KPMG

Neues Denken, Neues Handeln

Insurance Thinking Ahead
Versicherungen im Zeitalter von Digitalisierung und Cyber
Studienteil B: Cyber

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

1. Vorwort

Wie die zwei Seiten derselben Medaille begleitet die Zunahme von Cyber-Risiken die Entwicklung der Digitalisierung. Berichte über Cyber-Angriffe, bei denen millionenfach komplette Kundendatensätze – häufig inklusive Daten der Zahlungsmittel – gestohlen wurden, häufen sich. Dabei sind selbst grundsätzlich gut geschützte und bekannte Unternehmen schon Opfer von Hackerangriffen geworden. Die Systeme sind also anfällig und der Trend zum verstärkten Einsatz von Open Source-Software kann diese Anfälligkeit in den kommenden Jahren weiter erhöhen. Diese Entwicklung verstärkt zugleich den Bedarf an neuen Cyber-Versicherungen. Gelingt es den Versicherern hier, attraktive Produkte zu entwickeln, könnte dies für die Branche enormes Wachstumspotenzial bedeuten.

Mit dieser Studie soll ein Überblick über dieses neue Feld mitsamt konkreten Handlungsempfehlungen vermittelt werden. Zusätzlich wurde, wie schon in den Vorgängerstudien der Thinking Ahead-Serie, ein Prognosemodell entwickelt, um die weitere Entwicklung der Cyber-Versicherungsprämie in Deutschland, Österreich und der Schweiz in den verschiedenen Marktsegmenten simulieren zu können. Demnach könnte in diesen Ländern in den nächsten 20 Jahren eine Sparte heranwachsen, die von ca. 100 Millionen Euro jährlichem Prämienaufkommen in Deutschland Ende 2016 auf eine Größenordnung ähnlich der Kfz-Versicherung heute steigen könnte, also auf etwa 15 bis 20 Milliarden Euro.

Warum also zögern Versicherer mit dem Angebot von Cyber-Deckungen in Deutschland, insbesondere für das am Ende volumenstärkste Segment des kleinen und mittleren Gewerbes sowie bei Privatkunden? Mit dieser Frage haben wir uns gemeinsam mit Marktexperten und in Gesprächen mit Underwritern und Managern der Versicherer eingehend befasst. Wir wollten wissen, wie Cyber-Versicherung funktionieren kann, wie das Risiko in den Griff zu bekommen ist, wie die Tarifierung aussehen kann – und wie die Leistungsabteilungen auf Schäden vorbereitet werden können, die es in dieser Form noch nie gegeben hat.

Dies ist Teil B unserer Studie zur umfangreichen Analyse der Themengebiete Digitalisierung und Cyber. Teil A widmet sich der Digitalisierung einschließlich FinTechs und InsurTechs. Wie bereits bei den vorherigen Ausgaben der KPMG-Reihe Insurance Thinking Ahead ist auch diese Studie eine Gemeinschaftsleistung von KPMG-Spezialisten und Marktexperten, die uns in den vergangenen 15 Monaten in zahlreichen Gesprächen und Workshops begleitet haben. Für die spannenden Diskussionen und den wertvollen Input aller Teilnehmer möchten wir uns an dieser Stelle ganz herzlich bedanken.

Wir wünschen Ihnen eine anregende und aufschlussreiche Lektüre.

Jörg Wälder, Markus Heyen, Christian Sagawe, Hendrik C. Jahn
KPMG in Deutschland

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Inhalt

1. Vorwort **3**

2. Zielsetzung und Begriffsdefinition **7**

3. Cyber-Risiken und Cyber-Versicherung **13**

3.1 Cyber-Risiken, die Kehrseite der Digitalisierungsmedaille 13

3.2 Cyber als neues Risiko und Produkt für die Assekuranz 15

3.3 Cyber End-to-End 22

3.4 Marktpotenzial der Cyber-Versicherung 29

3.5 Kundensegmente in der Cyber-Versicherung und Cyber-Versicherung als standardisiertes Massenprodukt 40

3.6 Kritische Skills zum Handling von Cyber-Risiken und Cyber-Versicherung 43

3.7 Fachliche und organisatorische Abbildung der Cyber-Versicherungssparte 57

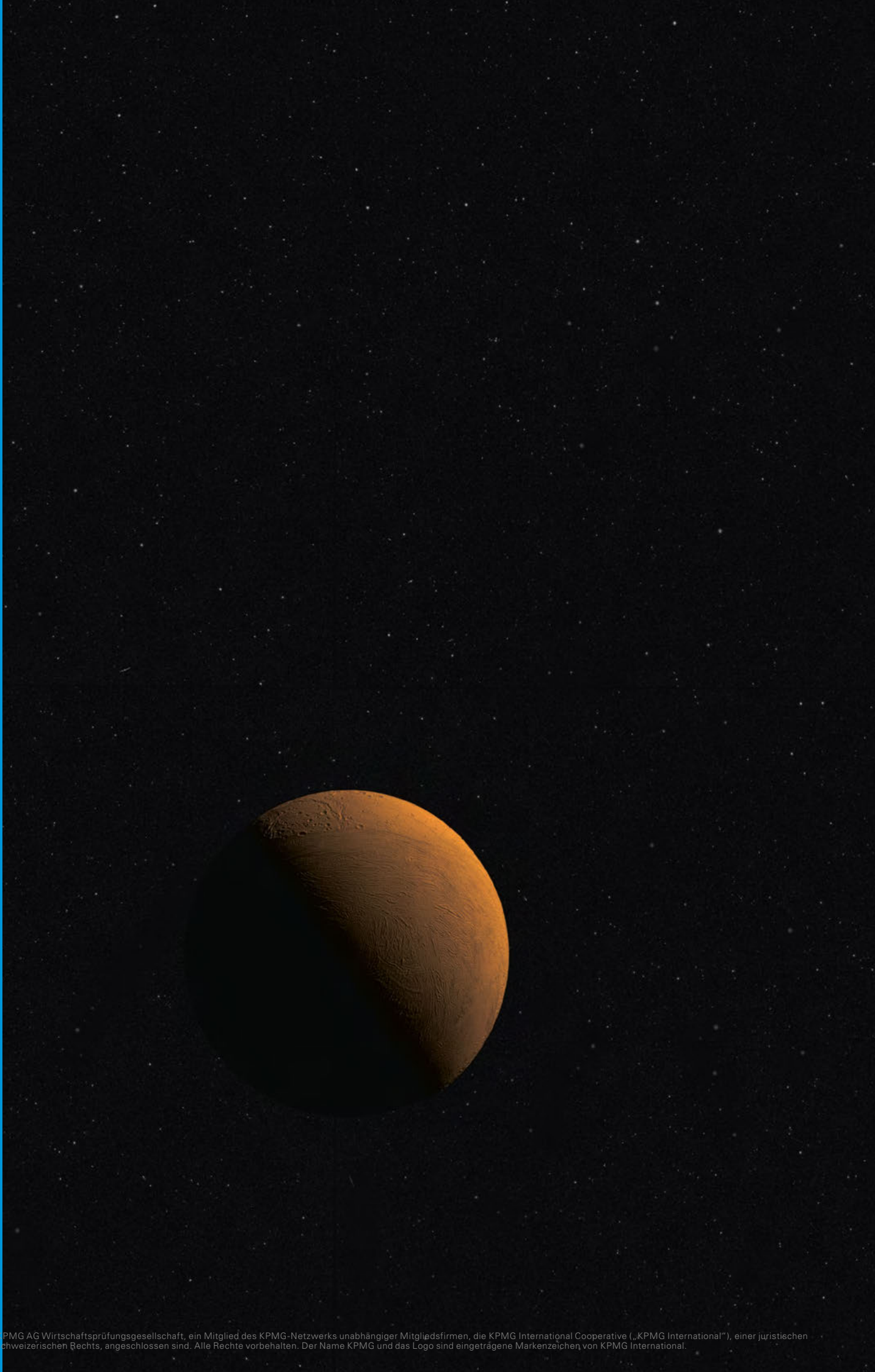
4. Schlusswort **61**

Ihre Ansprechpartner **64**

Methodik **65**

Quellen **66**

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.



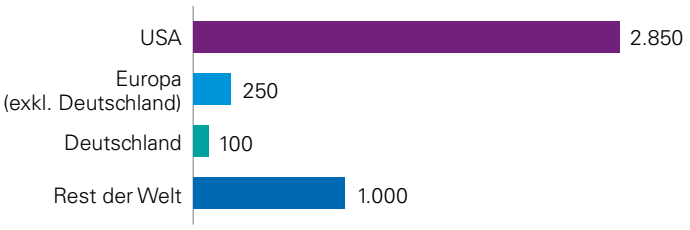
© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

2. Zielsetzung und Begriffsdefinition

Marktsituation

Das Bewusstsein für die Risiken, die mit der zunehmenden Digitalisierung entstehen, wächst. Dabei wird immer deutlicher, dass diesem Risiko für die Versicherer eine Chance gegenübersteht: eine neue Produktlinie für Versicherer – Cyber-Versicherungen. Während man sich im deutschen Markt scheinbar noch schwer damit tut, den richtigen Ansatz für dieses neue Geschäftsfeld zu finden, teilweise die damit verbundenen Risiken auch höher eingeschätzt werden als mögliche Chancen, schreiten andere Märkte, allen voran die USA, zügig voran. Dies lässt sich an den Marktprämienzahlen deutlich ablesen. Wir schätzen die aktuellen Cyber-Risiko-Portfolios (Jahresprämie) bis Ende 2016 wie folgt ein:

Abbildung 1:
Prämienvolumen Cyber-Versicherung 2016
erwarteter Jahresendbestand
in Millionen US-Dollar



Quelle: KPMG, Deutschland, 2017

Von einem globalen Gesamtmarktvolumen von ca. 4,1 Milliarden US-Dollar Ende 2016 entfallen 69 Prozent auf die USA, rund 24 Prozent auf Asien und andere außereuropäische Märkte sowie sechs Prozent auf Europa, exklusive Deutschland. Deutschland selbst steht aktuell nur für zwei Prozent der weltweiten Cyber-Prämie. Teilweise lässt sich das damit erklären, dass Cyber-Policen in den USA seit sieben bis acht Jahren aktiv im Markt angeboten werden, wohingegen dies in Deutschland erst seit vier Jahren der Fall ist. Zudem ist es charakteristisch für den deutschen Markt, dass man sich zunächst eingehend mit der Risikobeurteilung, der Produktgestaltung und der Preisfindung in neuen Versicherungssparten auseinandersetzt, bevor man sich neuartige Risiken in die Bücher nimmt. Das Vorgehen bei den D&O-Versicherungen ist ein Beispiel hierfür.

Zielsetzung der Studie Teil B — Cyber

Die Ausgangsbasis war eine Reihe von Fragen, denen wir im Rahmen der Studienarbeit nachgegangen sind:

- Welche strategische Relevanz und welches Potenzial hat Cyber-Versicherung für das Kompositgeschäft der Versicherer im deutschsprachigen Raum?
- Welche Produktgestaltung ist mit Blick auf die unterschiedlichen Kundensegmente und Versicherungsumfänge am sinnvollsten?
- Wie sehen die Risiken konkret aus und wie können sich die Versicherer die für ein professionelles Cyber-Versicherungsgeschäft unabdingbaren Fähigkeiten aneignen?
- Wie sollte die Tarifierung in einem Geschäft ohne Vergangenheitswerte gestaltet werden und wie reguliert man Schäden in einem Geschäft, zu dem es praktisch keine Schadenerfahrung gibt?

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

– Wie bildet man die Cyber-Sparte in seiner Organisation ab?
– Bleibt es bei einem relativ überschaubaren Prämienvolumen von einigen hundert Millionen Euro Jahresprämie in Deutschland oder entwickelt sich dieses Feld tatsächlich zu einer ernst zu nehmenden Sparte?
– Und schließlich ganz grundsätzlich: Lohnt sich der Aufwand, der mit dem Einstieg in das Cyber-Geschäft verbunden ist, angesichts der schwer greifbaren Risiken überhaupt?

Mit diesen Fragen haben wir uns im Rahmen der Studie gründlich auseinandergesetzt und liefern spätestens mit dem Prognosemodell in Kapitel 3.4 nicht nur qualitative, sondern auch quantitative Antworten.

Begriffsdefinition

Zu dem Begriff „Cyber" existieren diverse Beschreibungen – eine überzeugende Definition für Cyber im Kontext von Versicherung, so wie wir sie für Digitalisierung in Teil A dieser Studie gefunden haben, existiert in dieser Form nicht. Daher wurde mit einem in Deutschland auf „Cyber-Insurance" spezialisierten Versicherungsmakler, Dr. Sven Erichsen[1], sowie unseren Fachleuten für Cyber Forensic und Cyber Security eine erste allgemeingültige Definition entwickelt:

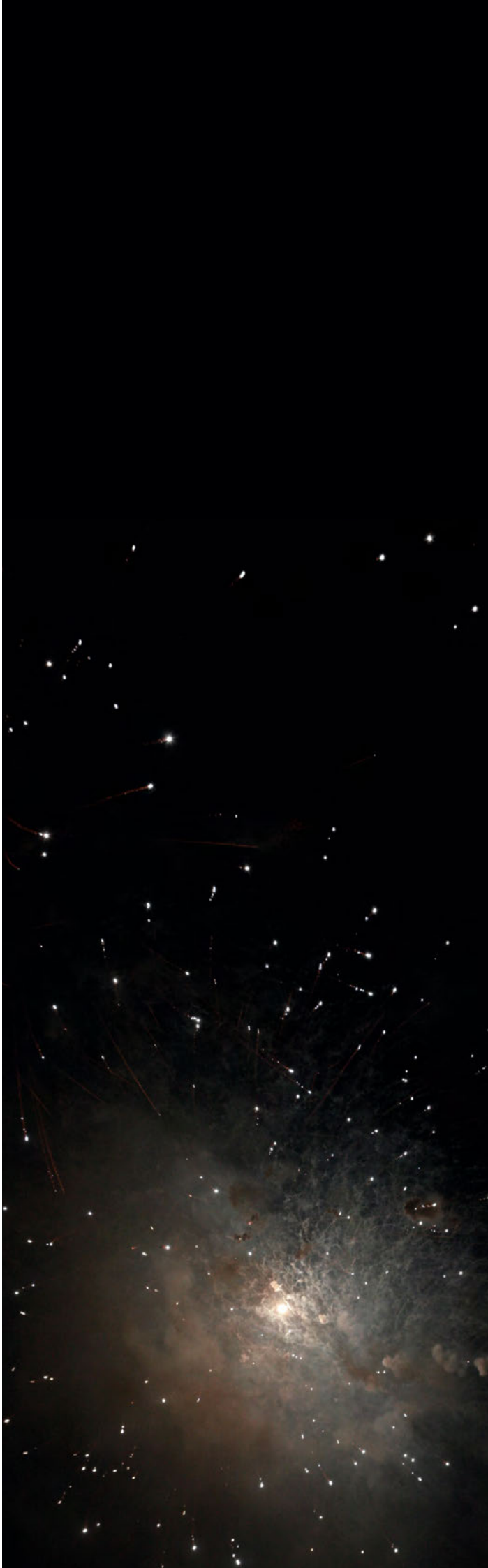
„Cyber-Versicherung beschäftigt sich mit den Folgen der unbefugten Nutzung von IT-Systemen oder eines Datenschutzvorfalles, beispielsweise bei

– rechtswidriger Aneignung und dem Missbrauch von Daten,
– dem Eindringen in technische Systeme zur Verarbeitung oder Übertragung von Informationen und deren schadenstiftenden Beeinflussung,
– den Folgen der Aneignung fremder Identitäten,
– Fällen von Mobbing und Reputationsschädigung von natürlichen und juristischen Personen in der digitalen Welt,
– Bedienungsfehlern."

Das Betätigungsfeld von Cyber-Versicherungen gliedert sich in drei Kernbereiche: Risikobewertung und -prävention, Schadenbearbeitung sowie finanzieller Ersatz für anfallende Kosten und Entschädigungen.

1 Dr. Sven Erichsen ist Geschäftsführer der 2013 von ihm gegründeten Erichsen GmbH. Zuvor war Dr. Erichsen Mitglied der Geschäftsführung von AON Deutschland.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.



© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Zahlen, Daten, Fakten

CYBER-CRIME

Kosten der Top-Ten-Wirtschaftsmächte für Cyber-Schäden in Mrd. US-Dollar

Allianz | 2015

1,6%

Anteil jährliche Schadensumme durch Cyber-Crime am BIP Deutschland – entspricht pro deutschem Staatsbürger für 2015

621 Euro

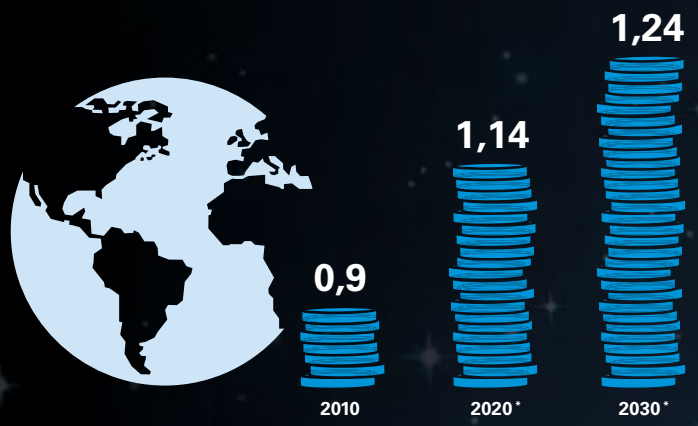
KPMG, Deutschland | 2015

>1,6 Mio.

