisse über aufgetretene Sicherheitslücken und Schadprogramme anderen Unternehmen zur Verbesserung ihrer IT-Prävention zur Verfügung gestellt werden.

Unternehmen sollen so von Störfällen anderer Unternehmen lernen und ihre IT-Sicherheitstechnik auf dem neuesten Stand halten können. Fast zwei Drittel der Unternehmen (63 %), die sich zur KRITIS zählen, begrüßen diese Kooperationsidee grundsätzlich.

Allerdings zweifelt ein Drittel (34 %) am Nutzen in der Praxis. Auch befürchten rund zwei Drittel der Betreiber kritischer Infrastrukturen (62 %) einen erheblichen bürokratischen Mehraufwand. Zwei Drittel dieser Unternehmen begegnen den Regelungen im IT-Sicherheitsgesetz also mit gemischten Gefühlen. Die Kooperationsidee wird sich in der Praxis noch bewähren müssen.

Abb. 25 Beurteilung der gesetzlichen Meldepflicht von erheblichen IT-Sicherheitsvorfällen

Mehrfachnennungen waren möglich.



[34] Vgl. Industrie und Handelskammer Nord, online abrufbar unter: www.ihk-nord.de → Presse → 20.06.2013; Cybercrime ist ein zunehmendes Risiko für norddeutsche Wirtschaft → mehr → Umfrage Cybercrime in der norddeutschen Wirtschaft → S. 10.

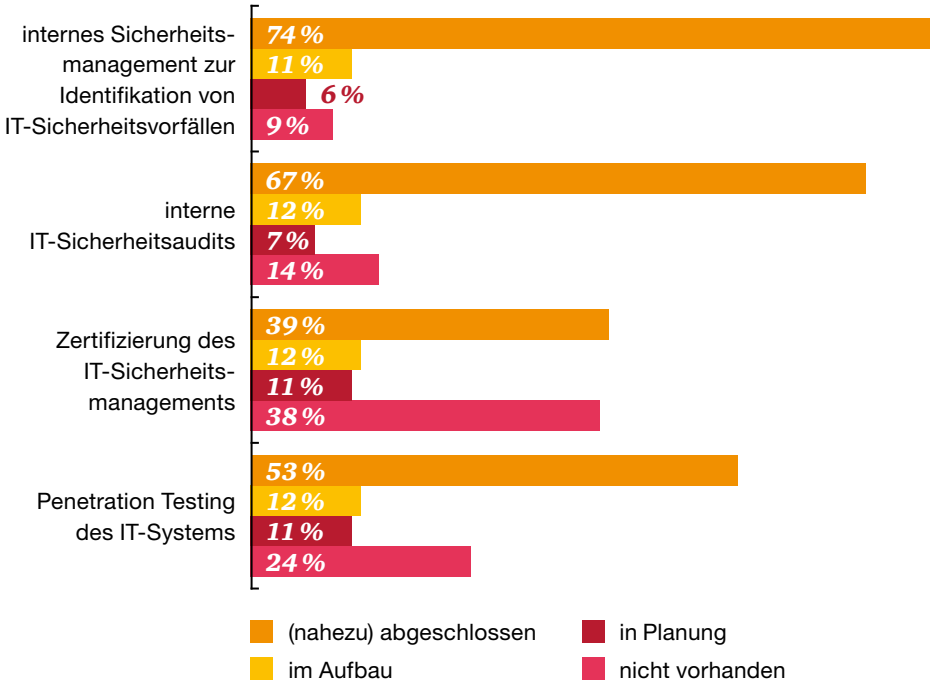
IT-Risk-Management

Nach den Angaben aller befragten Unternehmen verfügen drei Viertel über ein internes Sicherheitsmanagement zur Identifikation von IT-Sicherheitsvorfällen und 67 % führen interne Sicherheitsaudits durch. Unsere Erfahrungen lassen uns an einer derart weiten Verbreitung von IT-Sicherheitsmaßnahmen zweifeln. Immerhin sah offenbar auch der Gesetzgeber einen erheblich Handlungsbedarf, sodass er zumindest für Betreiber kritischer Infrastrukturen eine Nachweispflicht über die Einhaltung von IT-Sicherheitsstandards im IT-Sicherheitsgesetz geregelt hat (siehe Seite 48).

Anlass zur Skepsis über den nach den Angaben der Unternehmen erreichten IT-Sicherheitsstand gibt auch ein weiteres Ergebnis unserer Studie: Bislang haben nur 39 % der Unternehmen eine Zertifizierung durchgeführt, bei 23 % befindet sich diese noch in der Planung bzw. im Aufbau. Bei 38 % ist eine Zertifizierung derzeit nicht vorhanden.

Zu einem wirksamen IT-Risk-Management gehört zudem die permanente Suche nach Schwachstellen. Ein Penetration Testing[35] des IT-Systems lassen nach ihren Angaben nur 53 % der Unternehmen durchführen. Bei weiteren 23 % der Unternehmen befinden sich entsprechende Maßnahmen in Planung bzw. im Aufbau.

Abb. 26 Verbreitung und Status von IT-Sicherheitsmaßnahmen



Basis: alle befragten Unternehmen

[35] Penetration Testing: Sicherheitsprüfung des IT-Systems mit Methoden, die ein Angreifer anwenden könnte, um unautorisiert in das System einzudringen.

Im Vergleich zeigt sich, dass das IT-Risk-Management von Unternehmen, die ihrer Einschätzung nach zur KRITIS gehören, weiter fortgeschritten zu sein scheint. In der Regel weisen sie nach eigenen Angaben ein internes IT-Sicherheitsmanagement auf (78 %) und führen interne Sicherheitsaudits durch (78 %). Fast zwei Drittel dieser Unternehmen führen Penetration Testings des IT-Systems durch (62 %). Hingegen erfolgte bislang nur bei 42 % der Betreiber kritischer Infrastrukturen eine Zertifizierung des IT-Sicherheitsmanagements.

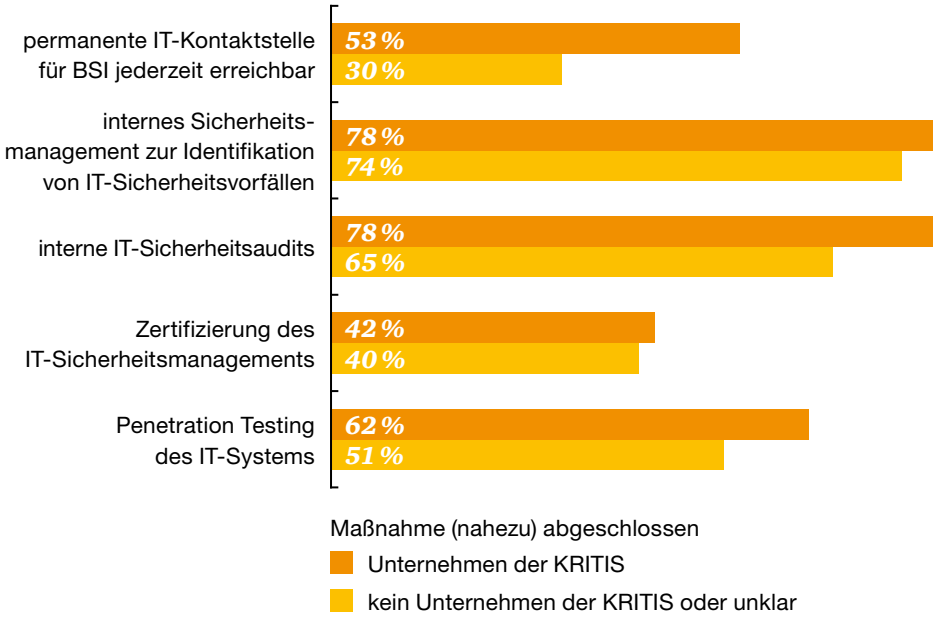
Die wenig verbreitete Zertifizierung lässt auch hier wiederum an dem laut eigener Einschätzung erreichten IT-Sicherheitsstandard bei den Betreibern kritischer Infrastrukturen zweifeln.

Des Weiteren verlangt das IT-Sicherheitsgesetz nach § 8b Abs. 3 BSIG die Einrichtung einer permanenten IT-Kontaktstelle, die jederzeit für das BSI erreichbar sein muss. Nur jedes zweite vom Gesetz vermutlich betroffene Unternehmen verfügt bereits hierüber (53 %).

Die Ergebnisse unserer Studie zur Verbreitung von E-Crime zeigen, dass grundsätzlich alle Unternehmen erheblichen IT-Sicherheitsrisiken ausgesetzt sind. Unter Einbeziehung der Verdachtsfälle war fast jedes zweite Unternehmen (47 %) von E-Crime (vermutlich) betroffen. Auch müssen wir von wachsenden E-Crime-Risiken ausgehen (siehe Seite 27), sodass das IT-Risk-Management vieler Unternehmen angesichts dieser Risikolage noch unzureichend ist.

Es ist zu hoffen, dass vom IT-Sicherheitsgesetz zusätzliche Impulse zur Erhöhung der IT-Sicherheitsstandards ausgehen, die auch auf Unternehmen ausstrahlen, die nicht zur KRITIS zählen.

Abb. 27 Verbreitung von IT-Sicherheitsmaßnahmen nach KRITIS-Zugehörigkeit



Basis: alle befragten Unternehmen

Compliance unter dem Regime des Marktes

CMS sind weit verbreitet und bei großen Unternehmen die Regel. Doch dadurch wächst auch der Druck auf kleinere Betriebe: Schon heute verpflichten Konzerne ihre Zulieferer vertraglich dazu, Compliance-Mindeststandards einzuhalten. Non-Compliance wird zum Wettbewerbsnachteil.

Vor allem im Korruptions- und Kartellrecht sind Unternehmen erheblichen Haftungsrisiken ausgesetzt. Gerade in diesem Bereich hat sich seit 2013 aber viel getan: Verfügte damals nur jedes zweite Unternehmen über ein Antikorruptions-programm, sind es inzwischen 79 %, weitere 15 % richten gerade ein solches System ein.

Die Verbreitung solcher Programme steigt mit der Größe der Unternehmen: Bei Großunternehmen mit mehr als 10.000 Mitarbeitern verfügen bereits 83 % über ein Antikorruptionsprogramm. Im Mittelstand zeigt sich ein anderes Bild: Bei Betrieben mit bis zu 1.000 Mitarbeitern sind bisher nur 35 % gegen Korruption gewappnet.

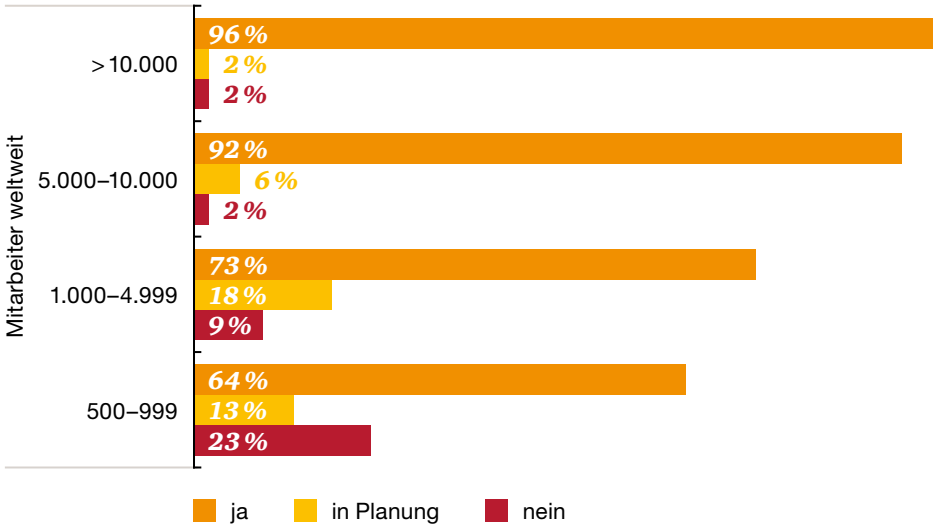
Verbreitung von Compliance-Programmen

Compliance-Programme sind schon seit Längerem in vielen Unternehmen eine Selbstverständlichkeit. 2013 verfügten 74 % der befragten Unternehmen über ein CMS, 2015 sind es 76 % und bei weiteren 13 % befindet es sich in der Planung.

Marktmechanismen bzw. der Druck in der Lieferkette führen zu einer forcierten Einführung von Compliance-Programmen (siehe Seite 57 ff.). Bei Großunternehmen mit mehr als 10.000 Mitarbeitern ist ein CMS mittlerweile die Regel, 96 % haben ein entsprechendes System eingeführt.

Mit sinkender Größe der Unternehmen nimmt zwar die Verbreitung ab, aber auch im Mittelstand bei Unternehmen mit 500 bis 999 Mitarbeitern ist ein CMS zunehmend anzutreffen, zwei Drittel haben ein solches eingeführt (64 %) und bei jedem zehnten Unternehmen befindet es sich in Planung (13 %). Allerdings zeigt sich im Mittelstand weiterhin die größte Zurückhaltung. Jedes fünfte Unternehmen mit unter 1.000 Mitarbeitern sieht derzeit kein CMS vor (23 %).

Abb. 28 Verbreitung und Status von CMS nach Unternehmensgröße



Basis: alle befragten Unternehmen

In unserer Studie zur Wirtschaftskriminalität 2013 behandelten wir ausführlich die erheblichen Haftungsrisiken im Korruptions- und Kartellrecht.[36] Es zeigte sich, dass trotz der erheblichen Strafverfolgungsrisiken nur jedes zweite (52 %) Unternehmen über ein Antikorruptionsprogramm verfügte und kaum mehr als ein Viertel (29 %) über ein kartellrechtliches Compliance-Programm. Zwei Jahre später sehen wir in beiden Deliktsfeldern eine positive Entwicklung. Allerdings sind die Defizite hinsichtlich der kartellrechtlichen Compliance weiterhin erheblich. Nur jedes zweite Unternehmen (55 %) hat ein entsprechendes CMS implementiert.

