Wirtschaftskriminalität in der analogen und digitalen Wirtschaft

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

MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG

pwc

Wirtschaftskriminalität in der analogen und digitalen Wirtschaft

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

MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG

pwc

Wirtschaftskriminalität in der analogen und digitalen Wirtschaft

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

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

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

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

April 2017, 36 Seiten, 17 Abbildungen, Softcover

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

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

© April 2017 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft.
Alle Rechte vorbehalten.
„PwC“ bezeichnet in diesem Dokument die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, die eine Mitgliedsgesellschaft der PricewaterhouseCoopers International Limited (PwCIL) ist. Jede der Mitgliedsgesellschaften der PwCIL ist eine rechtlich selbstständige Gesellschaft.

Vorwort

Unsere achte Studie bringt für die Versicherungswirtschaft auch ungute Nachrichten. Fast drei Viertel der Versicherer waren von Wirtschaftskriminalität betroffen (70 %). Dies liegt deutlich über dem Durchschnitt aller Branchen (51 %) und ist die höchste Belastung seit 2007. Dieser Anstieg beruht vor allem auf einer Zunahme der Vermögenskriminalität (61 %). Ein deutlicher Rückgang zeigt sich nur bei der Geldwäsche auf 10 %. Diese positive Entwicklung führen wir auf die Wirksamkeit der in der Versicherungswirtschaft seit Jahren etablierten Geldwäscheprävention zurück.

Versicherungsunternehmen werden häufiger als im branchenübergreifenden Durchschnitt durch externe Wirtschaftsstraftäter geschädigt. Dabei handelte es sich ganz überwiegend um Geschäftspartner und Dienstleister (75 % – alle Branchen 35 %). Versicherer sind außerdem wie andere Branchen auch ein Ziel der **Organisierten Kriminalität (OK)**, 13 % der Fälle von externen Tätern konnten auf OK zurückgeführt werden.

In dieser Studie erhoben wir systematisch auch die Verbreitung von E-Crime.[1] Jeder dritte Versicherer berichtete über **Cybercrime**. Dabei handelte es sich überwiegend um Formen wie Computerbetrug, Manipulation von Konto- und Finanzdaten, Ausspähen und Abfangen von Daten, Fälschung beweiserheblicher Daten und Diebstahl vertraulicher Kunden- und Unternehmensdaten.

Das Risiko eines **Daten- und Wissensverlusts** sehen die befragten Versicherungsunternehmen vor allem bei herkömmlichen Angriffsvektoren wie Abwerbung von Mitarbeitern (46 %), aber auch bei digitalen Angriffen auf mobile IT-Systeme wie Mobiltelefone (49 %). Geringere Risiken werden demgegenüber hinsichtlich des Entwendens und Kopierens von Firmenunterlagen gesehen (30 %). Tatsächlich erfolgte eine Schädigung in 64 % der Fälle von Daten- und Wissensverlust bei den betroffenen Versicherern durch schlichtes Entwenden oder Kopieren von Firmenunterlagen.

Die Versicherungswirtschaft nimmt den Schutz vor Cyberangriffen durch eine Vielzahl von IT-Sicherheitsmaßnahmen sehr ernst. Nahezu alle Versicherer, die sich zur kritischen Infrastruktur (KRITIS) zählen, verfügen über ein internes **IT-Sicherheitsmanagement** zur Identifikation von IT-Sicherheitsvorfällen (94 %), aber ein Penetration Testing ihrer IT-Systeme,[2] sehen in dieser KRITIS-Gruppe nur 86 % der Versicherer vor und nur jeder zweite hat eine Zertifizierung durchgeführt.

[1] 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.

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

In der Versicherungswirtschaft haben sich die Compliance-Anforderungen aufgrund regulatorischer Vorgaben, insbesondere durch Solvency II, deutlich erhöht. Infolge dieser Entwicklung sind **Compliance-Managementsysteme** in der Versicherungsbranche nahezu selbstverständlich. 87 % der Versicherer verfügen über ein Compliance-Programm (alle Branchen 76 %), das sich überwiegend auf die Vermeidung von Datenschutzverletzungen (97 %), Korruption (82 %) und Geldwäsche (79 %) erstreckt. Lücken bestehen jedoch vor allem hinsichtlich der kartellrechtlichen Compliance (43 %), obwohl die kartellrechtlichen Risiken in der Versicherungswirtschaft gemessen am Durchschnitt aller Branchen keinesfalls unterdurchschnittlich ausfallen.

Über **vertragliche Verpflichtungserklärungen** (29 %), Haftungsklauseln im Falle von Compliance-Verstößen (29 %) und sogenannten Audit Clauses (32 %) nehmen Versicherungsunternehmen Einfluss auf die Etablierung von Compliance-Programmen bei Dienstleistern und Zulieferern.

Allerdings bedarf es bei vielen Unternehmen weiterhin einer unabhängigen Bewertung der Qualität ihrer Compliance-Managementsysteme. Zwar ist 58 % der Versicherer der **Prüfungsstandard 980** des Instituts der Wirtschaftsprüfer in Deutschland bekannt, aber bislang haben sich nur 44 % nach diesem Standard zertifizieren lassen.

Mit unserer Studie möchten wir Versicherungsunternehmen über die Risiken und Präventionschancen sowohl analoger als auch digitaler Wirtschaftskriminalität informieren. Wir bedanken uns an dieser Stelle noch einmal herzlich bei allen Studienteilnehmern für ihre Auskunftsbereitschaft.

Frankfurt am Main und Halle an der Saale im April 2017

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

Inhaltsverzeichnis

Abbildungsverzeichnis

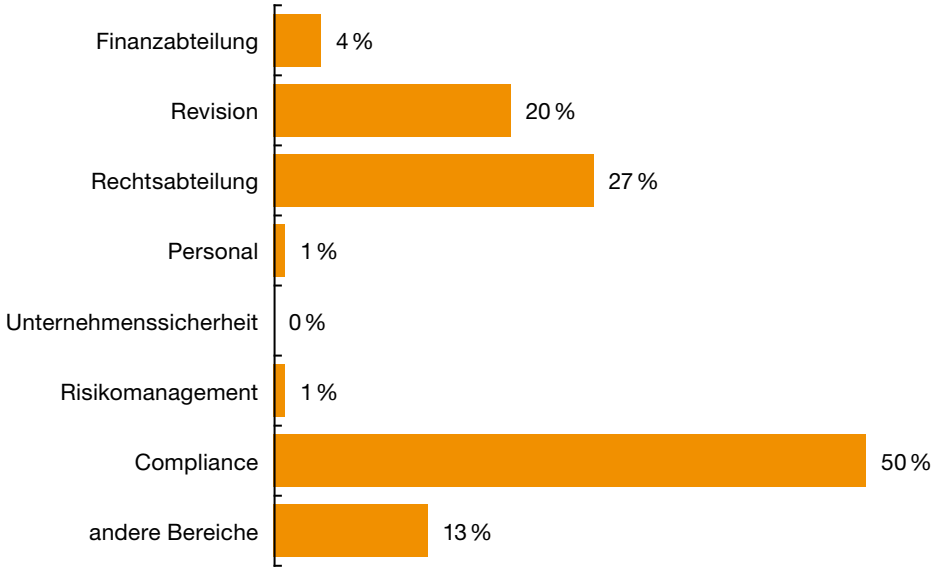
A Methodisches Vorgehen

Die achte Studie zur Wirtschaftskriminalität wurde im Auftrag von PwC und der Universität Halle-Wittenberg in Deutschland durchgeführt. Von September bis November 2015 wurden in Deutschland 720 Unternehmen von TNS Emnid telefonisch interviewt. Bei der vorliegenden Studie handelt es sich um eine Sonderauswertung von 70 Unternehmen aus der Versicherungswirtschaft, die mit Ergebnissen aus vorherigen Studien verglichen werden. Die Ergebnisse sind aufgrund der Stichprobenziehung repräsentativ. Details zur methodischen Durchführung können unserem Report *Wirtschaftskriminalität in der analogen und digitalen Wirtschaft 2016* entnommen werden.[3]

Die Hälfte der Befragten in der Versicherungswirtschaft ist in der Compliance-Abteilung tätig. Die verbleibenden Interviewpersonen stammen aus der Rechtsabteilung, der Revision und aus anderen 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 über mindestens 500 Mitarbeiter verfügen. In der Stichprobe Versicherungswirtschaft handelt es sich bei einem Drittel um mittelständische Versicherer mit weltweit 500 bis 1.000 Mitarbeitern (32 %). 20 % verfügen weltweit über mehr als 5.000 Mitarbeiter. International vertreten ist ein knappes Drittel der befragten Versicherungsunternehmen (30 %).

[3] Vgl. www.pwc.de/de/risiko-management/assets/studie-wirtschaftskriminalitaet-2016.pdf.

B Wachsende Risiken durch analoge und digitale Wirtschaftskriminalität

1 Deutliche Zunahme der Wirtschaftskriminalität

Die Versicherungswirtschaft war nach den Ergebnissen unserer aktuellen Studie überdurchschnittlich von Wirtschaftskriminalität betroffen, fast drei Viertel der Versicherer berichteten über mindestens einen Fall (70 %). Gegenüber den vorhergehenden Studien handelt es sich um eine signifikante Zunahme um 17 Prozentpunkte (2013: 53 %). Dieser Anstieg beruht vor allem auf der signifikanten Zunahme der Vermögenskriminalität (61 % – alle Branchen 37 %), die sich auf dem hohen Niveau von 2007 bewegt.

Hierbei handelt es sich um eine Entwicklung, die wir auch in der übrigen Wirtschaft feststellen; der Anteil der Betrugskriminalität stieg im Durchschnitt aller Branchen auf 37 %. Bemerkenswerterweise zeigt sich eine ähnliche Entwicklung auch in der polizeilichen Kriminalstatistik. Während die Diebstahls- und insbesondere die Raubkriminalität seit Jahrzehnten stagniert oder gar abnimmt, hat sich die Betrugskriminalität in den vergangenen zwei Jahrzehnten nahezu verdoppelt.[4] Generell zeichnet sich auch in anderen Industrieländern wie den USA und dem Vereinigten Königreich eine Entwicklung vom Diebstahl zum Betrug ab.[5] Manche Wissenschaftler betrachten den Betrug daher als das charakteristische Delikt des 21. Jahrhunderts.[6]

Eine beständige Zunahme beobachten wir außerdem bei urheberrechtlichen Verstößen. Nahezu jeder zehnte Versicherer war von Verstößen gegen Patent- und Markenrechte betroffen (9 %). Diese Risiken erreichen mittlerweile die durchschnittliche Verbreitung in der übrigen Wirtschaft (13 %).