Opfer von Cyber-Attacken täglich, weltweit

Norton | 2015

Anteil der Kosten durch Cyber-Crime am weltweiten BIP in Prozent



Zurich Insurance Company | 2015

* Schätzwerte

∅ 6,1 Mio. Euro

jährliche durch Cyber-Crime verursachte Kosten pro betroffenem Großunternehmen

KPMG, Deutschland | 2013

445 Mrd. US-Dollar

jährliche Kosten für die globale Wirtschaft infolge von Cyber-Crime

Allianz | 2015

11%

der Befragten Unternehmen verzeichnen Verluste durch Cyber-Schäden von jeweils mehr als 1 Mio. US-Dollar

AXA | 2016

Täterkreis in Prozent

Basis: Alle befragten Unternehmen, die in den letzten zwei Jahren von Datendiebstahl, Wirtschaftsspionage oder Sabotage betroffen waren (n = 550)
Quelle: Bitkom | 2015

20%

Anteil der deutschen Privatpersonen, denen persönliche Informationen im Internet gestohlen wurden

KPMG, Deutschland | 2013

Art von Cyber-Attacke auf Unternehmen in Prozent

KPMG, Deutschland | 2016

594 Mio.

Opfer von Cyber-Attacken jährlich, weltweit

Norton | 2015

69%

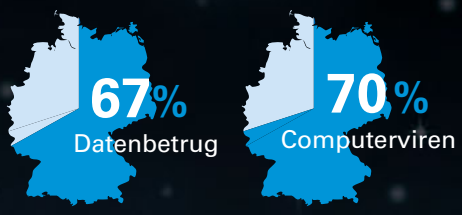
Anteil an betroffenen Industrieunternehmen, die in Deutschland in den vergangen zwei Jahren Opfer waren

Bitkom | 2016

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

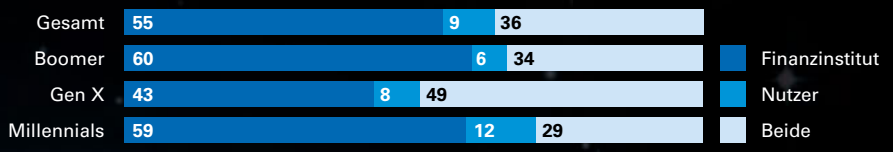
CYBER-RISIKO

Größtes wahrgenommenes Risiko für die Menschen in Deutschland

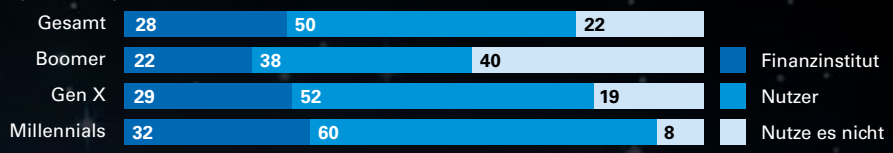


Norton | 2015

Wer ist verantwortlich, wenn durch Mobile Banking persönliche Konten gehackt werden?
(in Prozent)

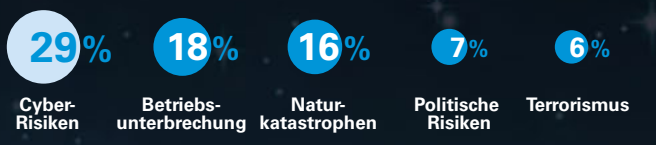


In wessen Verantwortung liegt es, dass mobile Geräte sicher für Online-Banking sind?
(in Prozent)



KPMG, Deutschland | 2015

Top-Risiken, auf die Unternehmen am schlechtesten vorbereitet sind



Die größten Risiken für die Unternehmen in den nächsten fünf Jahren

Allianz | 2015

Von Unternehmen meistgefürchtete Cyber-Risiken
(in Prozent)

Allianz | 2015

89 %
Anteil der Unternehmen, die Cyber-Crime als hohes oder sehr hohes Risiko einstufen

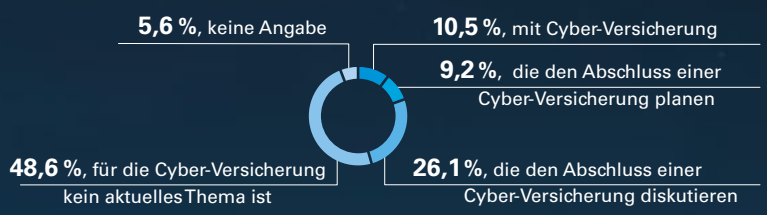
KPMG, Deutschland | 2013

Welche Folgen hatte eine Cyber-Attacke für Ihr Unternehmen?
(in Prozent)

KPMG, Deutschland | 2016

CYBER-VERSICHERUNG

Anteil Industrieunternehmen
(in Prozent)

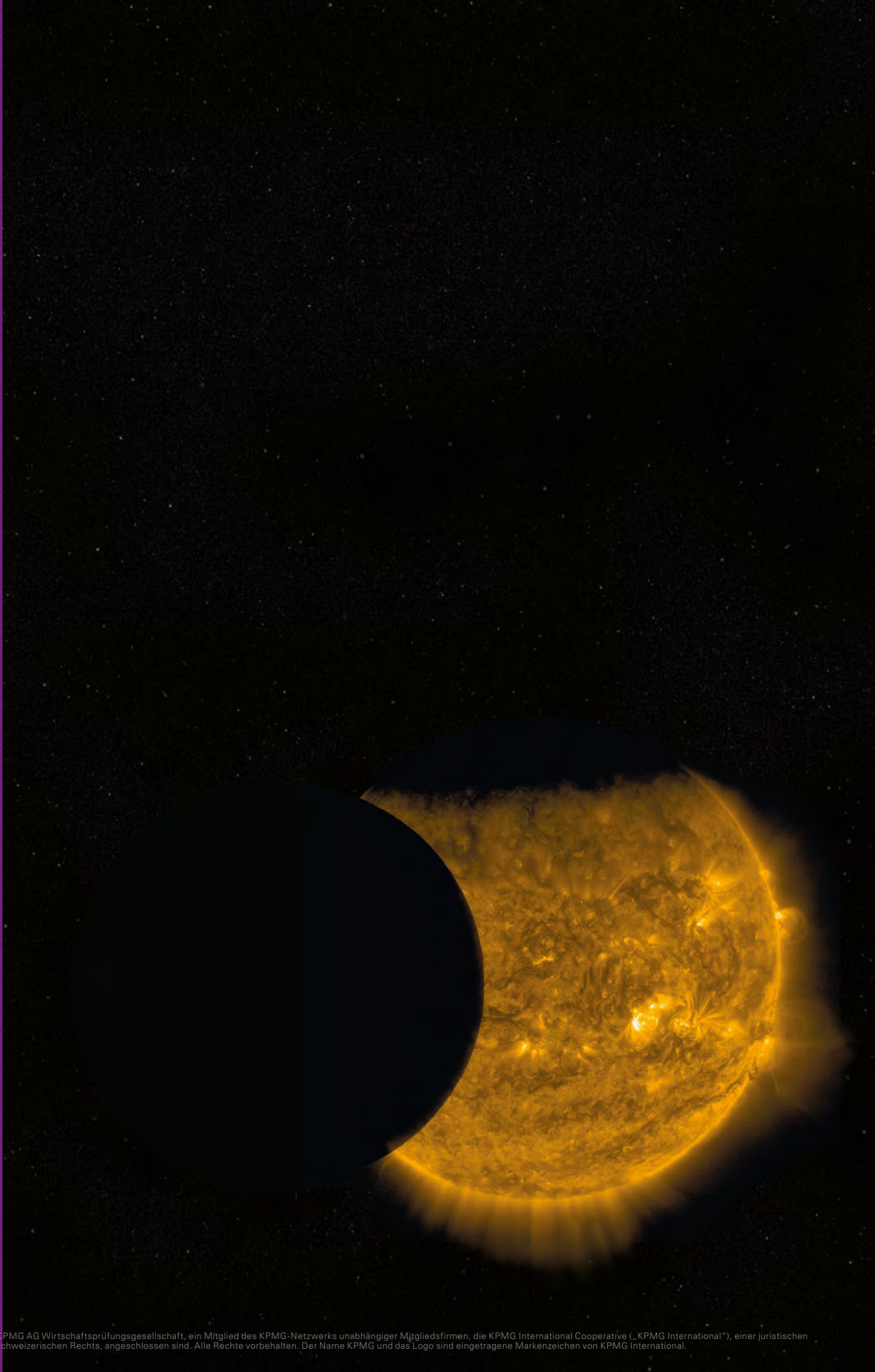


Bitkom | 2016

655 Mrd. US-Dollar
werden weltweit zwischen 2015 und 2020 voraussichtlich für Cyber-Security ausgegeben, um Geräte zu schützen

Norton | 2015

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.



© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

3. Cyber-Risiken und Cyber-Versicherung

3.1 Cyber-Risiken, die Kehrseite der Digitalisierungsmedaille

Cyber-Crime gehört auf die Agenda

Es lässt sich die allgemeine Entwicklung feststellen, dass viele der privaten und die meisten der geschäftlichen Prozesse in Zukunft digital abgewickelt werden. In dem Maße, in dem Geschäftsmodelle und ihre Prozesse mitsamt Daten in die digitale Welt verlagert werden, steigt die Gefahr von Cyber-Angriffen auf Systeme und digital gespeicherte Informationen. Das Bundeskriminalamt (BKA) erläutert hierzu, dass „Cybercrime-as-a-Service" immer mehr an Bedeutung gewinnt. Die digitale Untergrund-Economy stellt eine beachtliche Bandbreite an Dienstleistungen zur Verfügung, die jede Art von Cyber-Crime unterstützen. Dazu gehören unter anderem Distributed Denial of Service-Attacken (DDoS), Bereitstellung von Bot-Netzen oder der Einsatz von Malware. Mehr zu den einzelnen und typischen Angriffsarten in Kapitel 3.3.

Schwer kalkulierbare Kosten

Für die meisten Industrien ist die enge Verbindung zwischen Digitalisierung und Cyber-Risiken eine schlechte Nachricht, denn sie werden Vorsorge treffen müssen – und das kostet: Cyber-Spezialisten müssen hinzugezogen werden, organisatorische und systemseitige Maßnahmen stehen an und nicht zuletzt wird die Absicherung der Risiken durch entsprechenden Risikotransfer, also den Einkauf von Cyber-Versicherungsschutz, weitere Kosten verursachen, die heute noch schwer einschätzbar sind. Nicht dass die Assekuranz von diesen Zusatzaufwänden nicht in gleicher Form betroffen wäre, allerdings hat diese Situation für Versicherer nicht nur eine Schatten-, sondern auch eine Sonnenseite: Der neu entstehende Bedarf an Versicherungsschutz für Cyber-Risiken verspricht ein beachtliches Geschäft zu werden – vielleicht sogar die am schnellsten wachsende Sparte, die die Assekuranz je gesehen hat. Und dies in einem Marktumfeld, in dem im klassischen Versicherungsgeschäft kaum noch organisches Wachstum zu realisieren ist.

Umfassende Digitalisierung

Die rasante Entwicklung des Internet of Things mit voraussichtlich 50 Milliarden onlinefähigen Geräten bis 2020 führt zu einer rasant fortschreitenden Vernetzung aller privaten und geschäftlichen Bereiche. Ob es sich um Gebäude oder Fertigungsanlagen, um Fahrzeuge zu Land, Wasser und Luft oder um Computer, Handys bzw. jede andere Form von Datenverarbeitungs- und Kommunikationstechnologie handelt: Kein Bereich wird sich der digitalen Vernetzung entziehen können. Damit entsteht eine enorme, bisher ungekannte Komplexität.

Neben der für sich genommen bereits anspruchsvollen Herausforderung aufgrund der durch die zunehmende Vernetzung steigenden Komplexität, nimmt auch die Dynamik der technischen Entwicklung weiter zu. Als Katalysatoren wirken die Cloud-Technologie, immer leistungsfähigere Prozessoren und künstliche Intelligenz. Zwei Beispiele sollen die Dynamik bei den Datenvolumina illustrieren: 1998 wurden die ersten Google-Suchaufträge ausgeführt. Diese Zahl stieg auf über 7,7 Milliarden tägliche Suchaufträge in 2015. Etwa 4,75 Milliarden Inhalte werden heute täglich auf Facebook geteilt – so wird nachvollziehbar, dass 90 Prozent der weltweit gespeicherten Daten erst in den vergangenen 24 Monaten entstanden sind (vgl. statista, 2017).

Mehr Vernetzung, mehr Cyber-Risiko

Der Anstieg der allgemeinen Bedrohungslage durch Cyber-Risiken ist eng mit der wachsenden Vernetzung verknüpft. Das hat

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

„In Anlehnung an Karl Valentin – ‚Cyber ist schön, macht aber viel Arbeit'. Will meinen, dass Cyber der Assekuranz beachtliche Wachstumschancen bietet, eine Unterschätzung der fachlichen und risikotechnischen Komplexität aber fatale Folgen haben kann."

Sven Erichsen,
Gründer und Geschäftsführer der
Erichsen GmbH

etwa der Fall des US-Retailers Target Ende 2013 eindrucksvoll deutlich gemacht: Hackern war es gelungen, über die Steuerung der Klima- und Heizungsanlagen im Filialsystem der Gruppe in den Hauptrechner vorzudringen und dort 40 Millionen vollständige Kreditkarten-Datensätze von Target-Kunden zu stehlen. Dies war ein Datenschutzvorfall, bei dem das Unternehmen verpflichtet war, alle betroffenen Kunden qualifiziert zu unterrichten. Geht man zum Beispiel von bis zu 50 Euro Kosten pro betroffenem Kunden aus, kann alleine eine solche Benachrichtigung von Kunden in einem Datenschutzvorfall ein Unternehmen wie Target zwei Milliarden Euro kosten.

Die Schadenbilder sind sowohl für die Betroffenen als auch für die Versicherer neu. Entsprechend anspruchsvoll ist es für jeden Einzelnen, aber auch für Unternehmen und damit auch für Versicherer, den Überblick zu behalten und die Wirkungszusammenhänge zu verstehen. Dieses Verständnis ist eine wichtige Voraussetzung zur Beurteilung von Cyber-Risiken.

Denken wir beispielsweise daran, dass es möglich ist, während der Fahrt eines Pkw in dessen Systeme einzudringen und Fahrzeugsteuerungsfunktionen zu manipulieren. Die multimediale Unterhaltungs- und Kommunikationstechnik der Fahrzeuge entwickelt sich rasant weiter und verschmilzt zunehmend mit der Steuerungstechnik. Gleichzeitig soll es den Nutzern der Fahrzeuge ermöglicht werden, die eigenen Smartphones mit ihren individuellen Einstellungen in der On-Bord-Technologie zu spiegeln, was nur über die Öffnung von Schnittstellen möglich ist. Der bunte Mix von Hard- und Softwareherstellern, in Verbindung mit diversen zusätzlich erforderlichen Schnittstellen, macht Fahrzeuge angreifbarer. Man wird mit Sicherheit noch deutlich gefährlichere Eingriffe von außen in die Fahrzeugsteuerung sehen als den auf einem US-Highway abgebremsten Jeep, wie in den USA im Frühjahr 2016 – bis hin zu Massenereignissen, die Kumulrelevanz haben können.

Kritische Systeme haben hohes Angriffspotenzial

Aber auch bei anderen kritischen Systemen gab es erst kürzlich erfolgreiche Angriffe, wie etwa im Falle des Krankenhauses im nordrhein-westfälischen Neuss oder beim Deutschen Bundestag. Die betroffenen Systeme waren über einen längeren Zeitraum nicht funktionsfähig – beim Bundestag ging man sogar zunächst davon aus, die betroffene Hardware austauschen zu müssen. Obwohl die Unbrauchbarkeit von Systemen ärgerlich ist, ist dies noch nicht das schlimmste Szenario. Denn was passiert, wenn in einer wichtigen Verwaltungseinheit wie dem Bundestag oder gar in einem hochtechnisierten OP-Saal ein System nicht nur unbrauchbar gemacht, sondern manipulativ eingesetzt wird? Das Gesundheitswesen bietet hier erhebliche Angriffsfläche: Weil die Ausstattung in den Krankenhäusern immer IT-lastiger wird, aber auch weil immer mehr Patienten medizinische Online-Geräte bei sich tragen. Deren Zahl lag 2014 weltweit noch bei rund drei Millionen; bis 2018 wird sie aber voraussichtlich auf 19 Millionen Geräte steigen.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Regelmäßige Angriffe auf Großindustrie

In der Großindustrie gehören Cyber-Angriffe schon fast zum Alltag. So hat Volkswagen jüngst bekannt gegeben, dass das Unternehmen wöchentlich bis zu 6.000 Angriffe auf seine Systeme registriert. Bis vor Kurzem hatte Volkswagen noch von 6.000 Cyber-Angriffen pro Jahr gesprochen (vgl. Verlag Versicherungswirtschaft GmbH, 2015). Neben der absoluten Zahl der Angriffe steigt auch die durchschnittliche Schadenhöhe: Bezifferte sich der Schaden bei einem Datenschutzvorfall in der deutschen Großindustrie 2011 noch auf 3,4 Millionen Euro, sind die Kosten bis 2015 bereits um 79 Prozent auf 6,1 Millionen Euro pro Vorfall angestiegen (vgl. Jung, Marcus, 2013).

Deutschland im Fadenkreuz von Cyber-Attacken

Deutschland ist dabei das zentrale Angriffsziel: Nirgendwo sonst wird im Verhältnis zu den Größenkennziffern mehr Schaden durch Cyber-Crime angerichtet. Hierzulande geht man von einem jährlichen gesamtvolkswirtschaftlichen Schaden von rund 51 Milliarden Euro aus – was 1,6 Prozent des Bruttoinlandsprodukts entspricht (vgl. Bitkom, 2015). Deshalb wird wie bei Pandemien in der Medizin eine allgemeine Meldepflicht für Cyber-Attacken diskutiert. Für einige Betreiber kritischer Infrastrukturen in den Bereichen Energie, IT, Kommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen besteht eine solche Meldepflicht auf Basis des im Juli 2015 in Kraft getretenen IT-Sicherheitsgesetzes bereits. Allerdings beschränken sich die Vorgaben überwiegend auf erhöhte allgemeine Sicherheitsanforderungen. Lediglich für Betreiber von Kernkraftwerken und Telekommunikationsunternehmen wurde eine qualifizierte Meldepflicht festgeschrieben.

Fehlende Datengrundlage und Kompetenzen

Um die Cyber-Chancen in vollem Umfang zu nutzen, muss die Versicherungswirtschaft zunächst eine Reihe von Hürden überwinden: Das Umfeld ist ausgesprochen komplex und hochdynamisch, zudem liegen kaum Schadendaten als Kalkulationsgrundlage für Aktuare vor. Anders als auf dem US-Markt haben die europäischen, insbesondere aber die deutschen Versicherer auch noch keine Produkterfahrung im Cyber-Geschäft. Zusätzlich fehlen in Deutschland einige wichtige Kompetenzen zur Beurteilung von Cyber-Risiken sowie zur Schadenbearbeitung.

Um das bestehende Cyber-Risiko greifbar zu machen, sollten Versicherer sich Skills aneignen oder geeignete Partner finden, die besondere Expertise in den folgenden Feldern aufweisen:

- Risiko-Assessment und -Prävention,
- Cyber-Produktentwicklung und -Tarifierung,
- Vertrieb und Verwaltung neuer Cyber-Produkte,
- Cyber-Schadenmanagement und -regulierung.

„Die zunehmende Vernetzung und Digitalisierung von Fahrzeugen und die Schaffung innovativer mobiler Services sind ein dominierender Trend/ Treiber in der Kfz-Industrie. Über die steigende Anzahl an Zugangs-Endpunkten in das Fahrzeugökosystem auf Kundenseite steigt gleichzeitig die potenzielle Angriffsfläche für Cyber-Angriffe und damit auch das Erfordernis nach professionellen Risikopräventionsmaßnahmen."

Michael Kainzbauer,
CEO Toyota Insurance Management Ltd.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Statement Bundesamt für Verfassungsschutz (Dr. Hans-Georg Maaßen, Präsident)

Mit der fortgeschrittenen Digitalisierung, Industrie 4.0 und dem „Internet of Things" sollen nahezu alle Elemente der Wertschöpfungskette miteinander vernetzt werden. Daraus erwächst eine Vielzahl von Daten, die künftig in allen Wirtschaftszweigen relevant werden. Sie sind das „digitale Gold" der Zukunft. Mit den Chancen wachsen aber auch die Risiken, weil die voranschreitende Digitalisierung die Angriffsflächen vergrößert und neue Angriffsvektoren entstehen. Staat und Gesellschaft, insbesondere auch Unternehmen, müssen sich auf neue Bedrohungen vorbereiten. Mehr als die Hälfte der deutschen Wirtschaft gab an, bereits Opfer von Cyberspionage, Datendiebstahl oder Cybersabotage geworden zu sein. Insbesondere der Schutz von hochsensiblen, persönlichen Daten muss sichergestellt werden, da auch staatliche Cyberakteure ein hohes Maß an Interesse für diese Informationen aufweisen.

Für die Zukunft ist eine ganzheitliche Gefahrenvorsorge gefragt, um sich vor ungewolltem Know-how- und Datenabfluss effektiv zu schützen. Zugleich gilt es, für den Schadensfall ein kompetentes Schadensmanagement vorzuhalten.

Das Bundesamt für Verfassungsschutz (BfV) wie auch die Landesverfassungsschutzbehörden sehen sich im Wirtschaftsschutz als Dienstleister der Unternehmen in Deutschland. Sie stehen für eine vertrauensvolle Zusammenarbeit sowohl in der Prävention als auch bei der Bewältigung konkreter Gefährdungssituationen zur Verfügung.

Das BfV hat das Referat Wirtschaftsschutz (Tel.: 0221 792-3322 oder E-mail: Wirtschaftsschutz@bfv.bund.de) als Single Point of Contact für die Wirtschaft für alle Sicherheitsfragen eingerichtet, gleich ob Spionage, Cyberattacke, Sabotage oder Verdacht auf Terrorismus/Extremismus.

Hinzu kommt, dass die Versicherungsbranche zwar mehr und mehr das Potenzial des Marktes sieht, aber unsicher ist, worauf man sich genau einlässt und wie die Herausforderungen bewältigt werden können.