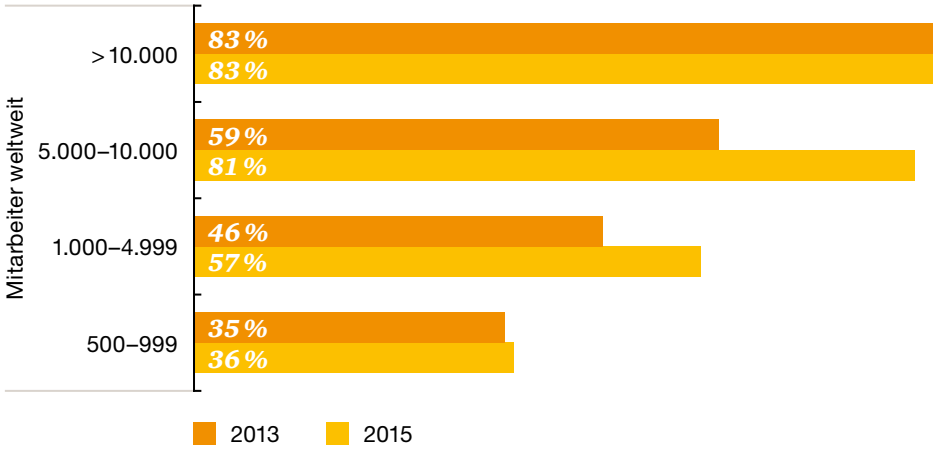
Über ein in der Entwicklung (nahezu) abgeschlossenes Antikorruptionsprogramm verfügen heute ihren Angaben zufolge 79 % der Unternehmen und bei 15 % befindet sich dieses gerade im Aufbau bzw. in der Planung.

Betrachten wir die einzelnen Unternehmensgruppen, so zeigt sich in der korruptionsrechtlichen Compliance eine größenabhängige Entwicklung, die vor allem von Großunternehmen getragen wird (sog. Top-down-Effekt). Bei Unternehmen mit mehr als 10.000 Mitarbeitern ist auf einem hohen Niveau von 83 % in den letzten zwei Jahren keine weitere Zunahme zu verzeichnen. Unternehmen mit 5.000 bis 10.000 Mitarbeitern schließen weitgehend zum Spitzenfeld der Großunternehmen auf. Hier wirkt sich offenkundig der Compliance-Druck in der Lieferkette aus. Wir verzeichnen hier hinsichtlich der Verbreitung von Antikorruptionsprogrammen einen deutlichen Anstieg von 59 % auf 81 %.

[36] Vgl. PwC, Wirtschaftskriminalität und Unternehmenskultur 2013, S. 32 ff. und 58 ff.

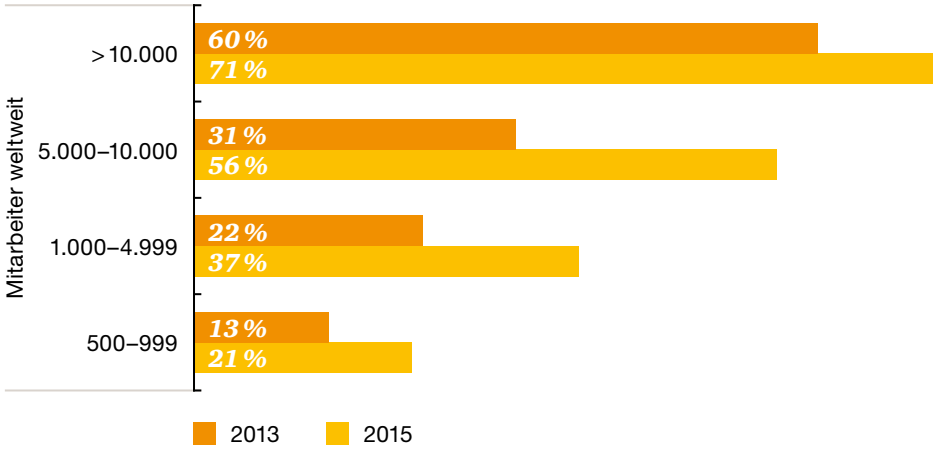
Gleiches gilt auch für Unternehmen mit 1.000 bis 4.999 Mitarbeitern, recht gering ist demgegenüber noch der Druck auf mittelständische Unternehmen mit 500 bis 999 Mitarbeitern.
In dieser Gruppe ist noch keine Entwicklung erkennbar, nur jedes dritte Unternehmen (36 %) verfügte 2015 über ein Antikorruptionsprogramm. Zu den Einzelheiten des Zusammenhangs zwischen dem Anstieg der Verbreitung von Compliance-Programmen und dem hier beschriebenen Druck in der Lieferkette verweisen wir auf die nachfolgenden Ausführungen auf Seite 57 ff.

Abb. 29 Verbreitung von Antikorruptionsprogrammen nach Unternehmensgröße



Basis: alle befragten Unternehmen

Abb. 30 Verbreitung kartellrechtlicher Compliance-Maßnahmen nach Unternehmensgröße



Basis: alle befragten Unternehmen

Hinsichtlich der kartellrechtlichen Compliance-Maßnahmen zeigt sich zwar ebenfalls eine deutliche Zunahme, aber nur die Hälfte der Unternehmen (55 %) verfügt über ein entsprechendes CMS. Im Bereich des Kartellrechts besteht daher weiterhin erheblicher Nachholbedarf.

Eine größenabhängige Entwicklung ist auch bei der kartellrechtlichen Compliance klar erkennbar. Für Großunternehmen mit mehr als 10.000 Mitarbeitern zeichnet sich allmählich eine gewisse Selbstverständlichkeit ab. Über zwei Drittel (71 %) haben ein entsprechendes CMS eingeführt, mit steigender Tendenz. Eine deutliche Entwicklung ist auch bei Unternehmen mit 5.000 bis 10.000 Mitarbeitern und bei Unternehmen mit 1.000 bis 4.999 Mitarbeitern erkennbar.

Bei mittelständischen Unternehmen mit 500 bis 999 Mitarbeitern bleibt die Verbreitung hingegen nahezu unverändert. Nur 21 % der Unternehmen dieser Größe verfügen über eine in der Entwicklung abgeschlossene kartellrechtliche Compliance. Allerdings ist einzuräumen, dass die Möglichkeiten, Kartelle zu bilden, für Unternehmen dieser Größe geringer sind. Der Problemdruck ist daher nicht mit dem größerer Unternehmen zu vergleichen.

Status der Compliance-Programme nach Deliktsgruppen

Ein zeitgemäßes Compliance-Programm hat viele Deliktsfelder abzudecken. Fast alle befragten Unternehmen haben ihr CMS auf den Schutz vertraulicher Kunden- und Unternehmensdaten ausgerichtet (89 %) oder bauen ein solches CMS auf (10 %). Auffällig ist, dass kaum ein Unternehmen bereit ist, in dieser Frage weitere Risiken einzugehen. Keines der Unternehmen hält Prävention in diesem Risikosektor für überflüssig.

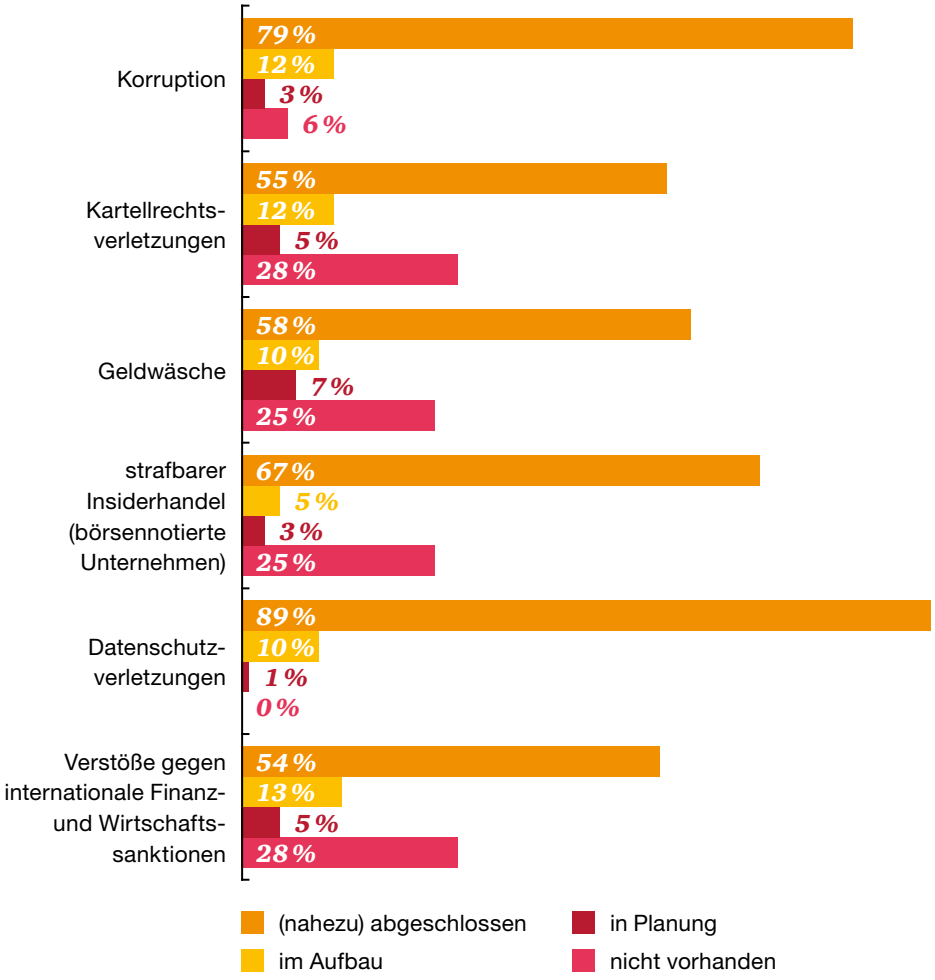
In der Gruppe der börsennotierten Unternehmen[37] sind für über zwei Drittel auch Maßnahmen gegen strafbare Insidertransaktionen (§ 38 WpHG[38]) selbstverständlich, nur ein Viertel verfügt hierüber derzeit nicht bzw. plant solche nicht.

Pflichten zur Bekämpfung der Geldwäsche bestehen nach § 2 ff. GWG[39] nicht nur für den Finanz- und Versicherungssektor, sondern auch für viele Unternehmen aus dem Nicht-Finanzsektor. Hierzu gehören vor allem Unternehmen, die mit Gütern handeln. Der Kreis der Verpflichteten im Nicht-Finanzsektor ist sehr weit gezogen. Nach den Angaben aller befragten Unternehmen verfügt überaschenderweise über die Hälfte (58 %) über eine in der Entwicklung abgeschlossene Geldwäsche-Compliance, bei 17 % befindet sich diese in der Planung bzw. noch im Aufbau.

Zum Aufgabenfeld eines modernen CMS gehört außerdem die Vermeidung von Verstößen gegen internationale Finanz- und Wirtschaftssanktionen. Hiervon sind ebenfalls nicht nur Unternehmen des Finanzsektors betroffen, sondern Unternehmen fast aller Branchen.

Jedes zweite Unternehmen hat das CMS auch auf die Vermeidung von Verstößen gegen internationale Finanz- und Wirtschaftssanktionen ausgerichtet (54 %).

Abb. 31 Status des CMS nach Deliktsgruppen



Basis: Unternehmen mit CMS

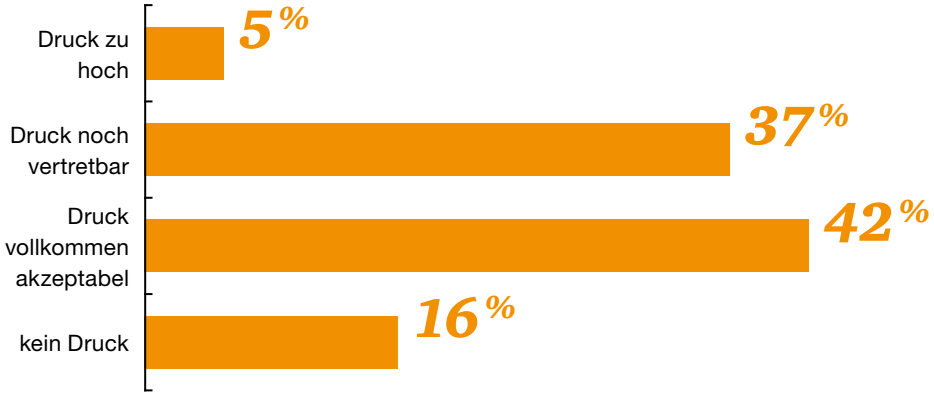
[37] Die entsprechende Frage wurde nach der Börsennotierung gefiltert. In der Stichprobe sind 27 % der Unternehmen börsennotiert.
[38] Gesetz über den Wertpapierhandel.
[39] Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten.

Compliance-Programme setzen sich durch. Dafür sorgt der Druck des Marktes. Große Unternehmen fordern von ihren Zulieferern Compliance-Mindeststandards ein.

Compliance in der Lieferkette aus Sicht der Auftragnehmer

Bereits in der Studie im Jahr 2011 kamen wir zum Schluss, dass es sich bei Compliance nicht um eine Modeerscheinung handelt und wir von einer global verlaufenden Top-down-Entwicklung auszugehen haben.[40] Großunternehmen sind die Schrittmacher dieser Entwicklung. Vor allem mittelständische Unternehmen können sich dem Druck ihrer großen Auftraggeber kaum entziehen. Nur 16 % der befragten Unternehmen gaben an, dass sie keinen Druck von ihren Auftraggebern verspüren, ein CMS einzuführen. 42 % der Unternehmen bezeichnen den Druck als vollkommen akzeptabel, mehr als jedes dritte Unternehmen meinte, er sei noch vertretbar, und nur 5 % empfinden ihn als zu hoch.

