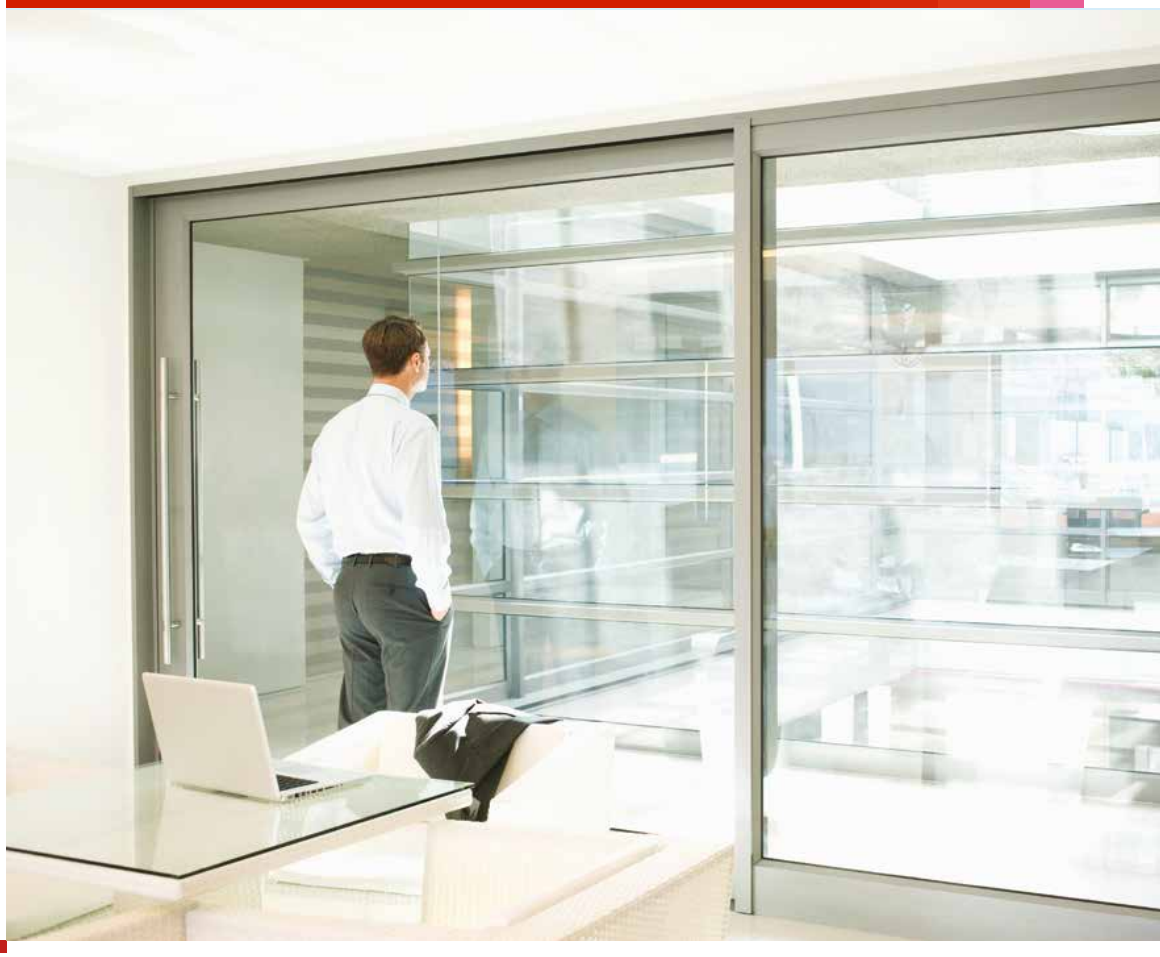
www.pwc.de

Wirtschaftskriminalität 2018 – Compliance in der Versicherungswirtschaft

Wachsende Risiken bei digitaler Wirtschaftskriminalität

Diese Sonderauswertung informiert Sie über die Sicherheitslage in der deutschen Versicherungswirtschaft.



MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG

pwc

Wirtschaftskriminalität 2018 – Compliance in der Versicherungswirtschaft

Wachsende Risiken bei digitaler Wirtschaftskriminalität

Diese Sonderauswertung informiert Sie über die Sicherheitslage in der deutschen Versicherungswirtschaft.

MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG

Wirtschaftskriminalität 2018 – Compliance in der Versicherungswirtschaft

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

Von Prof. Dr. jur. Kai-D. Bussmann, Gunter Lescher und Steffen Salvenmoser

Unter Mitarbeit von Dr. phil. Anja Niemeczek, Economy & Crime Research Center, Halle (Saale)

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

November 2018, 32 Seiten, 16 Abbildungen, Softcover

Zusammenfassung

Rasanter Anstieg der Fälle von Cybercrime

Die vorliegende vierte Sonderauswertung unserer Studie zur Wirtschaftskriminalität in der Versicherungsbranche zeigt einen leichten Rückgang der analogen Wirtschaftskriminalität, jedoch einen rasanten Anstieg der digitalen. Rund jeder zweite Versicherer (53 %) berichtete über mindestens eine Form von Cybercrime (alle Branchen 46 %). Im Vergleich zu unserer Studie aus dem Jahr 2016 entspricht dies einem Zuwachs von 19 Prozentpunkten. Damit sind mehr Versicherer von Cybercrime betroffenen als von analogen Formen (45 %) der Wirtschaftskriminalität. Zugenommen haben vor allem Fälle von Computerbetrug (25 %), das Ausspähen und Abfangen von Daten (13 %) sowie Verstöße gegen Patent- und Markenrechte (8 %).

CEO-Fraud als Risiko

Auch CEO-Fraud und Schädigungsversuche durch Ransomware gehören bei Versicherern mittlerweile in gleichem Ausmaß zum Bedrohungspotenzial wie in der übrigen Wirtschaft. 38 % der befragten Versicherer berichteten über einen versuchten CEO-Fraud in den letzten zwei Jahren (alle Branchen 40 %) und 13 % über Verschlüsselungs- bzw. Erpressungstrojaner mit geringen Schadensfolgen (alle Branchen 16 %). Bei 5 % der Versicherer führten Trojanerattacken sogar zu schweren Schäden.

Geldwäsche-Verdachtsfälle konstant hoch

Im Bereich der analogen Wirtschaftskriminalität bleibt der Anteil der Versicherer, die einen Verdacht auf Geldwäsche hatten, weiterhin überdurchschnittlich hoch (34 %; alle Branchen 12 %). Jeder zehnte Versicherer berichtete sogar über einen aufgedeckten Fall von Geldwäsche. Allerdings steht dieser Befund möglicherweise im Zusammenhang mit den gesetzlichen Vorgaben zur Geldwäscheprävention und den daraus resultierenden Kontrollmaßnahmen und Überwachungspflichten, die wiederum die Fallzahl erhöhen.

Vermögensdelikte und Datendiebstähle rückläufig

Hingegen beobachten wir bei den besonders häufigen Vermögensdelikten im langjährigen Vergleich einen Rückgang auf nunmehr 33 % der betroffenen Versicherer (alle Branchen 32 %). Eine positive Entwicklung zeigt sich auch beim Diebstahl vertraulicher Kunden- und Unternehmensdaten: Nur 5 % der befragten Versicherer berichteten über einen solchen Fall. Allerdings besteht weiterhin ein höherer Anteil an Verdachtsfällen auf Diebstahl vertraulicher Kunden- und Unternehmensdaten. 16 % der Versicherer berichteten über mindestens einen entsprechenden Verdachtsfall (alle Branchen 14 %).

Compliance-Systeme bleiben im Aufwind

Der Trend zur Compliance ist auch in der Versicherungswirtschaft unumkehrbar. Die Schwerpunkte der vom Compliance-Managementsystem (CMS) umfassten Rechtsgebiete liegen im Bereich der Vermeidung von Datenschutzverletzungen (92 %) und Korruption (86 %). Neu hinzugekommen sind kartellrechtliche Compliance-Programme (81 %); in der Studie von 2016 hatten nur 43 % der Versicherer das Thema Kartellrecht in ihren Compliance-Programmen.

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

Die befragten Versicherer sehen berechtigterweise einen starken Anstieg der rechtlichen Anforderungen an das CMS (76 %; alle Branchen 59 %) und haben hieraus Konsequenzen gezogen. Compliance-Programme sind in der Versicherungswirtschaft absolut selbstverständlich; 95 % der Versicherer verfügen über ein CMS (alle Branchen 75 %). Demgemäß hat die Mehrheit von ihnen in diesem Bereich ihre Personal- und Sachmittelausstattung verbessert. Eine leichte Aufstockung erfolgte bei jedem zweiten Versicherer (alle Branchen 33 %), eine deutliche sogar bei jedem fünften (alle Branchen 22 %) (vgl. S. 21). Auch stellen wir bei der Evaluation der CMS einen Anstieg um 14 Prozentpunkte fest. 58 % der Versicherer haben ihr CMS nach dem IDW Prüfungsstandard 980 auditiert, branchenübergreifend sind es lediglich 39 %.

Mit der vorliegenden Studie möchten wir Versicherungsunternehmen über die Risiken und Präventionschancen sowohl bei analoger als auch bei digitaler Wirtschaftskriminalität informieren. Allen Studienteilnehmern danken wir noch einmal herzlich für ihre Auskunftsbereitschaft.