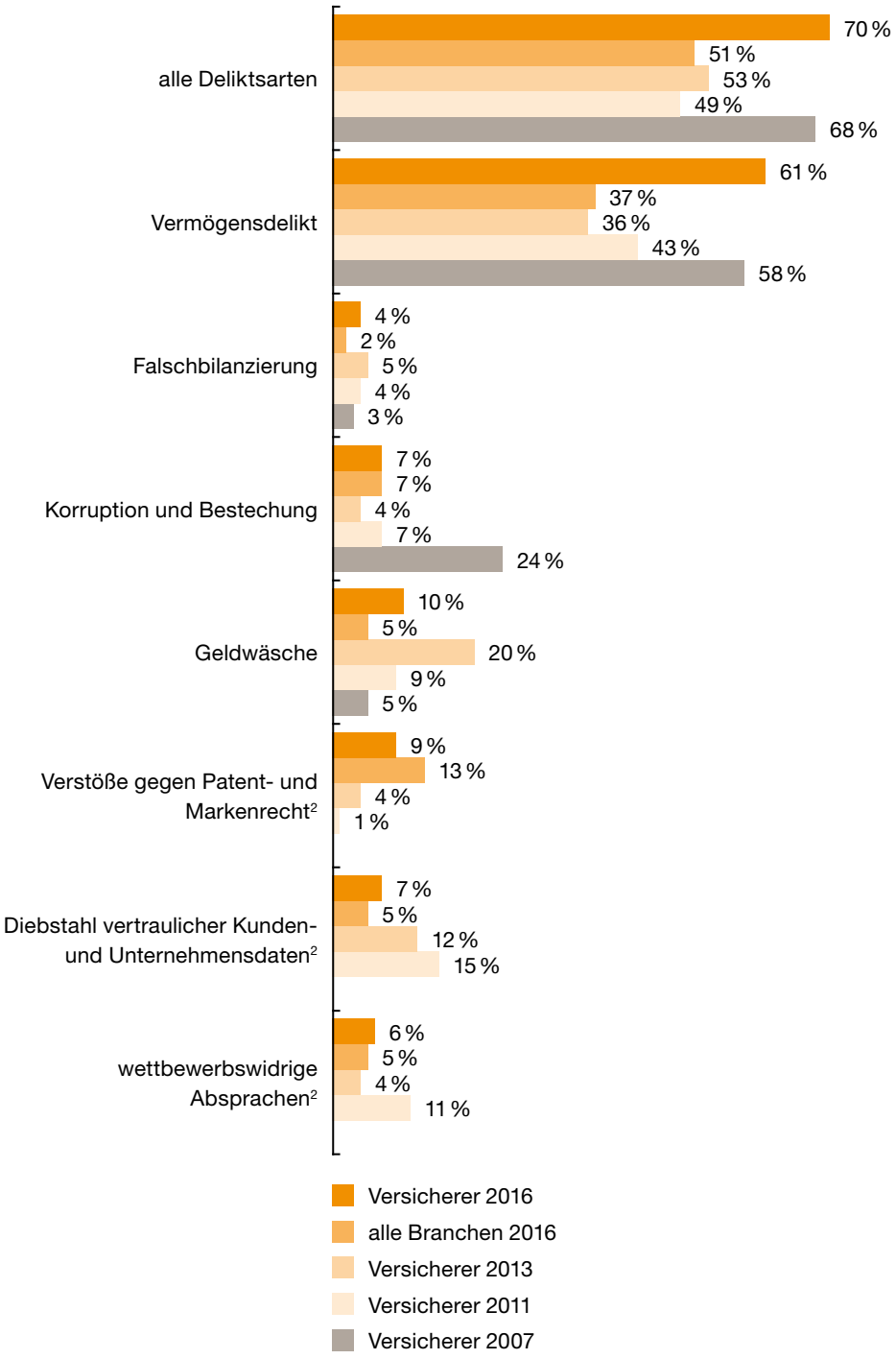
Seit 2007 nimmt hingegen die Anzahl der von Diebstahl vertraulicher Kunden- und Unternehmensdaten betroffenen Versicherungsunternehmen kontinuierlich ab, 7 % der Versicherer berichteten über derartige Vorfälle (alle Branchen 5 %). Wir führen diesen Rückgang auf den in der Versicherungswirtschaft erreichten hohen Compliance- und Datenschutzstandard zurück (siehe Abschnitt E 1). Auch bei der Geldwäsche zeichnet sich ein rückläufiger Trend ab. Nur jeder zehnte Versicherer berichtete über einen Fall von Geldwäsche; 2013 waren es noch doppelt so viele.

Gegenüber den Studien von 2011 und 2013 stagniert die Zahl der von Korruption betroffenen Versicherungsunternehmen auf einem niedrigem Niveau (7 %). Nahezu unverändert sind die ebenfalls wenigen Berichte über wettbewerbswidrige Absprachen (6 %).

[4] Vgl. Oberwittler, in: Albrecht/Groenemeyer, Handbuch soziale Probleme Bd. 2, 2. Aufl., 2012, S. 780 f.
[5] Vgl. Karstedt, in: van Erp/Huisman/Vande Walle, The Routledge Handbook of White-Collar and Corporate Crime in Europe, 2015, S. 61, m. w. N.
[6] Vgl. Albanese, Trends in Organized Crime, Vol. 8 (2005), S. 6–14; zu den Gründen: Bussmann, Wirtschaftskriminologie Band I, 2016, Rn. 1049 ff.

Abb. 2 Entwicklung von Wirtschaftskriminalität in der Versicherungsbranche 2007–2016[1]

Mehrfachnennungen waren möglich.



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

[2] 2007 nicht erhoben

2 Stagnation der Verdachtsfälle auf hohem Niveau

Insgesamt sank in den letzten fünf Jahren der Anteil der Verdachtsfälle nur leicht auf 63 %. Die Versicherungswirtschaft bleibt somit weiterhin stark von Wirtschaftskriminalität betroffen. Aber bei den berichteten Verdachtsfällen zeigt sich für Vermögensdelikte wiederum ein Anstieg, wenn auch weniger stark. 43 % der Versicherer berichteten über einen Verdachtsfall (alle Branchen 32 %). Wir beobachten daher einen Trend hin zu einer wachsenden Bedrohung der Versicherungswirtschaft, durch Vermögensdelikte geschädigt zu werden.

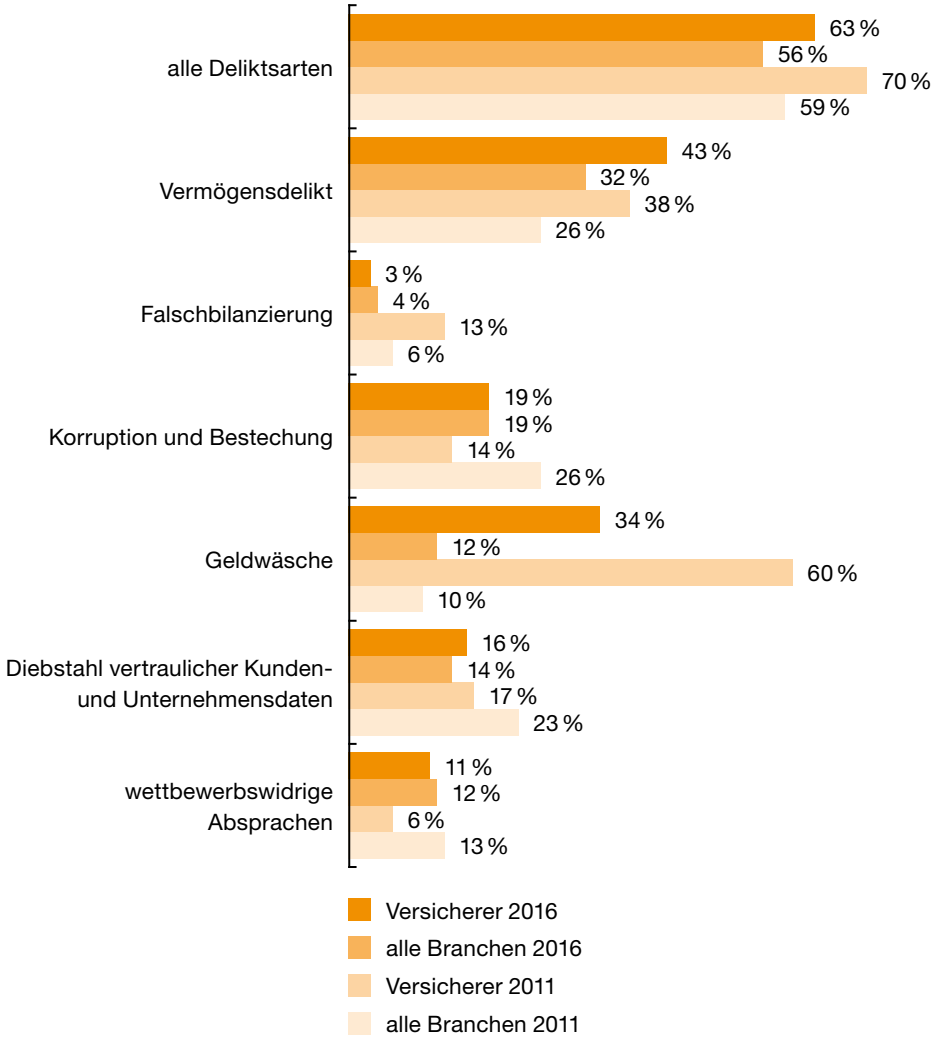
Eine geringe Zunahme um fünf Prozentpunkte stellen wir auch bei den Korruptionsdelikten fest; jeder fünfte Versicherer berichtete über einen Korruptionsverdacht (19 % – alle Branchen 19 %). Dies dürfte allerdings auf das steigende Bewusstsein aufgrund der weiten Verbreitung von Antikorruptionsprogrammen in der Versicherungswirtschaft zurückzuführen sein (82 %, siehe Abschnitt E 1). Gleiches dürfte für die stagnierende Zahl der Verdachtsfälle auf Diebstahl vertraulicher Kunden- und Unternehmensdaten gelten (16 % – alle Branchen 14 %). Hier könnte sich allerdings auch die erhöhte Sensibilität auswirken, die mit der Einführung eines entsprechenden Compliance-Managementsystems einhergeht. 97 % der Compliance-Programme bei den befragten Versicherern umfassen die Prävention gegen Datenschutzverletzungen (siehe Abschnitt E 1).

Einen leichten Anstieg beobachten wir außerdem bei der Wettbewerbskriminalität. Jeder zehnte Versicherer berichtete über einen Verdacht auf wettbewerbswidrige Absprachen (11 % – alle Branchen 12 %).