Abb. 32 Compliance-Druck aus Sicht der Auftragnehmer



Basis: alle befragten Unternehmen

5 % *der Unternehmen empfinden den Druck, ein CMS einzurichten, als zu hoch. Der Großteil dagegen hält es für akzeptabel, wenn Auftraggeber solche Systeme einfordern.*

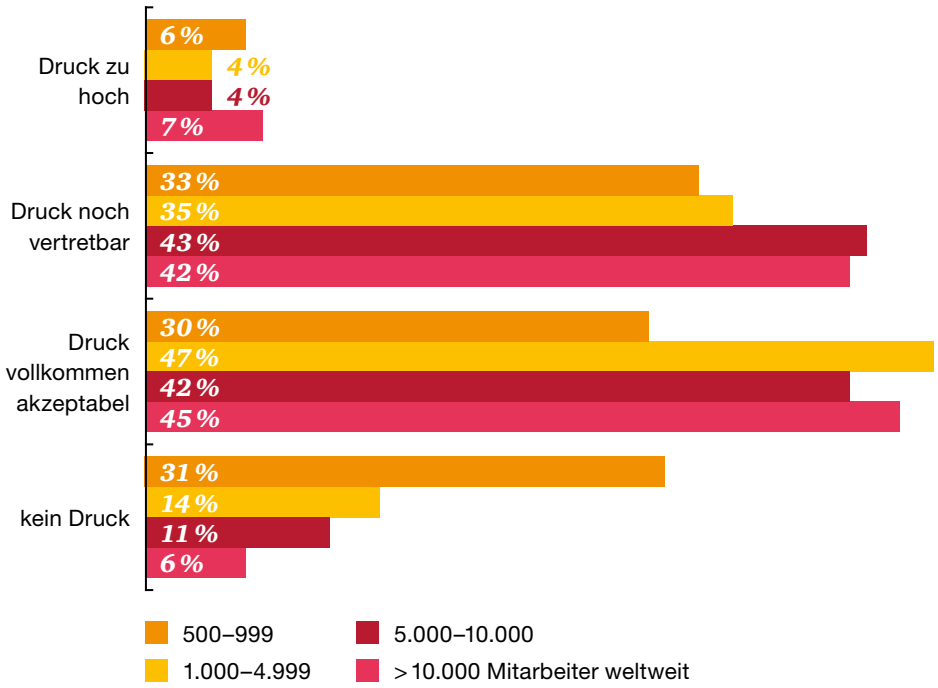
[40] Vgl. PwC, Wirtschaftskriminalität 2011, S. 41 ff.

Ein großer Teil der Unternehmen erkennt offenbar, dass der Aufbau eines CMS sinnvoll ist, und bezeichnet den ausgeübten Compliance-Druck daher als vollkommen akzeptabel.

Mit Blick auf die Unternehmensgröße zeigen sich keine bedeutsamen Unterschiede – mit einer Ausnahme: Nur 6 % der Unternehmen mit über 10.000 Mitarbeitern berichteten über keinen Druck gegenüber 31 % der Unternehmen mit 500 bis 999 Mitarbeitern. Kleinere Unternehmen stehen derzeit offenbar auf der „Compliance-Prioritätenliste" größerer Unternehmen noch nicht ganz oben. Künftig dürfte allerdings auch gegenüber kleineren Unternehmen der Druck in der Lieferkette erheblich zunehmen.

Demgegenüber berichten größere Unternehmen mit mehr als 4.999 Mitarbeitern über einen gewissen Druck, den sie allerdings als vollkommen akzeptabel bzw. noch vertretbar einstufen (42 % bzw. 43 %). Wir nehmen an, dass dieser Druck von noch größeren Unternehmen in der Lieferkette ausgeht, bei denen es sich zum Teil um Konzerne und Global Player handelt,[41] die sich selbst unter Beobachtung insbesondere US-amerikanischer Aufsichtsbehörden sehen.[42]

Abb. 33 Compliance-Druck aus Sicht der Auftragnehmer nach Unternehmensgröße



Basis: alle befragten Unternehmen

[41] In unserer Studie erfolgte bei den Unternehmen mit mehr als 10.000 Mitarbeitern keine weitere Differenzierung der Unternehmensgrößen.
[42] Siehe hierzu ausführlich PwC, Wirtschaftskriminalität und Unternehmenskultur 2013, S. 39 ff.

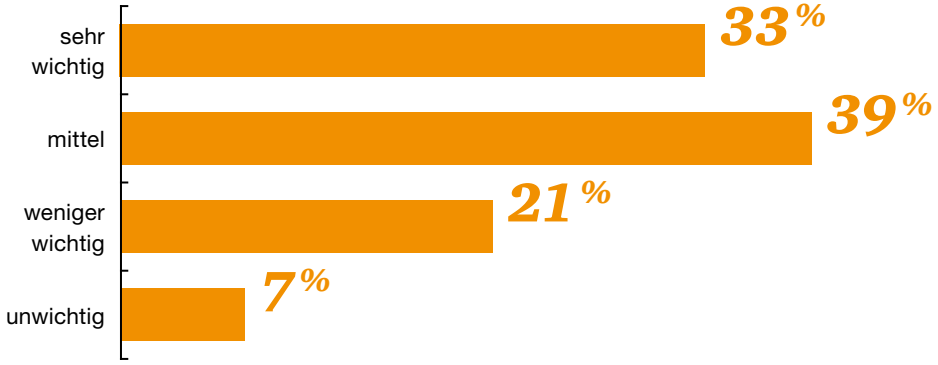
Compliance in der Lieferkette aus Sicht der Auftraggeber

Angesichts der zuvor dargestellten Ergebnisse ist es nicht überraschend, dass die große Mehrheit der Unternehmen von ihren Lieferanten und Dienstleistern erwartet, dass sie über ein CMS verfügen. Jedes dritte Unternehmen gab an, dass ihm dies sehr wichtig ist (33 %). Als unwichtig bzw. weniger wichtig bezeichnete es nur jedes vierte Unternehmen (28 %).

Berücksichtigen wir die Größe der Unternehmen, so bestätigt sich unsere „Top-down-These“: Der Druck geht vor allem von den größeren Unternehmen aus. Nur 7 % der befragten Unternehmen mit über 10.000 Mitarbeitern gaben an, dass ihnen ein CMS bei ihren Lieferanten und Dienstleistern weniger wichtig oder gar unwichtig ist, gegenüber fast der Hälfte der Unternehmen mit 500 bis 999 Mitarbeitern (47 %). Als sehr wichtig bezeichneten dies jedoch mehr als die Hälfte der Großunternehmen mit über 10.000 Mitarbeitern (55 %).

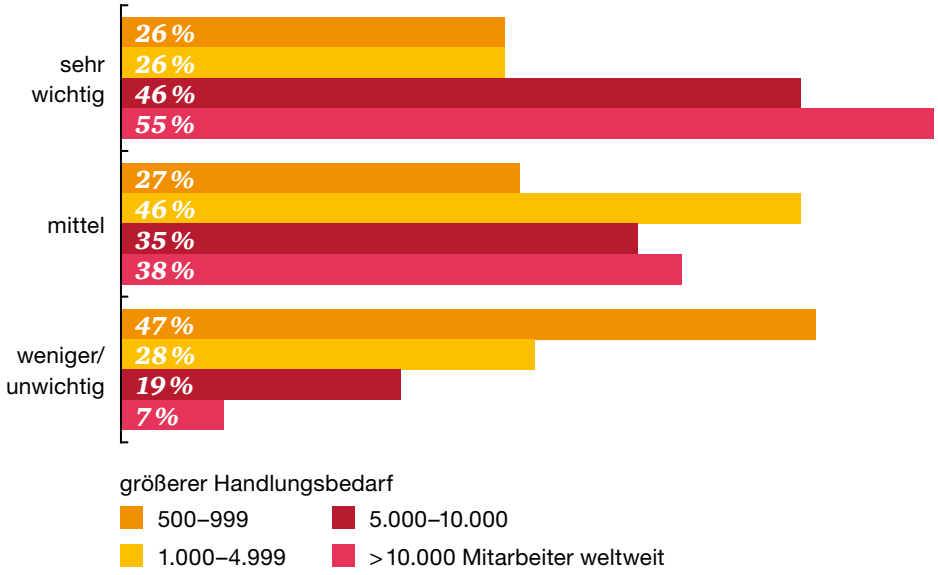
Compliance hat somit Eingang in die Marktwirtschaft gefunden, Marktgesetze sind die Treiber dieser Entwicklung. Auch über wirtschaftliche Bindungen und teilweise auch Abhängigkeiten in der Lieferkette verbreiten sich CMS.[43] Der Markt entwickelt Präventivkräfte. Nicht über ein CMS zu verfügen, droht zum Wettbewerbsnachteil zu werden.

Abb. 34 Bedeutung eines CMS aus Sicht der Auftraggeber



Basis: Unternehmen mit CMS

Abb. 35 Bedeutung eines CMS aus Sicht der Auftraggeber nach Unternehmensgröße



Basis: Unternehmen mit CMS

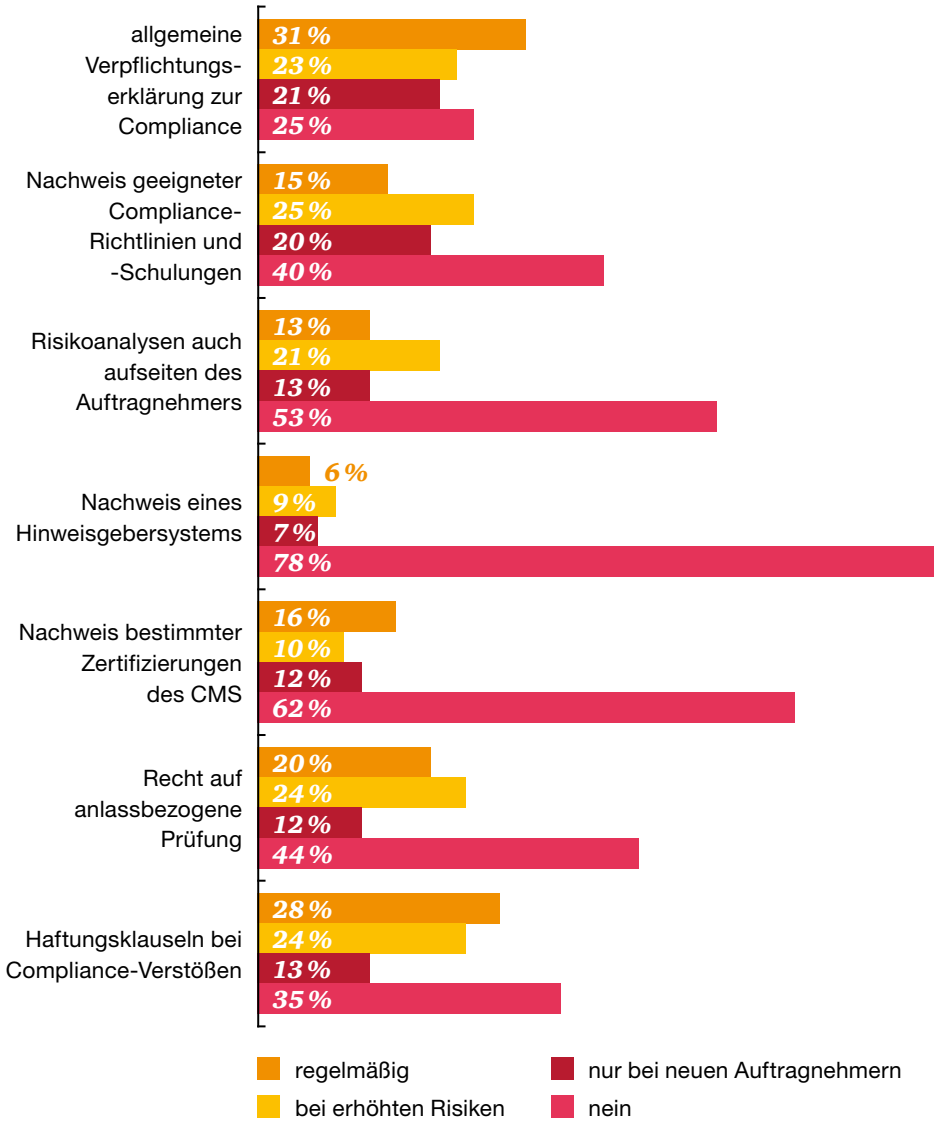
[43] Vgl. PwC, Wirtschaftskriminalität 2011, S. 41 ff.; Bussmann: Sozialisation in Unternehmen durch Compliance, in: Hellmann/Schröder (Hrsg.), Festschrift für Hans Achenbach, 2011, S. 57–82.

Compliance-Vertragskonditionen

Viele Unternehmen sind dazu übergegangen, Haftungsklauseln in ihren Verträgen mit Lieferanten und Dienstleistern aufzunehmen und sich Kontrollrechte einräumen zu lassen. Nahezu jedes dritte Unternehmen sieht in seinen Verträgen regelmäßig eine Verpflichtungserklärung sowie eine Haftungsklausel im Falle von Compliance-Verstößen vor, ein knappes Viertel im Falle von erhöhten Risiken. Jedes vierte Unternehmen lässt sich in der Regel ein Recht auf anlassbezogene Prüfungen zusichern (sog. Audit Clause).