Im Folgenden werden wir uns mit diesem Themenkomplex befassen und dabei folgende Schwerpunkte setzen:

- Betrachtung der heutigen und zukünftigen Risikosituation,
- Überlegungen zu möglichen Prämienvolumina im Markt für Cyber-Versicherung in der DACH-Region im Zeitraum von 2016 bis 2036,
- Erforderliche Skills bei Risiko-Assessment, Produktentwicklung, Underwriting, Schadenmanagement und Sourcing („make or buy"),
- Überlegungen zu der organisatorischen Abbildung des Cyber-Geschäfts als eigenständige Versicherungssparte.

Dass wir es bei den Cyber-Risiken nicht mit einem vorübergehenden Phänomen, sondern einer ernst zu nehmenden, nachhaltigen Bedrohung zu tun haben, zu deren Abwehr Strategien zu entwickeln sind, bestätigt auch die Einschätzung des Bundesamts für Verfassungsschutz, die uns freundlicherweise für diese Studie zur Verfügung gestellt wurde (siehe oben).

Wir haben im Markt und intern bei KPMG eine Vielzahl von Expertengesprächen geführt, die erheblich zur Klärung der Situation beigetragen haben. Weiterhin hat Dr. Sven Erichsen, basierend auf seiner Markterfahrung, mit uns die in der Praxis relevanten Felder diskutiert, an diversen KPMG-Marktgesprächen mit Versicherern teilgenommen und im Folgenden wertvolle Unterstützung zur Erörterung der in diesem Teil B adressierten Themenstellungen geleistet.

3.2 Cyber als neues Risiko und Produkt für die Assekuranz

Neue Risikosituation und Schadenfälle

Aus Sicht von Risiko-Managern ist das Cyber-Risiko eines unter vielen. Allerdings rückt es nicht zuletzt wegen den erheblichen Steigerungsraten bei Cyber-Crime immer stärker in den Fokus – ohne dass Risiko-Manager große Erfahrung damit hätten. Umso schwerer ist es für viele, insbesondere mittelständische Unternehmen und deren Risiko-Manager, Cyber-Risiken zu bewerten und Lösungen für die Vermeidung bzw. den Risikotransfer zu finden. Gleichwohl ist der Handlungsbedarf groß, denn nicht selten können schwerwiegende Cyber-Vorfälle Unternehmen in eine krisenhafte Situation bringen. Es braucht eine schnelle Reaktion und professionelles Handeln, um substanzielle finanzielle Folgen zu vermeiden. Insbesondere bei Datenschutzvorfällen sind Fingerspitzengefühl und Offenheit im Umgang mit den Betroffenen notwendig.

Zwei wesentliche Risikoarten

Datendiebstahl ist lukrativ, genau wie Cyber-Erpressung. So werden für einen unbenutzten Datensatz bis zu 100 Euro gezahlt. Cyber-Delikte sind für Kriminelle einfacher und vor allem sicherer, denn die Täter müssen sich selbst nicht mehr physisch zum Tatort begeben. Diese Entwicklung geht mit einer höheren Professionalisierung der Täter einher, zudem sind erhebliche Steigerungsraten bei organisierter Cyber-Crime zu beobachten. Ein weiteres Phänomen ist, dass Cyber-Täter immer häufiger international agieren. Im Netz sind neue Formen von organisierter Kriminalität entstanden, denn auch Kriminelle verlagern einen Teil ihrer „Wertschöpfungskette" ins Netz.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Die daraus entstehenden Schadenfälle lassen sich bis zu einem bestimmten Grad vermeiden, wenn die operativen, finanziellen und reputationsrelevanten Aspekte von Cyber-Risiken fachgerecht adressiert werden. Vor allem mittelständische Unternehmen tun sich bislang schwer, Sicherheitsrisiken ihrer Informations- und Technologielandschaft zu bewerten und geeignete Maßnahmen abzuleiten. Zwei wesentliche, sich teilweise überlappende Ausprägungen von Cyber-Risiken sind zu beobachten:

- IT-gesteuerte Prozesse können gestört oder zum Stillstand gebracht werden.
- Die in rasant zunehmendem Maße erhobenen und gespeicherten Daten können gestohlen und rechtswidrig eingesetzt werden.

Bewertung von Risiken

Bisher liegen nur wenige Analysen zur Bewertung von Cyber-Schäden vor. Zudem enthalten diese kaum konkrete Angaben zu den finanziellen Auswirkungen von Cyber-Attacken. Die monetären Folgen werden entweder überschlägig geschätzt – wie die Anzahl der Cyber-Angriffe im BSI-Lagebericht – oder aus Umfragen ermittelt. Eine jüngere Bitkom-Studie schätzt den volkswirtschaftlichen Schaden auf 51 Milliarden Euro pro Jahr. (vgl. Bitkom, 2015)

Kosten und Wertverluste durch Cyber-Vorfälle

Der Mangel an konkreten Informationen verhindert in vielen Unternehmen eine sichere Entscheidungsgrundlage für das Management. Bei Diskussionen zur Bewertung von Cyber-Risiken kommt es daher in erster Linie auf ein gemeinsames Verständnis der Kosten-Parameter des jeweiligen Risikos an. Folgende Kategorien könnten als Orientierungsgrößen für die Zuordnung von Kosten bzw. Wertverlusten dienen:

- Kosten für die Rekonstruktion und Wiederherstellung der Daten,
- Ergebniseinbußen (Betriebsunterbrechung, Umsatzverluste, Mehrkosten),
- Beratungskosten (Forensik, Rechtsberatung, Krisenkommunikation),
- Zahlung von Erpressungsgeldern, Belohnungen,
- Zahlung von Vertragsstrafen/Bußgeldern,
- Zahlungsmittelverluste durch rechtswidrigen Eingriff in Bank- und Kreditkartenkonten,
- Folgen aus Betrugsfällen (Fehlüberweisungen etc.),
- Reputationsschäden und deren wirtschaftliche Folgen.

Die folgenden konkreten, aus Datenschutzgründen leicht abgewandelten Beispiele zeigen die möglichen finanziellen Auswirkungen von Cyber-Angriffen:

- Ein unzufriedener Mitarbeiter hat Hackern den Zugang zur Datenspeicherung eines Online-Handelsunternehmens verschafft. Die Täter nutzten dazu eine Schadsoftware, die zwar schon nach vier Tagen von den hinzugezogenen

„Wir sind Zeugen und Teilnehmer einer digitalen Revolution, deren Folgen noch nicht abzusehen sind. Doch eine ‚smarte' Welt birgt auch Risiken in Spionage, Sabotage und Terrorismus. Das Bundesamt für Verfassungsschutz begegnet diesen Risiken durch Prävention, Sensibilisierung und Hilfe im Schadenfall."

Dr. Hans-Georg Maaßen,
Präsident des Bundesamts für Verfassungsschutz

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

IT-Security-Experten aus dem System entfernt werden konnte, aber dennoch erheblichen Schaden verursacht hat: Die Kosten für die Beseitigung der Schadsoftware, zuzüglich der Verluste aus viertägiger Betriebsunterbrechung, beliefen sich auf ca. 400.000 Euro.

– Ein Hotel mittlerer Größe mit 13 Millionen Euro Umsatz ist Opfer von Datendiebstahl geworden. Über mehrere Monate verschafften sich Hacker rechtswidrig Zugang zu dem in üblicher Form gesicherten Online-Portal, kopierten während dieser Zeit rund 100.000 Kundendatensätze und setzten sie zu kriminellen Zwecken ein. Die das Hotel treffenden Kosten aus diesem Datenschutzvorfall summieren sich bis heute auf sechs Millionen Euro für forensische Arbeiten, Rechtsberatung und Rechtsbeistand, für die Erfüllung gesetzlicher Informationspflichten, für Medienarbeit sowie für geltend gemachte Vermögensschäden seitens der Kreditkartenherausgeber, denn die Hacker konnten mit den gestohlenen Kreditkartendaten größere Geldbeträge stehlen.

Risiken kennen und richtig einschätzen

Eine besondere Herausforderung ist in der Geschwindigkeit begründet, in der sich technologische Veränderungen heute vollziehen. Dies gilt auch für Softwarelösungen. Daher ist es nicht verwunderlich, dass neue Software regelmäßig und in zunehmendem Maße Schwachstellen und damit Angriffspunkte für Hacker beinhaltet. Unternehmen sollten nicht nur eine technische, sondern auch kulturelle und organisatorische Sicherheitsarchitektur aufbauen, die hier mithält bzw. im besten Fall dieser Entwicklung voraus ist, ähnlich wie man dies zum Beispiel aus dem Brandschutz kennt. Menschliches Fehlverhalten, wie etwa der leichtfertige Umgang mit infizierten E-Mails oder die Nutzung ungeprüfter USB-Sticks, stellt gegenwärtig das größte Risiko für die IT-Sicherheitsarchitektur von Unternehmen dar.

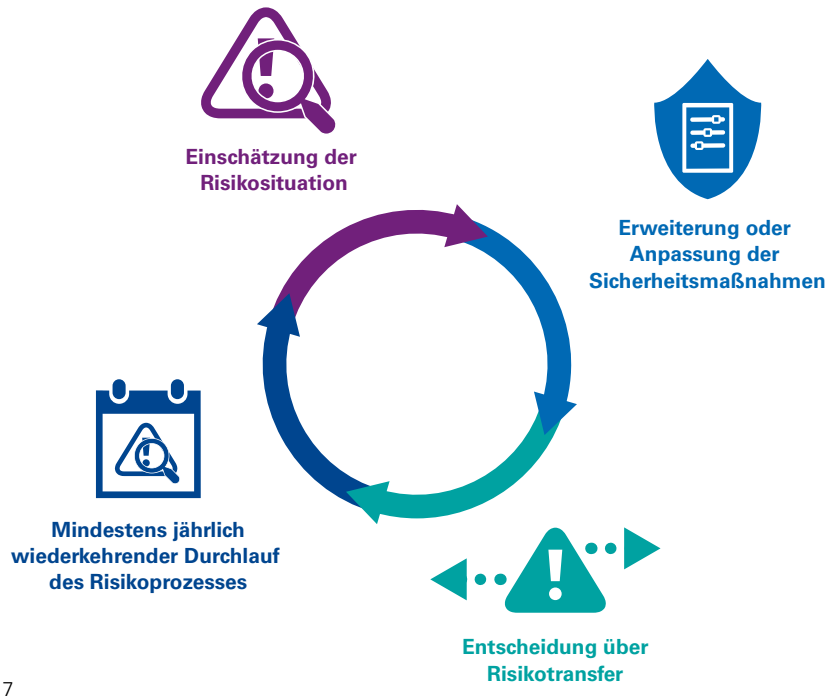
Aus Sicht des Risikomanagements im Unternehmen bedarf es einer kontinuierlichen Neubewertung der Risikolage, einer Anpassung der Sicherheitsmaßnahmen und der Beantwortung der Frage, welche Maßnahmen im Sinne von Risikotransfer (beispielsweise Einkauf von Cyber-Versicherungsdeckungen) durchgeführt werden sollen. Die Schritte lassen sich wie in Abbildung 2 dargestellt ordnen.

Cyber-Versicherer in Deutschland

Trotz aller Sicherheitsmaßnahmen bleiben (analog zum Brandschutz) substanzielle Risiken, die – wie man es auch aus der Feuerversicherung kennt – bilanzgefährdenden Charakter haben können. In jüngster Zeit wurden Cyber-Versicherungslösungen entwickelt, über die diese ergebnisgefährdenden Risiken zu einem guten Teil abgedeckt werden können.

In Deutschland bieten zurzeit vor allem die in Abbildung 3 gezeigten Versicherer Cyber-Versicherungsschutz für gewerbliche und/oder industrielle Risiken an.

Abbildung 2: Handling von Cyber-Risiken aus Sicht des Risikomanagements



Quelle: KPMG, Deutschland, 2017

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Weitere relevante Dienstleister

Häufig greifen Versicherer auf die technische Risikoanalyse spezieller IT-Sicherheitsberatungsunternehmen zurück, die sie und den jeweiligen Kunden sowohl bei der Einschätzung und Verbesserung der Risikosituation als auch im Schadenfall unterstützen können. Auch auf Datenschutzvorfälle spezialisierte Anwälte spielen eine zunehmend wichtige Rolle, ebenso werden regelmäßig Forensiker bei Datenschutzvorfällen hinzugezogen.

Hiscox beispielsweise arbeitet mit HiSolutions zusammen, einem Spezialisten für IT-Governance, Risk und Compliance. Im Schadenfall unterstützt HiSolutions den Spezialversicherer Hiscox zu festgelegten Konditionen. Auch KPMG arbeitet in ähnlicher Weise für mehrere Versicherer. Unsere Cyber-Experten führen zur Risikoeinschätzung auch Audits bzw. Risikodialoge durch, daneben werden Anwaltskanzleien oder Krisenberater hinzugezogen. Einen beispielhaften Ablauf einer Pre-Underwriting-Phase wie auch einer Schadenregulierung stellen wir in Kapitel 3.5 vor.

Abbildung 3: Beispiele für Anbieter von Cyber-Versicherungen
Stand: Dezember 2016

Quelle: KPMG, Deutschland, 2017

„Cyber-Risiken und damit einhergehend auch Cyber-Versicherung gewinnen zunehmend an Bedeutung. Während sich in der Großindustrie das Management schon intensiv mit diesem Thema auseinandersetzt, beobachten wir nun, dass sich auch der Mittelstand in Deutschland sowie kleinere und mittlere Gewerbebetriebe damit befassen und über das Versichern dieser Risiken nachdenken. Ähnlich wie bei der D&O in den 90er- und 2000er-Jahren, glauben wir, dass sich bei Cyber ein gänzlich neuer und bedeutender Versicherungsmarkt entwickeln wird."

Jens Lison,
Mitglied des Vorstands der
Allianz Versicherungs-AG,
Chief Underwriting Officer

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Angebote und Dienstleistungen von Versicherern in Deutschland (Fokus: Firmenkunden)

Die Angebote für private und gewerbliche Risiken unterscheiden sich erheblich. Im Privatbereich gibt es erst wenige umfassende Versicherungsangebote. Da das gewerbliche Cyber-Geschäft schon eine gewisse Marktreife hat, legen wir hier im Folgenden den Schwerpunkt. Für die Zukunft gehen wir aber davon aus, dass sich der Schwerpunkt im Hinblick auf das Volumen in Richtung des Privat- und Kleingewerbegeschäfts verschieben wird.

Angebote für gewerbliche Kunden

Gewerbebetriebe und Unternehmen können neben reinen Kostenschäden auch ihre Ertragskraft, ähnlich der Feuer-Betriebsunterbrechungs-Versicherung, gegen die Folgen aus Cyber-Schäden absichern. Nicht selten wird die Cyber-Versicherung daher auch als Feuerversicherung des 21. Jahrhunderts bezeichnet.

Weiterhin gewährt die Cyber-Versicherung Versicherungsschutz überwiegend für die bei dem Eintritt eines Schadens anfallende Schadenidentifikations- und Ursachenbehebungsleistungen. Wichtig dabei ist primär eine schnelle Erreichbarkeit von Forensik-Experten und Krisenmanagern. Die im Markt anzutreffenden Versicherungsbedingungen variieren in Struktur und Deckungsumfang erheblich, jedoch sind die in Tabelle 1 dargestellten Bausteine typisch.

Cyber-Versicherungen zielen damit auf die bisher bekannten Folgen von Cyber-Schäden ab. Insbesondere für mittelständische Kunden ist die Assistance-Leistung als Unterstützung bei Schadenfällen von großem Wert.

Tabelle 1: Bausteine von Cyber-Versicherungen für gewerbliche Kunden

Cyber-Haftung: Schadenersatzansprüche Dritter	Cyber-Eigenschaden: Kosten und Ausbleiben von Einnahmen
– Sicherheitsverletzungen im Cyber-Bereich, z. B. fehlgeschlagene Abwehr eines Hackerangriffs und Schädigung Dritter – Verletzung von Datenschutz- oder Vertraulichkeitspflichten, z. B. Veröffentlichung vertraulicher Mitglieder- oder Kundendaten – Unerlaubte Medienaktivität, z. B. Verstoß gegen Marken-, Persönlichkeits- oder Wettbewerbsrechte	– Umsatzverluste bei Betriebsunterbrechung durch IT-Systemausfall, z. B. infolge eines Denial of Service, Hackerangriffs oder von Sabotage durch eigene Mitarbeiter – Wiederherstellungs- und Rekonstruktionskosten bei Verlust oder Beschädigung von Daten und bei Verlust von Datenintegrität – Kosten bei Erpressungen (Lösegelder können separat versichert werden)
Zusätzliche Kosten: (Begleit-)Kosten im Schadenfall	
Bei der Bewältigung des Cyber-Schadenfalls fallen meist weitere Kosten an, z. B. für – Information betroffener Dateninhaber – Einschaltung spezialisierter Anwälte – IT-Forensik und sonstige Sachverständige – Krisenmanagement, PR-Berater	

Quelle: Dr. Sven Erichsen, 2017

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Angebote für Privatkunden

Versicherungslösungen für Teilbereiche des Cyber-Risikos einer Privatperson bieten zurzeit unter anderem ARAG, AXA, Cardiff Life, Concordia, Cosmos, DEVK Rechtsschutz, Janitos, Roland, R+V an. Die Versicherungsangebote lassen sich dabei in drei Kategorien einteilen:

Tabelle 2: Bausteine von Cyber-Versicherungen für Privatkunden

Rechtsschutz	Persönliche Risiken aus der Nutzung des Internets	Vermögensschäden
Rechtsschutzversicherer bieten Cyber-Bausteine für Schadenersatz-Rechtsschutz, also Verteidigungskosten gegen Ansprüche Dritter: – Rechtsschutz für im Internet abgeschlossene Verträge – Rechtsschutz gegen Unterlassensansprüche bei Urheberrechtsverstößen (Abmahnungen) – Arbeitsrechtsschutz, falls der Auslöser ein Beitrag im Internet war Diese Produkte werden von den Kunden auch bereits angenommen, insbesondere bei Betreuung durch die Ausschließlichkeitsorganisation (Erläuterungen durch die Agenten in persönlichen Gesprächen).	In diesen Versicherungsbausteinen geht es um die persönliche Integrität des Versicherungsnehmers. Versichert werden hier unter anderem: – Monitoring und Löschung rufschädigender Inhalte – Psychologische Beratung	Es wird Absicherung gegen Vermögensschäden bei Kauf/Verkauf einer Sache im Internet bzw. andere Schäden aus der Nutzung elektronischer Medien angeboten: – Absicherung gegen finanzielle Schäden durch missbräuchliche Verfügungen zulasten von Bankkonten im Rahmen des Online-Bankings oder auch sonstiger Konten (wie z. B. mit dem Miles & More-Guthaben) – Kreditkartenmissbrauch – Einzelne Anbieter übernehmen die Kosten der Datenrettung

Quelle: Dr. Sven Erichsen, 2017

Diese Versicherungsangebote decken den benötigten Versicherungsschutz aber noch nicht ab, weiterhin sind die Produkte uneinheitlich und teilweise schwer zu verstehen. Sie enthalten in der Regel nur einzelne der oben genannten Bausteine oder sind integriert in andere Policen, was im Schadenfall für den Kunden zudem kaum zu durchschauen ist – insbesondere, da die Cyber-Produkte der heutigen Generation noch eine Reihe an Selbstbehalten und Sublimits enthalten. Häufig fehlen auch Eigenschaden-Deckungen, eine adäquate Assistance-Leistung sowie die Verknüpfung mit weiteren Service-Bestandteilen. Regelmäßig fehlt es darüber hinaus an einer technischen Unterstützung im Schadenfall. Die aktuell verfügbaren Angebote für Privatkunden sind insofern noch ein gutes Stück vom tatsächlichen Bedarf entfernt.