Gegenüber unserer letzten Erhebung 2013 sank der Anteil der von Geldwäsche betroffenen Versicherer auf 10 %. Dieser Rückgang deckt sich mit einer starken Abnahme der Geldwäsche-Verdachtsfälle auf 34 %. Diese positive Entwicklung dürfte auf die Wirksamkeit der verbreiteten Geldwäscheprävention zurückzuführen sein (79 %, siehe Abschnitt E 1). Einen deutlichen Rückgang stellen wir ferner bei den Verdachtsfällen auf Falschbilanzierung fest (3 %).

Abb. 3 Entwicklung der Verdachtsfälle im Vergleich 2011–2016[1]

Mehrfachnennungen waren möglich.



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

3 Jeder dritte Versicherer von E-Crime betroffen

Für Versicherungsunternehmen erreicht das Risiko digitaler Wirtschaftskriminalität bereits beachtliche Dimensionen. Ein Drittel der Versicherer berichtete über mindestens einen Fall von E-Crime (34 %) und 39 % über einen Verdachtsfall. Angesichts des voranschreitenden Technologiewandels in Richtung digitale Wirtschaft ist zudem von einem weiteren Anstieg auch in der Versicherungswirtschaft auszugehen.

Im Vergleich zum analogen Betrug berichteten die Versicherer deutlich seltener über Fälle von Computerbetrug, aber es handelt sich auch hier um die häufigste Deliktsart (19 %). Jedes zehnte Versicherungsunternehmen war außerdem entweder durch Manipulation von Konto- und Finanzdaten (14 %) und/oder Ausspähen und Abfangen von Daten (10 %), Fälschung beweiserheblicher Daten (9 %) und/oder Diebstahl vertraulicher Kunden- und Unternehmensdaten (10 %) betroffen.

Dabei ist zu berücksichtigen, dass wir in unserer Erhebung einen engen Begriff von E-Crime zugrunde gelegt haben. Nicht jede digitale Begehungsform wurde als E-Crime angesehen, sondern nur solche Delikte, bei denen Informations- und Kommunikationstechnik als wesentliches Element der Tatausführung zur Verwirklichung der Wirtschaftsstraftat eingesetzt wird – wie beim Computerbetrug. Somit wurden alle Delikte ausgeschlossen, bei denen der Computer oder das Internet nur gewählt wurde, um beispielsweise die Begehung von Betrug zu vereinfachen. Zur Abgrenzung verwendeten 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).[7]

[7] Vgl. McGuire/Dowling, online abrufbar auf: www.gov.uk – Publications – Contains: Cybercrime – Cybercrime: a review of the evidence (7 Oct. 2013, Department: Home Office, Publication typ: Research and Analysis) – Chapter 1: Cyber-dependent crimes, S. 4.

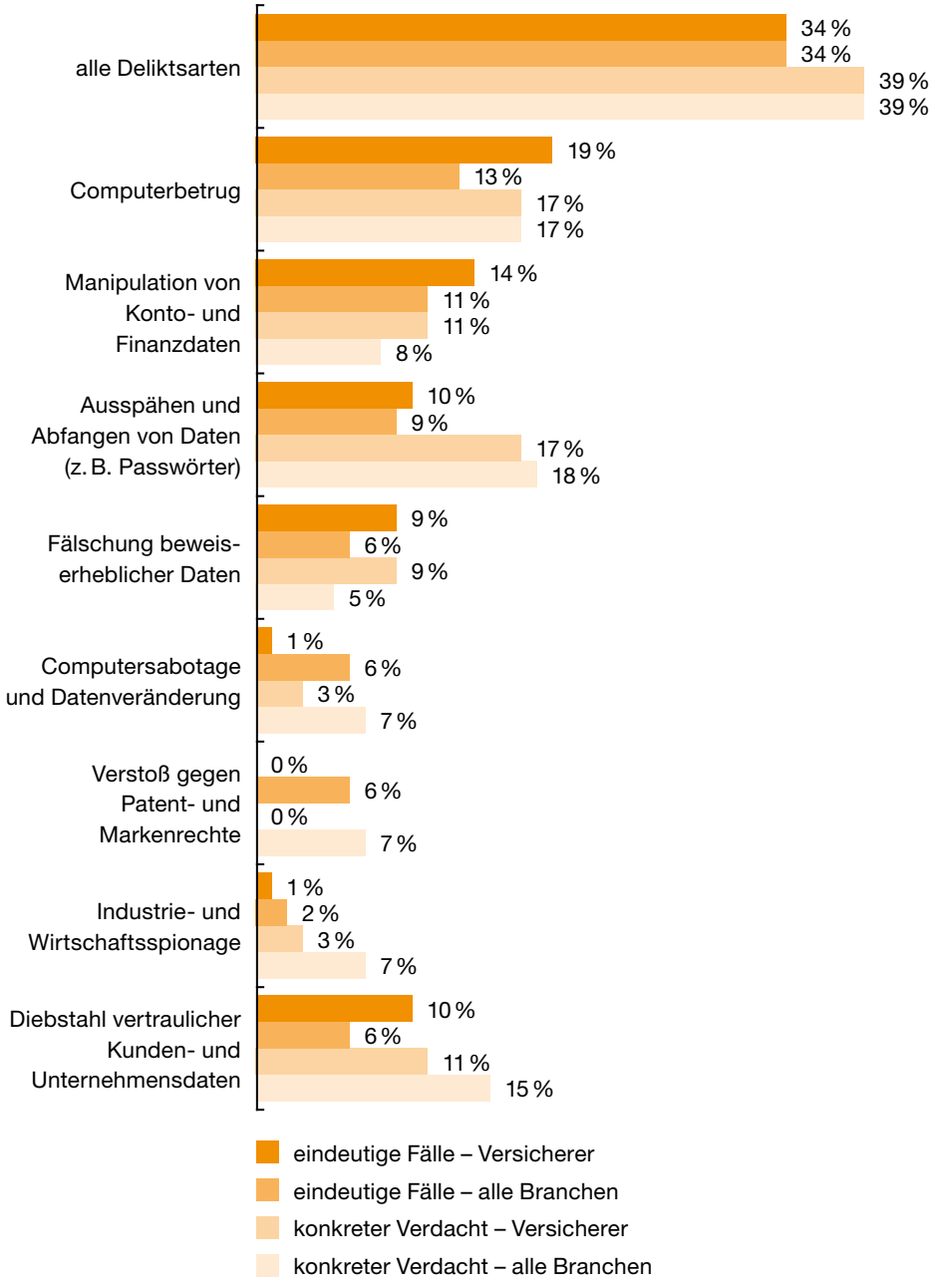
Beunruhigend sind Studien, nach denen über 80 % der Cyberangriffe organisiert durchgeführt werden.[8] Auch die OK richtet mittlerweile ihre Aktivitäten vermehrt auf lukrative Ziele in der digitalen Wirtschaft aus. Begleitet wird dieser Prozess durch eine wachsende Zahl nur loser Netzwerkstrukturen, die sich von hierarchischen Strukturen wie dem klassischen Paten ablösen und noch schwerer zu verfolgen sind. Diese Netzwerke beruhen auf ähnlichen Marktmechanismen wie legale Unternehmen.[9] Sie kennen auch Einheiten zur Forschung und Entwicklung. Diese Entwicklung im illegalen Markt macht diese illegalen Netzwerke für Staat und Wirtschaft so gefährlich. Zu dieser Einschätzung kommt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Lagebericht 2015:

> „Die Teilnehmer der Cyber-Sicherheitsumfrage 2015 der Allianz für Cyber-Sicherheit benennen weiterhin Organisierte Kriminalität und Wirtschafts-kriminalität 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 Fähig-keiten 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."[10]

[8] Vgl. UNODC, online abrufbar auf: www.unodc.org/ – Topics: Organized Crime – Emerging Crimes – Comprehensive study on cybercrime – Comprehensive study on cybercrime – S. 45 ff.
[9] Zum Ganzen vgl. Kleemans, Theoretical perspectives on organized crime, in: Handbook of Organized Crime, 2014, S. 32 f.
[10] BSI, Die Lage der IT-Sicherheit in Deutschland 2015, 2015, S. 36.

Abb. 4 Von E-Crime betroffene Versicherungsunternehmen

Mehrfachnennungen waren möglich.

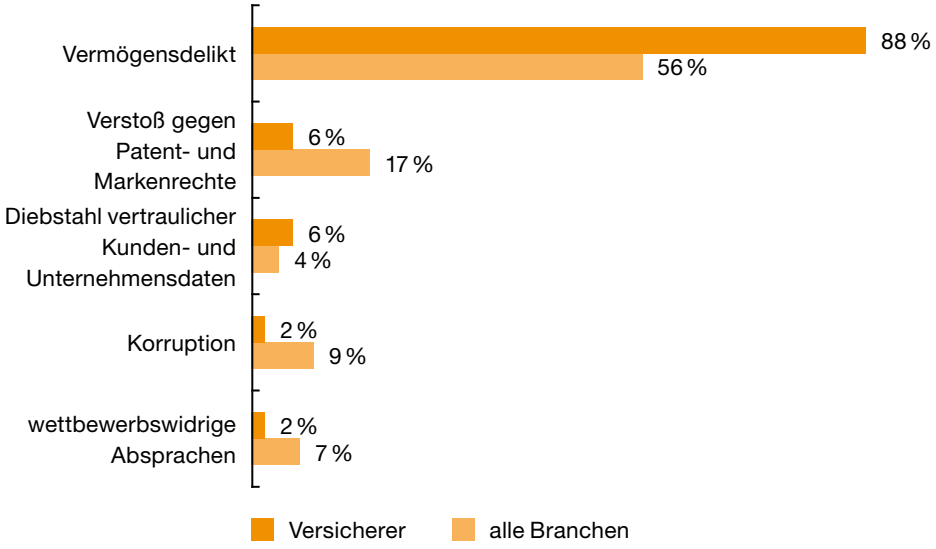


4 Schäden durch analoge und digitale Kriminalität

Versicherungsunternehmen waren nicht nur am häufigsten von Vermögensdelikten wie Betrug betroffen, sondern auch am folgenschwersten durch dieses Delikt. Nach den Erfahrungen der befragten Versicherer, aber auch der Unternehmen aus anderen Branchen, verursachen Vermögensdelikte am häufigsten den höchsten direkten und indirekten Schaden (88 % – alle Branchen 56 %). Alle anderen Wirtschaftsdelikte verursachen dem gegenüber seltener gravierende Schadensfolgen.

Abb. 5 Das klassische Wirtschaftsdelikt mit dem höchsten direkten und indirekten Schaden

Alle Delikte über 5 % der Nennungen.