Nicht wenige Verträge formulieren konkrete Anforderungen an die Ausgestaltung des CMS ihres Vertragspartners. 15 % der Unternehmen verlangen in der Regel Nachweise über geeignete Compliance-Richtlinien und -Schulungen. Ein Hinweisgebersystem verlangen die meisten Unternehmen hingegen nicht (78 %). Allerdings finden sich in Verträgen mit Lieferanten und Dienstleistern zunehmend Regelungen zur Zertifizierung des CMS. 16 % lassen sich dies regelmäßig vertraglich zusichern und 10 % im Falle erhöhter Risiken.

Abb. 36 Verbreitung von Compliance-Vertragskonditionen

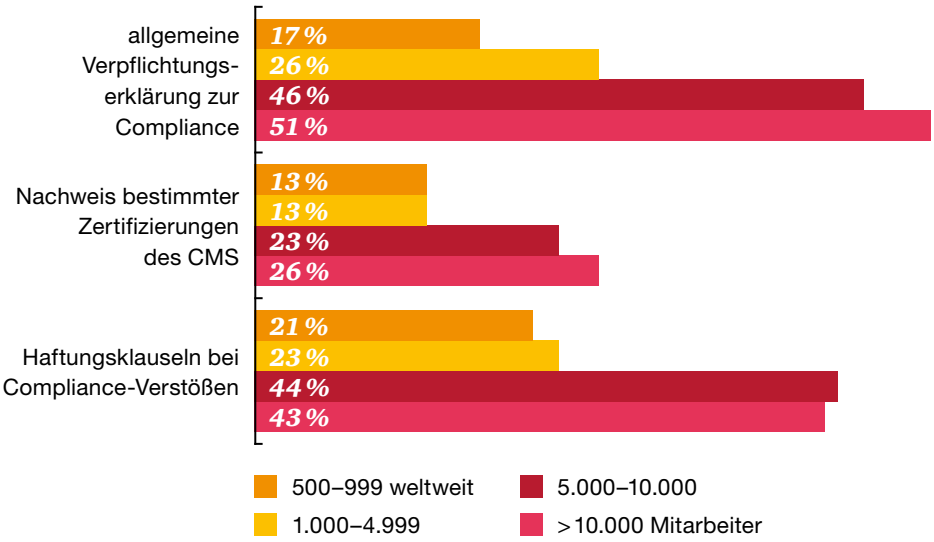


Basis: Unternehmen mit CMS

Eine allgemeine Verpflichtungserklärung oder Haftungsklauseln für den Fall von Compliance-Verstößen sind nahezu in jedem dritten Unternehmen selbstverständlicher Bestandteil von Verträgen mit Geschäftspartnern.

Großunternehmen mit mehr als 4.999 bzw. mehr als 10.000 Mitarbeitern üben nicht nur Druck hinsichtlich des Aufbaus eines CMS ihres Geschäftspartners aus, sondern ihre Verträge enthalten häufiger eine allgemeine Verpflichtungserklärung (46 % bzw. 51 %) und eine Haftungsklausel (44 % bzw. 43 %). Außerdem sehen die Verträge bei etwa jedem vierten Großunternehmen eine Klausel zur Zertifizierung des CMS ihres Vertragspartners vor (23 % bzw. 26 %).

Abb. 37 Regelmäßige Compliance-Vertragskonditionen nach Unternehmensgröße



Basis: Unternehmen mit CMS

Vor allem Großunternehmen machen ihren Vertragspartnern konkrete und detaillierte Auflagen zur Ausgestaltung des CMS sowie dessen Zertifizierung.

Compliance und Wertekulturen

An der Wichtigkeit einer integritätsförderlichen Unternehmenskultur zweifelt heute niemand. Ein erfolgreiches CMS kann sich nicht auf die Schaffung von Rechts- und Richtlinienbewusstsein und auf Kontrollen beschränken. Es gilt zudem, integritätsförderliche Werte zu kommunizieren und zu verinnerlichen, die das Normbewusstsein stützen und zugleich übergreifende Prinzipien im Unternehmen vermitteln.

Zu einer besonderen Herausforderung wird Compliance auf internationalem Terrain, wenn Unternehmen vor Ort auf andere gesellschaftliche Grundsätze und Werte stoßen, wenn die Interessen der Familie über die Rechtsordnung gestellt werden oder korrupte soziale Netzwerke alle Compliance-Bemühungen ins Leere laufen lassen.

Handlungsbedarf im Compliance-Management

Unternehmen verfügen über einen breiten Gestaltungsspielraum bei der Ausgestaltung ihres CMS. Gleichwohl gibt es mittlerweile ein allgemeines Verständnis über die zentralen Elemente eines effektiven CMS. Hierzu haben sicherlich sowohl rechtliche Regularien wie die Richtlinien des US Foreign Corrupt Practices Act (FCPA)[44] und des UK Bribery Act[45] als auch der Prüfungsstandard 980 des IDW (IDW PS 980)[46] und jüngst die Guidelines zum internationalen Standard ISO 19600 beigetragen.

Als Grundlage gilt zweifelsfrei der unmissverständlich kommunizierte Compliance-Wille der Unternehmensführung. Umso beunruhigender ist es, dass jedes zehnte Unternehmen, das seinen Angaben zufolge über ein entwickeltes CMS verfügt,[47] hier noch größeren Handlungsbedarf sieht. Noch häufiger berichteten die Befragten über ein unzureichendes Commitment des mittleren Managements, wenn es gilt, die Compliance-Ziele im Unternehmensalltag vorzuleben und umzusetzen. Jedes fünfte Unternehmen mit einem entwickelten CMS (19 %) sieht sich hier noch vor weitere Aufgaben gestellt. Ebenso häufig werden Schwächen hinsichtlich einer systematischen Risikoanalyse gesehen.

Fraglich ist außerdem, ob es für die Mehrheit der Unternehmen zutreffend ist, dass sie bereits über eine integritätsförderliche Unternehmenskultur verfügen. Etwa vier Fünftel der Unternehmen mit einem entwickelten CMS sehen diesbezüglich keinen oder nur geringen Handlungsbedarf; bei den Unternehmen, bei denen sich das CMS noch im Aufbau befindet, sind es drei Viertel.

Der Großteil der Unternehmen misst zudem einer unabhängigen Prüfung offenbar kein Gewicht bei. Die Mehrheit hat weder eine Auditierung nach dem IDW PS 980 noch eine Zertifizierung nach ISO 19600 durchgeführt. Die meisten der befragten Unternehmen werden sich wahrscheinlich auch in den nächsten zwei Jahren nicht nach einem dieser Standards prüfen lassen (siehe Seite 81).

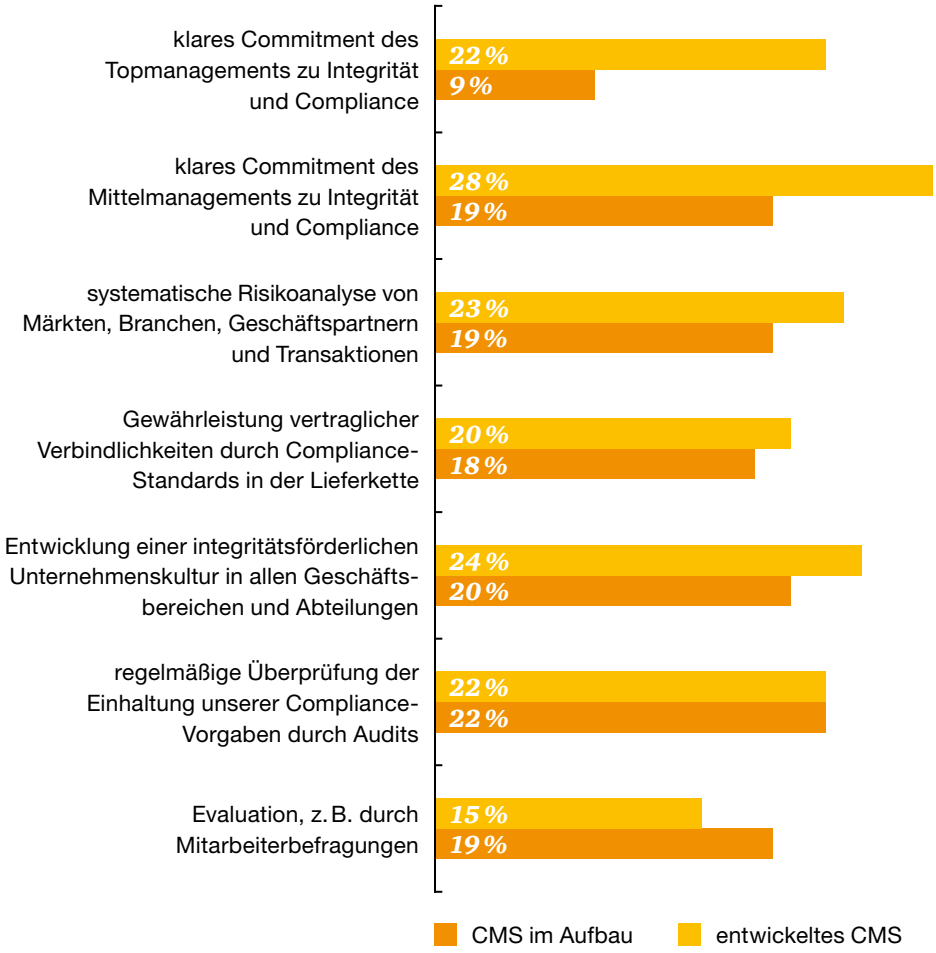
Im Vergleich zeigt sich insgesamt, dass in der Gruppe der Unternehmen, deren CMS sich noch im Aufbau befindet, ein nur graduell höherer Handlungsdruck gesehen wird. Die Herausforderungen an ein wirksames CMS werden unserer Einschätzung nach in dieser Gruppe aber vielfach unterschätzt.

---

[44] Richtlinie zum FCPA, S. 57, online abrufbar unter: http://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf.
[45] Richtlinie zum UK Bribery Act 2010, S. 23, online abrufbar unter: http://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf.
[46] Überblick siehe Withus, Betriebswirtschaftliche Grundsätze für Compliance-Management-Systeme, 2014.
[47] Zur Gruppe der Unternehmen mit einem entwickelten CMS gehören Unternehmen, die über ein CMS verfügen, dessen Aufbau aus ihrer Sicht bezogen auf mindestens zwei Deliktsfelder abgeschlossen ist. Hierzu zählen mehr als zwei Drittel der Unternehmen (68 %).

Die Unternehmensführung muss den Mitarbeitern den Compliance-Willen klar vermitteln und vorleben. Dieses Commitment gilt auch für das mittlere Management.

Abb. 38 Größerer Handlungsbedarf nach Status des CMS



Basis: alle befragten Unternehmen

Die stärksten Werte in den Unternehmen

An der Wichtigkeit einer integritätsförderlichen Unternehmenskultur zweifelt heute niemand. Ein erfolgreiches CMS kann sich nicht auf die Schaffung von Rechts- und Richtlinienbewusstsein und auf Kontrollen beschränken. Es gilt zudem, integritätsförderliche Werte zu kommunizieren und zu verinnerlichen, die das Normbewusstsein stützen und zugleich übergreifende Prinzipien im Unternehmen vermitteln. Zwar beobachten wir derzeit eine Tendenz zu einer wachsenden Verrechtlichung der Compliance, aber internationalen Studien zufolge scheint sich in Unternehmen zugleich eine wertebasierte Kultur zu entwickeln.[48]

Zu einer integritätsförderlichen Unternehmenskultur gehören nicht nur Werte, die insbesondere bereits die strafrechtlichen Verbote enthalten, sondern Werte, die zu einer Verinnerlichung des Rechts beitragen und den Weg dorthin ebnen. Wie auch sonst in der Gesellschaft benötigen die Mitarbeiter eines Unternehmens einen Werterahmen, der ihnen die Sicherheit gibt, Recht von Unrecht, Richtig von Falsch zu unterscheiden, und der ihnen das Vertrauen gibt, die Einhaltung der Regeln gegenüber Kollegen und Geschäftspartner einzufordern („Speak-up-Kultur“).

Bei einem nachhaltigen CMS handelt es sich somit um eine komplexe Aufgabe, die nur in Verbindung mit einem Wertemanagement gelöst werden kann. In einer offenen Frage, die sich thematisch nicht auf Compliance-Aspekte beschränkte, nannten uns die Unternehmen die Werte, die ihre Kultur am stärksten kennzeichnen.[49] Sie gaben eine Vielzahl von Werten an, die sich verschiedenen Wertefeldern zuordnen lassen, wie moralische Werte, Kooperations-, Kommunikations- und Leistungswerte.[50] Nur 11 % konnten keine Werte angeben. Werte sind daher bei den allermeisten Unternehmen fest im Bewusstsein verankert.

Ein Teil der Werte bezieht sich auf Aspekte, die man weniger mit der Förderung von Criminal Compliance in Verbindung bringen kann, wie Kunden- und Servicevermittlung (16 %), Qualitätsbewusstsein (12 %) oder Innovation/Kreativität (10 %).

11 % *der Unternehmen konnten keine Werte benennen. Umgekehrt heißt das jedoch: Die meisten Unternehmen haben einen Wertekanon entwickelt.*

[48] Vgl. Ferrell/Fraedrich/Ferrell, Business Ethics: Ethical Decision Making and Cases, 10. Aufl. 2015, S. 185 ff. m. w. N.
[49] Es durften bis zu drei Werte genannt werden, vielfach wurden allerdings auch mehr Werte genannt.
[50] Vgl. Grüninger, Werteorientiertes Compliance-Management-System, in: Wieland/Steinmeyer/Grüninger (Hrsg.): Handbuch Compliance-Management, S. 53.

Nicht alle genannten Werte lassen sich präzise voneinander abgrenzen, sodass Überschneidungen bestehen. Dies gilt vor allem für Werte wie Integrität (14 %) und Nachhaltigkeit (10 %). Ein großer Teil der am häufigsten genannten Werte ist konkreter und eignet sich aus Sicht der Forschung zur Etablierung einer integritätsförderlichen Unternehmenskultur.[51] Zu nennen sind insbesondere:

Verbindlichkeit und Konsistenz (22 %): Vorgesetzte zeigen dieselben Prioritäten, die sie von ihren Mitarbeitern erwarten, und kritisieren bei Compliance-Verstößen.