Frankfurt am Main und Halle an der Saale im November 2018

Steffen Salvenmoser ***Gunter Lescher*** ***Prof. Dr. jur. Kai-D. Bussmann***

Inhaltsverzeichnis

Abbildungsverzeichnis

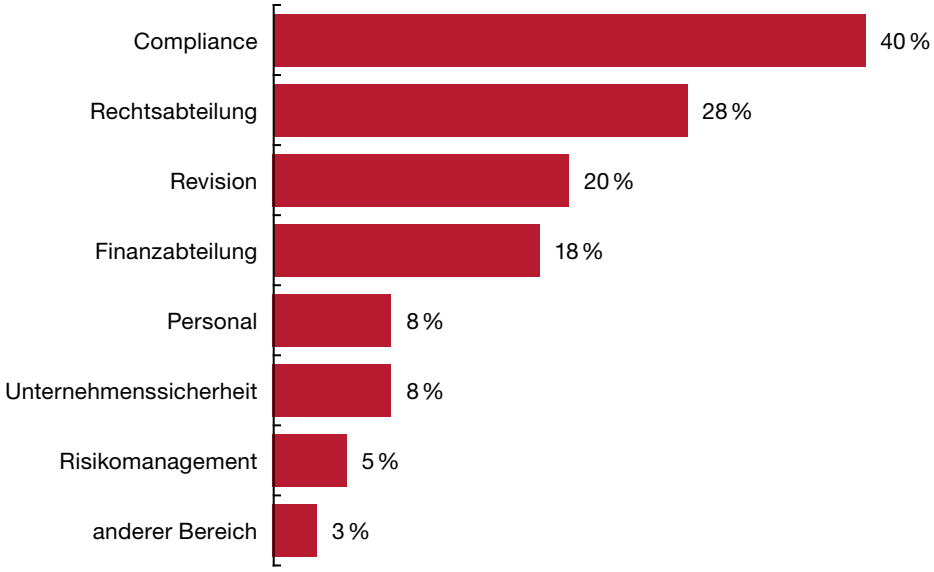
A Methodisches Vorgehen

Die neunte branchenübergreifende Studie zur Wirtschaftskriminalität wurde im Auftrag von PwC und der Martin-Luther-Universität Halle-Wittenberg in Deutschland durchgeführt. Von Juli bis September 2017 interviewte Kantar Emnid in Deutschland 500 Unternehmen. Bei der vorliegenden Studie handelt es sich um eine Sonderauswertung der Ergebnisse von 40 Unternehmen aus der Versicherungswirtschaft, die mit den Ergebnissen vorhergehender Studien verglichen werden. Aufgrund der Stichprobenziehung können die Ergebnisse als repräsentativ gelten. Details zur methodischen Durchführung können unserer branchenübergreifenden Wirtschaftskriminalitätsstudie 2018 entnommen werden.[1]

Die meisten Befragten in der Versicherungswirtschaft sind in der Compliance-Abteilung tätig (40 %). Die übrigen Interviewpersonen stammen aus den Bereichen Recht (28 %), Revision (20 %) und Finanzen (18 %) sowie aus sonstigen Bereichen.

Abb. 1 Funktion der Interviewperson in den befragten Versicherungsunternehmen

Mehrfachnennungen waren möglich.



In die Studie wurden fast ausschließlich Unternehmen einbezogen, die in Deutschland bzw. weltweit mindestens 500 Mitarbeiter beschäftigen. In der Stichprobe Versicherungswirtschaft handelt es sich bei einem Fünftel um mittelständische Versicherer mit weltweit 500 bis 1.000 Mitarbeitern (21 %). Über die Hälfte (56 %) verfügt weltweit über 1.000 bis 5.000 Mitarbeiter. International vertreten sind 58 % der befragten Versicherungsunternehmen, davon ein Fünftel weltweit.

[1] Vgl. PwC, Wirtschaftskriminalität 2018. Mehrwert von Compliance – forensische Erfahrungen, 2018, S. 12 f., www.pwc.de/de/risk/pwc-wikri-2018.pdf.

B Wachsende Risiken durch digitale Wirtschaftskriminalität

1 Rückgang der analogen Wirtschaftskriminalität

Im langfristigen Vergleich zeichnet sich auch in der Versicherungswirtschaft ein Rückgang der analogen Wirtschaftskriminalität ab. Mit Ausnahme eines Ausreißers im Jahr 2016 beobachteten wir im Zeitraum 2007 bis 2018 eine Verringerung der Gesamtkriminalität auf nunmehr 45 %. Gleiches gilt für den branchenübergreifenden Durchschnitt. Allerdings bleibt das Dunkelfeld weiterhin groß, wie sich auch an der kaum abnehmenden Zahl der Verdachtsfälle zeigt (siehe Kapitel B 2).

Auch bei den besonders häufigen Vermögensdelikten stellen wir im langjährigen Vergleich einen Rückgang auf nunmehr 33 % der betroffenen Versicherer fest (alle Branchen 32 %).[2] Eine positive Entwicklung beobachten wir seit 2007 auch beim Diebstahl vertraulicher Kunden- und Unternehmensdaten; nur 5 % der befragten Versicherer berichteten über einen derartigen Vorfall. Diese Entwicklung trifft auch auf die deutsche Wirtschaft insgesamt zu (alle Branchen 7 %).[3] Grund hierfür ist nach unserer Auffassung der auch in der Versicherungswirtschaft erreichte hohe Compliance- und Datenschutzstandard (siehe Kapitel C 1).

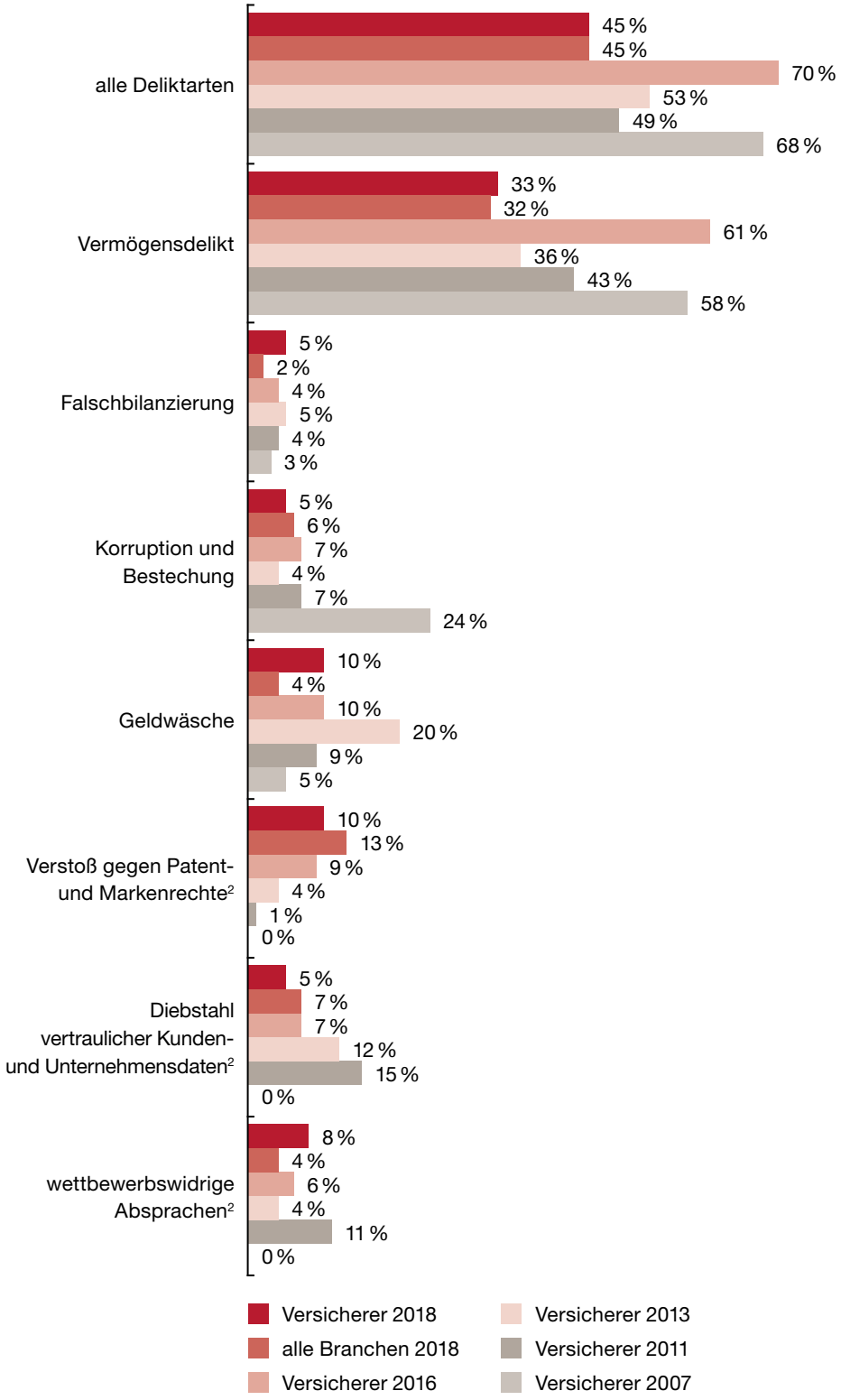
Eine Stagnation beobachten wir bei der Geldwäsche: Auch 2018 berichtete hier jeder zehnte Versicherer über einen entsprechenden Fall. Allerdings bleiben die Risiken für Geldwäsche hoch, wenn man die Verdachtsfälle mit berücksichtigt (34 %, siehe Kapitel B 2).[4] Unverändert niedrig ist der Anteil der von Korruption betroffenen Versicherer (5 %). Aber auch hier ist aber die Zahl der Verdachtsfälle mit 19 % deutlich höher (siehe Kapitel B 2).

Eine anhaltende Zunahme von Vorkommnissen stellen wir bei urheberrechtlichen Verstößen fest. Jeder zehnte Versicherer war von Verstößen gegen Patent- und Markenrechte betroffen (10 %). Hier entsprechen die Zahlen mittlerweile der durchschnittlichen Verbreitung in der übrigen Wirtschaft (13 %). Leicht zugenommen haben Berichte über wettbewerbswidrige Absprachen (8 %).