Fazit: Cyber-Risiken werden voraussichtlich einen immer größeren Stellenwert im Risiko- und Versicherungsmanagement von Unternehmen, Gewerbebetrieben und Privathaushalten einnehmen und bieten damit ein erhebliches Wachstumspotenzial für Versicherungsgesellschaften.

IT-Sicherheit ist Chefsache

Die Bewertung und Bewältigung dieser Risiken stellt neue Anforderungen, auf die weder die Unternehmen noch die Versicherungsgesellschaften vorbereitet scheinen. Unternehmensleiter sollten sich mit den Aspekten der IT-Sicherheit und des Risikotransfers qualifiziert beschäftigen und Maßnahmen fest-

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

legen, um nicht selbst in eine Haftungssituation zu geraten. IT-Sicherheit ist Chefsache – und die Versicherungsgesellschaften sollten ihren Kunden für dieses wachsende Risiko adäquaten Versicherungsschutz anbieten.

Die tradierten Versicherungsprogramme bieten – wie später noch genauer beleuchtet wird – nur wenig bis keinen Versicherungsschutz für dieses neue Risiko. Eine teilweise Abdeckung bietet bisher nur die Vertrauensschaden-Versicherung, die ebenfalls aber noch wenig verbreitet ist.

Gewerbliche Angebote sind deutlich besser entwickelt als das Angebot für Privatkunden

Das Cyber-Risiko ist in Unternehmen bisher noch weitestgehend nicht versichert. Das Angebot dazu steht allerdings bereit, denn die Versicherungswirtschaft hat auf die neuen Anforderungen reagiert und Cyber-Versicherungen entwickelt. Diese decken die bisher bekannten Cyber-Risiken auch weitestgehend ab und bieten umfassende Assistance-Leistungen im Schadenfall. Das versetzt insbesondere mittelständische Unternehmen ohne eigene Security-Expertise in die Lage, Schadenfälle schnell und professionell managen zu können. Gleichwohl sollten die Versicherer für die Beherrschung des Cyber-Risikos noch besondere Fähigkeiten/Skills in ihren Organisationen aufbauen bzw. von außen einkaufen (siehe auch Kapitel 3.5). Die Angebote für Privatpersonen sind dagegen noch nicht ausgereift und gehen teilweise am Bedarf der Kunden vorbei. Das hohe Volumenpotenzial in diesem Segment sollte in der nahen Zukunft aber zu einer ernsthafteren Auseinandersetzung mit Cyber-Versicherungen für Privathaushalte führen.

Cyber als Versicherungsleistung kann ebenso dynamisch wachsen, wie sich der Fortschritt der Technik vollzieht und sich die Risikosituation entwickelt. Und: Cyber-Versicherung bietet der Versicherungswirtschaft eine der wenigen echten Wachstumschancen.

3.3 Cyber End-to-End

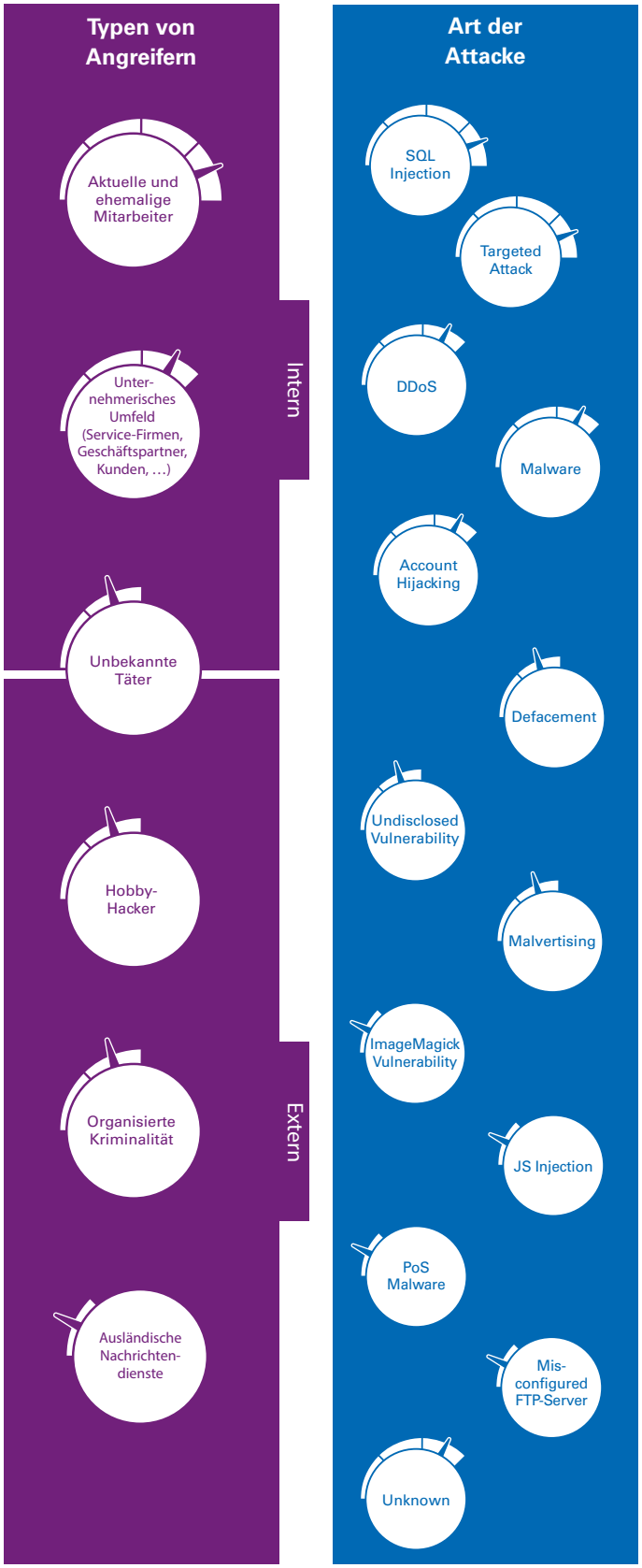
Von den Angreifertypen bis zur versicherten Gefahr

Wichtige Aspekte beim Umgang mit Cyber-Risiken liegen in der Herkunft der Angreifertypen, in der Art des gewählten Angriffs und im gewählten Ziel der Angreifer. Abbildung 4 stellt die verschiedenen Aspekte in diesem Zusammenhang dar und bewertet sie mit Blick auf ihre Eintrittswahrscheinlichkeit.

Angreifertypen

Um die Täter hinter den Cyber-Angriffen kategorisieren zu können, hat Alexander Geschonneck, Partner bei KPMG und Leiter des Bereichs Forensic, mit seinem Team weltweit 750 Fälle untersucht und ein aktuelles Täterprofil erstellt:

Abbildung 4: End-to-End-Prozess eines Cyber-Angriffs



Quelle: KPMG, Deutschland, 2017

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Ziele der Angriffe

Typische versicherte Ereignisse

Identität

- Identitätsdiebstahl

Zahlungsmittel

- Kreditkartenmissbrauch beim Online-Shopping
- Missbrauch von Online-Banking/ Online-Bezahlsystemen
- Internetbetrug und Manipulation des Online-Bankings

Arbeitsunfähigkeit

- Datenverlust
- Menschliches Versagen (Bedienungsfehler)
- Betriebsunterbrechung
- Hackerangriffe, zielgerichtet/nicht zielgerichtet (Denial of Service)
- Reputationsrisiken
- Schadsoftware
- Hardwareausfall
- Betrug oder Erpressung
- Spionage
- Viren
- Elektronische Störung/ Vorsätzliche Manipulation

Drittschaden

- Datenschutzvorfall
- Haftpflichtansprüche
- Hackerangriffe (zielgerichtet)
- Wettbewerbsverstöße
- Vertragsstrafen

Typische Dienstleistungen im Schadenfall

Privatpersonen

- Neuinstallation der Systeme
- Rechtsberatungskosten
- Psychologische Beratung bei Cyber-Mobbing

Fix it

Unternehmen

- Fehlersuche
- IT-Forensik
- Datensicherung des Fehlerfalls

Find it

- Neuinstallation der Systeme
- Einberufung eines Krisenstabs
- Rechtsberatungskosten
- Notfall- und Krisenkommunikation
- PR-Maßnahmen
- Imagekampagnen
- Einleitung eines Notbetriebsverfahrens für Ersatzprozesse
- Einberufung eines Notfallteams
- Schwenkung der IT-Systeme
- Sicherstellung des Mittelflusses für den laufenden Betrieb

Fix it

- Verbesserung der IT-Sicherheitsarchitektur
- Schwachstellenanalyse

Run it

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Der typische Cyber-Kriminelle ist

- mit 60-prozentiger Wahrscheinlichkeit Innentäter, also Teil der Organisation, die er angreift,
- männlich und zwischen Mitte 30 bis Mitte 50 Jahre alt,
- bereits mindestens sechs Jahre im Unternehmen beschäftigt,
- meist eine Führungskraft,
- eine respektierte, freundliche Person.

Die schon erwähnte Bitkom-Studie von 2015 ist zu einem ähnlichen Ergebnis gekommen. Die Bitkom hatte eine ungenannte Anzahl von Unternehmen befragt, welche Erfahrungen sie hinsichtlich der Angreifertypologie gemacht haben. Danach waren 52 Prozent aller Angriffe aktuellen oder früheren Mitarbeitern zuzuordnen. Aus den 18 Prozent der Fälle, bei denen die Täter keiner Gruppe zugeordnet werden konnten, dürfte vermutlich gut die Hälfte der Mitarbeitergruppe zuzuordnen sein, womit auch bei dieser Erhebung der Anteil der Innentäter auf rund 60 Prozent hinausläuft.

Die Außentäter, also die verbleibenden 40 Prozent, lassen sich wie in Abbildung 5 zuordnen.

Art der Attacke

Die Formen von Cyber-Attacken sind breit gefächert, die wichtigsten erläutern wir nachfolgend.

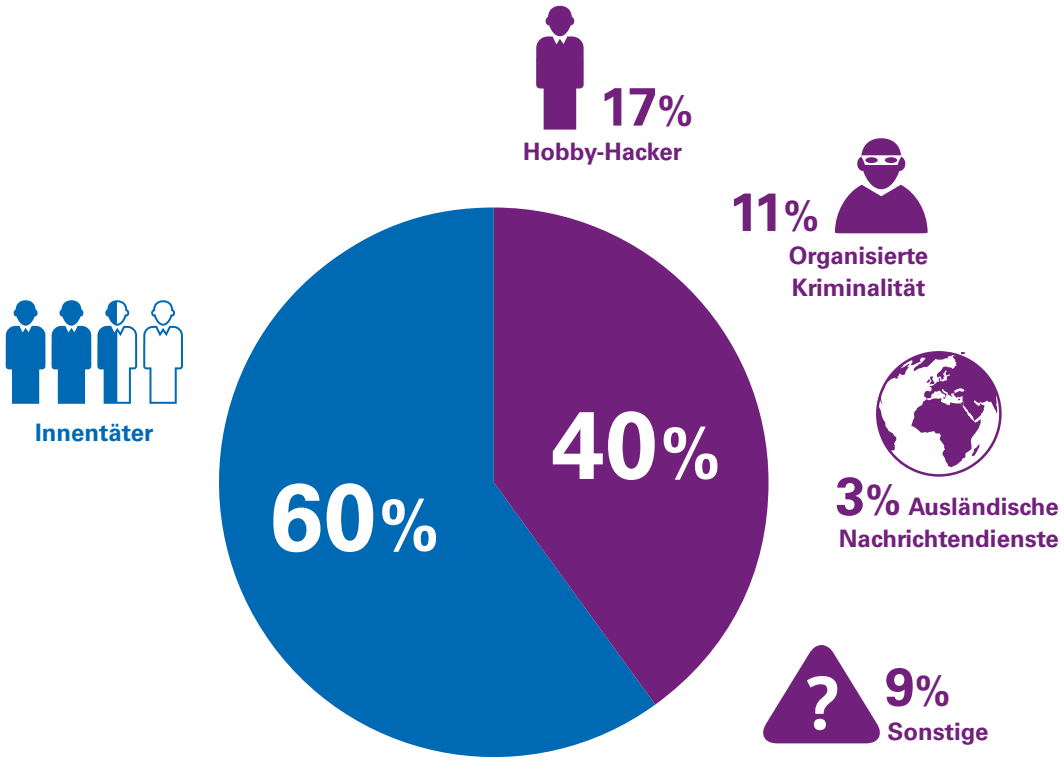
SQL Injection

Das Ziel dieses Angriffs ist es, die Kontrolle über einen Server zu gewinnen und/oder auf dem angegriffenen Server größtmöglichen Schaden anzurichten. Bei dieser Form des Angriffs werden mangelhafte Maskierungen oder mangelnde Überprüfungen von Metazeichen bei Benutzereingaben als Sicherheitslücken in SQL-Datenbanken ausgenutzt. Über die Anwendung, die den Zugriff auf die Datenbank steuert, werden eigene Datenbankbefehle eingeschleust. Dies kann in manchen Fällen so weit gehen, dass der Angreifer sich selbst Administratorenrechte einräumt.

Targeted Attacks/Advanced Persistent Threat (ATP)

Bei Angriffen dieser Art wird ein Opfer gezielt ausgewählt und attackiert. In der Regel verfügen die dahinter stehenden Täter

Abbildung 5: Anteil der Außentäter an Gesamttätergruppe (in Prozent)



Quelle: Allianz, 2016

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

über erhebliche Geldmittel und ausreichend Zeit. Die Zeitspanne zwischen der Infektion eines Systems und der Erkennung eines ATP-Angriffs beträgt meist mehrere Monate. In dieser Zeit können sich Angreifer ungehindert in dem attackierten System bewegen und Informationen ausspionieren. Besonders betroffen von derartigen Angriffen sind die Rüstungsindustrie, Hightech-Unternehmen wie Auto- und Schiffbau sowie Luft- und Raumfahrt und natürlich auch Forschungseinrichtungen.

Die Erstinfektion erfolgt in der Regel durch sogenannte „Watering Hole"-Angriffe, bei Bedarf ergänzt durch das Versenden von E-Mails mit präparierten Dateianhängen. Diese E-Mails sind qualitativ so hochwertig, dass die Opfer die Fälschung oft nicht erkennen. Technisch funktioniert das so: Die Mitarbeiter eines Unternehmens werden zunächst auf Facebook, Twitter etc. ausgespäht, bis man ein gemeinsames persönliches Interesse entdeckt (Wandern, Segeln, Fußball usw.). Weniger gut geschützte Seiten, die sich mit diesem Interessengebiet beschäftigen und von einem oder mehreren der Targets genutzt werden, werden von den Tätern auf sogenannte „Cross-Side-Scripting-Lücken" untersucht, die sich dann in der Regel auch finden lassen. In dieser Schwachstelle der Kommentarfunktion tragen die Täter einen Verweis auf ihren eigenen Server ein, der fortan im Hintergrund mitgeladen wird und bei Bedarf Angriffscodes ausführen kann. Sobald eines der potenziellen Opfer von dem Unternehmensrechner aus die Seite besucht, wird die IP-Adresse des eigentlichen Angriffsziels zwangsläufig übertragen. Auf dem Server ist ein Angriffscode nur für genau diese IP-Adresse hinterlegt, was bei einem üblichen PC häufig schon die Infektion des Systems des eigentlichen Targets bedeutet. Sollte dies nicht gelingen, werden E-Mails an die anderen identifizierten Mitarbeiter des Unternehmens verschickt, die Bezug auf die Aktivitäten des jüngsten Besuchers der Webpage nehmen – etwa, um neue Bilder hochzuladen oder neue Beiträge zum Thema zu posten. Diese E-Mails, verschickt von dem Server der zuvor gemeinsam besuchten Website, also scheinbar absolut authentisch, enthalten einen Link. Wer auf diesen unauffälligen Link klickt, hat den Tätern den Zugang zum eigenen System geöffnet.

Ein prominentes Beispiel für einen klassisch durchgeführten ATP-Angriff ist der im Mai 2015 bekannt gewordene Angriff auf das Netz des Deutschen Bundestags. Wie das BSI (Bundesamt für Sicherheit in der Informationstechnik) anschließend feststellte, war zu diesem Zeitpunkt bereits das zentrale System des internen Bundestagsnetzes kompromittiert. Dieser Vorfall war derart substanziell, dass die betroffenen Systeme des Deutschen Bundestags für längere Zeit abgeschaltet werden mussten.

DDoS-Attacken (Distributed Denial of Service)

Unter DDoS-Attacken versteht man die vorsätzliche Überlastung von Infrastruktursystemen. Meist erreichen die Angreifer diesen Zustand durch einen gezielten Angriff auf einen Server, einen Rechner oder sonstige Komponenten der IT-Infrastruktur.

„Die Anzahl der kriminellen Trittbrettfahrer wird dramatisch zunehmen, insbesondere dort wo kaum Schutzmaßnahmen umgesetzt sind – im Privatbereich und bei KMUs"

Dipl. Techn. Erik Venningdorf,
Vorstandsdirektor für Vertrieb,
Grazer Wechselseitige Versicherung AG

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Der Angriff macht bestimmte Dienste des Systems oder das System selbst arbeitsunfähig. Bei einer DDoS-Attacke erfolgt der Angriff nicht nur von einem bestimmten Angriffsrechner, sondern von einer Vielzahl von Rechnern gleichzeitig. Diese koordinierte Aktion hat für die Angreifer zwei Vorteile: Erstens ist der das System überlastende Datenverkehr signifikant höher und zweitens ist es sehr viel aufwendiger, die Angreifer zu identifizieren. Zu einem prominenten Beispiel für einen DDoS-Angriff kam es 2010, als die Aktivistengruppe „Anonymous" die Webpages von Visa und MasterCard tagelang blockiert und sogar das PayPal-Transaktionsnetz empfindlich gestört hat.

Schadprogramme (Malware)/Ransomware

Unter Schadprogrammen versteht man in diesem Zusammenhang jede Art von Software, die es Tätern ermöglicht, ganz oder teilweise die Kontrolle über Endgeräte zu erlangen mit dem Ziel, digitale Identitäten auszuspähen oder die Funktionen von Programmen auf diesen Endgeräten in krimineller Absicht zu manipulieren. Auch Fälle von digitaler Erpressung nehmen in diesem Kontext neuerdings stark zu. Verbreitet werden die Schadprogramme häufig über Anhänge in Spam-E-Mails, Drive-by-Exploits (automatisierte Ausnutzung von Sicherheitslücken auf einem PC) und über Botnetze (von Botnetzen spricht man, wenn eine Vielzahl von PCs per Fernsteuerung zusammengeschlossen und zu illegalen Aktionen missbraucht werden). Laut Bundeskriminalamt gibt es über 250 Millionen PC-basierte Schadprogramme. Und täglich werden es etwa 300.000 mehr. Das BKA geht davon aus, dass es in Deutschland monatlich zu rund einer Million Infektionen durch Schadprogramme kommt. Auch Smartphones und Tablets sind von den Angriffen nicht ausgenommen. Für diese Medien gibt es laut BKA inzwischen mehrere Millionen Schadprogramme.

Ransomware sind Schadprogramme – auch Erpressungstrojaner, Kryptotrojaner oder Verschlüsselungstrojaner genannt – die Cyber-Kriminelle nutzen, um Zugriff und Nutzung von Daten, aber auch von gesamten Computersystemen für die rechtmäßigen Nutzer zu verhindern. Die Daten auf den betroffenen Computern werden durch Ransomware verschlüsselt und nur gegen Zahlung eines „Lösegeldes" wieder zugänglich gemacht. Diese Schadsoftware kann im Darknet erworben werden, besonderer IT-Sachverstand ist für derartige Erpressungsversuche nicht erforderlich. Der Verschlüsselungstrojaner „Locky", der sich von Februar 2016 an rasend schnell in Deutschland verbreitet hat – von bis zu 17.000 Infektionen täglich war die Rede – und unter anderem das Fraunhofer-Institut in Bayreuth traf, gehört zu den bekanntesten Beispielen. Für die Entschlüsselung haben die Erpresser 0,5 Bitcoins (etwa 400 Euro) verlangt. Seit Juni 2016 wird die Verbreitung einer neuen Generation des Locky-Trojaners in Deutschland beobachtet, genannt „Zepto".