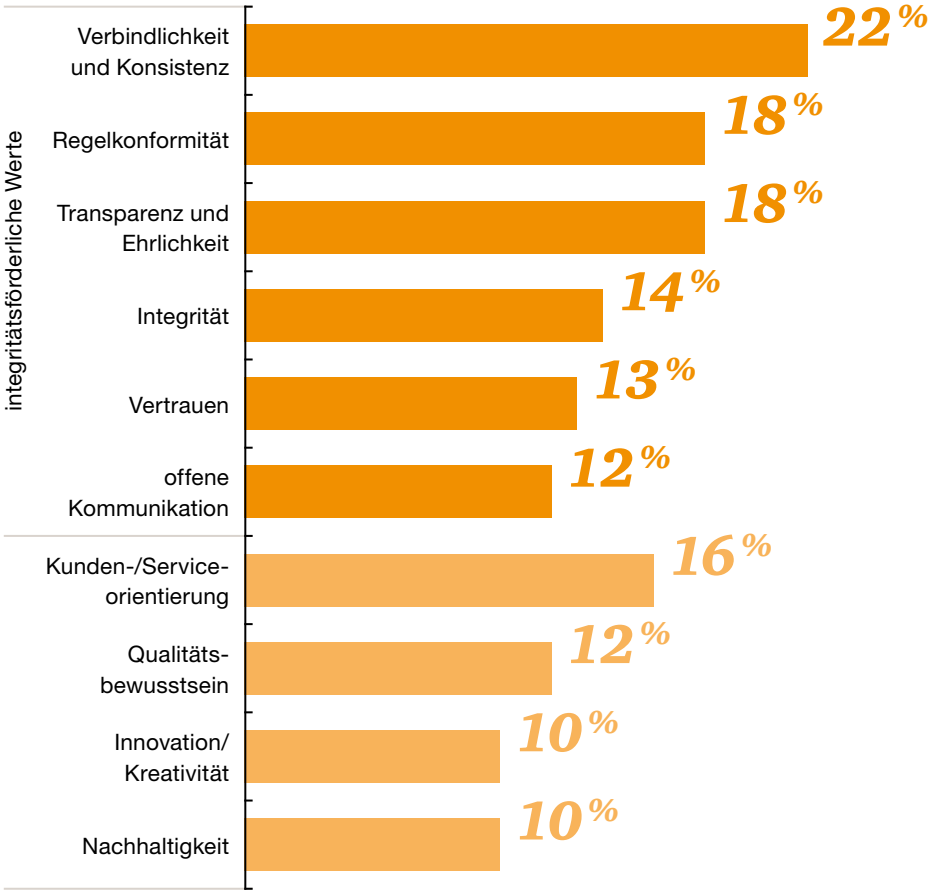
Regelkonformität (18 %): Dies bedeutet, Unternehmensrichtlinien nicht zu vernachlässigen, wenn es hilft, einen guten Job zu machen, und auch auf Geschäftsabschlüsse zu verzichten, wenn diese nur durch einen Compliance-Verstoß zu erreichen wären.

Transparenz und Ehrlichkeit (18 %): Dieser Wert betrifft Aufrichtigkeit in geschäftlichen Entscheidungen und im Umgang mit Kollegen.

Vertrauen (13 %): Im Unternehmen ist es wichtig, dass man Vorgesetzten vertrauen kann; sie vermitteln glaubhaft, dass beispielsweise Bestechung keine legitime Praxis darstellt.

Offene Kommunikation (12 %): Ohne diese Wertorientierung kann sich eine Speak-up-Kultur nicht etablieren. Mitarbeiter trauen sich, Probleme offen anzusprechen und auch über den Umgang mit Korruptionssituationen offen zu sprechen.

Abb. 39 Die zehn stärksten Werte in Unternehmenskulturen



Werte, die die Kultur des Unternehmens am stärksten kennzeichnen (bis zu drei Nennungen möglich)
Basis: alle befragten Unternehmen

[51] Vgl. Bussmann, Integrität durch nachhaltiges Compliance-Management. Über Risiken, Werte und Unternehmenskultur, in: CCZ 2/2016, 50–57.

Compliance in fremden Kulturen

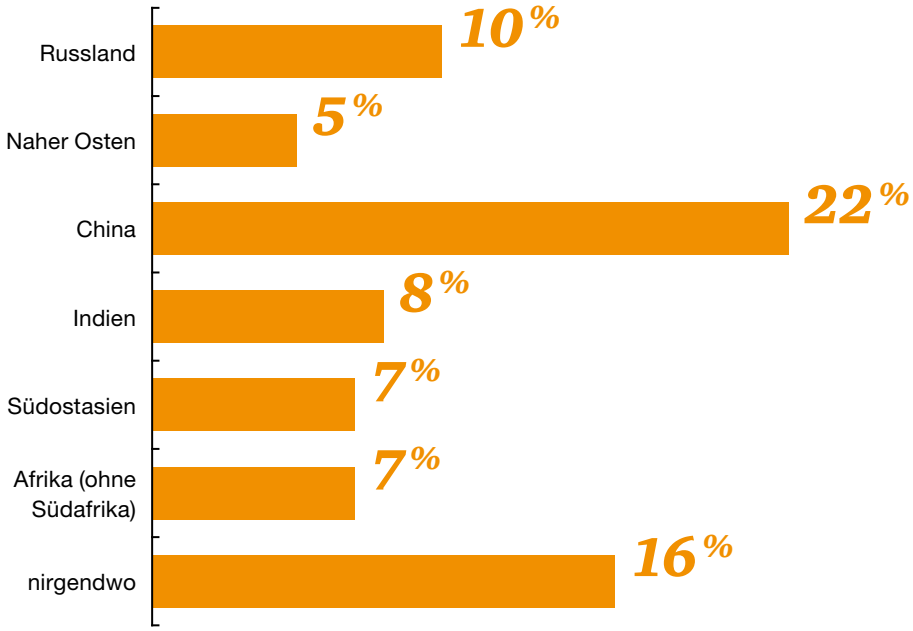
Die Umsetzung des eigenen Compliance-Programms im Ausland stellt oft eine Herausforderung dar. Wir haben die Unternehmen daher nach ihren Erfahrungen gefragt, wobei wir uns aus Vergleichsgründen auf weltweit operierende Unternehmen beschränken.

China (22 %), gefolgt von Ländern bzw. Regionen wie Russland (10 %), Afrika (7 %) und Indien (8 %), wurden am häufigsten genannt, wenn es um die größten Hindernisse bei der Umsetzung eines CMS ging. Die befragten Unternehmen konnten nur eine Nennung abgeben. Wir gehen davon aus, dass die Bedeutung des jeweiligen Marktes in die Beurteilung eingeflossen ist, sodass China schon aus diesem Grund mit Abstand am häufigsten genannt worden sein dürfte.

16 % gaben an, dass sie mit ihrem CMS nirgendwo auf größere Hindernisse stoßen und dies, obwohl sie weltweit vertreten sind. Die Erfahrungen der Unternehmen zeigen uns, dass es grundsätzlich möglich ist, auch in eigentlich schwierigen Ländern und Regionen ein wirksames CMS zu implementieren.

Abb. 40 Regionen und Länder mit den größten Hindernissen für Compliance aus Sicht weltweit operierender Unternehmen

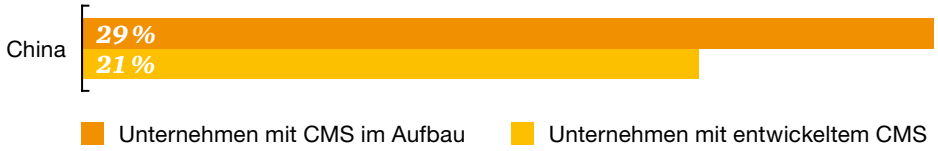
nur Nennungen mit einem Anteil von mindestens 5 %



Häufigkeit der Nennung der Region/des Landes mit den derzeit größten Hindernissen für Compliance. Mehrfachnennungen waren nicht möglich.
Basis: Unternehmen mit CMS und weltweiten Standorten

Bemerkenswert ist, dass Unternehmen, die bereits über ein entwickeltes CMS verfügen, in China auf geringere Hürden und Schwierigkeiten stoßen. Nur 21 % dieser Unternehmen nannten China als Land mit den derzeit größten Hindernissen bei der Umsetzung ihres CMS – gegenüber 29 % der Unternehmen, deren Compliance-Programm sich noch im Aufbau befindet. Dieses Ergebnis zeigt, dass man anfängliche Probleme und Herausforderungen durchaus überwinden und mit einem Compliance-Programm auch in schwierigen Regionen erfolgreich sein kann.

Abb. 41 Compliance-Hindernisse in China



Basis: Unternehmen mit CMS und weltweiten Standorten

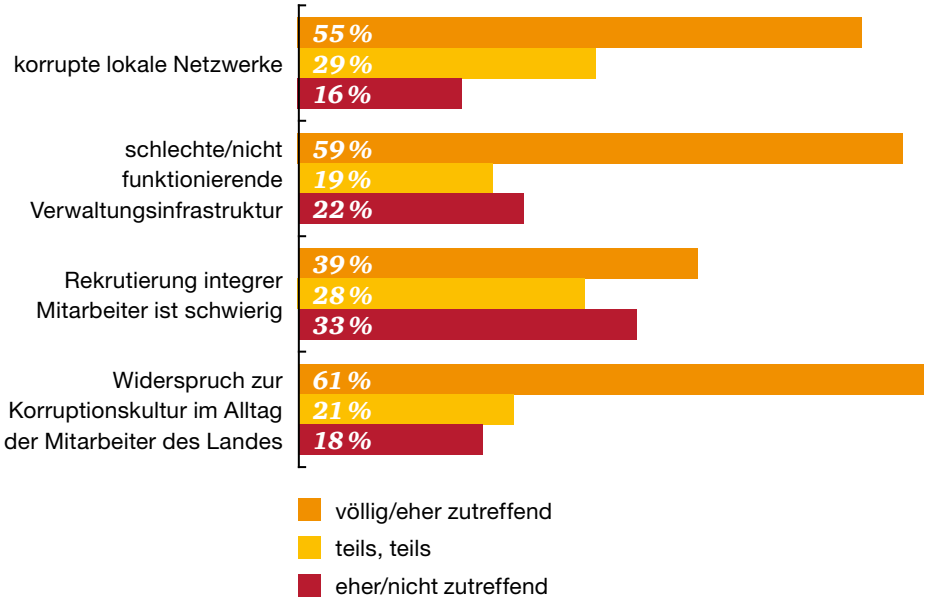
Die Umsetzung von Antikorruptionsprogrammen stößt in vielen Regionen und Ländern auf besondere Probleme. Dies ist auf unterschiedliche kulturelle und gesellschaftliche Werte und teilweise auch auf unzureichende staatliche Strukturen zurückzuführen.[52] Zudem werden Verwaltungsprobleme teilweise durch Bestechungsgelder zusätzlich verschärft, da sie für öffentlich Bedienstete zusätzliche Anreize schaffen, Verwaltungsprozesse zu verlangsamen und zu verkomplizieren. Korruption ist somit nicht die Lösung, sondern Teil des Problems einer ineffizienten Verwaltung.

Schwierige Verwaltungsstrukturen nannten über die Hälfte (59 %) der befragten Unternehmen als eine ihrer größten Herausforderungen in dem Land, in dem sie die größten Probleme bei der Umsetzung ihres CMS haben.

Zusätzlich bestehen kulturelle Probleme. In der Korruptionsforschung erwiesen sich korrupte soziale Netzwerke und kollektivistische Werteorientierungen als weitere zentrale Ursachen, die vor allem in Ländern mit schwachen und korrupten staatlichen Strukturen dominieren. Die Interessen der eigenen Familie, Sippe, Ethnie und engen Freunde werden in diesen Kulturen über das Recht, den Staat und das Unternehmen, dem man angehört, gestellt. Dies erklärt, dass für über die Hälfte (55 %) der Unternehmen korrupte soziale Netzwerke eine besondere Herausforderung darstellen.

Fast zwei Drittel (61 %) der befragten Unternehmen nannten überdies den Widerspruch zwischen dem eigenen Antikorruptionsprogramm und der Korruptionskultur im Alltag ihrer Mitarbeiter in den Ländern der betroffenen Auslandsvertretungen. Die Unternehmen können daher auch mit Problemen bei der Rekrutierung integrer Mitarbeiter konfrontiert sein. Allerdings sind die Erfahrungen hierzu eher geteilt. Für 39 % ist dies ein Problem, 28 % haben eher gemischte Erfahrung gemacht, ein Drittel (33 %) hält dieses Problem für bewältigbar.

Abb. 42 Art der Compliance-Herausforderungen in fremden Regionen und Kulturen



Basis: Unternehmen mit CMS und weltweiten Standorten

[52] Vgl. ausführlich Bussmann, Wirtschaftskriminologie Band I, 2015, Rn. 617 ff. m. w. N.

Haftungsrisiken und Rechtsreformen

Das IT-Sicherheitsgesetz setzt Sicherheitsstandards fest, die Unternehmen einhalten sollten, um sich wirksam vor Cyber-Attacken zu schützen. Bei Compliance-Systemen wird dagegen noch diskutiert, inwieweit auch hier gesetzliche Regelungen sinnvoll sein könnten, um eine gewisse Orientierung zu geben.

Vor allem Unternehmen, die bereits über ein entwickeltes CMS verfügen, sind aus Gründen der Rechtssicherheit und Vergleichbarkeit an verbindlichen Vorgaben interessiert.