[2] Den hohen Anteil im Jahr 2016 (61 % Vermögendelikte) werten wir als Ausreißer.
[3] Vgl. PwC, Wirtschaftskriminalität 2018. Mehrwert von Compliance – forensische Erfahrungen, S. 16.
[4] Siehe zum Risikopotenzial der Geldwäsche in der Versicherungswirtschaft Bussmann, Geldwäsche-Prävention im Markt, 2018, Springer, S. 125 ff.

Abb. 2 Entwicklung von Wirtschaftskriminalität 2007–2018[1]

Mehrfachnennungen waren möglich.



[1] Die Grafik enthält keine Fälle von Industrie- und Wirtschaftsspionage, da in der Versicherungswirtschaft keine berichtet wurden.

[2] 2007 nicht erhoben

2 Kein Rückgang der Verdachtsfälle

Anders als bei den aufgedeckten Fällen liegt der Anteil der Verdachtsfälle in der Versicherungswirtschaft unverändert bei 63 %. Im Vergleich zu den Branchen insgesamt (56 %) berichteten die Versicherer, wie schon in den vorherigen Studien, über überdurchschnittlich viele Verdachtsfälle.

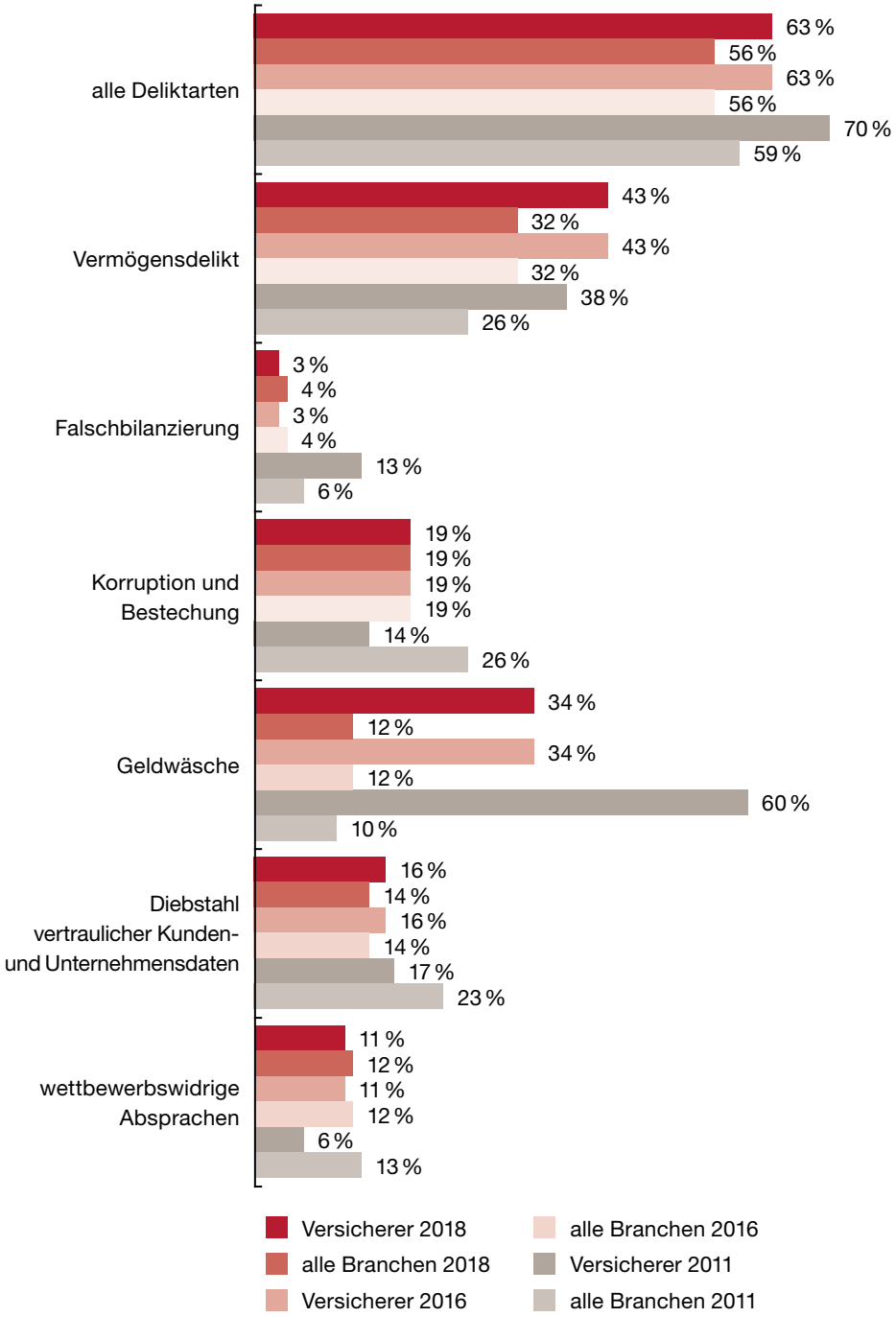
Dies gilt auch für den Verdacht auf ein Vermögensdelikt (43 %; alle Branchen 32 %). Überdurchschnittlich hoch ist zudem der Anteil derjenigen Versicherer, die über einen Verdacht auf Geldwäsche berichteten (34 %; alle Branchen 12 %). Gegenüber unserer Studie von 2011 stellen wir zwar eine positive Entwicklung fest (60 %), aber möglicherweise liegt die Fallzahl aufgrund der gesetzlich vorgeschriebenen Maßnahmen zur Geldwäscheprävention deutlich über dem Durchschnitt. Dies wäre besonders dann der Fall, wenn Kontroll- und Überwachungsmaßnahmen wirksam umgesetzt werden.

Unverändert ist auch der Anteil der Verdachtsfälle auf Korruption. Jeder fünfte Versicherer berichtete über einen derartigen Vorfall (19 %; alle Branchen 19 %). Ein CMS zur Korruptionsprävention gehört zum Standard der meisten Versicherer (86 %; siehe Kapitel C 1). Möglicherweise resultiert hieraus ein geschärftes Bewusstsein für das Thema Korruption, was wiederum zu einer konstanten Zahl an Verdachtsfällen führt. Das Kriminalitätsrisiko bleibt offenbar unverändert.

Ein Rückgang bei den Fällen von Verdacht auf Diebstahl vertraulicher Kunden- und Unternehmensdaten ist, anders als bei den aufgedeckten Fällen, nicht erkennbar. 16 % der Versicherer berichteten über mindestens einen Verdachtsfall (alle Branchen 14 %), aber nur 5 % über einen aufgedeckten Fall (siehe Abbildung 2). Diese Diskrepanz lässt auf ein weiterhin großes Dunkelfeld schließen. Zwar könnte die hohe Zahl der Verdachtsfälle auch auf eine erhöhte Sensibilität für das Thema zurückzuführen sein, die mit der Einführung eines entsprechenden CMS einhergeht, aber im Laufe der Jahre sollte sich dennoch eine allmähliche Reduzierung zeigen.

Abb. 3 Entwicklung der Verdachtsfälle 2011–2018[1]

Mehrfachnennungen waren möglich.



[1] Die Grafik enthält aufgrund zu geringer Fallzahlen keine Verdachtsfälle auf Industrie- und Wirtschaftsspionage (3 %) und Verstöße gegen Patent- und Markenrechte (4 %).

3 Starker Anstieg der Bedrohung durch Cybercrime

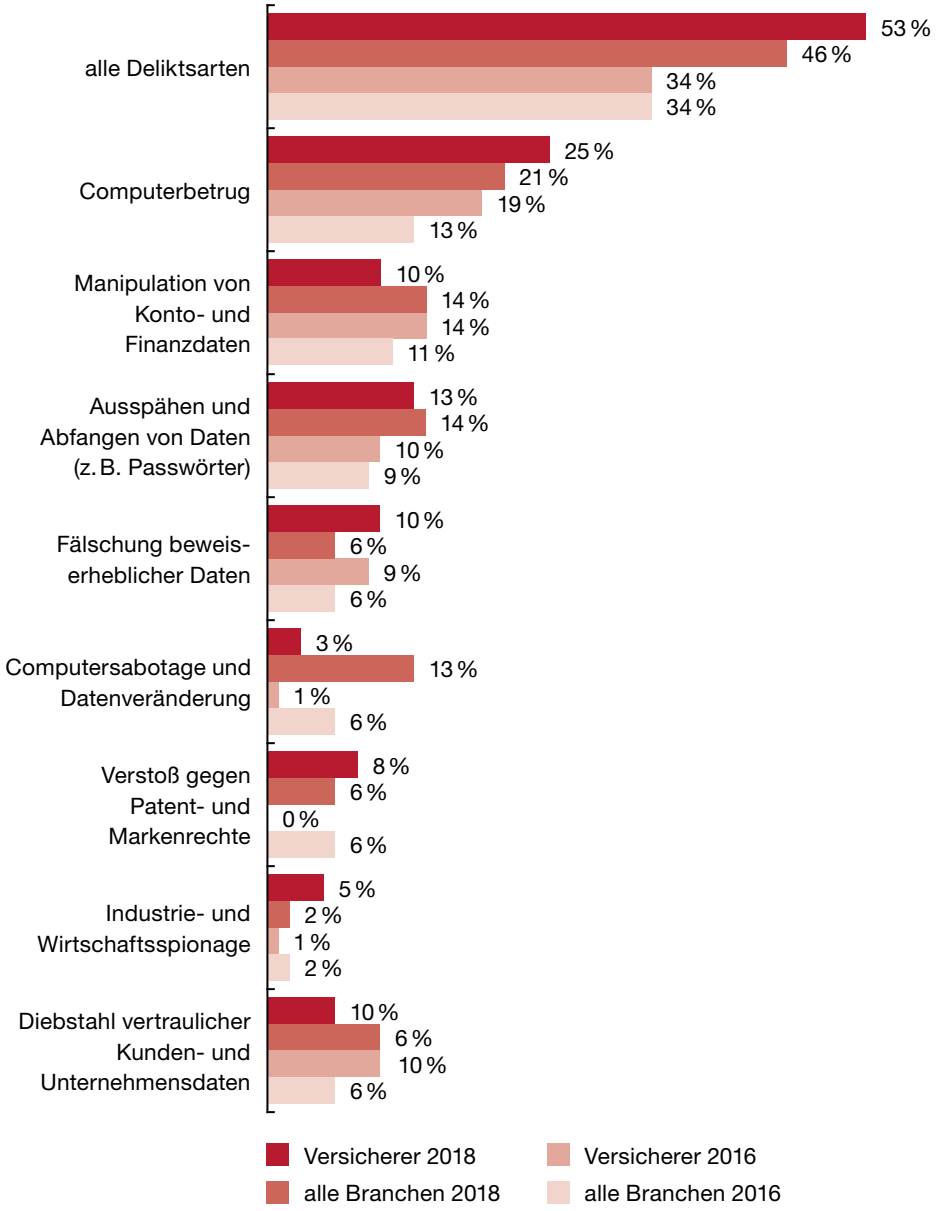
Im Vergleich zu unserer Studie von 2016 haben die Fälle von Cybercrime[5] in der Versicherungswirtschaft mit einem Anstieg um 19 Prozentpunkte stark zugenommen – das ist mehr als im branchenübergreifenden Vergleich. Jeder zweite Versicherer (53 %) berichtete über mindestens eine Form von Cybercrime (alle Branchen 46 %). Im Unterschied zur analogen Wirtschaftskriminalität beobachten wir somit eine wachsende Bedrohung durch Cybercrime. Gleichwohl unternimmt ein Drittel der Versicherer möglicherweise zu wenig gegen diese Risiken. Nur 69 % gaben an, das Thema Cybercrime und die damit verbundenen Rechtsgebiete über ein CMS zu anzugehen (siehe Kapitel C 1).