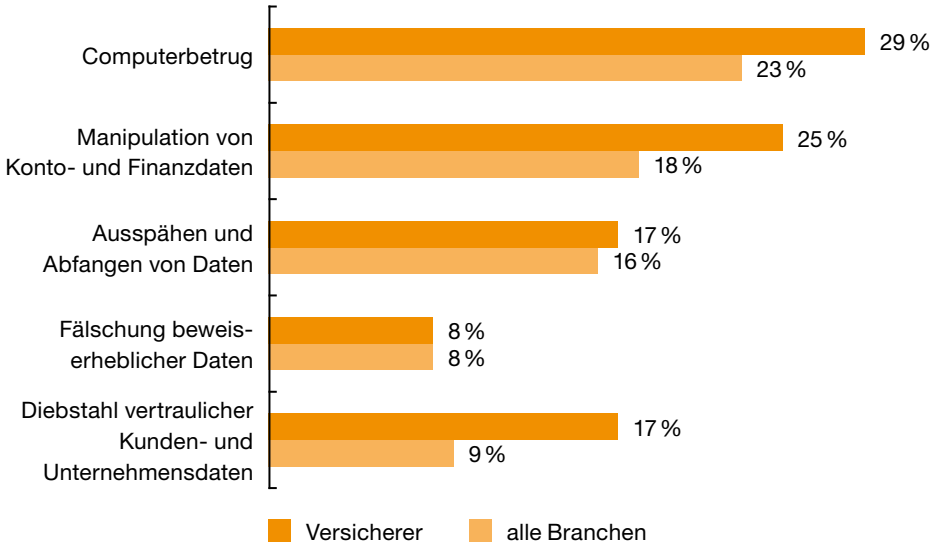
Basis: alle betroffenen Unternehmen

Innerhalb der E-Crime-Varianten sticht das Schadenspotenzial des Computerbetrugs sowohl in der Versicherungswirtschaft als auch im Durchschnitt aller Branchen nicht besonders hervor (29 %). Auch andere Cybercrime-Formen wie Manipulation von Konto- und Finanzdaten (25 %), Ausspähen und Abfangen von Daten (17 %) oder Diebstahl vertraulicher Kunden- und Unternehmensdaten (17 %) führen nach den Erfahrungen der befragten Versicherer zu erheblichen direkten und indirekten Schäden.

Auffällig ist allerdings, dass ein elektronischer Diebstahl vertraulicher Kunden- und Unternehmensdaten bei den befragten Versicherern deutlich häufiger zu höheren direkten und indirekten Schäden führt als im branchenübergreifenden Durchschnitt (17 %). Dies dürfte darauf zurückzuführen sein, dass die Versicherungswirtschaft in besonderem Maße auf das Vertrauen ihrer Kunden angewiesen ist und daher insoweit vergleichsweise anfällig ist.

Abb. 6 Das E-Crime-Delikt mit dem höchsten direkten und indirekten Schaden

Alle Delikte über 5 % der Nennungen.



Basis: alle betroffenen Unternehmen

C Tatort Versicherung

1 Bedrohung durch Geschäftspartner und Organisierte Kriminalität

In der Versicherungswirtschaft wurden die betroffenen Unternehmen häufiger als im branchenübergreifenden Durchschnitt durch externe Wirtschaftsstraftäter geschädigt (44 % – alle Branchen 30 %). Dabei handelte es sich ganz überwiegend um Geschäftspartner und Dienstleister (75 % – alle Branchen 35 %) und nur zum geringen Teil um Tätergruppen, zu denen keine Geschäftsbeziehung bestand (13 % – alle Branchen 48 %). In unserer Studie 2012 zeigte sich, dass es sich hierbei zu einem großen Teil um Provisionsbetrug durch Versicherungsvermittler handelt.[11] In den allermeisten Fällen bestand somit eine Geschäftsbeziehung zu den Tätern.

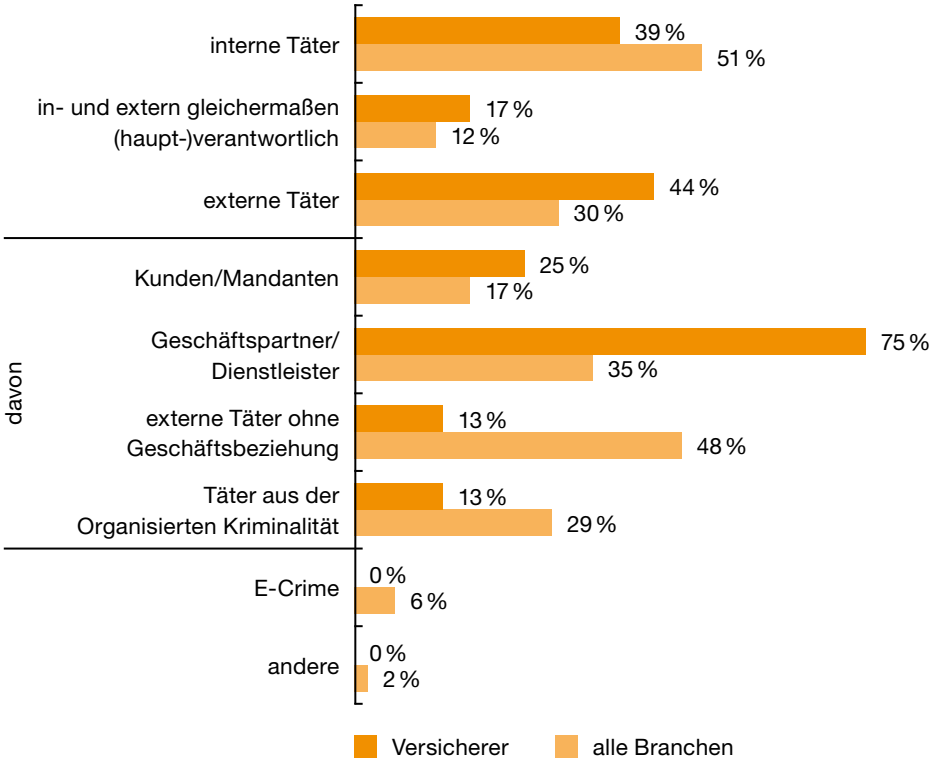
Beunruhigend ist für die Versicherungswirtschaft auch, dass ein Teil der externen Täter der Organisierten Kriminalität (OK) zugerechnet werden muss. Innerhalb der Gruppe der externen Täter wurde jeder zehnte Fall von den betroffenen Versicherern auf OK zurückgeführt (alle Branchen 29 %). Das Bundeskriminalamt (BKA) kommt in seinem Bundeslagebild zu einer ähnlichen Beurteilung der Risikolage:

> „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 Organisierten Kriminalität weiterhin den dritten Rang ein. […] Gemessen an der Gesamtschadenssumme aller OK-Verfahren war der durch Wirtschaftskriminalität verursachte Schaden sehr hoch.“[12]

[11] Vgl. PwC/Universität Halle-Wittenberg (Hg.), Wirtschaftskriminalität – Versicherungsbranche, 2012, S. 14 und 20.
[12] BKA, Bundeslagebild Organisierte Kriminalität 2014, 2015, S. 25.

Abb. 7 Beziehung der Täter zum geschädigten Unternehmen

Mehrfachnennungen waren möglich.



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

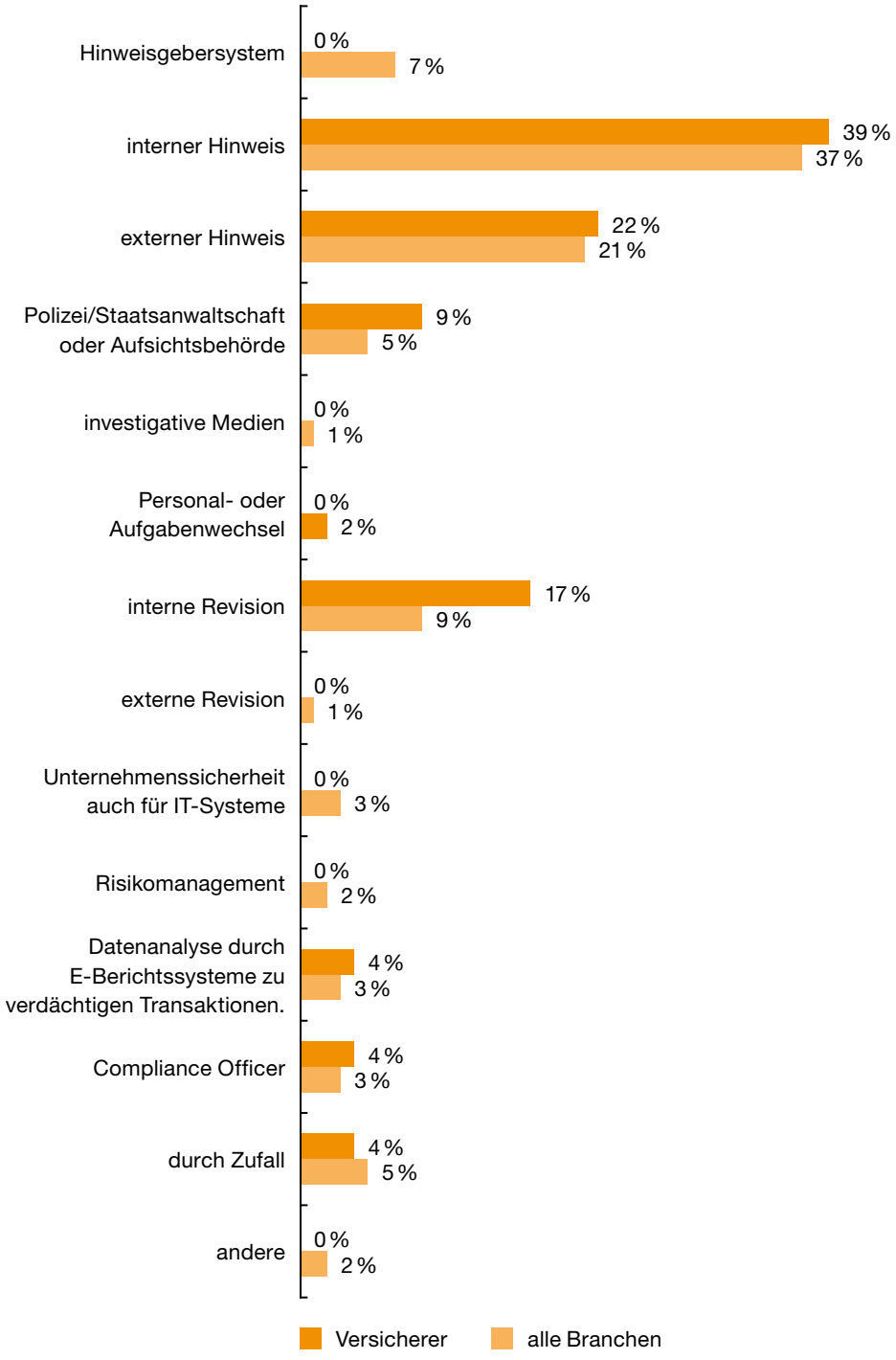
2 Erstentdeckung von Delikten – Interne Revision erfolgreicher

Auch diese Studie zeigt die besondere Bedeutung interner und externer Hinweisgeber. Dies gilt auch für die Versicherungswirtschaft. In mehr als jedem dritten Fall erfolgte die Erstaufdeckung durch einen internen Hinweis (39 % – alle Branchen 37 %) und in jedem fünften Fall durch einen Hinweisgeber außerhalb des betroffenen Versicherers (22 % – alle Branchen 21 %).