Unternehmen laufen Gefahr, das Haftungsrisiko im Kartellrecht zu unterschätzen. Kaum mehr als jedes zweite Unternehmen mit CMS verfügt über eine kartellrechtliche Compliance.

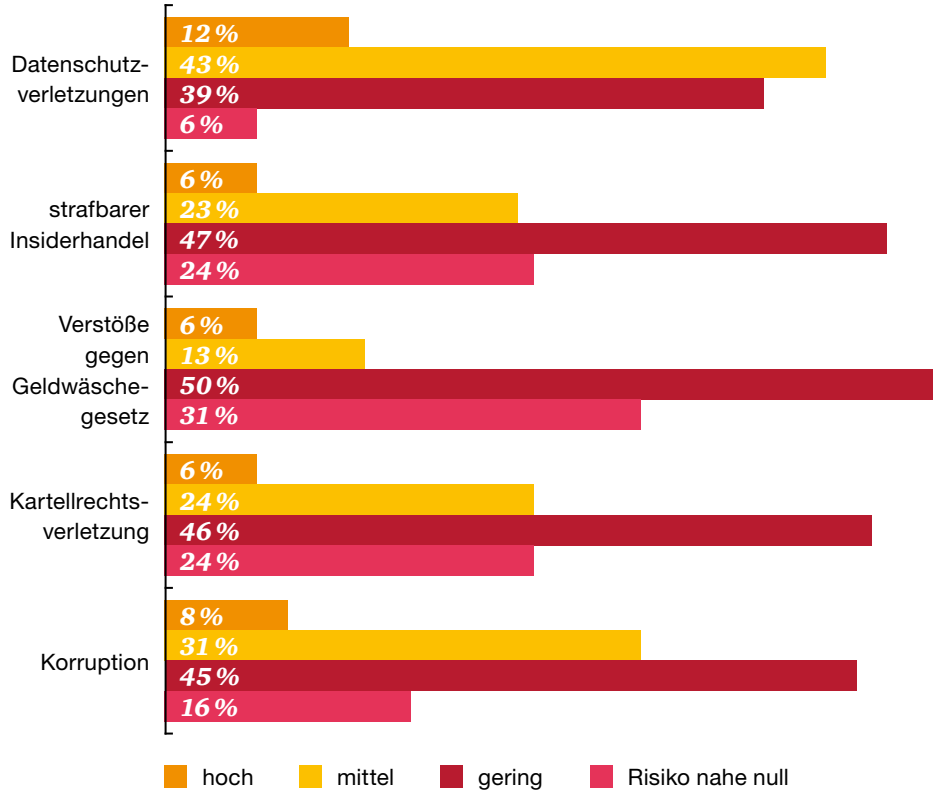
Haftungsrisiken in der eigenen Branche

Um die Entwicklung der zivil- und strafrechtlichen Haftungsrisiken künftig weiterverfolgen zu können, haben wir die Einschätzungen der Unternehmen zu diesen Risiken in ihrer Branche erhoben. Diese Einschätzungen sind auch ein indirekter Indikator für die Qualität des Compliance-Managements innerhalb einer Branche aus Sicht ihrer Mitglieder. Die wahrgenommenen Haftungsrisiken müssten mit zunehmendem Ausbau der Compliance-Programme allmählich abnehmen.

Die Ergebnisse unserer Befragung zeigen, dass nur die wenigsten Unternehmen die Haftungsrisiken innerhalb ihrer Branche bei nahe null einstufen (siehe Seite 72 f.). Die höchsten Haftungsrisiken sehen die Befragten im Bereich von Datenschutzverletzungen, 43 % gehen hier von einem mittleren Risiko aus, 12 % sogar von einem hohen. Wir führen dies auf die hohen datenschutzrechtlichen Standards in Deutschland und auch auf den hohen Stellenwert, den dieses Thema in den Medien genießt, zurück. Auf diese Weise erklärt sich auch, dass die Unternehmen die Entwicklung ihres CMS vornehmlich im Bereich des Datenschutzes abgeschlossen haben.

Im Bereich des Kartellrechts und Korruptionsstrafrechts vermuten die Befragten überwiegend eher geringe Haftungsrisiken innerhalb ihrer Branche (46 % bzw. 45 %). Wir meinen allerdings, dass vor allem die kartellrechtlichen Haftungsrisiken unterschätzt werden, verfügt doch bis heute kaum mehr als jedes zweite Unternehmen mit CMS über eine kartellrechtliche Compliance (55 %, siehe Seite 56). Die Gefahren der Strafverfolgung inklusive der Verhängung empfindlicher Bußgelder haben jedoch auch infolge der Kronzeugenregelungen der Europäischen Kommission und des Bundeskartellamts deutlich zugenommen.[53]

Abb. 43 Einschätzung der Haftungsrisiken in der eigenen Branche



Basis: alle befragten Unternehmen

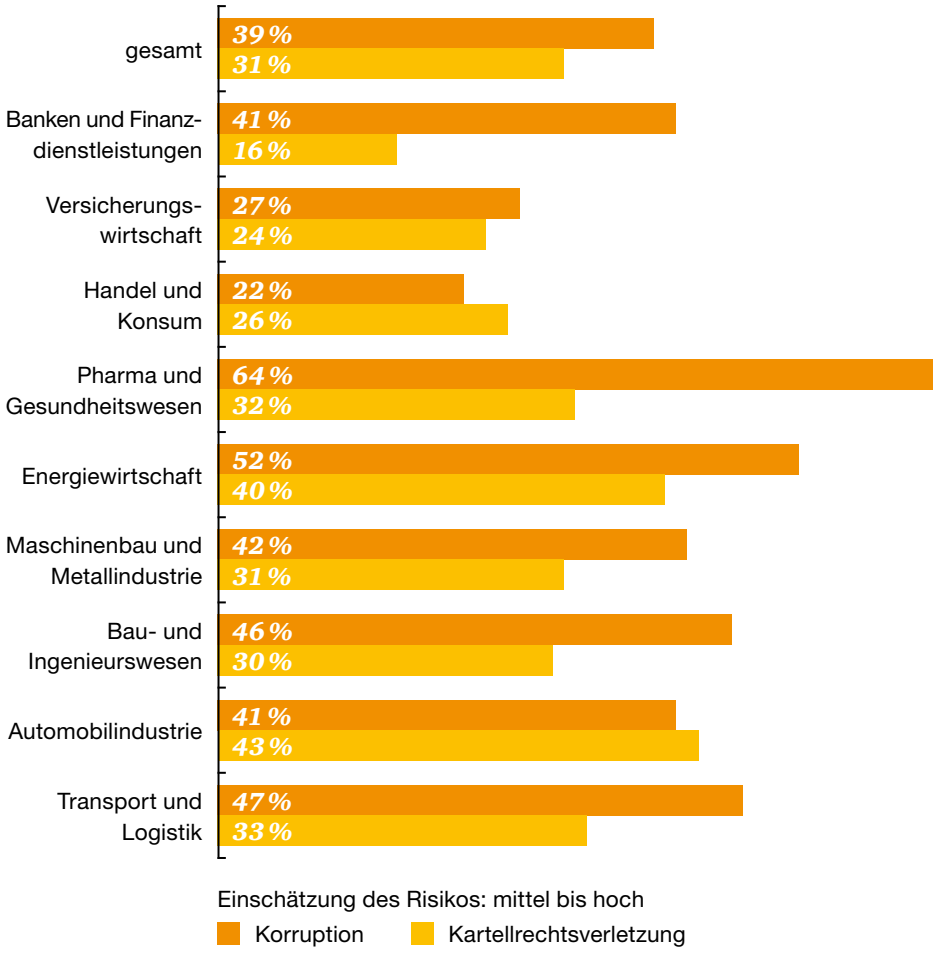
[53] Vgl. PwC, Wirtschaftskriminalität und Unternehmenskultur 2013, S. 58 ff.

Die Haftungsrisiken werden von den verschiedenen Branchen teilweise unterschiedlich beurteilt. Mit Blick auf das Korruptionsstrafrecht gehen 39 % der befragten Unternehmen aller Branchen von einem mittleren bis hohen Risiko aus. Das höchste Haftungsrisiko wird im Gesundheitswesen angenommen (64 %). Dies ist insofern bemerkenswert als die bestehende strafrechtliche Lücke bei der Strafbarkeit niedergelassener Ärzte vom deutschen Gesetzgeber noch nicht geschlossen wurde. Der vorgesehene eigene Straftatbestand zur Bekämpfung von Korruption im Gesundheitswesen (§ 299a StGB) wurde noch nicht verabschiedet.

Überdurchschnittlich hoch werden die korruptionsstrafrechtlichen Haftungsrisiken auch in der Energiewirtschaft (52 %), im Bau- und Ingenieurwesen (46 %) und im Bereich Transport und Logistik (47 %) eingeschätzt. Als überwiegend gering werden sie vor allem in der Versicherungswirtschaft (27 %) sowie in Handel und Konsumgüterindustrie (22 %) eingestuft.

Die kartellrechtlichen Haftungsrisiken werden im branchenübergreifenden Durchschnitt von einem knappen Drittel der Unternehmen innerhalb ihrer Branchen als mittel bis hoch eingestuft (31 %). Am höchsten werden diese Risiken in der Automobilindustrie (43 %) und Energiewirtschaft (40 %) eingeschätzt, am niedrigsten in Handel und Konsumgüterindustrie (26 %), in der Versicherungswirtschaft (24 %) sowie im Banken- und Finanzdienstleistungssektor (16 %).

Abb. 44 Einschätzung der Haftungsrisiken nach Branchen



Basis: alle befragten Unternehmen

Befürwortung von Compliance-Anreizen in der Unternehmenshaftung

In unserer letzten Studie zur Wirtschaftskriminalität 2013 haben wir ausführlich über die wachsenden Haftungsrisiken bei Korruption und wettbewerbswidrigen Absprachen berichtet. Für internationale Unternehmen, die dem FCPA oder dem UK Bribery Act unterliegen, bestehen im Falle von Korruptionsvorwürfen zusätzliche Strafverfolgungsrisiken. Aber auch im Kartellrecht haben die Haftungsrisiken vor allem aufgrund der Kronzeugenregelungen deutlich zugenommen.[54] Nur die wenigsten Unternehmen stufen die Haftungsrisiken innerhalb ihrer Branche als vernachlässigbar ein (siehe Seite 72).

In Deutschland erwägt der Gesetzgeber eine Reform der bußgeldrechtlichen bzw. strafrechtlichen Unternehmenshaftung. Dabei geht es zum einen um die Frage, ob Deutschland es weiterhin bei einer Haftung nach dem Ordnungswidrigkeitenrecht belässt oder aber ein eigenständiges Verbandsstrafrecht eingeführt werden sollte. Neben dieser eher rechtlichen wie rechtspolitischen Gestaltungsfrage richtet sich der Blick zunehmend auf Regelungen, die Unternehmen Anreize zum Aufbau eines effektiven CMS geben und im Falle eines strafbaren Vorfalls zugleich eine Honorierung ihrer Kooperation mit den Behörden vorsehen.

Wir haben die Unternehmen gebeten, sich zu diesen Reformvorschlägen zu äußern. Die große Mehrheit hält die Vorschläge für überlegenswert und vielfach sogar für sinnvoll, nur wenige lehnen sie ab. Unternehmen, die bereits über ein entwickeltes CMS verfügen, stehen diesen Reformvorschlägen aufgeschlossener gegenüber. Diese Gruppe umfasst zwei Drittel der Unternehmen.[55]

Eine gesetzliche Regelung, die Mindestaufsichts- bzw. Mindest-Compliance-Standards zur Schaffung von Rechtssicherheit enthält, halten 37 % der Unternehmen mit einem entwickelten CMS für sinnvoll und fast jedes zweite Unternehmen hält eine solche Regelung für überlegenswert (47 %).[56] Anders stellt sich das Meinungsbild bei Unternehmen dar, deren CMS sich allenfalls im Aufbau befindet. Hier befürworten nur 15 % eine solche Regelung. Aber auch in dieser Gruppe meinen immerhin 60 %, sie sei überlegenswert; 25 % lehnen sie ab.

Die unterschiedlichen Beurteilungen der beiden Gruppen sind verständlich. Unternehmen mit einem CMS sind an Rechtssicherheit interessiert. Anders als etwa die US-amerikanischen Guidelines zum FCPA enthält das deutsche Recht keine gesetzlich definierten Mindestanforderungen an Compliance-Programme (Ausnahme § 25h KWG[57] für Finanzinstitute).

---

[54] Vgl. PwC, Wirtschaftskriminalität und Unternehmenskultur 2013, S. 36 ff. und 70 ff.

[55] Zur Gruppe der Unternehmen mit einem entwickelten CMS gehören Unternehmen, die über ein CMS verfügen, dessen Aufbau aus ihrer Sicht bezogen auf mindestens zwei Deliktsfelder abgeschlossen ist. Hierzu zählen mehr als zwei Drittel der Unternehmen (68 %).

[56] Vgl. Gesetzgebungsvorschlag für eine Änderung der §§ 30, 130 OWiG durch den Bundesverband der Unternehmensjuristen – Fachgruppe Compliance, S. 9 f., online abrufbar unter: www.buj.net → Verband → Stellungnahmen → Gesetzgebungsvorschlag: Fachgruppe Compliance plädiert für Kronzeugenregelung in der Compliance → Gesetzgebungsvorschlag als PDF; Deutsches Institut für Compliance e. V.; Vorschlag für den Entwurf eines Gesetzes für Compliance-Maßnahmen in Betrieben und Unternehmen – Compliance-Anreiz-Gesetz, S. 9 f., online abrufbar unter: http://dico-ev.de/fileadmin/PDF/Arbeitsergebnisse/Arbeitsergebnisse/_CompAG_21_07_2014.pdf.