Zugenommen haben vor allem die Fälle von Computerbetrug (25 %), das Ausspähen und Abfangen von Daten (13 %) sowie Verstöße gegen Patent- und Markenrechte (8 %). Erhebliche Risiken bestehen zudem weiterhin aufgrund der Manipulation von Konto- und Finanzdaten, der Fälschung beweiserheblicher Daten und des Diebstahls vertraulicher Kunden- und Unternehmensdaten. Jeder zehnte Versicherer berichtete über derartige Fälle.

[5] Cybercrime umfasst Delikte, die nicht nur mittels bloßer Nutzung, sondern mittels gezielter Ausnutzung elektronischer Systeme und Kommunikationsmittel begangen wurden (auch: cyber-dependent crimes). Ausgeschlossen wurden Delikte, bei denen der Computer oder das Internet nur beiläufig gewählt wurden, etwa um die Begehung eines Betrugs zu vereinfachen.

Abb. 4 Von Cybercrime betroffene Versicherer 2016–2018

Mehrfachnennungen waren möglich.



4 CEO-Fraud und Ransomware

In unserer Studie wollten wir auch das Bedrohungspotenzial von CEO-Fraud, auch Fake President Fraud genannt, feststellen. Hierbei handelt es sich um eine Variante des Social Engineering[6], bei der Mitarbeiter, vorrangig aus dem Finanz- und Rechnungswesen, durch einen Anruf oder eine E-Mail vermeintlich im Auftrag des oberen Managements zur Überweisung eines größeren Geldbetrags auf ein ausländisches Konto aufgefordert werden.[7] Dabei werden die Mitarbeiter zumeist unter Druck gesetzt, den Transfer schnellstmöglich durchzuführen und Verschwiegenheit zu wahren, da es sich angeblich um ein geheimes oder vertrauliches Projekt handelt.[8]

Die Täter, die überwiegend der organisierten Kriminalität zuzurechnen sind,[9] sammeln zunächst öffentlich zugängliche Informationen über ein Unternehmen, etwa aus Wirtschaftsberichten, dem Handelsregister, der Website sowie Werbebroschüren, und tätigen gegebenenfalls zusätzlich direkte Anrufe, um Informationen zu erlangen und ihre gefälschte Kommunikation glaubwürdig zu gestalten.[10]

Das latente Risiko einer Schädigung durch CEO-Fraud ist auch in der Versicherungswirtschaft hoch: 38 % der befragten Versicherer berichteten über einen derartigen Versuch in den letzten zwei Jahren. Dies entspricht dem branchenübergreifenden Durchschnitt von 40 %. In 5 % der Fälle bei Unternehmen aller Branchen waren die Täter erfolgreich.[11] Die Schadensfolgen sind erheblich. Aus der Versicherungsbranche wurde kein erfolgreicher Fall dieses gravierenden Wirtschaftsdelikts gemeldet. In den letzten Jahren gaben in der Gesamtstudie zur Wirtschaftskriminalität sieben Unternehmen einen CEO-Fraud an, dieser verursachte im Durchschnitt einen Schaden von 4,4 Millionen Euro (alle Branchen). Erfolgreiche CEO-Fraud-Attacken erwiesen sich als die schadensträchtigsten Delikte im Bereich Cybercrime.[12]

---

[6] Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland, 2016, S. 22: „Social Engineering ist weiterhin eine vielfach genutzte Methode, um Cyber-Angriffe erfolgreich auszuführen oder zu unterstützen. Für Angreifer ist es einfacher, die Schwachstelle Mensch als oftmals schwächstes Glied der IT-Sicherheitskette zu überwinden, anstatt komplexe technische Sicherheitsmaßnahmen mit viel Aufwand zu umgehen."

[7] Vgl. BSI, Lagebericht IT-Sicherheit 2016, S. 23; Bundeskriminalamt (BKA), Bundeslagebild Wirtschaftskriminalität 2016, S. 8.

[8] Vgl. BSI, Pressemitteilung vom 10.07.2017.

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

[10] Vgl. BSI, Lagebericht IT-Sicherheit 2016, S. 23; BKA, Bundeslagebild Wirtschaftskriminalität 2016, S. 9.

[11] Die befragten Versicherer berichteten über keinen erfolgreichen CEO-Fraud, dies kann jedoch auch an der vergleichsweisen kleinen Stichprobe liegen (n = 40 Versicherer).

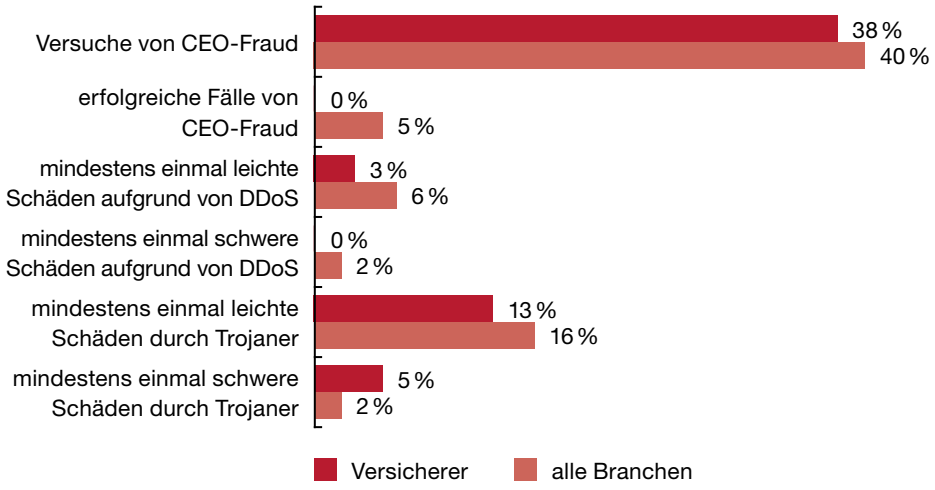
[12] Vgl. PwC, Wirtschaftskriminalität 2018. Mehrwert von Compliance – forensische Erfahrungen, 2018, S. 19 f., www.pwc.de/de/risk/pwc-wikri-2018.pdf.

Alarmierend sind auch die Berichte über Fälle von Distributed-Denial-of-Service (DDoS)-Attacken[13] sowie Verschlüsselungs- bzw. Erpressungstrojaner, auch unter dem Oberbegriff Ransomware[14] zusammengefasst. In unserer Studie berichteten 3 % der Versicherer über zumindest leichte DDoS-Fälle und 13 % über Trojaner – mit jeweils geringen Schadensfolgen.[15] Bei 5 % der Versicherer führten Trojanerattacken allerdings zu schweren Schäden. In unserer Gesamtstichprobe von 500 Unternehmen berichteten vier Unternehmen über die Zahlung des geforderten Lösegelds.

Im Ergebnis zeigt unsere Studie, dass Cybercrime für die Versicherer ein ebenso hohes Bedrohungspotenzial aufweist wie für die Gesamtwirtschaft.

Abb. 5 Von CEO-Fraud und Erpressung betroffene Versicherer

Mehrfachnennungen waren möglich.



[13] Vgl. BSI, Lagebericht IT-Sicherheit 2016, S. 29: „Bei einem Distributed-Denial-of-Service-Angriff (DDoS-Angriff) wird versucht, die Verfügbarkeit eines Dienstes durch eine Vielzahl von Anfragen oder Datenpaketen zu beeinträchtigen. Die Angriffe erfolgen in der Regel entweder durch Botnetze und/oder als Reflection-Angriffe (DRDoS-Angriffe) unter missbräuchlicher Ausnutzung öffentlich erreichbarer und fehlerhaft konfigurierter Server von Dritten."

[14] Vgl. BSI, Lagebericht IT-Sicherheit 2016, S. 20: „Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (ransom) wieder freigeben. Das Lösegeld soll meist in Krypto-Währungen wie Bitcoin gezahlt werden. Cyber-Angriffe durch Ransomware sind eine Form digitaler Erpressung."