Allerdings gelingt es der Internen Revision häufiger als im Durchschnitt aller Branchen, Wirtschaftskriminalität aufzudecken (17 % – alle Branchen 9 %). Auch gegenüber den Ergebnissen unserer Studie 2012 zeigt sich eine deutliche Zunahme der Erstentdeckungen durch die Interne Revision der befragten Versicherer (2012: 3 % – alle Branchen 8 %). Zudem hat der Anteil der Zufallsfunde gegenüber 2012 leicht abgenommen (Versicherer 2016: 4 % – 2012: 8 %). Dies spricht insgesamt gesehen für eine höhere Wirksamkeit der Internen Revision in den befragten Versicherungsunternehmen.

Hinweisgebersysteme können eine weitere wichtige Quelle für Informationen sein. Im Vergleich zum branchenübergreifenden Durchschnitt (7 %) werden in der Versicherungswirtschaft über diesen Weg bei den befragten Unternehmen jedoch keine Verstöße entdeckt; 2012 lag ihr Anteil bei den befragten Versicherern bei 4 %, 2016 bei 0 %. Strafverfolgungsbehörden (9 % – alle Branchen 5 %) und investigative Medien sind rein quantitativ gesehen ebenfalls von eher untergeordneter Bedeutung.

Abb. 8 Gründe für die Erstentdeckung von Delikten im Vergleich



Basis: Anteil an den berichteten Fällen

D IT-Risk-Management in der Versicherungswirtschaft

1 Versicherer unterschätzen die Risiken des Entwendens bzw. Kopierens von Firmenunterlagen

Cybercrime ist die Kehrseite der digitalen Wirtschaft und die OK hat Cybercrime als einträgliches Geschäftsfeld für sich entdeckt, wie auch das BSI in seinem Lagebericht 2015 betont.[13] Wie unsere Studie zeigt, sind auch für die Versicherungswirtschaft diese Risiken erheblich. Jeder dritte Versicherer berichtete über einen Fall von E-Crime (siehe auch Abschnitt B 3).

Die befragten Versicherungsunternehmen beurteilen das Risiko eines Daten- und Wissensverlust bei nahezu allen Angriffsvektoren weitgehend ähnlich wie Unternehmen in anderen Branchen (siehe Durchschnittswerte, Abb. 9). Die höchsten Risiken werden sowohl bei herkömmlichen Angriffspunkten wie Abwerbung von Mitarbeitern gesehen als auch bei den digitalen Angriffen auf mobile IT-Systeme (beispielsweise Mobiltelefone). Nahezu jedes zweite Versicherungsunternehmen stuft diese Risiken als mittel bis hoch ein (46 % bzw. 49 %).

Demgegenüber wird das Risiko von Angriffen auf stationäre IT-Geräte allgemein deutlich niedriger eingeschätzt, nur jeder dritte Versicherer sieht hier nennenswerte Risiken. Ein geringes Risiko besteht nach der Einschätzung der meisten Versicherungsunternehmen auch hinsichtlich des Entwendens und Kopierens von Firmenunterlagen (30 %), der Informationsgewinnung durch gezielte Beeinflussung von Mitarbeitern auf Messen oder Tagungen (32 %), der Auswertung offener Quellen (19 %) sowie des Abhörens von Telefonen und unberechtigten E-Mail-Lesen (26 %) und des Abhörens von Besprechungen/Geschäftsräumen (3 %).

Unsere Studie zeigt allerdings, dass neben den Risiken durch Angriffe auf digitale Informations- und Kommunikationstechnologien auch herkömmliche Risiken nicht unterschätzt werden sollten. Anhand der branchenübergreifenden Auswertung von tatsächlichen Fällen zeigt sich nämlich (ohne Grafik), dass die Angriffe entgegen der Einschätzung der befragten Unternehmen tatsächlich seltener als angenommen auf IT-Systeme erfolgten wie stationäre (20 %), mobile IT-Systeme (10 %) und die Cloud (2 %),[14] sondern am häufigsten durch schlichtes Entwenden bzw. Kopieren von Firmenunterlagen (42 %).[15] Bei den befragten Versicherern erfolgte ein Daten- und Wissensverlust bei tatsächlichen Fällen ebenfalls am häufigsten auf diese geradezu klassisch zu nennende Weise (64 %).

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.

---

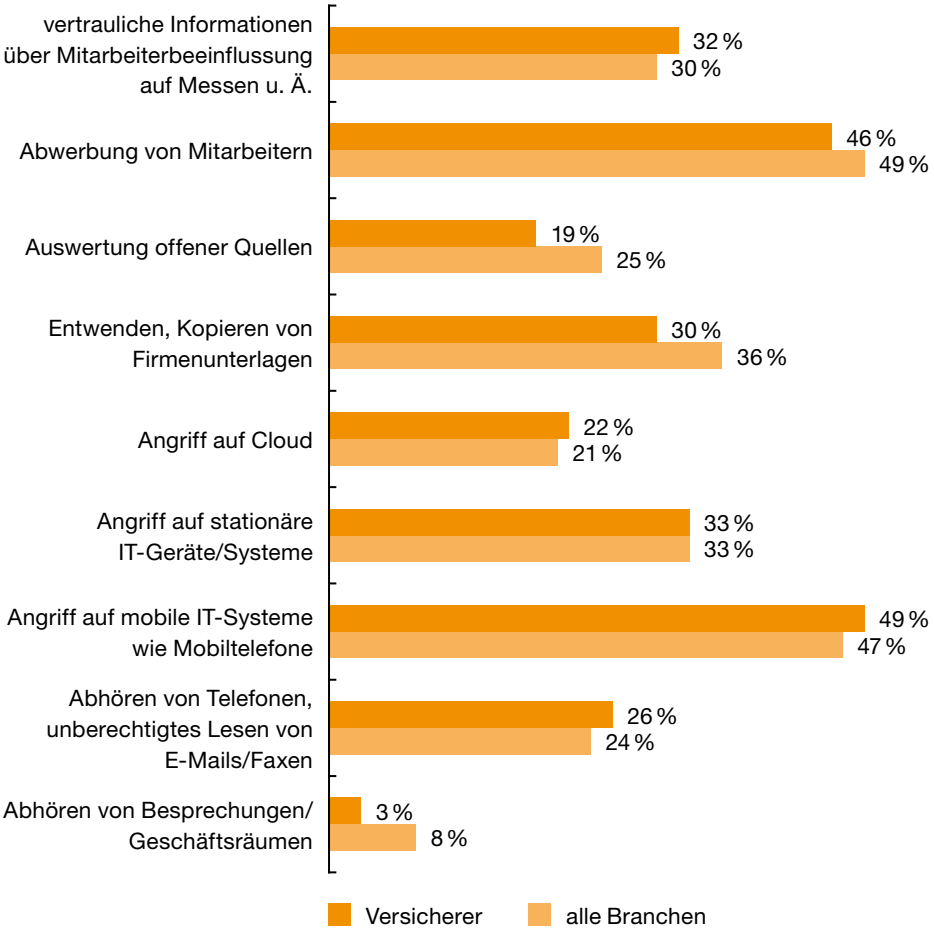
[13] Vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2015, S. 36.

[14] Den Risiken des Cloud Computing haben wir uns bereits in der Studie von 2013 ausführlicher gewidmet, vgl. PwC/Universität Halle-Wittenberg (Hg.), Wirtschaftskriminalität und Unternehmenskultur 2013, 2013, S. 19 ff.

[15] Vgl. PwC/Universität Halle-Wittenberg (Hg.), Wirtschaftskriminalität in der analogen und digitalen Wirtschaft 2016, S. 36 f. abrufbar auf: www.pwc.de/de/risiko-management/assets/studie-wirtschaftskriminalitaet-2016.pdf.

Abb. 9 Einschätzung der Risiken der Angriffsvektoren des Daten- und Wissensverlusts

Mehrfachnennungen waren möglich.
Einschätzung der Risiken mittel bis hoch.



Basis: alle Versicherer und nur Unternehmen aus der Gruppe „alle Branchen“ mit keiner oder geringer Forschung und Entwicklung

2 Zertifizierungen von IT-Sicherheitsmaßnahmen noch nicht selbstverständlich

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.[16]

[16] Vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2015, 2015, S. 40 ff.

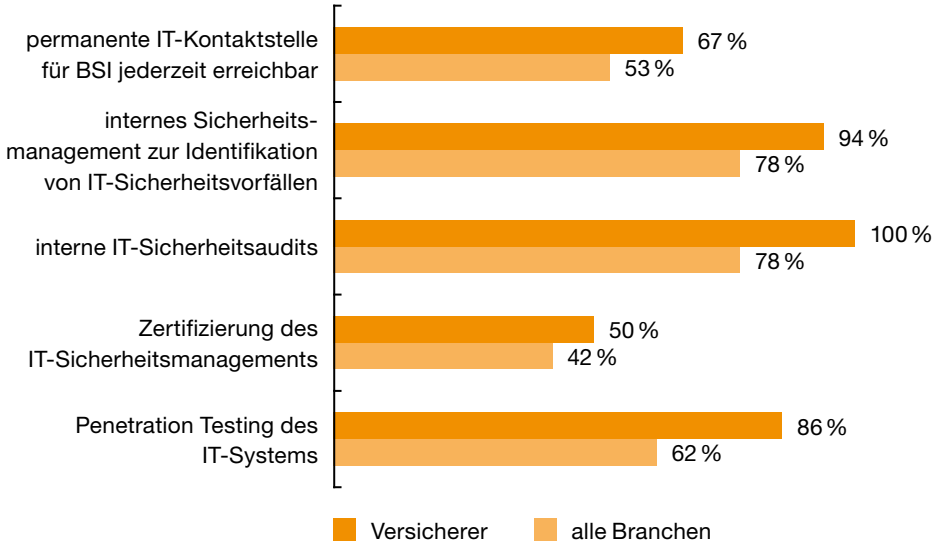
Wir haben erhoben, welche Unternehmen nach eigener Einschätzung vom IT-Sicherheitsgesetz betroffen sind.[17] Im Durchschnitt aller Branchen geht jedes fünfte Unternehmen davon aus (21 %), dass es zur KRITIS im Sinne des Gesetzes zu zählen ist, bei den befragten Versicherungsunternehmen rechnet sich demgegenüber jedes vierte dazu (26 %).