Account Hijacking/Identity Theft

Das BKA definiert eine digitale Identität als „die Summe aller Möglichkeiten und Rechte eines einzelnen Nutzers sowie seiner personenbezogenen Daten und Aktivitäten innerhalb der Gesamtstruktur des Internets". Hierzu gehören auch alle Arten von Nutzer-Accounts, also beispielsweise auch Zugangsdaten in den Bereichen:

Kommunikation (E-Mail, Messenger etc.), E-Commerce (Onlinebanking, Onlinebrokerage, Internet-Vertriebsportale etc.), Online-Zugriff auf firmeninterne Daten und technische Ressourcen, Zugang und nutzerbezogene Daten zu behördlichen Plattformen (E-Government, elektronische Steuererklärungen etc.) und Cloud-Computing. Weiterhin sind unter der digitalen Identität auch alle zahlungsrelevanten Informationen wie Kreditkarten- und Bankkontodaten zu verstehen.

Die am häufigsten eingesetzten Instrumente, um illegal an derartige Informationen zu kommen, sind Trojaner, Phishing, Einbruch in Server in Verbindung mit dem Kopieren von Anmeldeinformationen sowie Spyware und sogenannte „Keylogger".

Gestohlene Identitäten werden an speziellen Speicherorten im Darknet abgelegt, den sogenannten Dropzones, auf die andere Kriminelle zugreifen können. Bei einzelnen Angriffen auf Systeme großer Internetunternehmen sind in den vergangenen Jahren regelmäßig Identitätsdatensätze in zweistelliger Millionenhöhe erbeutet worden – im Falle von eBay waren es 2014 sogar 145 Millionen. Zu den Datensätzen gehörten Namen, verschlüsselte Passwörter, E-Mail-Adressen, Geburtstage, Adressen, Telefonnummern usw. Selbst hochgeschützte staatliche Systeme, wie die Personaldatenverwaltung der US-Regierung, sind vor solchen Angriffen nicht sicher. Das zeigte ein Vorfall aus dem Jahr 2015: Cyber-Kriminellen gelang es, personenbezogene Daten von 21,5 Millionen Regierungsangestellten und Bewerbern zu stehlen. Im selben Jahr wurde die US-Steuerbehörde erfolgreich angegriffen, wodurch Steuerzahlerdaten in erheblichem Umfang in die Hände der Täter gelangten.

Eine weit verbreitete Form des digitalen Identitätsdiebstahls ist schließlich das „Phishing" beim Online-Banking. Banken haben mit verschiedenen Schutzmaßnahmen auf die rapide steigende Zahl von Fällen reagiert, beispielsweise durch die Einführung von elektronisch generierten, transaktionsspezifischen TANs sowie einer Sensibilisierungskampagne der Kunden. Dies war zunächst erfolgreich, sodass die Phishing-Zahlen 2012 in Deutschland halbiert werden konnten. Doch die Täterseite rüstete nach und kann mittlerweile auch das Verfahren mit elektronischen TANs erfolgreich angreifen. Trojaner spielen hierbei eine Schlüsselrolle, der Trend zur verstärkten Nutzung von Smartphones beim Onlinebanking spielt dem Phishing dabei in die Hände – mit der Folge, dass die Fallzahlen seit 2014 wieder deutlich ansteigen.

Fake President Fraud

Bei dieser Betrugsmasche steht ein Identitätsdiebstahl am Anfang: Ein mit Banktransaktionen betrauter Mitarbeiter einer

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Firma erhält von einem (vermeintlichen) Geschäftsführer oder Vorstand eine E-Mail, in deren Adresse es entweder einen kaum wahrnehmbaren Buchstabendreher gibt oder aber die E-Mail tatsächlich aus dem (kompromittierten) E-Mail-Postfach des entsprechenden Executives stammt – allerdings ohne sein Zutun. Mehrfach auf die besondere Vertraulichkeit seiner E-Mail hinweisend, ordnet der vermeintliche Executive eine oder mehrere Bank-Transaktionen an, die sich fast immer in der Größenordnung mehrerer Millionen Euro bewegen. Um Bedenken zu zerstreuen, wird häufig ein vermeintlicher Anwalt oder Notar in den Vorgang integriert, den Namen und die Telefonnummer liefert der vermeintliche Chef in seiner E-Mail gleich mit. Der Mitarbeiter wird angewiesen, ausschließlich per E-Mail mit dem vermeintlichen Chef und sonst niemandem in der Firma, daneben nur mit dem benannten Anwalt, zu kommunizieren. Selbst wenn Mitarbeiter an dieser Stelle misstrauisch werden: Gegen Anweisungen zu verstoßen und weitere Personen in den Vorgang einzubeziehen, trauen sich viele Betroffene dann doch nicht. In dieser Weise werden häufig ausländische Tochtergesellschaften in internationalen Gruppen angesprochen, womit die Wahrscheinlichkeit eines Widerspruchs weiter sinkt. Die geforderten Transaktionen gehen dann auf Konten in ausländischen Drittländern, die überwiesenen Beträge werden von diesen Konten häufig in weniger als einer Stunde abgezogen. Sobald der Betrug bekannt wird, sind Geld und Täter verschwunden. Die Fallzahlen für Fake President Fraud sind in den vergangenen Jahren rasant angestiegen. Mit schärferen Berechtigungssystemen und Mitarbeiterschulungen lässt sich die Wahrscheinlichkeit des Eintretens solcher Fälle reduzieren. Ausschließen können wird man solche Fälle aber auch für die Zukunft wohl nicht.

Ziele der Angriffe

Man geht davon aus, dass sich heute rund 90 Prozent aller Cyber-Angriffe gegen Unternehmen richten und nur zehn Prozent gegen Privatpersonen. Über die Hälfte aller deutschen Unternehmen sollen 2015 von erfolgreichen Cyber-Attacken betroffen gewesen sein.

Gewerbliche Ziele

Wie gehen betroffene Unternehmen mit dem Thema Cyber um? Der Versicherungsmakler Marsh führt regelmäßig Erhebungen zum Thema Cyber bei seinen gewerblichen und industriellen Kunden in Deutschland durch. Im dritten Quartal 2016 hat Marsh Details aus der diesjährigen Cyber-Risiko-Befragung, veröffentlicht (vgl. MARSH, 2016):

- Unternehmen fürchten besonders Betriebs- und Systemstörungen (39 Prozent der Befragten) sowie das „organisierte Verbrechen und Hacker" (27 Prozent der Befragten).
- Cyber-Risiken spielen 2016 für 73 Prozent aller Unternehmen eine Rolle. 17 Prozent aller Unternehmen sehen in Cyber sogar ein Top-5-Risiko. 2015 hatten gerade einmal acht Prozent Cyber-Risiken auf diesem Rang gesehen.
- Nur 16 Prozent der deutschen Unternehmen siedeln die Verantwortung für Cyber-Risiken auf dem C-Level an. Für 69 Prozent der Unternehmen sind Cyber-Risiken dagegen eine „Sache der IT-Abteilung".
- Die Zahl der deutschen Unternehmen, die sich mit Cyber-Versicherungen beschäftigen, ist von 2015 auf 2016 stark gestiegen. 35 Prozent der befragten Unternehmen wollen in den nächsten zwölf Monaten ein Angebot für eine Cyber-Versicherung einholen, neun Prozent der Unternehmen sind gerade im Begriff, eine Cyber-Versicherung abzuschließen und weitere neun Prozent haben bereits eine Cyber-Versicherung abgeschlossen – immerhin doppelt so viele wie noch 2015.
- Trotz eines akuten Bedrohungsgefühls durch Cyber-Attacken haben über 40 Prozent aller Unternehmen bis heute keinen Krisenreaktionsplan für Cyber-Angriffe.
- In über 90 Prozent aller deutschen Unternehmen ist die Gefährdung durch Zulieferer bzw. Abnehmer nicht Betrachtungsgegenstand des Cyber-Risikomanagements.

Obwohl sich deutsche Unternehmen der Bedrohungssituation durch Cyber-Risiken zunehmend bewusst werden, gibt es mit Blick auf Risiko-Assessment, Risiko-Management sowie Risiko-Transfer noch weitgehend unbearbeitete Betätigungsfelder. Im Vergleich zu den Vorjahren nimmt jetzt aber wohl ein deutlich größerer Teil der Unternehmen die Herausforderung Cyber-Risiken in Angriff.

Private Ziele

Aber auch aufseiten der Privatpersonen lässt sich eine Verschärfung der Bedrohungslage beobachten. Die für Kriminelle erforderlichen Instrumente stehen heute schon im Darknet zur Verfügung – angefangen bei gestohlenen Identitätsdaten über fachliche und technische Unterstützung bei der Ausführung elektronischer Diebeszüge bis zu sichereren Abnahmeplätzen für gestohlenes Geld oder Waren. Zu berücksichtigen ist außerdem, dass die Online-Devices und -Accounts von Privatpersonen in aller Regel deutlich schlechter geschützt sind als die von Unternehmen. Privatpersonen scheinen insofern vergleichsweise leichte Opfer zu sein. Ein deutlicher Anstieg der Fälle bei Privatpersonen scheint demnach nur eine Frage der Zeit zu sein.

Versicherbare Ereignisse und Schäden und typische Leistungen im Schadenfall

Der Deckungsumfang bei der Cyber-Versicherung auf den angelsächsischen Märkten und dem deutschen Markt variiert. Zudem erleben die Märkte aufgrund der sich schnell ändernden Anatomie der Cyber-Risiken eine dynamische Entwicklung der Deckungen.

Im Vorfeld der Etablierung einer neuen Versicherungssparte „Cyber" schlagen wir vor, die in den Deckungen dieser Sparte versicherbaren Schäden nach Eigenschäden und Fremdschäden zu trennen – analog der Sachversicherung einerseits und der Haftpflichtversicherung andererseits. Vom Wesen her sind beide Versicherungsformate aber Teil einer Cyber-Sparte.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Eigenschäden

In das Segment der Eigenschäden gehören alle Schäden, die als Folge einer Datenschutzverletzung oder einer unbefugten Nutzung von IT-Systemen bei dem Versicherungsnehmer selbst entstehen. Dazu zählen insbesondere die Wiederherstellungskosten von IT-Systemen, ein Ertragsausfall oder Mehrkosten zur Aufrechterhaltung der Produktion, die Kosten für die Benachrichtigung der von Datenschutzvorfällen Betroffenen sowie auch die Kosten für Rechtsberatung, IT-Forensik und Krisenmanagement. Eigenschäden umfassen unter anderem Ereignisse wie Identitätsdiebstahl, Cyber-Mobbing und Reputationsbeschädigung, das Ausspähen von Account-Zugangsdaten und Zahlungsmitteldaten, das Verschlüsseln von Daten zwecks Erpressung, das Unbrauchbarmachen von IT-Infrastruktur oder auch den Diebstahl von Geschäftsgeheimnissen wie Produktinformationen, Patenten usw. Auch eine durch Ereignisse dieser Art verursachte Arbeitsunfähigkeit mit entsprechenden wirtschaftlichen Folgen für Personen oder Unternehmen fällt unter das Segment Eigenschäden.

Fremdschäden

Unter Fremdschäden werden Schadenersatzansprüche Dritter verstanden, die sich gegen die versicherten Unternehmen oder Person(en) richten. Solche Schadenersatzansprüche entstehen, wenn der Versicherungsnehmer bzw. mitversicherte Personen die Rechte Dritter verletzt bzw. verletzten – im Rahmen von Datenschutzvorfällen oder im Zusammenhang mit dem Umgang mit Daten bzw. IT-Systemen.

Die versicherten Leistungen unterscheiden wir ebenfalls nach Eigen- und Fremdschäden.

Leistungen bei Eigenschäden

Bei den Eigenschäden, also bei Schäden, die den Versicherungsnehmer und/oder die versicherten Personen selbst sowie deren materielles und virtuelles Vermögen betreffen, lassen sich im Wesentlichen die folgenden Leistungsformen differenzieren:

- Durchführung des Schadenmanagements
- Kosten für das Einschalten von Spezialisten, wie Rechtsanwälten, Sachverständigen, Forensikern etc.
- Kosten für Reparatur und Austausch
- Mehrkosten bei Betriebsausfall
- Fortlaufende Kosten und ausfallender Gewinn bei Betriebsunterbrechung
- Vermögensverluste, beispielsweise durch den Eingriff in Konten und die unautorisierte Durchführung von Transaktionen
- Kosten für die Benachrichtigung von Dateninhabern, deren Daten durch einen Datenschutzvorfall sichtbar geworden sind oder entwendet wurden
- Ausfall von Einkommen bei Privatpersonen
- Kosten für psychologische Betreuung
- Kosten für sonstige Dienstleister

Leistungen bei Fremdschäden

Die Leistungsformen bei Fremdschäden ähneln vom Grundsatz her denen der klassischen Haftpflichtversicherung. Auch wenn sich die zu klärenden Umstände im Schadenfall deutlich von denen klassischer Haftpflichtsparten unterscheiden, finden wir auch bei den Cyber-Fremdschäden die Abwehr unbegründeter Ansprüche im Sinne eines passiven Rechtsschutzes sowie die Befriedigung berechtigter Ansprüche.

Bei den Cyber-Produkten für Gewerbe und Industrie lassen sich im deutschen Markt bereits klare Standards bei den Leistungsformen erkennen. Sie folgen im Wesentlichen den zuvor beschriebenen Kriterien.

Für Privatpersonen jedoch gibt es diese Standards bei den Leistungsformen bislang noch nicht. Teilweise werden Deckungsbestandteile als Annexprodukte zu anderen Privatversicherungsprodukten angeboten, etwa zur Hausratversicherung. Daneben gibt es bereits reine Cyber-Produkte für Privatkunden, dies jedoch bisher nur mit, im Vergleich zu den gewerblichen Cyber-Produkten, eingeschränktem Deckungsumfang.

Die Bedrohungslage bei Privatpersonen ist der von gewerblichen Kunden technisch und auch in den Schadenbildern durchaus ähnlich. Die Versicherung dieser Risiken ist auch gleichermaßen anspruchsvoll aus Sicht des Versicherers, insbesondere in Bezug auf die Tarifierung, die Kumulproblematik und die Schadenbearbeitung. Aus unserer Sicht spricht viel dafür, den Cyber-Versicherungsschutz für Privatpersonen sowohl von der Produktlogik her als auch in Hinsicht auf Risikobewertung, Underwriting sowie Schadenregulierung ähnlich zu behandeln wie das gewerbliche Geschäft.

3.4 Marktpotenzial der Cyber-Versicherung

Einhelliger Konsens in puncto starkes Wachstum des Cyber-Marktes

Der deutsche Markt für Cyber-Versicherung ist mit einer Jahresprämie von ca. 30 Millionen Euro Ende 2015 noch relativ klein. Da die Cyber-Versicherung bisher nicht als eigenständige Sparte geführt wird, können die Volumenzahlen nicht aus Verbandsstatistiken abgelesen werden. Vielmehr müssen Marktteilnehmer befragt werden. Die Anschlussfrage zur Status-quo-Erfassung lautet, wohin sich der Cyber-Markt im Laufe der nächsten Jahre entwickeln könnte.

Versicherer und Makler erwarten übereinstimmend, dass das Prämienvolumen im Cyber-Geschäft auf dem deutschen Markt stark ansteigen wird – überwiegend sogar „sehr stark". Auch wurde in praktisch jedem unserer Gespräche auf die USA verwiesen, wo das jährliche Prämienvolumen 2015 bereits rund 2,5 Milliarden US-Dollar betrug.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Prognosen aus dem Markt

Die Munich Re sieht den weltweiten Cyber-Markt 2016 bei drei Milliarden US-Dollar und erwartet einen Anstieg auf acht bis zehn Milliarden US-Dollar bis zum Jahr 2020 – was einem Wachstum von etwa 200 Prozent in den nächsten vier Jahren entspricht. Laut Experten im US-Markt soll bis 2020 alleine für die USA ein Prämienvolumen von 7,5 Milliarden US-Dollar erreicht werden. Wachstumsprognosen für das Cyber-Geschäft in dieser Größenordnung überraschen nicht, denn zwischen 2012 und 2016 ist das weltweite Prämienvolumen um 250 Prozent gewachsen. Absolut heißt das: von 850 Millionen auf drei Milliarden US-Dollar.

Zusätzlicher Katalysator für die Wachstumsgeschwindigkeit im Cyber-Geschäft könnte die Gesetzgebung werden, beispielsweise die „General Data Protection Regulation", deren Implementierung zeitnah bevorsteht. Aus Sicht der Verantwortlichen in Unternehmen wird ein Verzicht auf einen Risikotransfer, also den Einkauf eines Ergebnis- bzw. Bilanzschutzes in Form einer Cyber-Versicherung, immer schwerer vertretbar. Bei Aktiengesellschaften werden spätestens die Aufsichtsräte dafür sorgen, dass das Thema Cyber auf die Agenda kommt.

Einen zeitlich weiteren Blick in die Zukunft wirft der CEO der Allianz Global Corporate & Specialty (AGCS), Chris Fischer Hirs. In einem Interview prognostizierte er 2015 einen Anstieg des weltweiten Prämienaufkommens für Cyber-Versicherungen bis 2025 auf über 20 Milliarden US-Dollar. Schon 2015 habe der jährliche Schaden durch Cyber-Crime seiner Schätzung nach bei mehr als 440 Milliarden US-Dollar gelegen, wovon über 50 Milliarden US-Dollar auf Deutschland entfallen seien.

Eine logische Folge der konkreten Bedrohungslage durch Cyber-Crime werde ein drastischer Anstieg der Cyber-Prämie sein. Chris Fischer Hirs erwartet außerdem, dass „innerhalb der nächsten fünf bis zehn Jahre die Deckungskomponente ‚Betriebsunterbrechung' zu einem wichtigen Element der Cyber-Versicherung wird".

Auch die XL Group erwartet, dass Cyber-Deckungen „zum Standard werden für mittlere und größere Unternehmen". Der HDI meint, dass „eine Cyber-Police unter Umständen so selbstverständlich zu den Versicherungsspesen eines Unternehmens gehören wird wie heute eine Feuer- oder eine Haftpflichtversicherung". Die Chubb verweist in einer Veröffentlichung von 2016 darauf, dass eines der Deckungselemente von Cyber-Versicherungen die in den USA am stärksten wachsende Kriminalitätsform adressiert: den Identitätsdiebstahl.

Allianz und AXA können sich eine Verzehnfachung der Cyber-Prämie in Deutschland binnen fünf Jahren vorstellen – also einen Anstieg von aktuell 30 Millionen Euro auf bis zu 300 Millionen Euro im Jahr 2021. Hierbei beziehen sich die Versicherer allerdings ausdrücklich auf die Segmente Industrie und Gewerbe und klammern damit das Privatkundensegment aus.

© Wiener Städtische Versicherung, Elke Mayr

„Die Cyber-Risiko-Versicherung wird in zehn Jahren fixer Bestandteil des Versicherungsschutzes von Privatpersonen und Unternehmen sein."

Magister Hermann Fried,
Vorstandsdirektor für Vertrieb,
Wiener Städtische Versicherung

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Wir haben uns die Frage gestellt, wie die entsprechenden Prognosen für die Cyber-Prämien im deutschsprachigen Raum aussehen mögen. Hierbei ist es auch interessant, das dritte Kundensegment, die Privatkunden, in die Betrachtung einzubeziehen.

Mit Hilfe von Externen und KPMG-Fachleuten wurde ein Prämienmodell entwickelt, das die Entwicklung der Cyber-Prämie im deutschsprachigen Raum in allen drei Kundensegmenten über die kommenden 20 Jahre simulieren kann.