[15] Ein leichter Fall mit geringen Schäden wird bei kurzzeitigen Systemausfällen ohne nennenswerte Beeinträchtigungen angenommen, bei denen nur einzelne Rechner betroffen sind und ein Backup ohne großen Aufwand möglich ist.

C Compliance in der Versicherungswirtschaft

1 Zunehmende Verbreitung von Compliance-Managementsystemen

Die Compliance ist in der Versicherungswirtschaft auch organisatorisch fest verankert: 95 % der Versicherer verfügen über ein Compliance-Managementsystem (CMS) (alle Branchen 75 %, ohne Grafik), in unserer vorherigen Studie aus dem Jahr 2016 waren es noch 87 %.

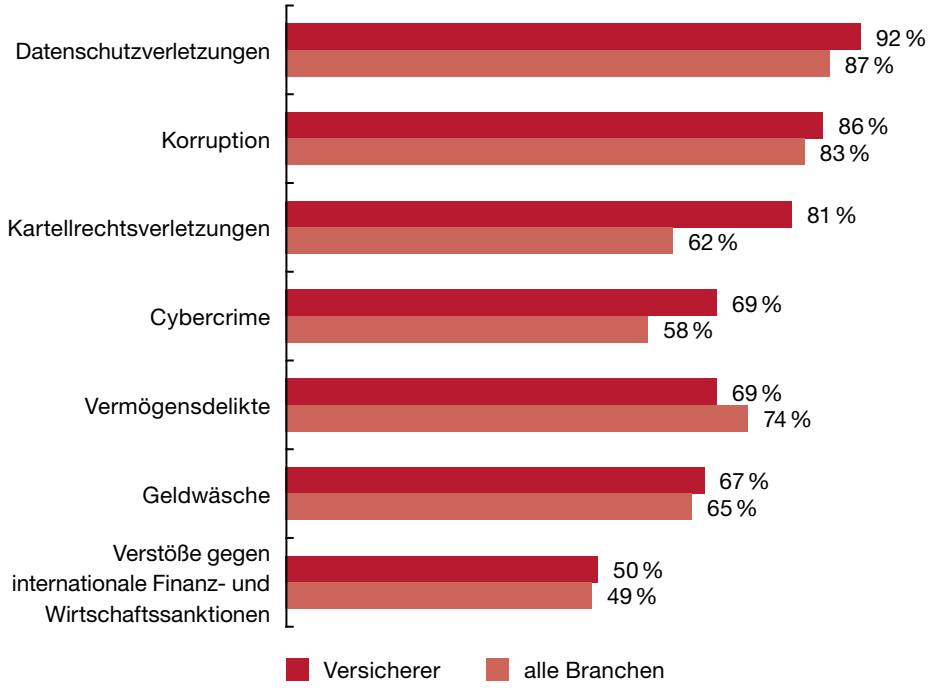
Am häufigsten zielen die Compliance-Programme der Befragten auf die Vermeidung von Datenschutzverletzungen (92 %), Korruption (86 %) und Kartellrechtsverstößen (81 %). In der Studie von 2016 verfügten nur 43 % der Versicherer über kartellrechtliche Compliance-Maßnahmen; dieses Risiko wurde also seitdem verstärkt angegangen.

Angesichts der erhöhten Geldwäscherisiken in der Versicherungswirtschaft[16] – jeder Dritte berichtet über einen Verdachtsfall (34 %; alle Branchen 12 %) – überrascht das Ergebnis: Nur zwei Drittel der Versicherer beabsichtigen, die Geldwäscheprävention über ihr CMS abzudecken (67 %). Hierbei ist jedoch anzumerken, dass die gesetzlich geforderten Maßnahmen zur Geldwäscheprävention möglicherweise gesondert, also außerhalb eines unternehmensweit themenübergreifend etablierten CMS, umgesetzt werden. Auch ein CMS zur Prävention gegen Vermögensdelikte (69 %) und Cybercrime (69 %), das die damit verbundenen Rechtsgebiete abdeckt, ist noch keinesfalls selbstverständlich.

[16] Vgl. Bussmann, Geldwäsche-Prävention im Markt, 2018, Springer, S. 125 ff.

Abb. 6 Status des CMS nach Deliktsgruppen

Mehrfachnennungen waren möglich.



Basis: alle Unternehmen mit CMS

Diese Einschätzung bestätigte sich auch in unseren vertiefenden Interviews. So äußerte ein Befragter:

„Das Bewusstsein der Geschäftsführung und des Vorstandes, dass nur ein funktionsfähiges und wirksames Compliance-Managementsystem tatsächlich von der Aufsichtsbehörde akzeptiert wird und auch tatsächlich Schaden vom Unternehmen abhält, ist groß und wächst weiter, sodass auch die entsprechenden Ressourcen bereitgestellt werden. Allerdings unter der Prämisse, dass die Compliance-Funktion auf eine Weise aufgestellt ist, die sich in den Digitalisierungsprozess integriert und Impulse zur Geschäftsoptimierung und zur Prozessoptimierung erzeugt."

2 Wahrgenommene Schwächen im Compliance-Management

Wir haben die Unternehmen in vertieften Interviews auch nach Schwachpunkten in ihrem CMS befragt. Dabei wurden die folgenden sechs Punkte genannt, über die wir ausführlich in unserer Wirtschaftskriminalitätsstudie 2018[17] berichtet haben:

- Kommunikationsprobleme
- mangelnde Konsistenz der Regelungen
- mangelnde Integration in die Geschäftsprozesse
- mangelhafte Umsetzung in global agierenden Unternehmen
- zu formales CMS
- mangelnde Awareness

[17] Vgl. PwC, Wirtschaftskriminalität 2018. Mehrwert von Compliance – forensische Erfahrungen, 2018, S. 26 f.

Zu der Herausforderung einer Integration des CMS in die Geschäftsprozesse äußerten die Befragten zum Beispiel:

„Eine Schwäche besteht in der Integration der verschiedenen Compliancerelevanten Instrumente. Wenn Sie zum Beispiel das innerbetriebliche Kontrollsystem nehmen, wie dieses mit dem Richtlinien-Managementsystem verbunden ist, und wie diese beiden wiederum mit unserem Geschäftsprozess-Managementsystem und mit unserem IT-Fachverfahren-Management-System verbunden sind. Wir müssen noch daran arbeiten, dass diese ganzen Teilsysteme zu einem gesamten, konsistenten und vor allen Dingen in ihren Bezügen stets aktuellem Gesamtsystem werden."

Zum Thema Strategie wurde etwa formuliert:

„Wir sind dabei, eine integrierte Software einzuführen, die eben diese Querbezüge zwischen den ganzen Teilinstrumenten überwacht bzw. zu überwachen erlaubt und uns aktiv auf Inkonsistenzen hinweist. Und von denselben Systemen, die wir in den nächsten Jahren zusammen mit externen Dienstleistern implementieren bzw. fortentwickeln werden, versprechen wir uns natürlich auch eine immer höhere Automatisierung in den Compliance-Überwachungsprozessen. Dadurch hoffen wir, auch die Personalressourcen-Intensität abzusenken."

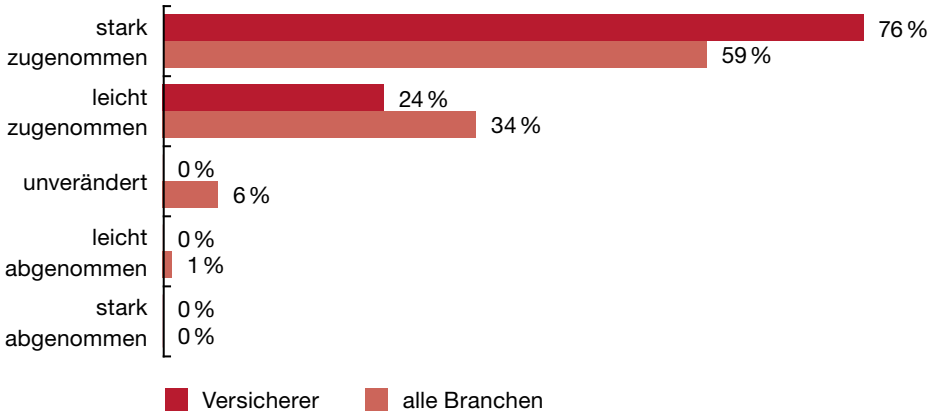
3 Deutliche Verschärfung der Anforderungen an das Compliance-Managementsystem

Aus rechtlicher Sicht haben die Anforderungen an das CMS zugenommen. So können nach der höchstrichterlichen Rechtsprechung des Bundesgerichtshofs (BGH) Compliance-Maßnahmen im Rahmen der Strafzumessung bei einer Verbandssanktionierung im Sinne des § 30 Ordnungswidrigkeitengesetzes (OWiG) berücksichtigt werden.[18] Nach einem begangenen Rechtsverstoß kommt es für die Strafzumessung trotz eines bereits implementierten Compliance-Programms auch darauf an, die entsprechenden Maßnahmen so zu optimieren, „dass vergleichbare Normverletzungen zukünftig jedenfalls deutlich erschwert werden".[19] Somit besteht im Prinzip eine Rechtspflicht zur stetigen Evaluierung und Anpassung der vorhandenen Compliance-Maßnahmen.