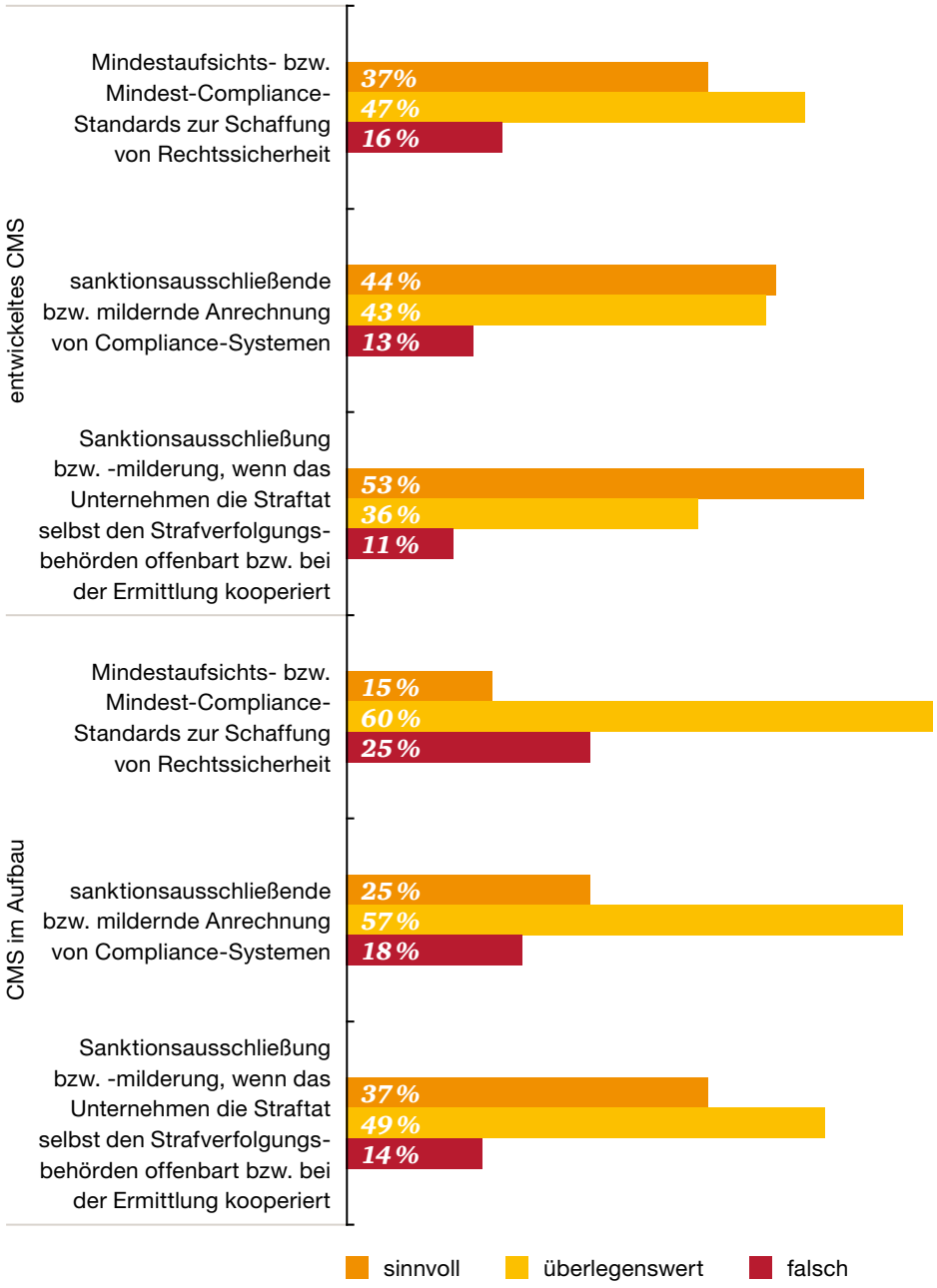
[57] Gesetz über das Kreditwesen.

Unternehmen mit einem entwickelten CMS zeigen sich auch deutlich häufiger an einer Regelung zur sanktionsausschließenden bzw. -mildernden Anrechnung von CMS interessiert. 44 % bewerten dies als sinnvoll, gegenüber 25 % aus der Vergleichsgruppe.[58]

Unternehmen mit einem CMS versprechen sich nicht nur Vorteile im Wettbewerb, sondern auch in der Auseinandersetzung mit der Justiz, wenn man sich trotz aller Compliance-Bemühungen einem strafrechtlichen Ermittlungsverfahren ausgesetzt sieht. Schon jetzt sehen Compliance-Programme vielfach dezidiert eine Kooperation mit den Strafverfolgungsbehörden vor.

Unternehmen mit einem CMS trauen sich wohl auch eher zu, strafbare Compliance-Verstöße aufzudecken, sodass sie für eine Strafanzeige verständlicherweise ein Entgegenkommen von den strafrechtlichen Ermittlungsbehörden erwarten.[59] Aus diesem Grund befürwortet über die Hälfte dieser Unternehmen eine Regelung, die diese Möglichkeit anders als in der bisherigen Rechtslage dezidiert vorsieht (53 %). Weitere 36 % halten dies für überlegenswert.

Abb. 45 Beurteilung gesetzlicher Regelungen im Falle einer Reform der Unternehmenshaftung



Basis: alle befragten Unternehmen

[58] Vgl. Stellungnahme der Bundesrechtsanwaltskammer zur Einführung einer Unternehmensstrafe, S. 10, online abrufbar unter: www.brak.de → Stellungnahmen der BRAK → Stellungnahmen 2013 → Mai Stellungnahme der BRAK 2013/09; Gesetzgebungsvorschlag für eine Änderung der §§ 30, 130 OWiG durch den Bundesverband der Unternehmensjuristen – Fachgruppe Compliance, S. 8, online abrufbar unter: www.buj.net → Verband → Stellungnahmen → Gesetzgebungsvorschlag: Fachgruppe Compliance plädiert für Kronzeugenregelung in der Compliance → Gesetzgebungsvorschlag als PDF; Deutsches Institut für Compliance e. V.; Vorschlag für den Entwurf eines Gesetzes für Compliance-Maßnahmen in Betrieben und Unternehmen – Compliance-Anreiz-Gesetz, S. 3 ff., online abrufbar unter: http://dico-ev.de/fileadmin/PDF/Arbeitsergebnisse/Arbeitsergebnisse/_CompAG_21_07_2014.pdf.

[59] Vgl. Gesetzgebungsvorschlag für eine Änderung der §§ 30, 130 OWiG durch den Bundesverband der Unternehmensjuristen – Fachgruppe Compliance, S. 8, online abrufbar unter: www.buj.net → Verband → Stellungnahmen → Gesetzgebungsvorschlag: Fachgruppe Compliance plädiert für Kronzeugenregelung in der Compliance → Gesetzgebungsvorschlag als PDF.

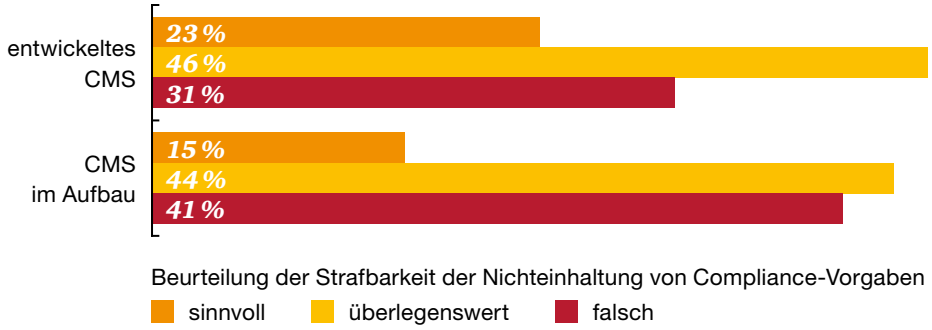
Seit November 2015 gilt: Mitarbeiter können strafrechtlich wegen Korruption belangt werden, wenn sie damit gegen die Compliance-Vorgaben ihres Unternehmens verstoßen.

Aufgeschlossenheit gegenüber Reform des Korruptionsstrafrechts im privaten Sektor

Im November 2015 trat eine Neufassung des Straftatbestands zur Bekämpfung der Bestechlichkeit und Bestechung im geschäftlichen Verkehr in Kraft.[60] Durch die Reform des § 299 StGB droht Mitarbeitern nicht nur bei Formen von Korruption in einer Wettbewerbssituation eine Strafverfolgung (sog. Wettbewerbsmodell), sondern auch dann, wenn sie gegen Compliance-Vorgaben ihres Unternehmens verstoßen (sog. Geschäftsherrenmodell).[61] Auf diese Weise erhält das Compliance-Management eines Unternehmens eine auch in symbolischer Hinsicht wohl nicht zu unterschätzende Unterstützung durch das Strafrecht, wobei den betroffenen Unternehmen durch das Erfordernis des Strafantrags ein Ermessensspielraum erhalten bleibt.

Die Mehrheit der befragten Unternehmen beurteilt diese Reform als sinnvoll oder als überlegenswert. Unternehmen mit einem entwickelten CMS befürworten jedoch eher eine Ausdehnung der Strafbarkeit. Ein knappes Viertel dieser Unternehmen hält eine solche Reform für sinnvoll (23 %) und fast die Hälfte für überlegenswert (46 %). Demgegenüber äußern sich Unternehmen kritischer, deren Compliance sich noch im Aufbau befindet: 41 % halten die Einführung des Geschäftsherrenmodells für falsch.

Abb. 46 Beurteilung der Reform des § 299 StGB im Sinne des Geschäftsherrenmodells



Basis: alle befragten Unternehmen

[60] Zur Begründung siehe Gesetzentwurf: BT-Drs. 18/4350; vgl. beispielsweise auch Kubiciel, in: Zeitschrift für Internationale Strafrechtsdogmatik (ZIS) 13/2014, 667 ff.; Dannecker, Schröder, in: Zeitschrift für Rechtspolitik (ZRP) 2015, 48 ff.; krit. Schünemann, in: ZRP 2015, 68 ff.

[61] § 299 Abs. 1 Nr. 2 StGB n. F.: „ […] ohne Einwilligung des Unternehmens einen Vorteil für sich oder einen Dritten als Gegenleistung dafür fordert, sich versprechen lässt oder annimmt, dass er bei dem Bezug von Waren oder Dienstleistungen eine Handlung vornehme oder unterlasse und dadurch seine Pflichten gegenüber dem Unternehmen verletze.“ Ähnlich die Variante für die aktive Bestechung gemäß § 299 Abs. 2 Nr. 2 StGB n. F.

Beurteilung eines Korruptionsstraftatbestands im Gesundheitswesen

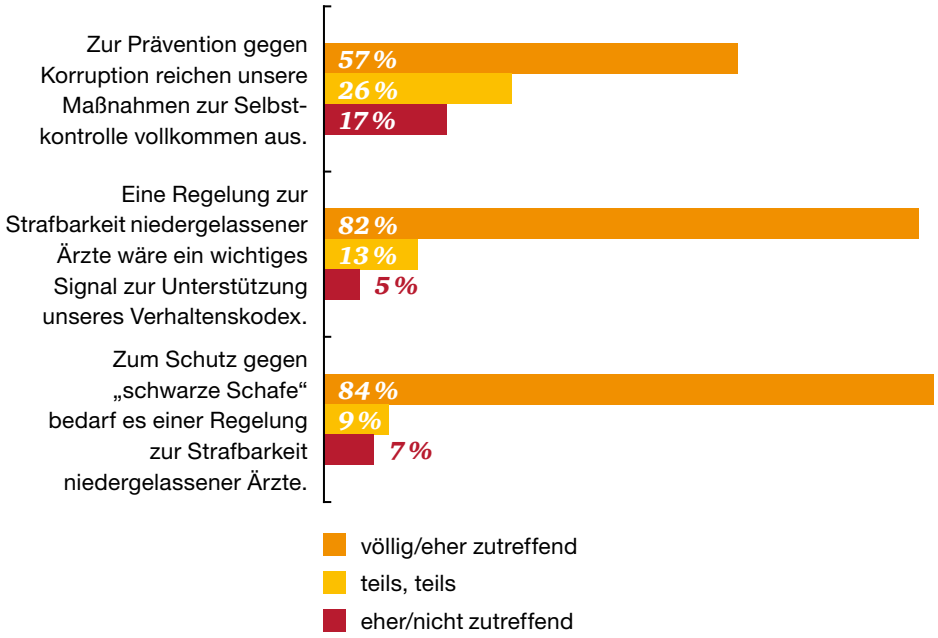
Der Gesetzgeber beabsichtigt in seinem Regierungsentwurf vom August 2015 die Einführung eines neuen Gesetzes zur Bekämpfung von Korruption im Gesundheitswesen (§ 299a StGB).[62] Diese Reform wurde nach der Entscheidung des Großen Senats des BGH vom März 2012 notwendig, nach der die geltenden Korruptionstatbestände nicht auf niedergelassene Vertragsärzte angewendet werden können und somit eine Strafbarkeitslücke besteht.[63]

Über die Hälfte (57 %) der befragten Unternehmen im Gesundheitswesen[64] gab an, dass ihre Maßnahmen zur Korruptionsprävention zur Selbstkontrolle vollkommen ausreichen, ein Viertel (26 %) äußerte sich skeptisch und 17 % teilen diese Einschätzung nicht. Die Branche neigt somit hinsichtlich ihrer Fähigkeit zur Selbstregulierung nur zu einer tendenziell positiven Beurteilung.