Entwicklung eines Prämienmodells für den deutschen Sprachraum bis 2036

Bei der Entwicklung unseres Cyber-Prämienmodells für den deutschsprachigen Raum sind wir auf Basis unserer Gespräche von den Rahmenbedingungen in Abbildung 6 ausgegangen.

Wandel kommt erst noch

Die Cyber-Bedrohungslandkarte (Abbildung 7) zeigt deutlich, dass wir uns in puncto Digitalisierung und Vernetzung erst am Anfang einer Entwicklung befinden, die die Welt substanziell verändern kann. Die Möglichkeiten für neue Geschäftsmodelle scheinen dabei ebenso unbegrenzt wie für neue Cyber-Risiken. Angesichts der wertezerstörenden, im schlimmsten Fall sogar existenzgefährdenden Kraft von Cyber-Crime sowohl für Unternehmen als auch für private Haushalte, sollten sich zukünftig alle Kundensegmente mit technischen bzw. organisatorischen Schutzmaßnahmen sowie den Möglichkeiten des Risikotransfers durch Versicherung auseinandersetzen. Der Europa um wenigstens fünf Jahre vorauseilende US-Cyber-Markt zeigt dementsprechend auch bereits starkes Wachstum in allen drei Kundensegmenten.

Feuer und Cyber ähneln sich, sind aber fundamental unterschiedlich

Von der Grundstruktur her kann man die Cyber-Versicherung gut mit der Feuerversicherung vergleichen. Risk Assessment und Risk Engineering sind Pflicht, die Eigenschäden können existenzgefährdende Größenordnungen annehmen und unterteilen sich in Schäden an eigenen Assets sowie in Schäden durch Betriebsunterbrechung bzw. Arbeitsunfähigkeit – das kennen wir so aus der Struktur der Sachversicherung, hier zum Beispiel ausgeprägt als Feuer-Sach- und Feuer-Betriebsunterbrechungsversicherung. Auch in der Feuerversicherung gibt es Fremdschadenphänomene, die beispielsweise in Form der Feuerhaftungsversicherung abgedeckt werden können. Werden die jährlich bearbeiteten Feuerschäden und die eingenommenen Jahresprämien auf das Cyber-Geschäft übertragen, zeigt sich: Dem Cyber-Schadenvolumen von 51 Milliarden Euro im Jahr 2015 müsste ein Prämienpotenzial für Cyber-Versicherungen in der Größenordnung des gesamten deutschen Schaden-/Unfallbuches gegenüberstehen. Wir haben diese Übertragung aber letztendlich verworfen, da „Feuer“ und „Cyber“ sich in einem wichtigen Punkt doch deutlich unterscheiden: Während der Eintritt eines Feuerschadens in aller Regel auf ein naturwissenschaftliches Ereignis bzw. technisches oder menschliches Versagen zurückzuführen ist, handelt es sich bei Cyber-Schäden um durch Kriminelle gezielt herbeigeführte Ereignisse. Und diese sind mit den Mitteln des Risk Engineerings deutlich schwieriger zu beeinflussen, sodass das versicherungstechnische Risiko schwerer zu kalkulieren ist.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Abbildung 6:
Rahmenbedingungen des KPMG-Cyber-Prämienmodells (Auszug)

Schäden durch Cyber-Crime in 2015

Das Gesamtvolumen der durch Cyber-Kriminalität verursachten Schäden wird für das Jahr 2015 mit weltweit 450 Mrd. Euro angegeben, für Deutschland mit 51 Mrd. Euro (1,6 % des BIP). Die Tendenz für die Zukunft ist stark steigend.

Schäden durch Cyber-Crime in 2015

Wachsende Verlagerung von Dienstleistungen und Geschäftsmodellen in die digitale Welt

Immer mehr onlinefähige Geräte

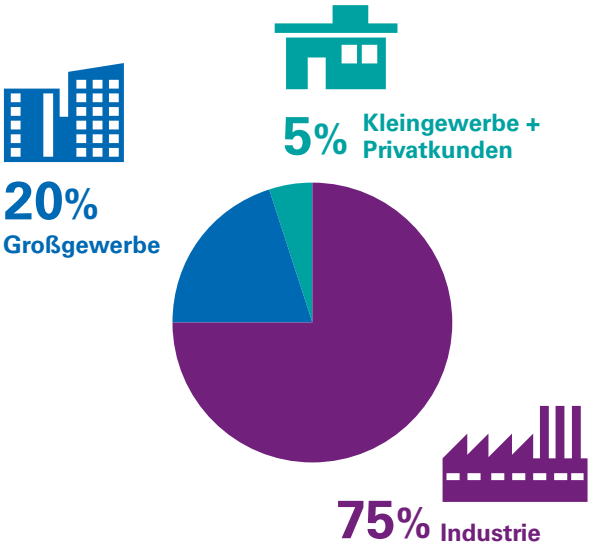
Stärkere Vernetzung der Welten

Prämienvolumen des Cyber-Marktes 2016

Während der US-Amerikanische Cyber-Markt in der Größenordnung von 2,5 Mrd. Euro Prämienvolumen liegt, hat der deutsche Cyber-Markt vergleichsweise geringe 30 Mio. Euro Prämienvolumen Anfang 2016.

Prämienvolumen des Cyber-Marktes 2016

Der Markt zeigt eine hohe Wachstumsdynamik in Cyber im laufenden Jahr 2016, wobei das Industriesegment in absoluten Zahlen am stärksten zulegen wird, auch das Großgewerbegeschäft wächst stark an. Der deutsche Cyber-Markt könnte in das Jahr 2017 mit einem Bestandsprämienvolumen von 90 – 100 Mio. Euro starten.



Aussicht:
Marktverlagerung Richtung Privatkundengeschäft

Quelle: KPMG, Deutschland, 2017

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Abbildung 7: Cyber-Bedrohungslandkarte

Quelle: Dr. Anastassia Lauterbach,
Cyber-Risiko-Expertin und Unternehmerin, 2017

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

So einfach kann man ein potenzielles Cyber-Prämienvolumen also nicht hochrechnen. Nachdem wir im Markt kein geeignetes technisches Modell hierfür gefunden haben, haben wir selbst ein Prämienmodell für Cyber entwickelt. Auf den folgenden Seiten werden wir dieses Modell näher erläutern und die Ergebnisse unserer Berechnungen darstellen. Vorab einige Grundlagen und Annahmen:

- Das KPMG-Cyber-Prämienmodell umfasst den deutschsprachigen Raum, also auch die Märkte Österreich und Schweiz (DACH).
- Eine neue Versicherungssparte Cyber hat das Potenzial, Kraftfahrt im Laufe der kommenden 20 Jahre als volumenstärkste Schaden-/Unfallsparte abzulösen.
- Während wir davon ausgehen, dass die Prämie in der deutschen Kfz-Versicherung über die nächsten Jahre spürbar an Volumen einbüßen wird (vergleiche KPMG Thinking Ahead #1, November 2015), zeigt das KPMG-Cyber-Prämienmodell ein Wachstum der jährlichen Cyber-Prämie im deutschsprachigen Raum bis 2036 auf zwölf Milliarden Euro (Low Case), über 20 Milliarden Euro (Average Case) bis hin zu 26 Milliarden Euro (High Case) an.
- Folgende Cyber-Kundensegmente differenzieren wir für unsere Betrachtung (siehe auch Kapitel 3.5 für Details):
  - Privatkunden (standardisiertes Geschäft)
  - Kleingewerbe, bis fünf Millionen Euro Jahresumsatz (standardisiertes Geschäft)
  - Großgewerbe, bis 100 Millionen Euro Jahresumsatz (vorkonfiguriertes Geschäft)
  - Industrie, ab 100 Millionen Euro Jahresumsatz (individuelles Geschäft)
- Starkes Wachstum wird in allen Cyber-Kundensegmenten zu beobachten sein, die mit Abstand volumenstärksten Segmente werden letztlich aber das Kleingewerbe und die privaten Haushalte sein.
- Die durchschnittliche Prämienhöhe pro Vertrag wird im unteren Kundensegment deutlich niedriger sein als in den Segmenten mit größeren Kunden, die hohe Anzahl der Kleingewerbekunden und der privaten Haushalte wird dies aber deutlich überkompensieren und für die Gesamtgröße der Portfolios ausschlaggebend sein.
- Neben der Entwicklung der Prämien haben wir auch den Markt der Dienstleister für Cyber-Risiko-Prävention sowie das Reparatur- und Servicegeschäft rund um die Cyber-Schadenfälle betrachtet. Die Wechselwirkung zwischen Investitionen in Cyber-Sicherheit und professionellem Schadenmanagement einerseits und dem absoluten Prämienaufkommen in der Cyber-Sparte andererseits werden schnell deutlich.

Im Folgenden befassen wir uns mit den unserem Prognosemodell zugrunde liegenden Annahmen und den sich hieraus ableitenden Prognosewerten.

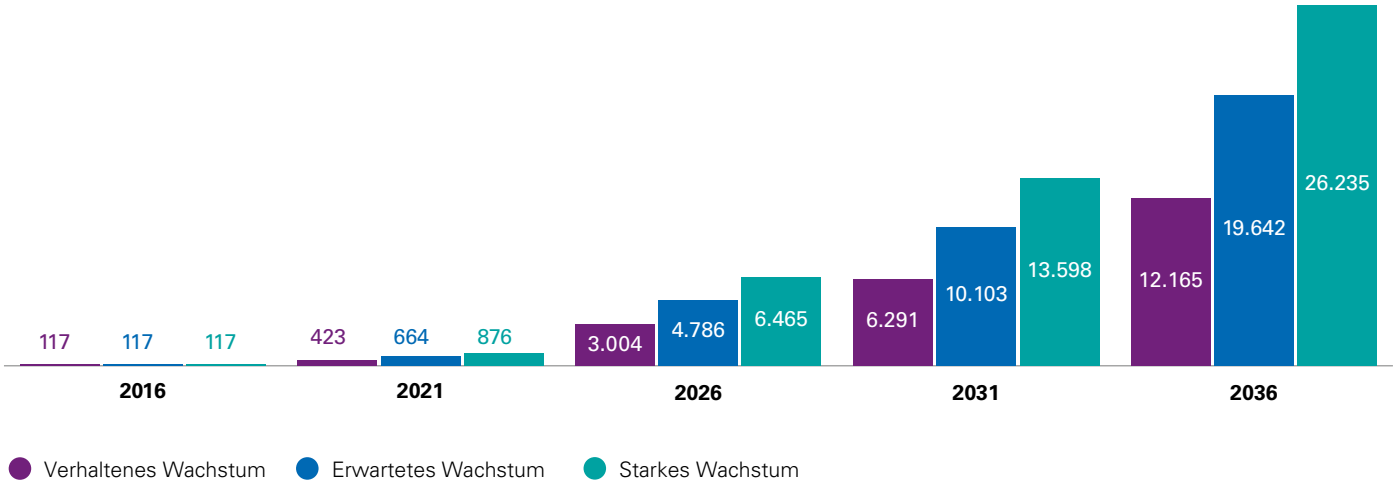
© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Die Szenarien des KPMG-Cyber-Prognosemodells

Die nachfolgenden Schaubilder (Abbildungen 8 bis 11) illustrieren die Prämienvolumina, die das KPMG-Prognosemodell für die Märkte Deutschland, Österreich und Schweiz bis 2036 als Summe aller Kundensegmente ermittelt hat.

Es werden dabei drei Szenarien unterschieden, um einen Bogen von konservativer bis progressiver Betrachtungsweise zu spannen.

Abbildung 8: Prognose Entwicklung Cyber-Prämie bis 2036 in der DACH-Region
Bruttoprämie, Jahresendbestand, in Millionen Euro



Quelle: KPMG, Deutschland, 2017

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

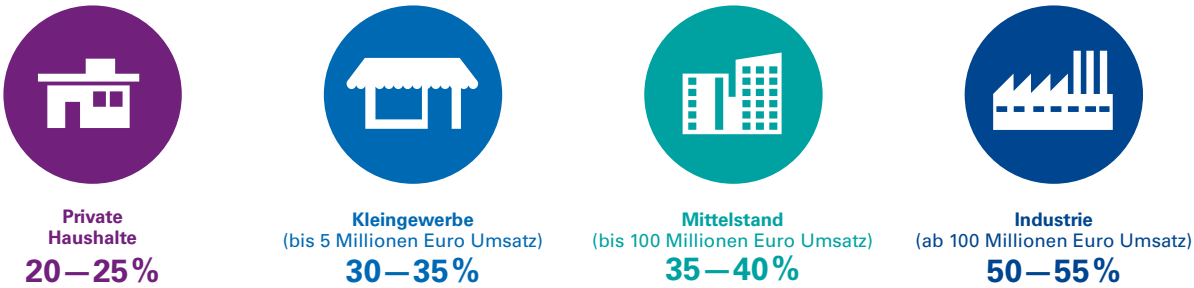
Szenario 1:
Verhaltene Bereitschaft zur Absicherung von Cyber-Risiken

Dieses eher konservative Szenario unterstellt, dass sich der Anstieg der Cyber-Kriminalitätsfälle verlangsamt und die Bereitschaft von Unternehmen und privaten Haushalten verhalten bleibt, eine Cyber-Versicherung abzuschließen.

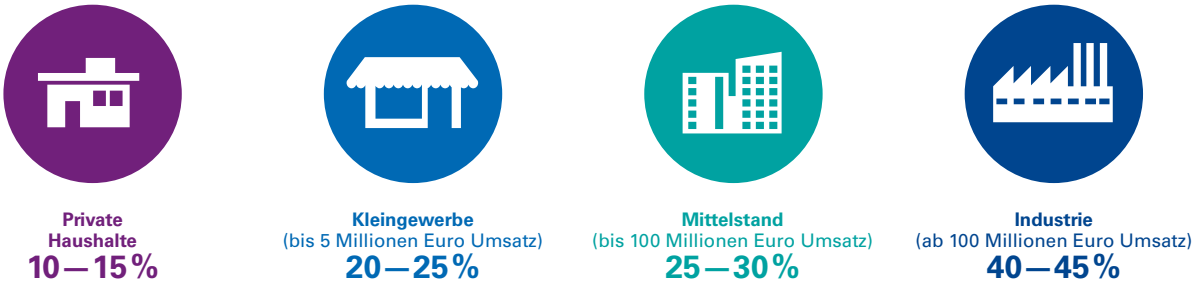
Das Prämienvolumen in der Cyber-Sparte erreicht in diesem Szenario im Jahr 2036 für die gesamte DACH-Region 12,16 Milliarden Euro. Auf Deutschland entfallen davon 9,41 Milliarden (Abbildung 9).

Abbildung 9: Szenario 1, verhaltenes Wachstum

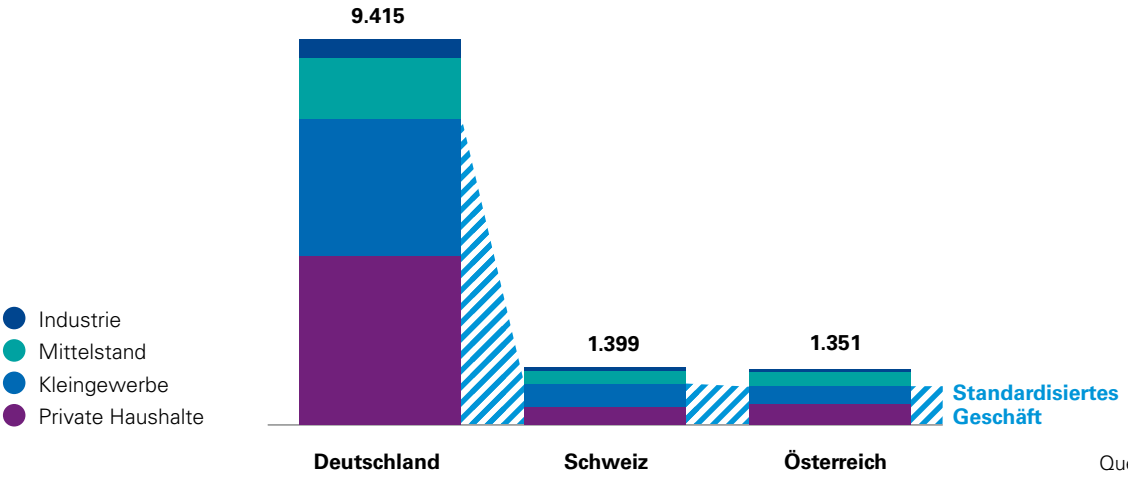
Penetrationsraten für den Eigenschadenteil an der Deckung am Ende des 20-jährigen Betrachtungszeitraums:



Penetrationsraten für den Fremdschadenteil an der Deckung am Ende des 20-jährigen Betrachtungszeitraums:



Prämienvolumen Cyber-Versicherung 2036 in der DACH-Region
Bruttoprämie, Jahresendbestand, in Millionen Euro



Quelle: KPMG, Deutschland, 2017

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Szenario 2:
Bereitschaft zur Absicherung von Cyber-Risiken entwickelt sich erwartungsgemäß

Dieses Szenario stellt die erwartete Entwicklung dar. Die Zahl der Cyber-Kriminalitätsfälle entwickelt sich in der absehbaren Geschwindigkeit und die Bereitschaft von Unternehmen und privaten Haushalten, Deckungsschutz für Cyber-Risiken zu erwerben, steigt entsprechend an.

Das Prämienvolumen in der Cyber-Sparte beläuft sich in diesem Szenario im Jahr 2036 auf insgesamt 19,64 Milliarden Euro in der DACH-Region. Deutschland trägt dazu demnach 15,20 Milliarden Euro bei (Abbildung 10).

Abbildung 10: Szenario 2, erwartetes Wachstum

Penetrationsraten für den Eigenschadenteil an der Deckung am Ende des 20-jährigen Betrachtungszeitraums:

Private Haushalte
35—40 %

Kleingewerbe
(bis 5 Millionen Euro Umsatz)
45—50 %

Mittelstand
(bis 100 Millionen Euro Umsatz)
55—60 %

Industrie
(ab 100 Millionen Euro Umsatz)
70—75 %

Penetrationsraten für den Fremdschadenteil an der Deckung am Ende des 20-jährigen Betrachtungszeitraums:

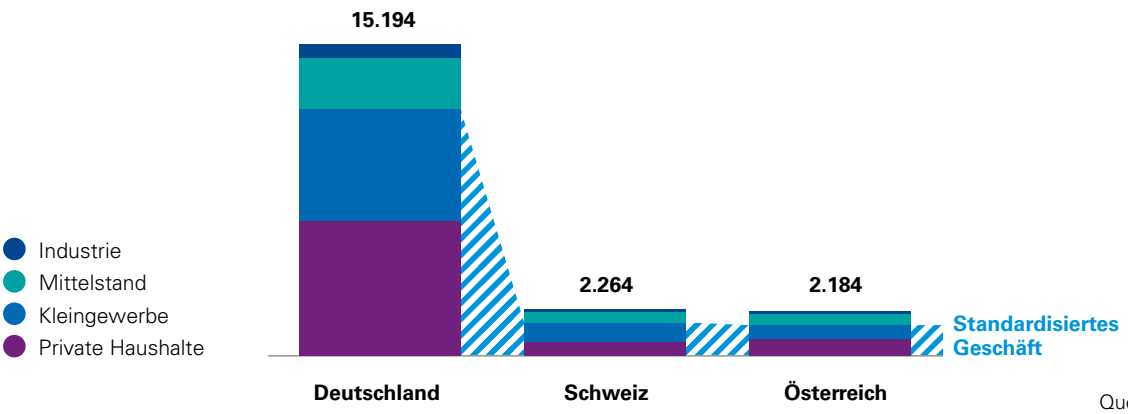
Private Haushalte
15—20 %

Kleingewerbe
(bis 5 Millionen Euro Umsatz)
40—45 %

Mittelstand
(bis 100 Millionen Euro Umsatz)
45—50 %

Industrie
(ab 100 Millionen Euro Umsatz)
65—70 %

Prämienvolumen Cyber-Versicherung 2036 in der DACH-Region
Bruttoprämie, Jahresendbestand, in Millionen Euro



Quelle: KPMG, Deutschland, 2017

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Szenario 3:
Bereitschaft zur Absicherung von Cyber-Risiken entwickelt sich stärker als erwartet

Dieses eher progressive Szenario unterstellt, dass sich der Anstieg der Cyber-Kriminalitätsfälle über die Erwartungen hinaus beschleunigt und die Bereitschaft von Unternehmen und privaten Haushalten stärker als erwartet ansteigt, eine Cyber-Versicherung abzuschließen.