Im Vergleich zur übrigen Wirtschaft hat sich die Versicherungswirtschaft deutlich besser gegen Cyberangriffe gewappnet. Beschränken wir uns im Vergleich auf Unternehmen, die sich zur KRTIS zählen, so verfügen fast alle Versicherer über ein internes Sicherheitsmanagement zur Identifikation von IT-Sicherheitsvorfällen (94 %), gegenüber dem branchenübergreifenden Durchschnitt von nur drei Vierteln der Unternehmen (78 %). Interne IT-Sicherheitsaudits sind sogar die Regel (100 % – alle Branchen 78 %).[18] Auch ein Penetration Testing des IT-Systems[19] gehört für die meisten Versicherungsunternehmen zu den selbstverständlichen IT-Sicherheitsmaßnahmen (86 % – alle Branchen 62 %).

Es ist allerdings davon auszugehen, dass generell in der Wirtschaft und auch in der Versicherungswirtschaft weiterhin ein großer Handlungsbedarf in Bezug auf die Verbesserung der bestehenden IT-Sicherheitsmaßnahmen besteht. Der Gesetzgeber sieht nicht ohne Grund erheblichen Handlungsbedarf und hat zumindest für Betreiber kritischer Infrastrukturen eine Nachweispflicht über die Einhaltung von IT-Sicherheitsstandards im IT-Sicherheitsgesetz vorgesehen. Bemerkenswert ist ebenfalls, dass nur jedes zweite Versicherungsunternehmen eine Zertifizierung ihres Sicherheitsmanagements durchgeführt hat (50 % – alle Branchen 42 %).

Abb. 10 Verbreitung von IT-Sicherheitsmaßnahmen bei Versicherern der KRITIS

Maßnahme (nahezu) abgeschlossen.



Basis: nur Versicherer und andere Unternehmen der KRITIS

[16] Vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2015, 2015, S. 40 ff.
[17] Eine nähere Bestimmung der kritischen Infrastrukturen für den Sektor der Versicherungen erfolgte auch in der am 22.04.2016 ausgefertigten „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“ nicht.
[18] Ergebnisse für alle befragten Versicherer: internes Sicherheitsmanagement 88 %, interne IT-Sicherheitsaudits 86 %, Zertifizierung des IT-Managements 37 %, Penetration Testing 75 %.
[19] Penetration Testing: Sicherheitsprüfung des IT-Systems mit Methoden, die ein Angreifer anwenden könnte, um unautorisiert in das System einzudringen.

E Compliance und Werte

1 Status des Compliance-Managements in der Versicherungswirtschaft nach Deliktsgruppen

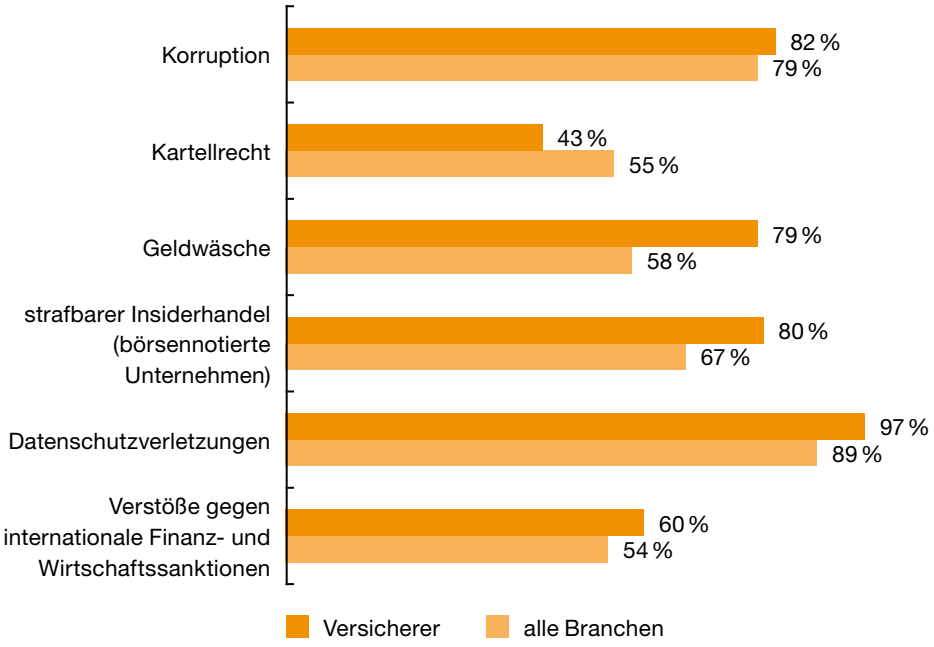
In der Versicherungswirtschaft sind Compliance-Managementsysteme mittlerweile fest etabliert, 87 % der Versicherer verfügen über ein solches (alle Branchen 76 %). Die Compliance-Programme erstrecken sich zumeist auf die Vermeidung von Datenschutzverletzungen (97 %), die Prävention gegen Korruption (82 %), der Geldwäscheprävention (79 %) sowie strafbare Insiderdelikte gemäß § 38 WpHG (80 %).

Allerdings zeigen sich auch Lücken. Dies betrifft zum einen Verstöße gegen internationale Finanz- und Wirtschaftssanktionen (60 % – alle Branchen 55 %), aber vor allem die Prävention gegen wettbewerbswidrige Absprachen. Eine kartellrechtliche Compliance ist in der Versicherungswirtschaft noch keinesfalls selbstverständlich, weniger als die Hälfte der Compliance-Programme der befragten Versicherer umfasst auch diese Deliktsgruppe (43 % – 55 % alle Branchen).

Die kartellrechtlichen Risiken sollten in der Versicherungswirtschaft jedoch auch im Vergleich zu anderen Branchen keinesfalls unterschätzt werden. So berichteten 6 % der Versicherer über wettbewerbswidrige Absprachen (alle Branchen 5 %) und jeder zehnte äußerte einen Verdacht auf einen strafbaren Wettbewerbsverstoß (11 % – alle Branchen 12 %, siehe Abschnitt B 1 und 2). Die kartellrechtlichen Risiken entsprechen somit in dieser Branche dem Durchschnitt.

Abb. 11 Status des CMS nach Deliktsgruppen

Status (nahezu) abgeschlossen.



Basis: Unternehmen mit CMS

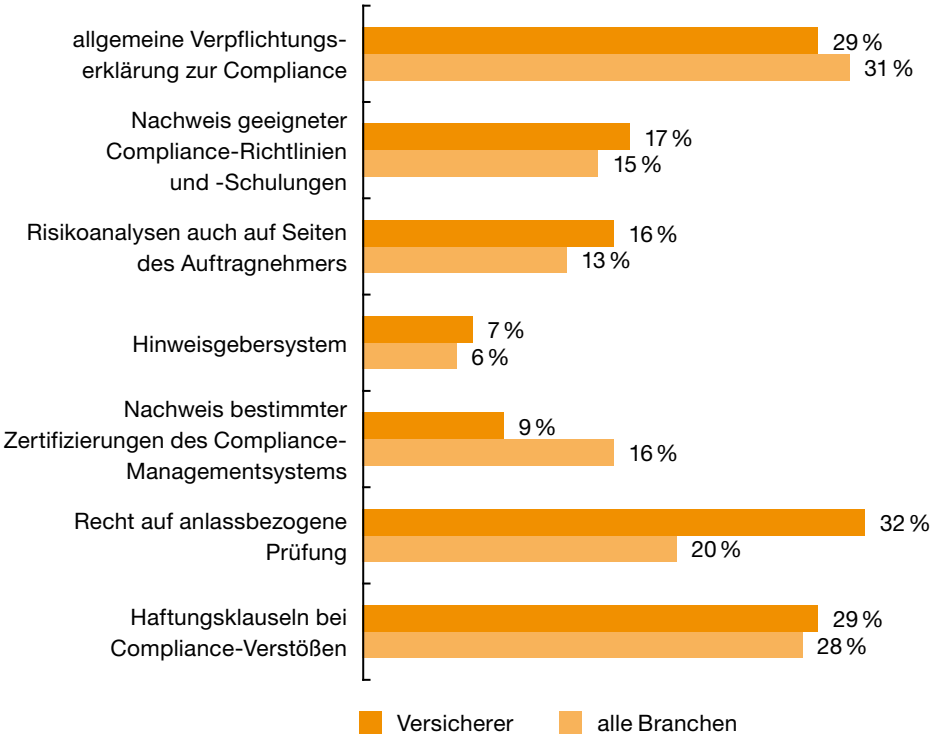
2 Bedeutung von Compliance-Klauseln in den Verträgen

Auch in der Versicherungswirtschaft beginnt der Markt das Regime zu übernehmen und über die Vertragsgestaltung auf die Etablierung von Compliance-Programmen bei Dienstleistern und Zulieferern Einfluss zu nehmen.[20]

Der Druck zur Einführung eines CMS erfolgt auch in der Versicherungswirtschaft über Haftungsklauseln und die vertragliche Einräumung von Kontrollrechten. Weit über ein Viertel der Versicherer sind dazu übergegangen, in ihren Verträgen eine Verpflichtungserklärung vorzusehen (29 % – alle Branchen 31 %). Ebenso häufig sind Haftungsklauseln im Falle von Compliance-Verstößen (29 % – alle Branchen 28 %). Eine große Bedeutung besitzt in der Versicherungswirtschaft auch die Verwendung einer sogenannten Audit Clause. Jeder dritte Versicherer lässt sich ein Recht auf anlassbezogene Prüfungen zusichern (32 % – alle Branchen 20 %).

Einige Verträge formulieren zusätzlich konkrete Anforderungen an die Ausgestaltung des CMS ihres Vertragspartners. 17 % der Versicherer verlangen Nachweise über geeignete Compliance-Richtlinien und -Schulungen (alle Branchen 15 %). Vereinzelt finden sich in den Vertragskonditionen Regelungen zur Zertifizierung des CMS (9 % – alle Branchen 16 %). Ein Hinweisgebersystem verlangen bislang nur wenige Unternehmen (7 % – alle Branchen 6 %).

Abb. 12 Verbreitung von (regelmäßigen) Compliance-Vertragskonditionen



Basis: Unternehmen mit CMS

[20] Vgl. auch Bussmann/Salvenmoser/Jeker, Compliance ist im Markt, aber noch nicht im Recht – Ergebnisse aus einer Unternehmensbefragung, in: CCZ 5, 2016, S. 236 ff.