Auf der anderen Seite sieht eine deutliche Mehrheit (82 %) der Unternehmen in einer Regelung zur Strafbarkeit niedergelassener Ärzte durchaus ein wichtiges Signal zur Unterstützung ihres Verhaltenskodex, nur eine Minderheit teilt diese Auffassung nicht (5 %). Konsens besteht vor allem darüber, dass es zum Schutz gegen „schwarze Schafe“ einer entsprechenden strafrechtlichen Regelung bedarf (84 %), während dies nur von 7 % der Unternehmen im Gesundheitswesen abgelehnt wird, 9 % sind geteilter Meinung.

Die Mehrheit der Unternehmen im Gesundheitswesen begrüßt somit die Einführung eines strafrechtlichen Schutzes vor Korruption in der Branche. Die Notwendigkeit einer derartigen Regelung zeigt auch unsere Studie zur Wirtschaftskriminalität in der Pharmaindustrie 2013, deren Ergebnisse auf hohe Korruptionsrisiken schließen lassen. Ein großer Anteil der befragten Pharmaunternehmen gab hier an, dass bei fast allen geschäftlichen Aktivitäten, in die Ärzte involviert sind, ein mittleres bis sehr hohes Korruptionsrisiko besteht.[65]

Abb. 47 Beurteilung eines Korruptionsstraftatbestands im Gesundheitswesen (§ 299a StGB)



Basis: Unternehmen im Gesundheitswesen

[62] Regierungsentwurf eines Gesetzes zur Bekämpfung von Korruption im Gesundheitswesen, online abrufbar unter: www.bmjv.de → suche 299a → RegE vom 05.08.2015 als PDF.
[63] Beschluss des BGH vom 29.03.2012 – Großer Senat für Strafsachen (GSSt) 2/11.
[64] Die Stichprobe der Unternehmen aus dem Gesundheitswesen umfasst Unternehmen aus der Pharmaindustrie (n = 24) und anderen Unternehmen aus dem Gesundheitswesen (n = 32).
[65] Vgl. PwC, Wirtschaftskriminalität Pharmaindustrie 2013, S. 12.

Compliance-Audit

CMS sind als Best Practice auf dem Weg, zum Standard zu werden. Doch nur eine Minderheit der befragten Unternehmen lässt die Sicherheitsprogramme von externen Fachleuten prüfen. Nur 39 % verfügen über eine Zertifizierung, bei 38 % ist das nicht einmal geplant.

Am geläufigsten ist die Zertifizierung nach IDW PS 980, die sich auch für mittelständische Unternehmen eignet. Der internationale CMS-Standard ISO 19600, der erst im Dezember 2014 eingeführt wurde, ist vor allem in Großunternehmen bekannt.

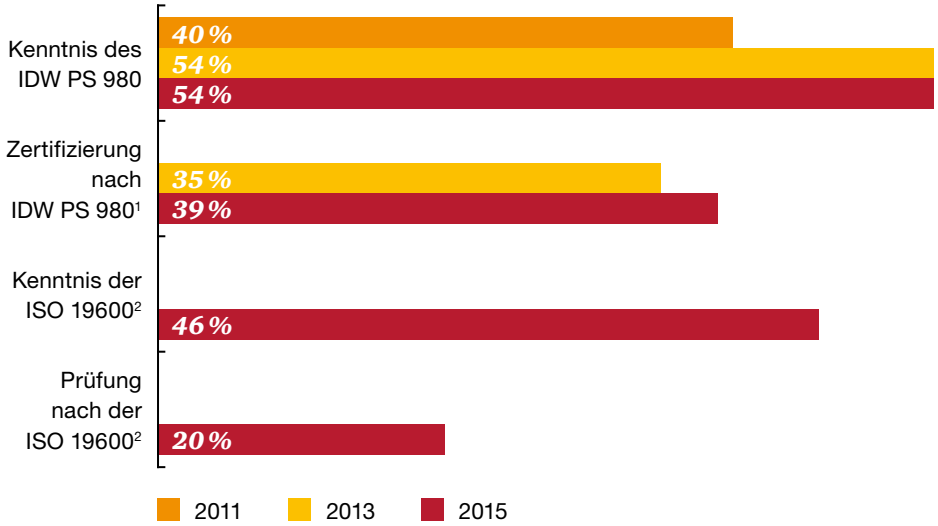
Bedeutung des IDW PS 980 und der ISO 19600

Der IDW PS 980[66] ist mehr als der Hälfte der Unternehmen (54 %) bekannt und über ein Drittel der Unternehmen (39 %), die den Standard kennen, haben eine Auditierung ihres CMS auf dieser Basis durchgeführt. Der erst im Dezember 2014 eingeführte internationale Standard für CMS ISO 19600[67] erreicht bereits eine hohe Bekanntheit, 46 % haben hiervon Kenntnis und 20 % dieser Unternehmen haben eine Zertifizierung nach diesem neuen Standard vornehmen lassen.

Der IDW PS 980 ist mittelständischen Unternehmen wie auch Großunternehmen gleichermaßen bekannt. Bemerkenswerterweise beschränkt sich das Interesse an einer Zertifizierung nach diesem Standard nicht auf Großunternehmen mit über 10.000 Mitarbeitern: Eine derartige Evaluation ist auch für mittelständische Unternehmen mit 500 bis 999 Mitarbeitern attraktiv; bei knapp der Hälfte (45 %) wurde eine Auditierung des CMS anhand von IDW PS 980 durchgeführt. Dies dürfte auch eine Folge des Drucks in der Lieferkette sein, wie die Ergebnisse unserer Studie nahelegen. Jedes vierte Großunternehmen mit mehr als 4.999 Mitarbeitern sieht unter anderem in seinen Verträgen regelmäßig auch eine Klausel zur Zertifizierung des Compliance-Managements seines Vertragspartners vor (23 % bzw. 26 %, siehe Seite 61).

Die ISO 19600 weist den höchsten Bekanntheitsgrad bei Großunternehmen mit über 4.999 Mitarbeitern auf. Auch erfolgte eine entsprechende Auditierung häufiger bei Großunternehmen.

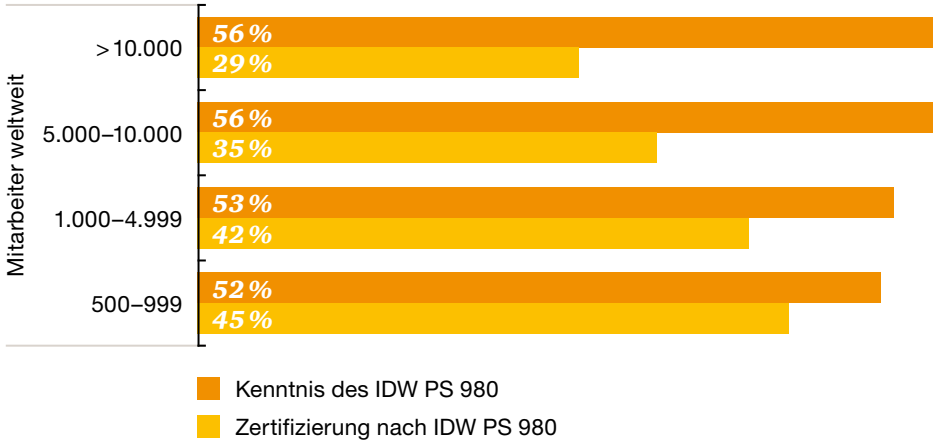
Abb. 48 Kenntnis des IDW PS 980 und der ISO 19600 sowie Zertifizierung des CMS



Basis: Anteil der Unternehmen mit Zertifizierung nach IDW PS 980 bzw. ISO 19600 für Unternehmen, die den jeweiligen Standard kennen

[1] Keine Daten für 2011.
[2] Keine Daten für 2011 und 2013.

Abb. 49 Kenntnis des IDW PS 980 und erfolgte Zertifizierung nach Unternehmensgröße

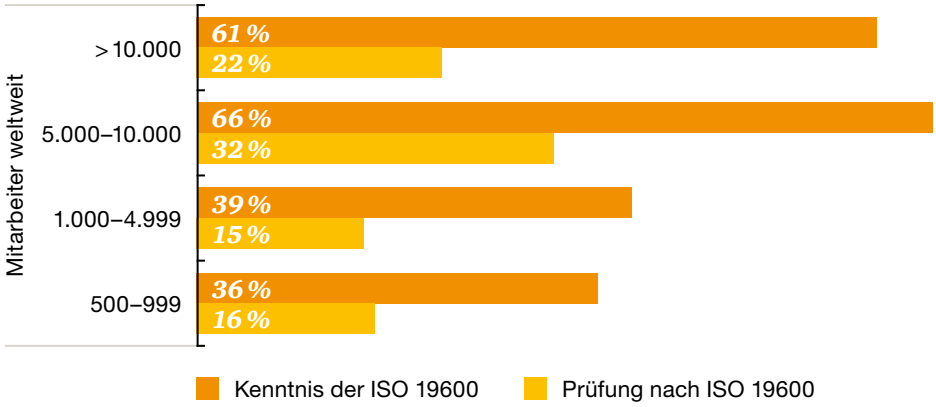


Basis: Anteil der Unternehmen mit Zertifizierung nach IDW PS 980 für Unternehmen, die den Standard kennen

[66] IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980), IDW Verlag.
[67] International Standard ISO 19600: 2014 Compliance management systems — Guidelines, 15.12.2014, Genf.

Der Anteil der Unternehmen, die ihr CMS zertifizieren lassen, stagniert. Die meisten führen ein Audit nur auf Druck von Geschäftspartnern durch.

Abb. 50 Kenntnis der ISO 19600 und erfolgte Zertifizierung nach Unternehmensgröße



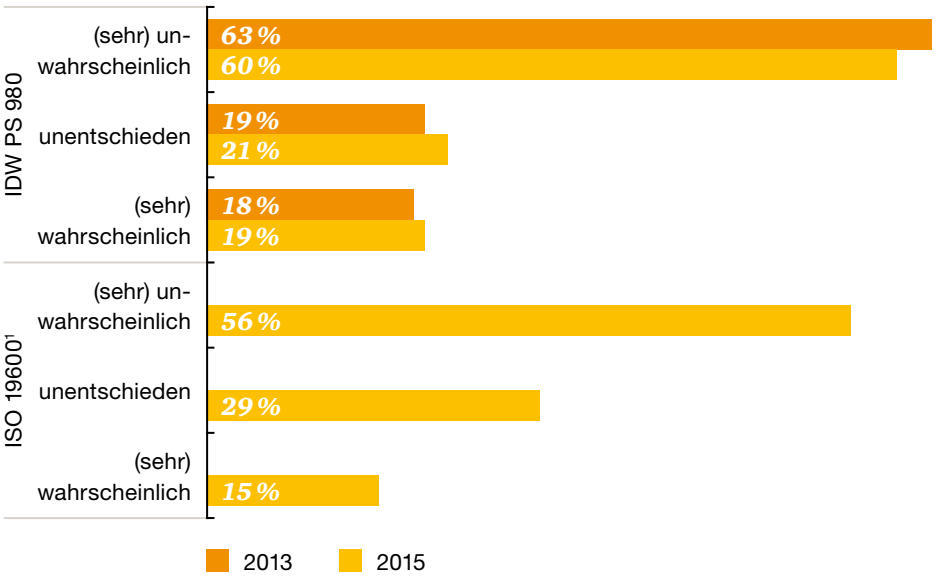
Basis: Anteil der Unternehmen mit Prüfung nach ISO 19600 für Unternehmen, die den Standard kennen

Compliance-Audit noch nicht selbstverständlich

Obwohl ein CMS heute zur Best Practice gehört, beabsichtigen knapp zwei Drittel der Unternehmen auch in den nächsten zwei Jahren nicht, eine Auditierung nach IDW PS 980 vornehmen zu lassen. Ein Fünftel ist noch unentschieden und ein weiteres Fünftel wird sein CMS „wahrscheinlich" einer Evaluation unterziehen. Ähnlich verhalten ist das Interesse an der ISO 19600.

In den letzten zwei Jahren ist hier somit keine merkliche Entwicklung zu erkennen. Noch zu wenige Unternehmen sind bereit, eine unabhängige Prüfung der Qualität ihres CMS durchzuführen.

Abb. 51 Wahrscheinlichkeit einer Zertifizierung nach IDW PS 980 und ISO 19600 in den nächsten zwei Jahren



Basis: IDW PS 980 bzw. ISO 19600 bekannt und Zertifizierung noch nicht durchgeführt

[1] Keine Daten für 2013.

Ihre Ansprechpartner

PwC

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

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

Steffen Salvenmoser
Partner
Forensic Services
Tel.: +49 69 9585-5555
steffen.salvenmoser@de.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 157 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. 9.800 engagierte Menschen an 29 Standorten. 1,65 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 in der analogen und der digitalen Wirtschaft 2016

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

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

Unter Mitarbeit von Dr. phil. Anja Niemeczek (Dipl.-Psych.), M.Sc. oec. Marcel Vockrodt, Economy & Crime Research Center, Halle (Saale), Ass. jur. Nicole Selzer, Dipl. jur. Tobias Günther und Dr. oec. Marc Jeker

Durchführung der Befragung durch Oliver Krieg, Director Social & Opinion, TNS Emnid, Bielefeld

Februar 2016, 86 Seiten, 51 Abbildungen, Softcover

Alle Rechte vorbehalten. Vervielfältigungen, Mikroverfilmung, die Einspeicherung und Verarbeitung in elektronischen Medien sind ohne Zustimmung der Herausgeber 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 Aktiengesellschaft 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 2016 PricewaterhouseCoopers Aktiengesellschaft Wirtschaftsprüfungsgesellschaft. Alle Rechte vorbehalten.
„PwC“ bezeichnet in diesem Dokument die PricewaterhouseCoopers Aktiengesellschaft Wirtschaftsprüfungsgesellschaft, die eine Mitgliedsgesellschaft der PricewaterhouseCoopers International Limited (PwCIL) ist. Jede der Mitgliedsgesellschaften der PwCIL ist eine rechtlich selbstständige Gesellschaft.