Das Prämienvolumen in der Cyber-Sparte wächst in diesem Szenario bis 2036 auf 26,24 Milliarden Euro in der DACH-Region. Der deutsche Anteil daran liegt bei 20,38 Milliarden Euro (Abbildung 11).

Abbildung 11: Szenario 3, starkes Wachstum

Penetrationsraten für den Eigenschadenteil an der Deckung am Ende des 20-jährigen Betrachtungszeitraums:

Private Haushalte
55—60 %

Kleingewerbe
(bis 5 Millionen Euro Umsatz)
55—60 %

Mittelstand
(bis 100 Millionen Euro Umsatz)
70—75 %

Industrie
(ab 100 Millionen Euro Umsatz)
80—85 %

Penetrationsraten für den Fremdschadenteil an der Deckung am Ende des 20-jährigen Betrachtungszeitraums:

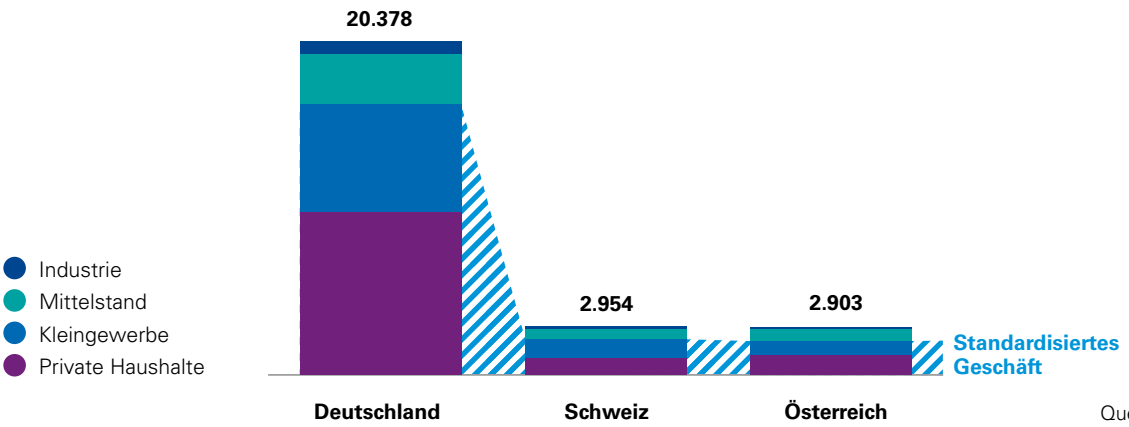
Private Haushalte
25—30 %

Kleingewerbe
(bis 5 Millionen Euro Umsatz)
45—50 %

Mittelstand
(bis 100 Millionen Euro Umsatz)
55—60 %

Industrie
(ab 100 Millionen Euro Umsatz)
70—75 %

Prämienvolumen Cyber-Versicherung 2036 in der DACH-Region
Bruttoprämie, Jahresendbestand, in Millionen Euro



Quelle: KPMG, Deutschland, 2017

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

„Es gibt zwei Arten von Unternehmen: Die, die wissen, dass sie gehackt wurden und die, die es noch nicht wissen."

Dr. Georg Bräuchle,
Chief Market Officer und Geschäftsführer
der Marsh GmbH

Zentrale Erkenntnisse aus der Anwendung des KPMG-Cyber-Prämienmodells

- **Die Versicherungssparte Cyber kann Kraftfahrt im Laufe der kommenden 20 Jahre als volumenstärkste Schaden-/Unfallsparte im deutschen Versicherungsmarkt ablösen.**
- **Das jährliche Prämienvolumen der Cyber-Sparte wird bis 2036 auf etwa zwölf Milliarden Euro (Low Case), auf über 20 Milliarden Euro (Average Case) bzw. auf bis zu 26 Milliarden Euro (High Case) ansteigen.**
- **In allen Cyber-Kundensegmenten wird es starkes Wachstum geben; der mit deutlichem Abstand größte Anteil der zukünftigen Cyber-Prämien, dies haben alle drei Szenarien bestätigt, wird auf private Haushalte und kleinere Unternehmen entfallen.**
- **Das „standardisierte Geschäft" (siehe Abbildung 12) wird 2036 für bis zu 78 Prozent des Cyber-Marktes stehen.**
- **Der Cyber-Markt entwickelt sich von oben nach unten, das heißt zuerst kaufen große Industrieunternehmen Cyber-Deckungen, dann der Mittelstand und große Gewerbeunternehmen, später dann zieht der Absatz bei kleineren Gewerbebetrieben und privaten Haushalten an. Das heißt auch, dass wir eine Entwicklung von hochgradig individuellen Lösungen hin zu einem maximal standardisierten Massengeschäft erleben werden.**
- **Es wird zwei Hauptelemente des Cyber-Versicherungsgeschäftes geben: Deckungen für Eigen- und Deckungen für Fremdschäden. Auch wenn man der Versuchung erliegen könnte, diese Teile einfach der Sach- bzw. Haftpflichtversicherung zuzuordnen, erscheint uns dies aus fast allen Aspekten dieses anspruchsvollen Geschäfts als nicht zielführend. Als Vorbild zur Strukturierung sehen wir die Kraftfahrtversicherung mit einem Kasko- und einen Haftpflichtteil. Wir erwarten, dass sich die Marktdurchdringung bei den Deckungen für Eigenschäden schneller vollzieht als bei denen für Fremdschäden.**

Kurz: Unserem Modell nach wird die Nachfrage nach Cyber-Versicherungen stark ansteigen. Wer von diesem neuen Geschäftsfeld in welchem Umfang profitieren wird, hängt allerdings stark davon ab, mit welcher Ernsthaftigkeit sich die Marktteilnehmer mit dem Thema befassen.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Selbst Szenario 3 kann übertroffen werden

Alle drei Szenarien zeigen gleichermaßen, dass das Segment der kleineren Unternehmen mit bis zu fünf Millionen Euro Jahresumsatz sowie das Segment der privaten Haushalte bis 2036 den deutlich am stärksten wachsenden Teil des Cyber-Versicherungsmarkts bilden werden.

Es ist durchaus vorstellbar, dass sogar Szenario 3 in der Praxis noch übertroffen wird, da Cyber-Schäden zu einem Phänomen werden könnten, das die meisten Menschen regelmäßig betreffen wird. In diesem Fall wird die Zahl der privaten Haushalte mit Cyber-Versicherungsschutz vermutlich deutlich höher als die in Szenario 3 unterstellten 55 Prozent bei Eigenschadendeckung und 25 Prozent bei Fremdschadendeckung liegen. Im Vergleich haben die Hausrat- bzw. die Privathaftpflichtversicherung heute höhere Penetrationswerte aufzuweisen.

Gleiches gilt für die Gewerbe- und Industriekunden. Auch hier sind höhere Penetrationsraten als die in Szenario 3 angenommenen vorstellbar, falls sich Cyber-Risiken in den nächsten beiden Jahrzehnten zu einem generell bilanzgefährdenden Risiko entwickeln sollten.

Unterschiede innerhalb des deutschsprachigen Raums

Im Vergleich der drei Länder Deutschland, Österreich und Schweiz wird sich die Cyber-Versicherung unserer Überzeugung nach weitestgehend parallel entwickeln. Die unterschiedlichen Volumina mit Blick auf das Jahr 2036 spiegeln im Wesentlichen die unterschiedliche Größe der Kennziffern der jeweiligen Länder wider, nicht aber eine unterschiedliche Risikosituation oder ein erwartetes anderes Versicherungseinkaufsverhalten der Kunden.

Zu den Märkten Österreichs und der Schweiz gibt es jeweils eine auffällige Besonderheit: In der Schweiz erwarten wir ein um etwa zehn Prozent höheres Prämienniveau bei gleichem Deckungsumfang, was auf die im Vergleich höheren Kosten für Dienstleistungen jeder Art in diesem Markt zurückzuführen ist. Das Schweizer Cyber-Prämienvolumen lag Anfang 2016 bei etwa vier Millionen Euro. In Österreich verläuft die Entwicklung des Cyber-Versicherungsangebots etwas langsamer als in den beiden anderen Ländern, aber alle namhaften Versicherer wollen binnen drei Jahren entsprechende Angebote im Markt haben. Wir erwarten daher, dass dieser Markt zu Deutschland und der Schweiz aufschließen wird. Das österreichische Cyber-Prämienvolumen lag Anfang 2016 bei etwa drei Millionen Euro.

„Für Unternehmen wird eine Cyber-Versicherung zukünftig ein elementarer Bestandteil des Risikomanagements werden. Dies betrifft nicht nur ‚digitale' Branchen, sondern ist vielmehr eine branchenübergreifende Tendenz. Wir sehen daher ein erhebliches Wachstumspotenzial für den Cyber-Versicherungsmarkt in Österreich und CEE."

Robert Haider,
Geschäftsführer Vienna International Underwriters GmbH

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

„Die Cyber-Versicherung hat enormes Potenzial und gehört in absehbarer Zeit in jedes gut sortierte Produktsortiment eines Versicherers. Diese Sparte bedarf allerdings einiger neuer Fähigkeiten, insbesondere im Bereich von Produktgestaltung und Pricing, aber auch bei der Schadenregulierung."

Ralf Knispel,
Abteilungsleiter Cyber-Versicherung,
ERGO Versicherung AG

Marktwachstum in drei Phasen

Unabhängig vom gewählten Szenario erwarten und differenzieren wir bei der Marktentwicklung bis 2036 drei Marktwachstumsphasen:

Phase 1: Beginnende Nachfrage nach Produkten; trotz geringen Angebots kann die Nachfrage gedeckt werden; teilweise extrem hohe Wachstumsraten von über 100 Prozent aufgrund des kleinen Marktes

Phase 2: Etablierung der Sparte; höhere Bekanntheit und Akzeptanz; starker und sprunghafter Anstieg der Nachfrage

Phase 3: Gemäßigtes Wachstum; Cyber-Sparte ist voll etabliert; Nachfrage ist größtenteils gesättigt; der Markt wächst weiter, jedoch mit moderateren Wachstumsraten

Aktuell befinden wir uns in Phase 1. Wir gehen davon aus, dass Phase 2 in den nächsten fünf bis zehn Jahren erreicht werden könnte. Szenario 1 geht hier tendenziell vom unteren Rand der Phasendauer aus, die anderen beiden eher vom oberen. Wie schnell Phase 2 erreicht wird, hängt davon ab, wie sich das Risikobewusstsein für Cyber-Bedrohungen entwickelt – auch abhängig von spektakulären Schadenfällen, Verminderung von Kulanzzahlungen, staatlicher Förderung etc.

3.5 Kundensegmente in der Cyber-Versicherung und Cyber-Versicherung als standardisiertes Massenprodukt

Paradigmenwechsel steht bevor

Noch sind Cyber-Versicherungen in Deutschland ein Thema, welches sich fast ausschließlich in der Industrie und dem Großgewerbe abspielt. Allerdings scheint es 2016 bei den Unternehmen zu einem Paradigmenwechsel zu kommen: Aus einem exotischen Thema wird ein Pflichtprogramm für das Management.

Marktweit wird von einem deutlichen Anstieg bei den Angeboten und Abschlüssen von Cyber-Risiko-Deckungen für größere Unternehmen berichtet. Gleichzeitig schildern insbesondere Risikospezialisten, Forensiker und andere Akteure aus dem Cyber-Dienstleistungssegment einen sprunghaften Anstieg der Nachfrage. Unser Eindruck ist, dass die Auseinandersetzung mit Cyber-Risiken bei größeren Unternehmen unabdinglich wird. Auch für mittelgroße Unternehmen scheint der Markt in Bewegung zu kommen. Auf dieses Segment spezialisierte Makler sprechen von einem schlagartigen Anstieg von angeforderten Angeboten und bei Abschlüssen.

Kleingewerbe und private Haushalte unterscheiden sich deutlich von dem Cyber-Geschäft mit Unternehmen

Das Kleingewerbe und private Haushalte sind vom Grundsatz her den gleichen Cyber-Risiken ausgesetzt wie die mittleren und

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Abbildung 12: Kundengruppen Cyber-Versicherung

Quelle: KPMG, Deutschland, 2017

großen Unternehmen. Allerdings unterscheidet eine Reihe von Aspekten dieses Segment signifikant von dem der mittleren und großen Unternehmen:

- Das Bewusstsein für Cyber-Risiken und die Qualität der ergriffenen Schutzmaßnahmen bleiben weit hinter dem Top-Segment zurück.
- Dieses Marktsegment existiert aus Sicht der Versicherer in Deutschland bisher so gut wie nicht. Es gibt daher keinerlei Vergangenheitserfahrung. Bei dem Top-Segment gibt es zumindest schon eine gewisse, wenn auch noch sehr überschaubare Erfahrung.
- Die Wirtschaftskraft der potenziellen Versicherungsnehmer in diesem Segment ist deutlich geringer als bei Mittelstand und Industrie. Die Bereitschaft, größere Summen in die Risiko-Prävention zu investieren, ist insofern begrenzt.
- Die Prämienhöhe pro Cyber-Versicherungsvertrag ist für sich gesehen in diesem Segment deutlich geringer. Individuelle Lösungen sind insofern wirtschaftlich kaum tragbar, maximale Standardisierung ist Pflicht.

Wandel im Kleingewerbe und bei privaten Haushalten kündigt sich an

Nicht nur ein Blick auf den Cyber-Markt in den USA legt nahe, dass dieses Kundensegment auch in Deutschland zeitnah in Bewegung kommen wird. Dafür spricht auch, dass die Angriffe auf kleinere Unternehmen und private Haushalte deutlich zunehmen. Die Wahrnehmung der Bedrohung durch Cyber-Risiken ist also für dieses Segment nur eine Frage der Zeit. Damit gehören auch diese Kundengruppen in eine Cyber-Zukunftsbetrachtung und zu den von uns zur Modellbetrachtung unterschiedenen Kundensegmenten.

Den Bedarf an Versicherungsschutz haben alle vier Segmente gemein. Die spezifische Ausprägung unterscheidet sich allerdings signifikant von Segment zu Segment: Während es für größere Unternehmen auch in Zukunft individuelle Cyber-Lösungen geben wird, ist dieser Aufwand schon für mittelgroße Unternehmen wirtschaftlich nicht ohne Weiteres darstellbar. Der Markt arbeitet daher mit vorkonfigurierten Lösungen, also mit Deckungsangeboten, die einem gewissen Grundstandard folgen und für den einzelnen Kunden individualisiert werden.

Bei kleineren Unternehmen und für private Haushalte ist der erzielbare Deckungsbeitrag pro Einzelvertrag deutlich geringer und damit steigt der Anspruch an Standardisierung und Automatisierung. Wir unterscheiden aus Cyber-Produktsicht deswegen drei Segmente:

1. Individuelle Versicherungslösungen
2. Vorkonfigurierte Versicherungsprodukte
3. Standardisierte Versicherungsprodukte

Cyber-Schutz für private Haushalte und Kleingewerbe

Um das Cyber-Geschäft mit kleineren Unternehmen und privaten Haushalten erfolgreich betreiben zu können, muss es

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

„Wir bei Hiscox sehen Cyber wie folgt gekennzeichnet: Zeitkritisch, kompliziert, hohe Einzel- wie auch Kumulexposure, aktuarielles Pricing in neuer Dimension, hochanspruchsvolle Schadenregulierung. Kurz: Diese Sparte ist nicht geeignet für einen ‚semiprofessionellen' Ansatz."

Robert Dietrich,
Hauptbevollmächtigter Hiscox Deutschland,
Hiscox Partner

dem Versicherer gelingen, in allen relevanten Wertschöpfungsschritten maximal automatisiert zu arbeiten. Dies kann zu einem schwierigen Spagat werden: Auch in dem unteren Segment ist eine individuelle Risikoprüfung sowie eine spezifische Preisfindung erforderlich. Zudem sind Schäden zu regulieren, die in ihrer Höhe weniger durch eine Geldleistung zum Ausgleich von Sach-, Betriebsunterbrechungs- und Fremdschäden, sondern vielmehr durch Schadenmanagement und -regulierungskosten bestimmt werden.

In diesem Segment ist es erfolgskritisch, Risikobewertung, Risiko-Prävention, Preisfindung und das Case Management stark standardisiert und automatisiert abzuwickeln. Dies erfordert technische Lösungen, wie es sie nach unserer Wahrnehmung heute noch nicht am Markt gibt. Diese technische Lösung gilt es mit Partnernetzwerken von Spezialisten zu kombinieren – und auch die gibt es nicht „von der Stange".

Wie unser Cyber-Marktmodell zeigt, erwarten wir langfristig das deutlich größte Cyber-Versicherungsvolumen genau in diesem Kundensegment. Unterstellt man beispielsweise, dass ein Haushalt (nicht die Einzelperson) eine nach heutigen Maßstäben umfassende Deckung aller sinnvollerweise in Frage kommenden Eigen- und Fremdschadenkomponenten in einem Cyber-Versicherungsvertrag abdeckt, müsste die Jahresprämie hierfür heute bei 150–200 Euro liegen. Dabei würden einige vorstellbare Deckungskomponenten, wie etwa der Ausfall von Arbeitsfähigkeit (als Folge von Reputationsschäden) noch nicht eingepreist sein. Die Weiterentwicklung der Vernetzung unserer Welt und infolgedessen der Cyber-Produkte sowie die absehbare generelle Zunahme an Schäden bei privaten Haushalten führen nach unserer Erwartung zu einem Anstieg der Cyber-Jahresprämie pro versichertem Haushalt auf eine Größenordnung von 400–800 Euro im Jahr 2036.

Die Versuchung könnte demnach groß sein, den technischen Hürden in fast schon traditioneller Manier durch manuelle „Work Arounds" zu begegnen. Dieses Vorgehen erscheint jedoch nicht erfolgversprechend. Gerade in diesem Segment werden Versicherer einige Anstrengungen unternehmen müssen und entweder selbst geeignete Lösungen aufbauen oder aber einen Partner finden, der ihnen einen wesentlichen Teil dieser Aufgaben abnimmt.

Für alle Kundensegmente gilt die in Kapitel 3.3 beschriebene, grundsätzlich sehr ähnliche Struktur, die nach Eigenschäden, Identitätsdiebstahl, Zahlungsmittelbetrug, Betriebsunterbrechung/Arbeitsunfähigkeit sowie Drittschäden differenziert. Auch bei der Bepreisung sind wir dieser Logik gefolgt. Bei den Deckungsformen, die im deutschen Markt heute noch nicht üblich sind, haben wir die Tarifierungswerte aus anderen Märkten, insbesondere aus den USA, herangezogen. Weiterhin gibt es Deckungselemente, die sich aus dem technischen Fortschritt ergeben werden – Stichwort: Connected Car, Smart Home – aber bis heute in keiner uns bekannten Tarifierungslogik abgebildet werden. Hier haben wir mit Annahmen gearbeitet.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

3.6 Kritische Skills zum Handling von Cyber-Risiken und Cyber-Versicherung

Expertise und technische Voraussetzungen gefragt

Es ist keineswegs trivial, in das Geschäft der Cyber-Versicherung einzusteigen: Von der Risikobeurteilung, den technischen und organisatorischen Maßnahmen zur Risikoreduktion über die professionelle Gestaltung und Bepreisung von Deckungen bis hin zur Abwicklung von Schäden ist im Cyber-Geschäft alles neu.