Über die Hälfte (59 %) der befragten Unternehmen aller Branchen beobachteten daher in den vergangenen fünf Jahren richtigerweise eine deutliche Verschärfung der rechtlichen Anforderungen an das CMS; eine Umkehr dieser Entwicklung erwartet hingegen kaum ein Unternehmen (1 %). In der Versicherungswirtschaft fällt das Urteil noch deutlicher aus: Drei Viertel (76 %) der Versicherer sehen eine deutliche Zunahme der Anforderungen. Ein wesentlicher Grund hierfür liegt in der stetig wachsenden aufsichtsrechtlichen Regulierung der Versicherungsbranche und den zunehmend konkreteren Erwartungen der deutschen und europäischen Aufsichtsbehörden an die Umsetzung einer angemessenen Geschäftsorganisation. Letztere schließt, neben weiteren Schlüsselfunktionen, die Compliance-Funktion explizit mit ein.

[18] Vgl. BGH, Urteil vom 9. Mai 2017 – 1 StR 265/16.
[19] Vgl. a. a. O.

Abb. 7 Entwicklung der Anforderungen an Compliance-Managementsysteme

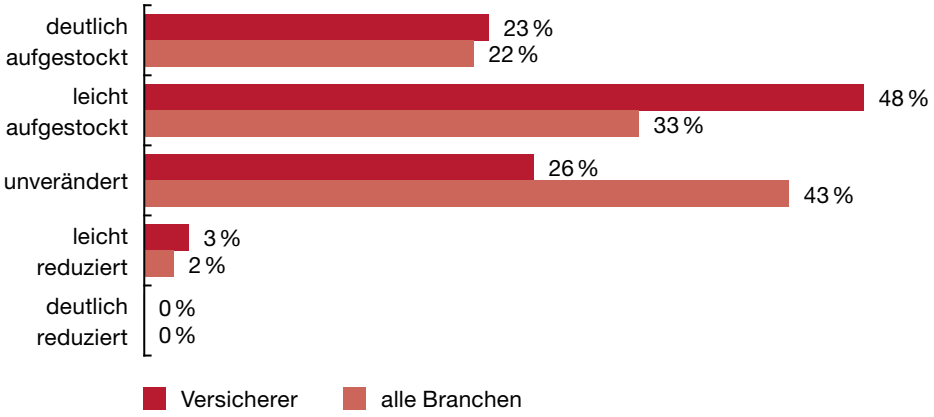


Basis: alle Unternehmen mit CMS

4 Erhöhung der Personal- und Sachmittelausstattung der Compliance-Abteilung

Die Mehrheit der Unternehmen aller Branchen begegnet den wachsenden rechtlichen Anforderungen an das CMS mit einer verbesserten Personal- und Sachmittelausstattung der Compliance-Abteilung. Das gilt insbesondere für die Versicherungswirtschaft. Jeder zweite Versicherer (48 %) hat sein diesbezügliches Budget in den letzten zwei Jahren leicht aufgestockt (alle Branchen 33 %), über ein Fünftel der Versicherer sogar deutlich (23 %; alle Branchen 22 %). Über eine leichte Reduzierung ihrer Personal- und Sachmittelausstattung in den Compliance-Abteilungen berichteten nur 3 % der Versicherer.

Abb. 8 Entwicklung der Personal- und Sachmittel für die Compliance in den letzten zwei Jahren



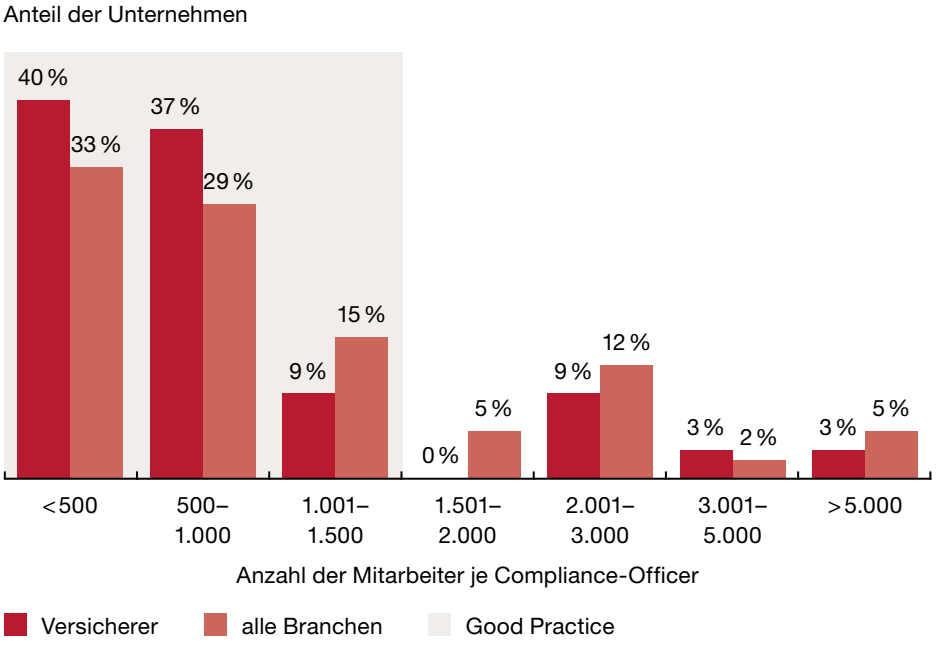
Basis: alle Unternehmen mit CMS

5 Erhöhung der personellen Ausstattung der Compliance-Abteilung

Dieser positive Trend zeigt sich in der Personalrelation zwischen dem Compliance-Officer und der Anzahl der Mitarbeiter. Auf eine volle bzw. zwei halbe Compliance-Officer-Stellen kommen in der Versicherungswirtschaft knapp 1.100 Mitarbeiter – deutlich mehr als im branchenübergreifenden Durchschnitt mit rund 1.500 Mitarbeitern.[20] Hier ist jedoch zu berücksichtigen, dass die Einrichtung einer Compliance-Funktion als Schlüsselfunktion aufsichtsrechtlich festgelegt und grundsätzlich unabhängig von der Größe des Versicherers erforderlich ist, was wiederum eine entsprechende personelle Ausstattung bedingt. Zudem ist aus praktischer Sicht zu beachten, dass das Risiko eines aufsichtsrechtlichen Verstoßes in der Versicherungswirtschaft gegebenenfalls eine branchenübergreifend überdurchschnittliche personelle Ausstattung erfordert.

Die Mehrheit der Versicherer sieht auch im branchenübergreifenden Vergleich ein deutlich besseres personelles Verhältnis. Bei 40 % der Versicherer kommt auf weniger als 500 Mitarbeiter eine Compliance-Officer-Stelle (alle Branchen 33 %) und bei 37 % eine Stelle auf 500 bis 1.000 Mitarbeiter (alle Branchen 29 %).

Abb. 9 Personelle Ausstattung der Compliance-Abteilung



Basis: alle Unternehmen mit CMS

[20] In unsere Berechnung sind Teilzeitstellen mit 0,5 Tagen eingegangen.

D Compliance-Maßnahmen

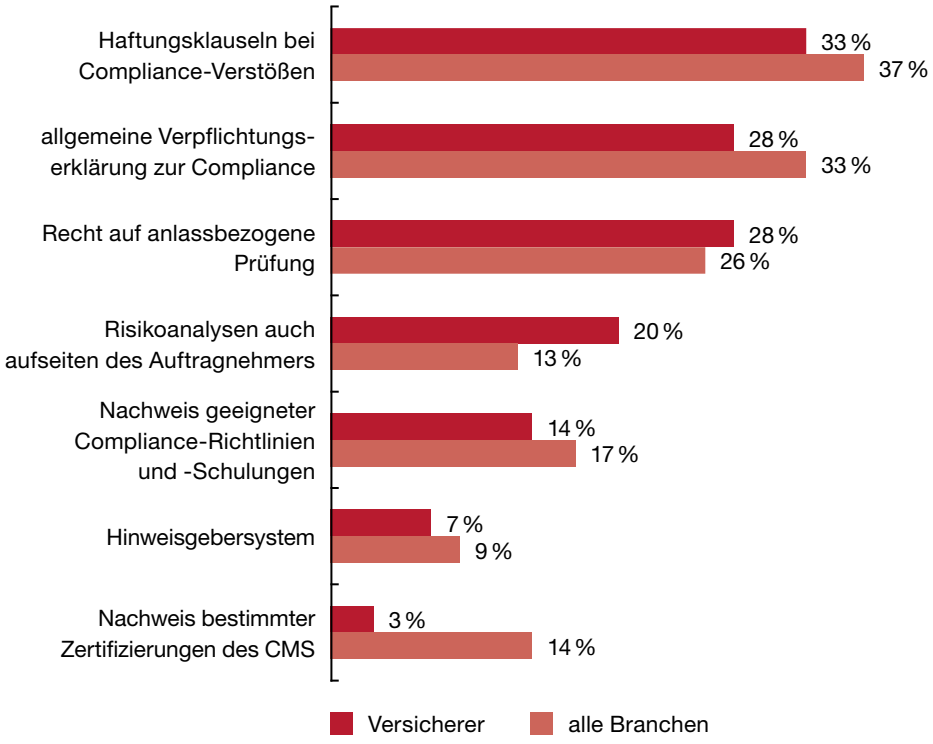
1 Compliance-Vertragskonditionen

Über das Instrument der Vertragsgestaltung üben auch die Versicherer Einfluss auf das CMS ihrer Vertragspartner aus, wenn auch etwas zögerlicher als im branchenübergreifenden Vergleich. Das Spektrum der häufigsten Klauseln in den Verträgen der Versicherer reicht von Haftungsklauseln bei Compliance-Verstößen (33 %; alle Branchen 37 %), allgemeinen Verpflichtungserklärungen (28 %; alle Branchen 33 %) und der Zusicherung eines Rechts auf anlassbezogene Prüfungen (28 %; alle Branchen 26 %) bis hin zur Verpflichtung zu Risikoanalysen aufseiten des Vertragspartners (20 %; alle Branchen 13 %).