3 Die stärksten Werte in Unternehmen der Versicherungswirtschaft

Ein erfolgreiches Compliance-Managementsystem kann sich nicht auf die Schaffung von Normbewusstsein und auf Kontrollen beschränken. Es gilt, eine integritätsförderliche Unternehmenskultur zu implementieren bzw. diese zu fördern. Hierzu bedarf es Werte, die zu einer Verinnerlichung des rechtlichen Rahmens beitragen und zugleich übergreifende Prinzipien im Unternehmen vermitteln. 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 Geschäftspartnern einzufordern (auch als „Speak-up-Kultur“ bezeichnet).

In einer offenen Frage, die sich thematisch nicht auf Compliance-Aspekte beschränkte, nannten uns die Unternehmen Werte, die ihre Kultur am stärksten kennzeichnen.[21] Auch bei den befragten Versicherungsunternehmen bezieht sich ein Teil der Werte auf Aspekte, die man weniger mit der Förderung von Criminal Compliance in Verbindung bringen kann, wie Kunden- und Serviceorientierung (34 % – alle Branchen 16 %), Sicherheit (11 % – alle Branchen 4 %) oder soziale Partnerschaft (9 % – alle Branchen 6 %).

Ein großer Teil der am häufigsten genannten Werte eignet sich aus Sicht der Forschung zur Etablierung einer integritätsförderlichen Unternehmenskultur.[22] Die Versicherer nannten folgende Werte:

Verbindlichkeit und Konsistenz (23 % – alle Branchen 22 %): Vorgesetzte zeigen dieselben Prioritäten, die sie von ihren Mitarbeitern erwarten, und kritisieren bei Compliance-Verstößen.

Regelkonformität (21 % – alle Branchen 18 %): Dies bedeutet, Unternehmensrichtlinien nicht zu vernachlässigen: somit auch auf Geschäftsabschlüsse zu verzichten, wenn diese nur durch einen Compliance-Verstoß zu erreichen wären.

Transparenz und Ehrlichkeit (13 % – alle Branchen 18 %): Dieser Wert betrifft die Aufrichtigkeit in geschäftlichen Entscheidungen und im Umgang mit Kollegen.

Vertrauen (20 % – alle Branchen 13 %): Im Unternehmen ist es wichtig, dass man Vorgesetzten vertrauen kann; sie vermitteln glaubhaft, dass beispielsweise Bestechung keine legitime Praxis darstellt.

Offene Kommunikation (10 % – alle Branchen 12 %): Ohne diese Wertorientierung kann sich eine Speak-up-Kultur, in der sich Mitarbeiter trauen, Probleme offen anzusprechen und auch über den Umgang mit Compliance-Verstößen offen zu sprechen, nicht etablieren.

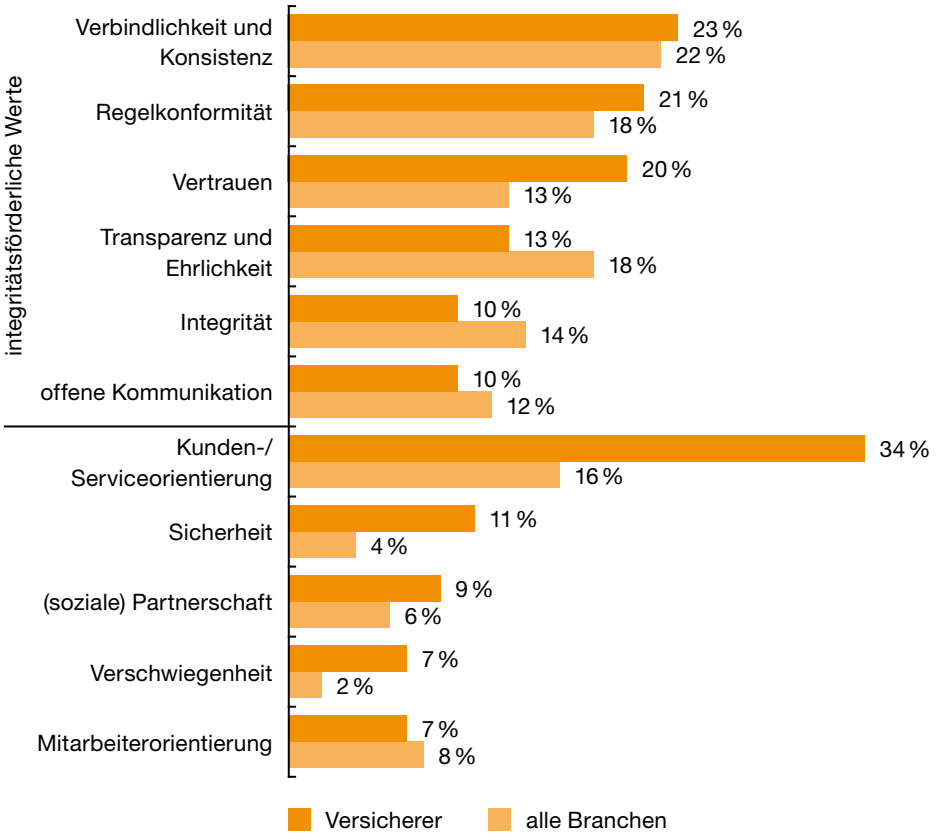
[21] Es durften bis zu drei Werte genannt werden, teilweise wurden allerdings auch mehr Werte genannt.

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

Im Vergleich mit allen Branchen besitzt in der Versicherungswirtschaft vor allem Kunden- und Serviceorientierung einen großen Stellenwert als eigenständiger Wert (34 % – alle Branchen 16 %). Integritätsförderliche Werte wie Verbindlichkeit, Regelkonformität und Vertrauen wurden in dieser Branche häufiger als im Durchschnitt genannt. Vertrauen schaffen und erhalten ist offenkundig ein Wert, der Versicherern im Vergleich zum Durchschnitt aller Branchen wichtiger ist. Im Übrigen zeigen sich keine signifikanten Abweichungen.

Abb. 13 Die stärksten Werte in Unternehmenskulturen

Werte, die die Kultur des Unternehmens am stärksten kennzeichnen (bis zu drei Nennungen möglich).



Basis: alle befragten Unternehmen

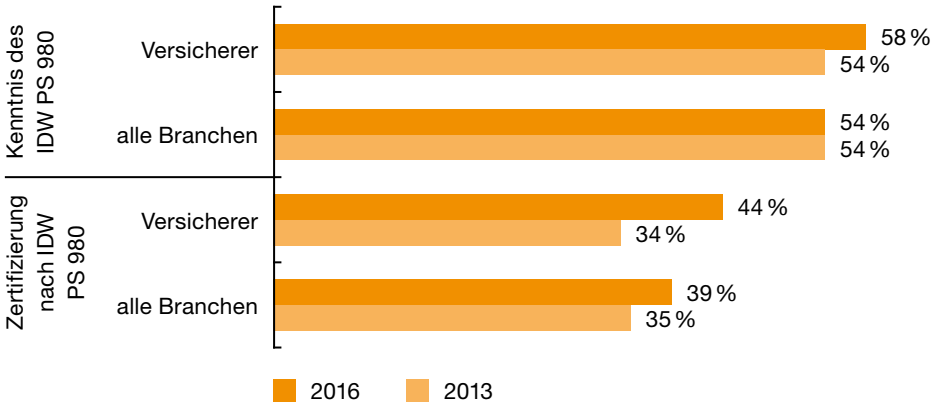
F Zunehmende Prüfung des CMS nach IDW PS 980

1 Bedeutung des IDW PS 980 im Vergleich

In der Versicherungswirtschaft nahm die Bekanntheit des Prüfungsstandards 980 des Instituts der Wirtschaftsprüfer (IDW) gegenüber 2013 leicht zu, sie stieg um vier Prozentpunkte auf 58 % (alle Branchen 54 %).[23] In der Tendenz ist der Prüfungsstandard bei größeren Versicherungsunternehmen etwas bekannter als bei kleineren (ohne Grafik).

Zugenommen hat auch die Zahl der Unternehmen in dieser Branche, die eine Zertifizierung nach diesem Standard durchgeführt haben (siehe Abb. 14). In der aktuellen Studie berichteten 44 % der Versicherungsunternehmen über eine entsprechende Prüfung des Compliance-Managementsystems, im Vergleich aller Branchen ist dies überdurchschnittlich (alle Branchen 39 %, siehe Abb. 14). Allerdings zeigt sich kein eindeutiger Zusammenhang zwischen der Größe der Versicherer und der Zertifizierung ihres Compliance-Managementsystems (ohne Grafik).

Abb. 14 Kenntnis des IDW PS 980 und erfolgte Zertfizierung nach Unternehmensgröße



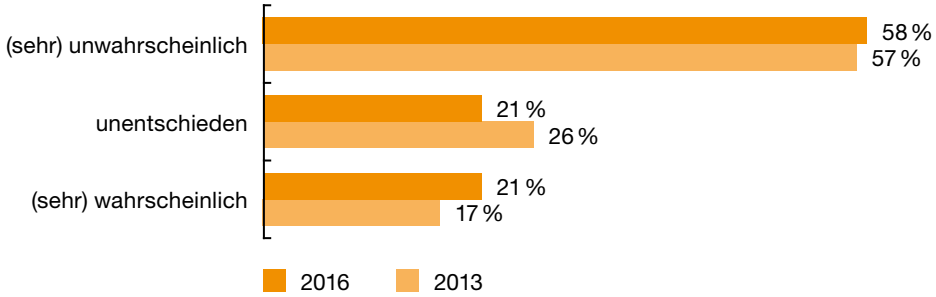
Basis: Anteil der Unternehmen mit Zertifizierung nach IDW PS 980 nur für Unternehmen, die den Standard kennen

[23] IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980), IDW Verlag.

2 Compliance-Audit noch nicht selbstverständlich

Ein Compliance-Managementsystem ist in der Versicherungsbranche aufgrund der regulatorischen Vorgaben gemäß Solvency II heute verpflichtend einzurichten und es zeigt sich gegenüber 2013 insbesondere aufgrund der Anforderungen gemäß des Verhaltenskodizes des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV) für den Versicherungsvertrieb ein stetig wachsendes Interesse an einer unabhängigen Zertifizierung nach IDW PS 980. Zwar beabsichtigen 58 % der befragten Versicherer, soweit sie noch keine Auditierung nach IDW PS 980 vorgenommen haben, auch in den nächsten zwei Jahren eine solche nicht durchzuführen (alle Branchen 60 %). Allerdings wollen über ein Viertel der Versicherer (21 %) ihr Compliance-Managementsystem einer Evaluation unterziehen (alle Branchen 19 %), ein gutes Fünftel ist noch unentschieden (21 % – alle Branchen 21 %).