Einige Verträge beinhalten zudem konkrete Anforderungen an die Ausgestaltung des CMS ihres Vertragspartners. 14 % der Versicherer verlangen Nachweise über geeignete Compliance-Richtlinien und -Schulungen (alle Branchen 17 %). Nur wenige Versicherer erwarten jedoch bislang ein Hinweisgebersystem (7 %; alle Branchen 9 %) oder eine Zertifizierung des CMS (3 %; alle Branchen 14 %).

Abb. 10 Verbreitung von Compliance-Vertragskonditionen

Mehrfachnennungen waren möglich.



Basis: alle Unternehmen mit CMS

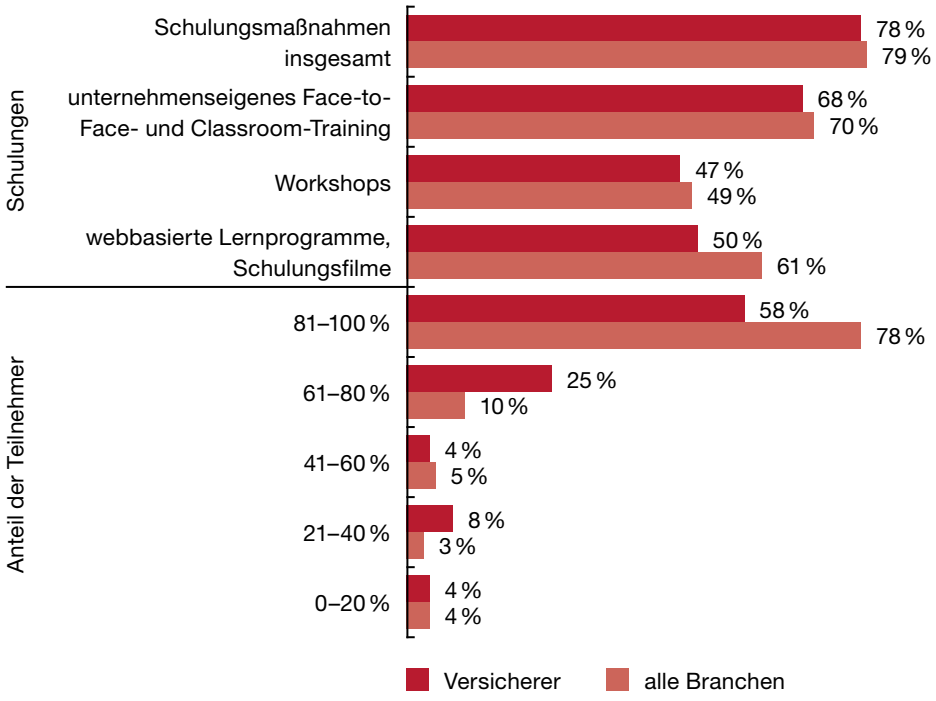
2 Praxis der Schulungen zum Umgang mit Korruptionssituationen

Essenzielle Bestandteile eines CMS sind Schulungs- und Informationsangebote zum Umgang mit Korruptionssituationen. Sie sind jedoch noch nicht für jeden Versicherer selbstverständlich. Nur 78 % der Compliance-Programme der Versicherer sehen Schulungsmaßnahmen vor. Dies entspricht zwar dem branchenübergreifenden Durchschnitt (79 %), aber mit dem Angebot werden bei den Versicherungen deutlich weniger relevante Funktionsträger erreicht. Bei nur 58 % der Versicherer absolvierten mehr als 80 % der relevanten Mitarbeiter und Manager die Schulungen (alle Branchen 78 %).

Am häufigsten erfolgen Schulungen in Form eines Präsenztrainings (68 %). Aber auch digitale Trainingsformate werden zunehmend eingesetzt. Jeder zweite Versicherer führt webbasierte Schulungen durch; dies ist allerdings weniger als der branchenübergreifende Durchschnitt (61 %).

Abb. 11 Schulungsformate

Mehrfachnennungen waren möglich.



Basis: alle Unternehmen mit CMS

3 Unzureichende Öffnung von Hinweisgebersystemen

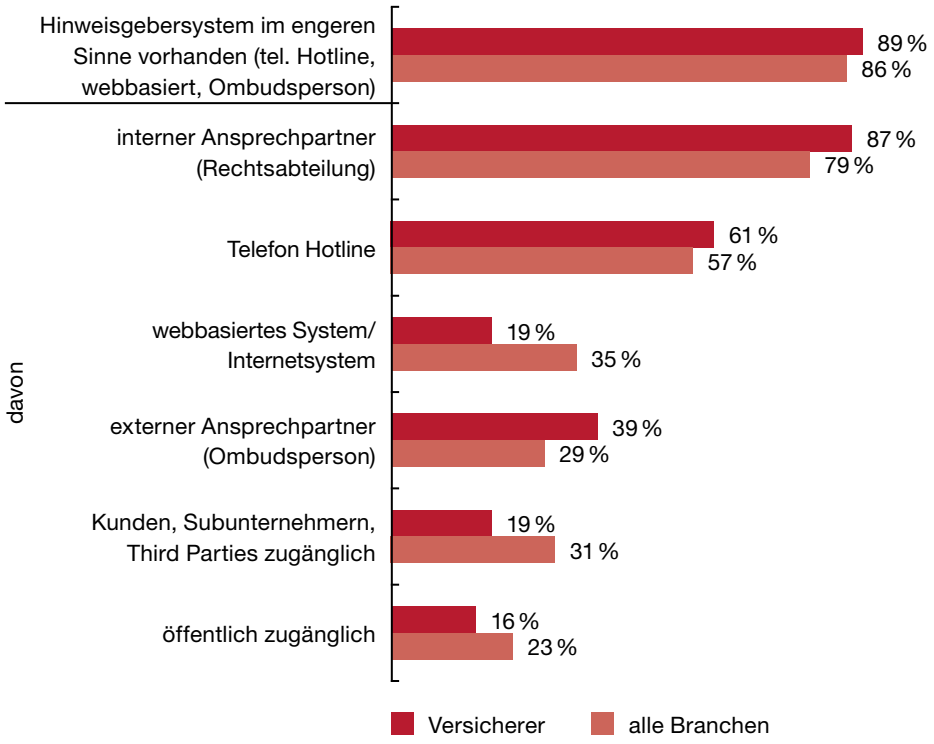
Hinweisgebersysteme sind mittlerweile auch bei Versicherern selbstverständlich. Am weitesten verbreitet ist mit 87 % ein interner Ansprechpartner, etwa in der Rechtsabteilung. Allerdings bietet diese Option meist nur eingeschränkte Anonymität, sodass wir sie nicht als Hinweisgebersystem im engeren Sinne ansehen. Ein solches wäre nach unser Meinung zum Beispiel eine telefonische Hotline, ein webbasiertes System oder eine Ombudsperson.

Am häufigsten sehen die Versicherer eine telefonische Hotline vor (61 %; alle Branchen 57 %). Im Vergleich zu den anderen Branchen werden auch Ombudspersonen deutlich häufiger eingesetzt (39 %; alle Branchen 29 %), während webbasierte Hinweisgebersysteme deutlich weniger üblich sind (19 %; alle Branchen 35 %).

Ein gravierender Schwachpunkt vieler Hinweisgebersysteme von Versicherern liegt in ihrer mangelnden Öffnung für Externe. Hinweisgebersysteme sollten nicht auf interne Personen beschränkt sein, so fordern es etwa auch die Richtlinien zum Foreign Corrupt Practices Act (FCPA).[21] Empirisch zeigen auch unsere Studien, dass rund ein Fünftel der Hinweise von externen Personen kommen.[22] Bei den befragten Versicherern sind jedoch nur 19 % der Hinweisgebersysteme auch Geschäftspartnern und Subunternehmen (alle Branchen 31 %) und 16 % allgemein öffentlich zugänglich (alle Branchen 23 %). Auch im branchenübergreifenden Vergleich sind die Hinweisgebersysteme der Versicherer noch zu unternehmensintern ausgerichtet.

Abb. 12 Varianten und Zugänglichkeit von Hinweisgebersystemen

Mehrfachnennungen waren möglich.



Basis: alle Unternehmen mit CMS

[21] Vgl. Richtlinie zum FCPA, S. 61: Im Abschnitt „Confidential Reporting and Internal Investigation" wird ein „[…] mechanism for employees and others to report suspected or actual misconduct or violations […]" verlangt.

[22] Vgl. zum Beispiel PwC, Wirtschaftskriminalität und Unternehmenskultur, 2013, S. 83.

4 Evaluation des Compliance-Managements

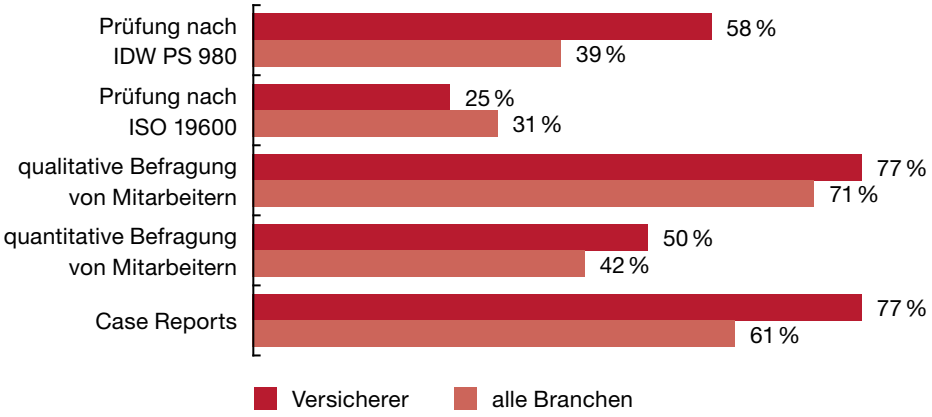
Compliance-Programme gehören in der Versicherungswirtschaft zum Standard. 95 % der Versicherer verfügen über ein CMS, das sind mehr als in unserer Studie von 2016; damals waren es 87 %. Einen Anstieg um 14 Prozentpunkte beobachten wir auch bei der Evaluation. 58 % der Versicherer haben ihr CMS nach dem IDW Prüfungsstandard 980 auditiert, häufiger als im branchenübergreifenden Vergleich (39 %). Demgegenüber sind Prüfungen nach der Norm ISO 19600 von untergeordneter Bedeutung (25 %). Eine Erklärung hierfür könnte sein, dass die Versicherer mehrheitlich dem Verhaltenskodex für den Vertrieb von Versicherungsprodukten des Gesamtverbands der Deutschen Versicherungswirtschaft beigetreten sind. Ein Beitritt bedeutet auch, dass das jeweilige Unternehmen sein CMS einer Prüfung (meist nach IDW PS 980) unterzieht. Dabei stehen die Maßnahmen zur Umsetzung des Verhaltenskodex im Mittelpunkt.

Die Mehrheit (77 %) der befragten Versicherer sieht jedoch Case Reports, Fallanalysen, vor. Auch diese Form der Evaluation ist in der Versicherungswirtschaft weiter verbreitet als in den Branchen insgesamt (61 %). Fallanalysen haben jedoch den Nachteil, dass sie sich auf aufgedeckte Fälle beschränken, also auf das sogenannte Hellfeld. Demgegenüber erlauben Mitarbeiterbefragungen auch einen tieferen Einblick in das Dunkelfeld. Mehr als drei Viertel (77 %) der Versicherer wählten zur Evaluation die Methode einer qualitativen Mitarbeiterbefragung.

Persönliche Interviews können jedoch keine Anonymität gewährleisten. Auch werden nur kleine Fallzahlen erreicht, sodass repräsentative Aussagen schwer möglich sind.[23] Qualitative Befragungen liefern zwar einen guten ersten Eindruck, sollten aber durch quantitative, standardisierte Befragungen repräsentativ abgesichert werden. Sie wurden jedoch nur bei der Hälfte der Versicherer eingesetzt, allerdings häufiger als in den Branchen insgesamt (42 %).

Abb. 13 Art der Evaluation des CMS

Mehrfachnennungen waren möglich.



Basis: alle Unternehmen mit CMS

[23] Siehe ausführlich zu Methoden unter anderem DICO e. V. , L07 – Hinweise und Kriterien zur Messung einer Unternehmenskultur, 2016, S. 9 ff., www.dico-ev.de/wp-content/uploads/2017/06/L07_Unternehmenskultur_12S_2016_WEB.pdf>.

E Forensische Praxis betroffener Versicherungsunternehmen

1 Bedeutung externer Ermittler

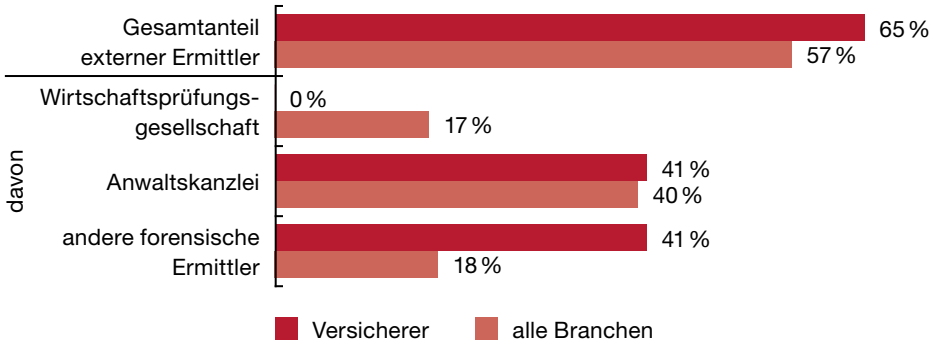
Im Falle eines Compliance-Verstoßes ist die Einleitung eigener Aufklärungsbemühungen durch interne oder beauftragte externe Spezialisten für die betroffenen Versicherer selbstverständlich (93 %; alle Branchen 85 %, ohne Grafik).

Die Untersuchungen wurden überwiegend von der Internen Revision geleitet (44 %; alle Branchen 38 %) und bei einem Drittel der betroffenen Versicherer von der Rechtsabteilung (31 %; alle Branchen 31 %). Der Schwerpunkt der Compliance-Abteilung liegt typischerweise eher auf der Prävention, sodass nur in rund einem Fünftel der Fälle die internen Ermittlungen von der Compliance-Abteilung geleitet wurden (18 %; alle Branchen 24 %, ohne Grafik).

Zwei Drittel der Versicherer führten ihre Untersuchungen auch mit Unterstützung externer Ermittler durch (65 %; alle Branchen 57 %). Am häufigsten handelte es sich um Anwaltskanzleien (41 %) und andere forensische Ermittler (41 %). Letztere umfassen vermutlich auch Ermittler aus Schadens-/Leistungsbereichen (sogenannte Versicherungsdetektive).

Abb. 14 Beauftragung externer Ermittler

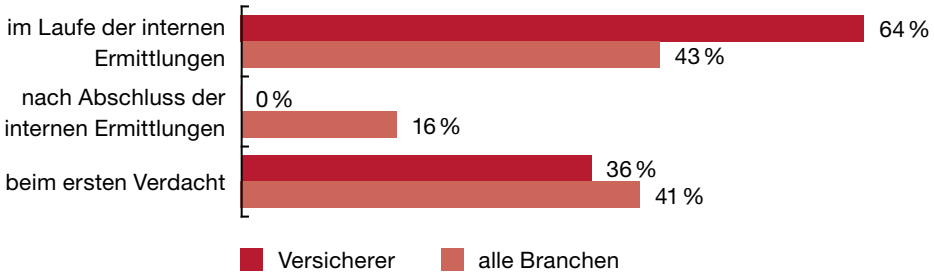
Mehrfachnennungen waren möglich.



2 Zeitpunkt der Beauftragung externer Ermittler

Als Zeitpunkt für die Beauftragung eines externen Ermittlers sollte möglichst der erste Verdachtsmoment gewählt werden. Nur jeder dritte Versicherer (36 %) beauftragte den externen Ermittler bereits beim ersten Verdacht, zwei Drittel vollzogen diesen Schritt erst im Laufe der internen Ermittlungen (64 %; alle Branchen 43 %).

Abb. 15 Zeitpunkt der Beauftragung externer Ermittler



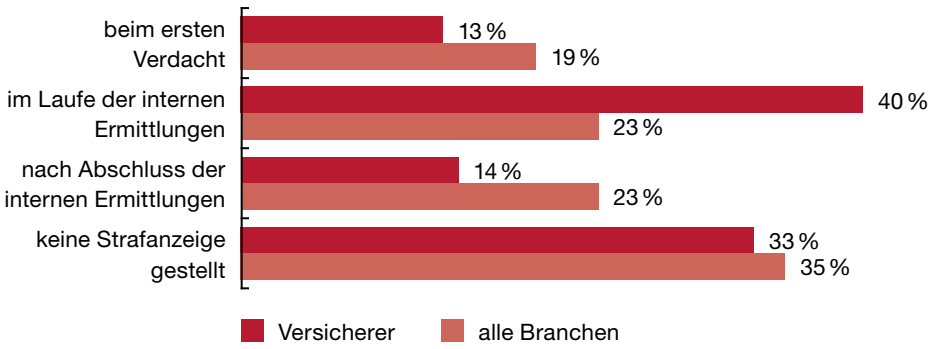
3 Praxis der Strafanzeige

Allgemein fallen, wie unsere Studie gezeigt hat, die Erfahrungen betroffener Unternehmen mit der Ermittlungstätigkeit von Polizei und Staatsanwaltschaft heterogener aus als dies bei internen Untersuchungen der Fall ist.[24] Das gilt auch für die befragten Versicherer. Nur 45 % von ihnen waren mit der Ermittlungstätigkeit von Polizei und Staatsanwaltschaft zufrieden. Demgegenüber waren 80 % mit der Arbeit der externen Ermittler und 100 % mit den hauseigenen Ermittlungen zufrieden (ohne Grafik).

Dieser Umstand könnte erklären, weshalb nur jeder dritte Versicherer keine Strafanzeige gestellt hat (33 %; alle Branchen 35 %). Nur in rund jedem zehnten Fall erfolgte eine Strafanzeige bereits beim ersten Verdacht (13 %; alle Branchen 19 %).

Die meisten Versicherer (40 %) warteten die Ergebnisse der eigenen Ermittlungen ab, bevor sie Strafanzeige stellen (alle Branchen 23 %). Als Gründe für eine späte Strafanzeige gaben die befragten Versicherer, ähnlich wie die Unternehmen in den anderen Branchen, vor allem an, dass sie sich von der internen Untersuchung eine schnellere Aufklärung versprochen hätten (50 %; alle Branchen 64 %). Eher nachrangig waren Motive wie die Vermeidung von Unruhe im Unternehmen (25 %; alle Branchen 55 %) oder der Verlust der Kontrolle über die eigene Ermittlungstätigkeit (25 %; alle Branchen 32 %). Über Befürchtungen mit Blick auf mögliche Publizitätsrisiken berichteten die befragten Versicherer, anders als im branchenübergreifenden Vergleich, nicht (alle Branchen 36 %, ohne Grafik).

Abb. 16 Zeitpunkt der Strafanzeige



[24] Vgl. PwC, Wirtschaftskriminalität 2018. Mehrwert von Compliance – forensische Erfahrungen, 2018, S. 65, www.pwc.de/de/risk/pwc-wikri-2018.pdf.

Ihre Ansprechpartner

PwC

Gunter Lescher
Partner
Forensic Services
Tel.: +49 211 981-2968
gunter.lescher@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 158 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC. Mehr als 11.000 engagierte Menschen an 21 Standorten. 2,2 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

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