Abb. 15 Wahrscheinlichkeit einer Zertifizierung nach IDW PS 980 in den nächsten zwei Jahren



Basis: IDW PS 980 bekannt und Zertfizierung noch nicht durchgeführt

G Haftungsrisiken und Rechtsformen

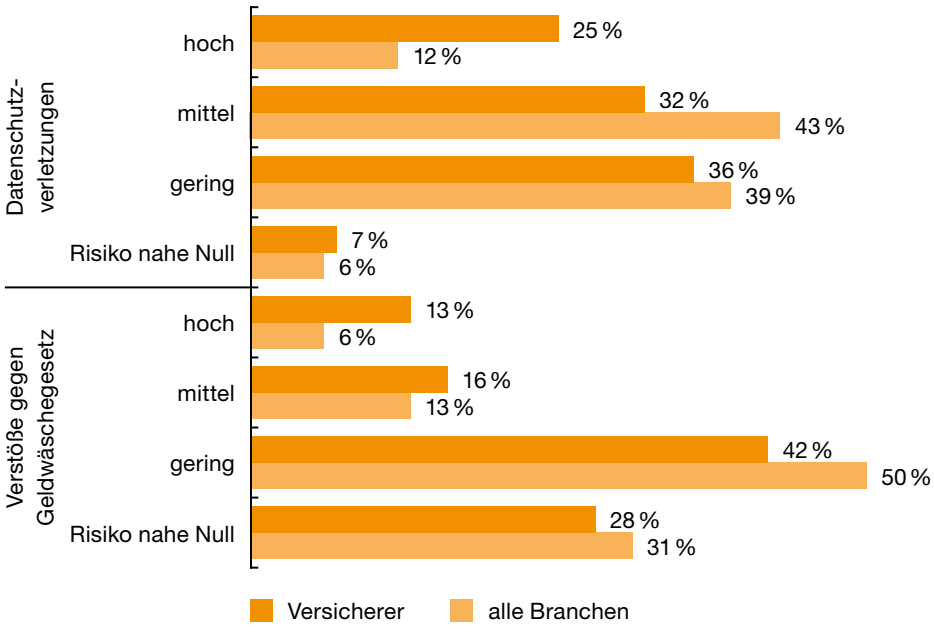
1 Einschätzung der Haftungsrisiken in der eigenen Branche

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. Im folgenden Vergleich beschränken wir uns auf die beiden Deliktsfelder, bei denen die Versicherungsunternehmen die höchsten Haftungsrisiken vermuten: Datenschutzverletzungen und Geldwäsche.

Die höchsten Haftungsrisiken sehen die befragten Unternehmen in allen Branchen im Falle von Datenschutzverletzungen.[24] Weniger als 10 % sehen das Risiko bei Null. Auffällig ist, dass ein Teil der Versicherer für ihre Branche von deutlich höheren Risiken ausgehen als der Durchschnitt aller Branchen. Jedes vierte Versicherungsunternehmen stufte diese Haftungsrisiken als hoch ein (25 % – alle Branchen 12 %), jeweils rund ein Drittel geht von einem mittleren bzw. geringen Haftungsrisiko aus.

Sehr viel geringer werden allgemein die Haftungsrisiken aufgrund von Verstößen gegen das Geldwäschegesetz eingestuft. 42 % der Versicherer vermuten nur ein geringes Haftungsrisiko (alle Branchen 50 %) und rund ein Viertel sehen das Risiko bei nahe Null (28 % – alle Branchen 31 %). Insgesamt gesehen gehen die befragten Versicherer für ihre Branche von etwas höheren Risiken aus, wobei zu konzedieren ist, dass bei Versicherungsunternehmen die Qualität des jeweiligen Geldwäsche-Compliance-Systems eher überdurchschnittlich ist.

Abb. 16 Einschätzung der Haftungsrisiken in der eigenen Branche



Basis: alle befragten Unternehmen

[24] Siehe Überblick über alle Delikte: PwC/Universität Halle-Wittenberg (Hg.), Wirtschaftskriminalität in der analogen und digitalen Wirtschaft 2016, S. 72.

2 Beurteilung gesetzlicher Regelungen im Falle einer Reform der Unternehmenshaftung

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.[25] 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.[26] Dies gilt vor allem für Unternehmen in der Versicherungswirtschaft. Eine gesetzliche Regelung, die Mindestaufsichts- bzw. Mindest-Compliance-Standards zur Schaffung von Rechtssicherheit enthält,[27] hält fast jeder zweite Versicherer für sinnvoll und fast ebenso häufig für überlegenswert (46 % bzw. 42 %). Außerdem befürwortet jeder dritte Versicherer eine Regelung zur sanktionsausschließenden bzw. -mildernden Anrechnung von CMS (35 %) und mehr als die Hälfte 58 % halten eine solche Regelung für überlegenswert.[28]

Des Weiteren würde nahezu jedes zweite Versicherungsunternehmen eine Regelung begrüßen, die dezidiert eine Kooperation mit den Strafverfolgungsbehörden sanktionsausschließend bzw. -mildernd berücksichtigt (45 %), 43 % erachten eine solche Regelung für überlegenswert. Die Mehrheit der Versicherer traut sich offenkundig zu, strafbare Compliance-Verstöße aufzudecken, sodass sie für eine Strafanzeige verständlicherweise ein Entgegenkommen von den strafrechtlichen Ermittlungsbehörden erwarten.[29]

---

[25] Vgl. Gesetzesantrag des Landes NRW, Entwurf eines Gesetzes zur Einführung der strafrechtlichen Verantwortlichkeit von Unternehmen und sonstigen Verbänden aus dem Jahr 2013, online abrufbar auf: https://www.justiz.nrw.de/JM/leitung/jumiko/beschluesse/2013/herbstkonferenz13/zw3/TOP_II_5_Gesetzentwurf.pdf.

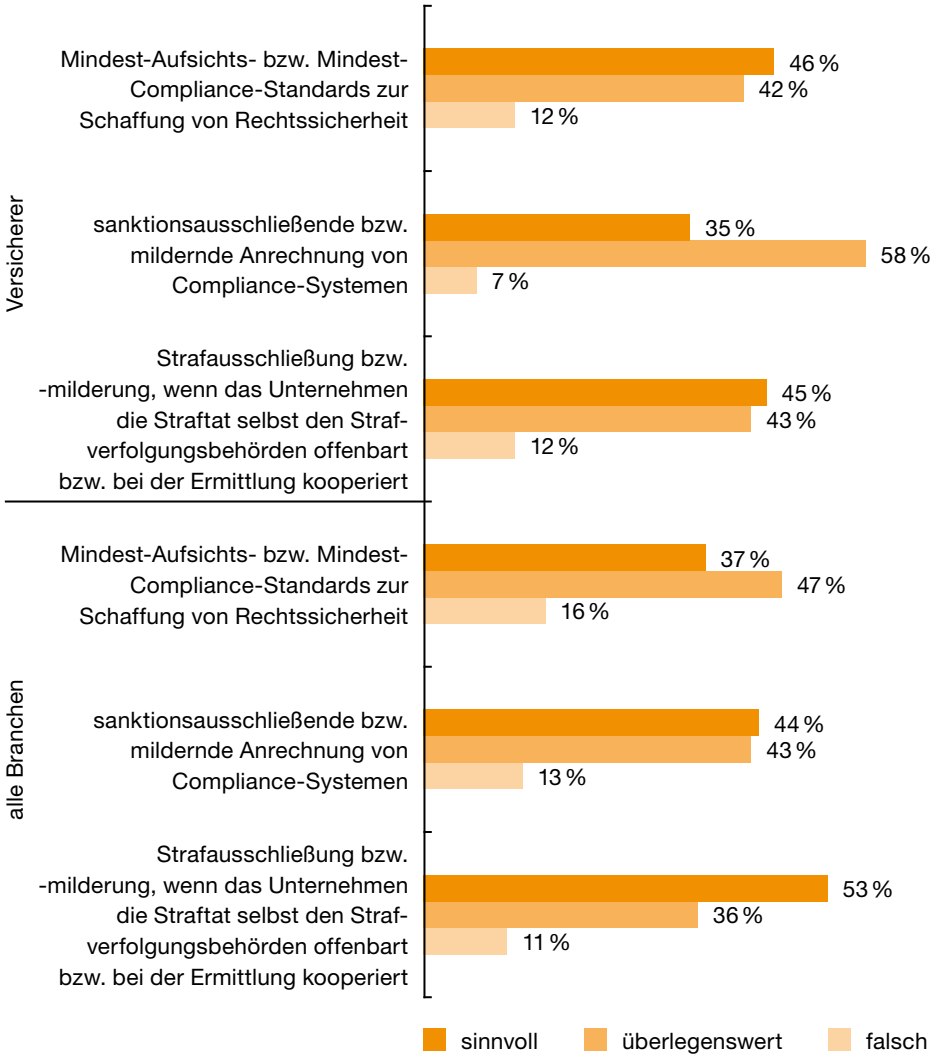
[26] Vgl. auch Bussmann/Salvenmoser/Jeker: Compliance ist im Markt, aber noch nicht im Recht – Ergebnisse aus einer Unternehmensbefragung, in: CCZ 5, 2016, S. 236 ff.

[27] Vgl. auch Gesetzgebungsvorschlag für eine Änderung der §§ 30, 130 OWiG durch den Bundesverband der Unternehmensjuristen – Fachgruppe Compliance, S. 9 f., online abrufbar auf: www.buj.net/resources/Server/BUJ-Stellungnahmen/BUJ_Gesetzgebungsvorschlag_OWiG.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 auf: www.dico-ev.de/wp-content/uploads/2016/10/CompAG_21_07_2014.pdf.

[28] Vgl. auch Stellungnahme der Bundesrechtsanwaltskammer zur Einführung einer Unternehmensstrafe, S. 10, online abrufbar auf: http://www.brak.de/zur-rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2013/mai/stellungnahme-der-brak-2013-09.pdf; Bundesverband der Unternehmensjuristen – Fachgruppe Compliance (s. Fn. 27), S. 8; Deutsches Institut für Compliance e. V., Vorschlag für ein Compliance-Anreiz-Gesetz (s. Fn. 27), S. 3 ff.

[29] Vgl. Bundesverband der Unternehmensjuristen – Fachgruppe Compliance (s. Fn. 27), S. 8.

Abb. 17 Beurteilung gesetzlicher Regelungen im Falle einer Reform der Unternehmenshaftung



Basis: alle Unternehmen mit CMS

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 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. Mehr als 10.300 engagierte Menschen an 22 Standorten. 1,9 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