Expertise ist gefragt – vor allem in den Handlungsfeldern Risikobewertung/Risiko-Prävention, Produktentwicklung/Underwriting/Vertrieb und Schadenregulierung bzw. Case Management. Neben den besonderen, aus fachlicher Sicht erforderlichen Kompetenzen ist ebenfalls zu berücksichtigen, dass für den erfolgreichen Betrieb der Cyber-Versicherungssparte spezielle technische Voraussetzungen zu erfüllen sind.

Wie in Abbildung 13 dargestellt sollten die Versicherer im Einzelnen Cyber-Know-how insbesondere mitbringen für:

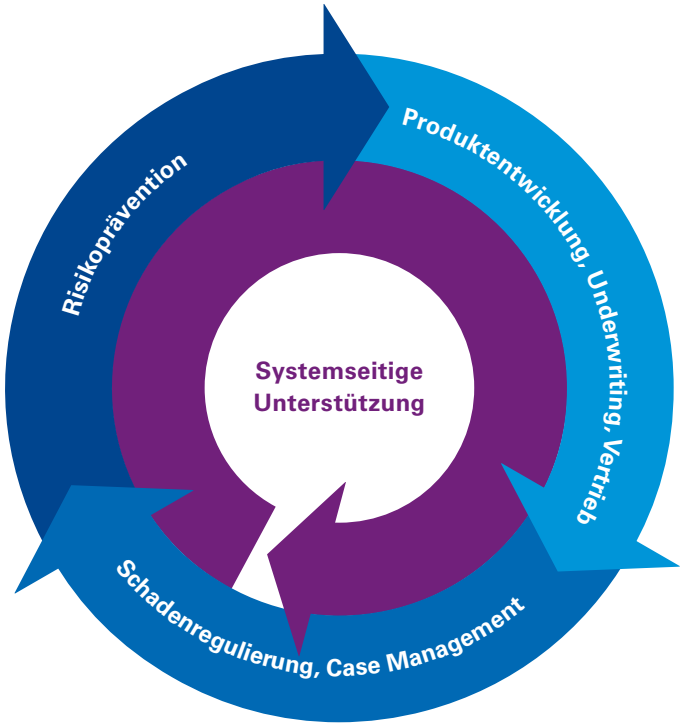
- Risiko-Prävention: Ähnlich der Feuer-Industrieversicherung ist eine Underwriting-Entscheidung in der Cyber-Sparte ohne ein zuverlässiges Bild von der individuellen Bedrohungslage für das zu versichernde Risiko kaum vorstellbar. Entsprechend sind Maßnahmen zur Risiko-Prävention zwischen dem Versicherer und dem Versicherungsnehmer zu vereinbaren.
- Produktentwicklung/Underwriting/Vertrieb: Hier steht die aktuarielle Berechnung eines risikoadäquaten technischen Preises im Fokus.
- Schadenregulierung/Case Management: Wichtig ist hier das Verständnis, dass die Schadenbearbeitung einen starken Fokus im Bereich des Case Management bzw. der Assistance Services im Schadenfall aufweist, dass eine schnelle Reaktionszeit kritisch ist und dass die Leistungen entweder selbst durch den Versicherer abzubilden oder über Partner einzukaufen sind.

Handlungsfeld 1: Risiko-Prävention

Ähnlich der Feuer-Industrieversicherung gehört an den Anfang der Befassung mit Cyber-Risiken die Ermittlung und Analyse der vorliegenden Bedrohungslage – ein anspruchsvolles Unterfangen, da sich diese Bedrohungslage im Markt, aber auch auf das einzelne Risiko bei den Unternehmen bzw. privaten Haushalten sehr schnell ändern kann. Dahinter können technische Veränderungen ebenso wie taktische Varianten der Cyber-Kriminellen stehen.

Die daraus resultierende Dynamik muss bei der Einschätzung der Risikosituation und dem Entwurf von Abwehrstrategien berücksichtigt werden. Wir haben es bei einem Cyber-Angriff nicht wie bei einem Brand mit über Jahrzehnten vom Grundsatz her gelernten Schadenentstehungs- und -entwicklungsmustern zu tun. Vielmehr stehen wir Kriminellen gegenüber, die mit immer raffinierteren Strategien immer bessere technische

Abbildung 13: Skill-Set für den Umgang und die Versicherung von Cyber-Risiken



Quelle: KPMG, Deutschland, 2017

Instrumente einsetzen. Es ist ein Wettlauf gegen den Fortschritt der schadenstiftenden Technik und gegen die kriminelle Intelligenz der aus dem Hinterhalt operierenden Angreifer.

Ein neuer Markt entsteht

Folgerichtig hat Cyber-Prävention, worunter wir alle technischen, organisatorischen und schulischen Maßnahmen zum Schutz gegen Cyber-Risiken verstehen, in den vergangenen Jahren enorm an Bedeutung gewonnen. Mit Blick auf die in Zukunft deutlich verschärfte Bedrohungslage dürfte sich das Feld der Cyber-Prävention dynamisch weiterentwickeln und einen interessanten neuen Markt für Cyber-Sicherheits-Spezialisten entstehen lassen.

Der Cyber-Sicherheitsmarkt unterteilt sich im Wesentlichen in drei Felder:

- Software-Lösungen: Virenschutz, Firewalls, VPN-Lösungen etc.
- Hardware-Lösungen: Hardware-Firewalls, externe Festplatten als Back-up etc.
- Dienstleistungen: Sicherheitsanalysen, Trainings, Zertifizierungen, Entwicklung von technischen bzw. organisatorischen Sicherheitsstandards etc.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Der Markt für Cyber-Risiko-Prävention wurde für Deutschland in einer Bitkom-Studie für 2015 auf insgesamt 3,7 Milliarden Euro geschätzt, wovon mit 2,9 Milliarden Euro etwa 78 Prozent auf Dienstleistungen entfallen dürften. Als Ursachen für den hohen Anteil von IT-Sicherheitsdienstleistungen und Software kann eine zunehmende Vernetzung und die damit einhergehende wachsende Komplexität von IT-Sicherheitsgütern genannt werden. Diese fordert spezialisierte Software und Dienstleistungen für intelligente IT-Sicherheitslösungen.

Das Wachstum des deutschen Marktes für Cyber-Risiko-Prävention liegt bei ca. zehn Prozent jährlich (Tabelle 3).

Aufrüstung privater Haushalte

Der hiervon auf private Haushalte entfallende Teil ist mit 224 Millionen Euro vergleichsweise gering. Das liegt insbesondere daran, dass der überwiegende Teil der privaten Haushalte sich bisher auf kostenfreie Virenschutzprogramme verlässt oder gar keinen Virenschutz installiert hat (Tabelle 4).

Tabelle 3: Umsatz des Marktes für Cyber-Risiko-Prävention

in Milliarden Euro	2014	2015
Markt für Software und Services zur Verbesserung der IT-Sicherheit	3,5	3,7
Dienstleistungen	2,7	2,9
Identitäts- und Zugriffsverwaltung	0,2	0,2
Netzwerksicherheit	0,1	0,1
Endgerätesicherheit	0,3	0,3
Web-, Nachrichten- und Datensicherheit	0,2	0,2

Quelle: Bitkom, 2015

Tabelle 4: Cyber-Prävention in privaten Haushalten

	in Prozent	in Euro
Anteil Haushalte ohne Virenschutz (%)	17	
Anteil Haushalte mit kostenlosem Virenschutz (%)	61	
Anteil Haushalte mit kostenpflichtigem Virenschutz (%)	22	
Durchschnittliche Kosten je Haushalt pro Jahr in Euro		25
Ausgaben privater Haushalte in Millionen		224

Quelle: Bitkom, 2015

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Einen völligen Verzicht auf Virenschutz bei privaten Haushalten werden wir in Zukunft vermutlich kaum noch erleben, auch dürfte der Anteil kostenpflichtig bezogener Virenschutzprogramme stark ansteigen. Der deutsche Markt für Cyber-Sicherheits-Software für private Haushalte wird in den nächsten Jahren stark wachsen.

Auch die Vorzeichen bei den Ausgaben der Unternehmen für Cyber-Präventionsmaßnahmen stehen auf Wachstum, wobei insbesondere größere Unternehmen den Umgang mit Cyber-Risiken mittlerweile ernsthaft angehen.

Kleingewerbe und Mittelstand hängen zurück

Ähnlich stellt sich das Bild bei kleineren Unternehmen mit zehn bis 99 Mitarbeitern dar. Nach Auskunft des Cyber-Sicherheits-Providers Kaspersky investieren diese Unternehmen im Schnitt lediglich 27 Euro pro Mitarbeiter und Jahr, was dem durchschnittlichen monatlichen Taschengeld pro Kind in Deutschland entspricht.

Nicht viel höher ist die Investitionsbereitschaft bei mittelgroßen Unternehmen zwischen 100 und 999 Mitarbeitern. Laut Kaspersky liegt die durchschnittliche jährliche Investition hier bei 38 Euro pro Mitarbeiter und Jahr. Erst bei größeren Unternehmen mit mehr als 1.000 Mitarbeitern steigt die Investition auf 110 Euro pro Mitarbeiter und Jahr.

„Unternehmen fehlt die Transparenz und Balance bezogen auf das jeweilige Cyber-Risk Exposure. Es ist häufig unklar, wie viel Angriffsflächen die Unternehmen selbst oder über im Rahmen der Digitalisierung zunehmend vernetzter Dienstleister oder Partner bieten.“

Dr. Michael Falk,
Partner, Security Consulting,
KPMG AG Wirtschaftsprüfungsgesellschaft

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Exkurs
Cyber Security bei KPMG: Prävention im Firmenkundenbereich

Cyber-Risiken sind für Unternehmen häufig schwer greifbar und damit auch nur bedingt vermeidbar: Häufig fehlen Einblicke in die Motivation potenzieller Angreifer ebenso wie ein realistisches Bild der aktuellen Verwundbarkeit des Unternehmens.

Vielfältige potenzielle Ziele

Der Weg zu einer effizienten Cyber-Abwehr führt aber immer über eine intensive Beschäftigung mit der eigenen Risikoposition: Was muss in jedem Fall geschützt werden? Dabei gilt es, breit zu denken. Know-how über Prozesse und Verfahren sowie geistiges Eigentum aus Forschung und Entwicklung können ebenso angegriffen werden wie Kundendaten, Angebotskalkulationen für Großprojekte oder Einkaufskonditionen. Auch der Ausfall von Produktion oder Logistik kann erhebliche Schäden verursachen – angefangen mit der reinen Betriebsunterbrechung bis hin zu Vertrags- bzw. Konventionalstrafen bei Nichterfüllung vertraglicher Verpflichtungen.

Eigene Schwachstellen analysieren

Die Verwundbarkeit des Unternehmens lässt sich aus den tatsächlichen oder vermuteten Schwachstellen in der IT-Landschaft ableiten. Die größten Fehler lassen sich über fünf zentrale Maßnahmen adressieren:

1. Übersicht über die eingesetzten Softwarekomponenten im Unternehmen (application whitelisting): Sobald das Unternehmen die Kontrolle über die installierten Komponenten verliert, ist die Installation von Malware ein Kinderspiel.

2. Standardisierte und nach Herstellervorgaben und durch Experten gesicherte Konfigurationen definieren und umsetzen.

3. Regelmäßige Aktualisierung der eingesetzten Anwendungs- und Systemsoftware und umgehende Installation neuer Sicherheits-Patches.

4. Minimierung der privilegierten Berechtigungen, insbesondere für externe Zugriffe zu Wartungszwecken: Sie sind ein beliebtes Einfallstor für Angreifer. Anders gesagt: Wenn ein dem Unternehmen unbekannter Nutzer aus China mit administrativen Rechten Daten aus Forschung und Entwicklung einsehen kann, kann etwas nicht stimmen.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

5. Implementierung mehrstufiger Sicherheitsperimeter zur Absicherung von Netzwerkverbindungen und Datenverkehr (Firewall, DMZ, Proxy, Malware-Protection).

Stärkung der Widerstandsfähigkeit

Der Trend geht dabei weg von immer mehr präventiven Maßnahmen hin zur Stärkung der Widerstandsfähigkeit von Unternehmen. Dazu sollten Anomalien in den IT-Systemen auf Basis von Log- und Statusinformationen ausgewertet werden. Anschließend sollte zeitnah und zielgerichtet auf diese Veränderungen reagiert werden.

Damit die Sicherheitskonzeption langfristig wirksam bleibt, sollten Unternehmen ihr Risikoprofil regelmäßig aktualisieren, die Bedrohungslage einschätzen (Cyber-Threat-Radar) und die eigenen Systeme auf Schwachstellen prüfen. Das Wichtigste dabei sind klar geregelte Verantwortlichkeiten mit der notwendigen Rückendeckung durch das Management (Management Commitment).

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Es fällt auf, dass der Markt für Cyber-Risiko-Prävention schon deutlich reifer ist als der Markt für Cyber-Versicherungsdeckungen. 2015 standen 3,7 Milliarden Euro Ausgaben für die Risiko-Prävention einer Cyber-Versicherungsprämie von gerade einmal 30 Millionen Euro gegenüber.

Die Services und Produkte zur Cyber-Risiko-Prävention gehören nicht zum eigentlichen Kerngeschäft eines Versicherers. Es ist aus unserer Sicht aber unabdinglich, dass im Cyber-Markt aktive Versicherungsunternehmen sich intensiv mit aktuellen Entwicklungen, Marktteilnehmern, Leistungen und Services der Cyber-Risiko-Prävention auseinandersetzen. Nur so können sie sich im Rahmen des Underwriting auf ausreichende Sicherungsstandards verlassen, die in der Lage sind, das Residualrisiko kontrollierbar zu machen und angemessen zu preisen.

An dieser Stelle sei bereits festgehalten, dass Versicherer in den Cyber-Sicherheits-Dienstleistern vermutlich sehr nützliche Partner haben, und zwar sowohl in Fragen der Risikoeinschätzung als auch bei der Bewältigung komplexer Schadenfälle.

Handlungsfeld 2: Produktentwicklung/Underwriting/Vertrieb

Aufgrund fehlender Schadenerfahrung ist es eine Herausforderung für Versicherer, eine angemessene Prämie für neue Cyber-Produkte zu berechnen. Die Ermittlung eines „technischen Preises" gestaltet sich ohne Schadenhistorie traditionell sehr schwierig.

Cyber-Risiken sind in Deutschland erst seit wenigen Jahren in das Bewusstsein einer breiteren Öffentlichkeit getreten. Wesentliche Ereignisse waren unter anderem die NSA-Affäre Ende 2013, der Hack des Mobiltelefons von Bundeskanzlerin Angela Merkel sowie der Angriff auf den Deutschen Bundestag 2015.

Bisher gibt es auch noch keine statistisch verwertbaren Schadendaten zu den in Deutschland bereits bestehenden Cyber-Versicherungen. Versicherer geben an, dass pro Jahr sieben bis zehn Prozent der Cyber-Versicherungsverträge einen Schadenfall haben. Diese Größenordnung deckt sich mit der Einschätzung der in diesem Gebiet tätigen Forensik-Unternehmen.

Zurzeit werden die Prämien primär anhand von Branche, Umsatz, Deckungssummen und Risikosituation kalkuliert. Das Manko der fehlenden Schadendaten versucht man durch eine möglichst breite Diversifizierung der gezeichneten Risiken zu kompensieren. Im Fokus der im Schadenfall bereitgestellten Ressourcen steht meist die Kumulkontrolle.

Ergänzt werden diese Maßnahmen durch eine intensive Marktbeobachtung und einen regelmäßigen Erfahrungsaustausch mit IT-Sicherheitsexperten, damit kommende Risikotrends frühzeitig erkannt werden. Neue technische Erkenntnisse sowie Erfahrungen aus Schadenfällen müssen schnellstmöglich im Underwriting verarbeitet werden. Die mit Cyber-Versicherung betraute Organisation muss schnell lernen – deutlich schneller als in anderen Sparten.

Deckungssummen

Auf dem deutschen Markt soll für einzelne Kunden eine Gesamtkapazität von bis zu 350 Millionen Euro verfügbar sein, wobei die Deckungsstrecke einzelner Versicherer zwischen fünf Millionen und 100 Millionen Euro liegt. Um eine Deckungsstrecke von beispielsweise 200 Millionen Euro darstellen zu können, bedarf es eines Beteiligungskalenders, der eine ganze Reihe von Versicherern umfasst.

Deckungssummen bis zu 300 Millionen Euro

Einige Dax-Unternehmen haben nach unseren Informationen bereits Deckungsstrecken in der Größenordnung von 200 oder 300 Millionen Euro abgeschlossen. Im Mittelstand werden in der Regel Deckungsstrecken zwischen einer und zehn Millionen Euro abgeschlossen, wobei die Wahl der Deckungssumme stark von der Branche des Unternehmens abhängt.

Im Lloyds-Markt stehen für deutsche Risiken zusätzliche Kapazitäten in etwa von der gleichen Höhe zur Verfügung. Diese können sowohl als Co-Insurance als auch in gelayerten Programmen platziert werden.

Für den US-Markt sollte sich die Situation ähnlich darstellen. Neben den nationalen Kapazitäten greift der US-Markt in erheblichen Umfang auf Lloyds zurück.

In einigen großen Schadenfällen (Target, Anthem, Sony) mussten Versicherer bereits Leistungen in der vollen Höhe der Deckung leisten – in diesen Fällen zwischen 60 und 100 Millionen US-Dollar.

Einschätzung der Risikosituation

Für die Steuerung wichtiger Prozesse und Transaktionen über IT und/oder Web sowie zum Schutz vertraulicher oder sensibler Daten müssen zunächst Parameter gefunden werden, um dann eine Kostenschätzung abgeben zu können.

Für sensible Daten sollte am besten auf die Zahl von Datensätzen abgestellt und ein Kostensatz pro Datensatz zugrunde gelegt werden. US-amerikanische Studien gehen von Kosten pro Datensatz von 158 US-Dollar weltweit aus ("$158 is the average cost per lost or stolen record", Ponemon Cost of Data Breach Study 2016, Ponemon Institute June 2016). Der durchschnittliche Schaden liegt nach dieser Studie bei vier Millionen US-Dollar. "To calculate the average cost of data breach, we collect both the direct and indirect expenses incurred by the organization. Direct expenses include engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates."

Für Deutschland beziffert die Studie die Kosten pro Datensatz sogar mit 194 US-Dollar. Diese Summe halten wir aber nach der bisherigen Schadenerfahrung in Deutschland für zu hoch und schätzen die Kosten pro Datensatz in Deutschland auf rund 50 Euro und sehen die durchschnittliche Schadenhöhe bei etwa 750.000 Euro.

Für die Bewertung von Systemausfällen gibt es keine allgemeinen Parameter. Hier muss (ähnlich der Einschätzung eines Feuer-Betriebsunterbrechungsschadens) eine individuelle Betrachtung im Unternehmen stattfinden. Dabei hat sich die folgende Vorgehensweise bewährt:

1. Selektion kritischer Geschäftsprozesse

2. Definition relevanter Parameter für die Störung dieser Prozesse (z. B. vier Wochen Ausfallzeit)

3. Bewertung der finanziellen Folgen von Ausfällen bzw. möglicher Wiederherstellungskosten

4. Bewertung der Wiederherstellungs- und Anlaufkosten.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Exkurse: Cyber-Kumulrisken und Vertrieb

Cyber-Kumulrisiken

Die Vernetzung der IT-Systeme untereinander wird immer größer. Jede Sicherheitsmaßnahme auf einem Gerät erhöht auch die Sicherheit aller anderen Geräte, da die Verteilung von Schadsoftware erschwert wird. Jeder PC, der sicherer wird, reduziert das Gesamtrisiko.

Umgekehrt gilt das natürlich ebenfalls: Durch die voranschreitende Vernetzung entsteht ein erhöhtes Kumulrisiko, etwa durch die breitflächige Ausnutzung einer Sicherheitslücke bei kritischen Systemen (zum Beispiel Microsoft- oder SAP-Systeme etc.). Die Munich Re sieht ein breitflächiges Kumulrisiko, insbesondere beim Ausfall eines der großen Cloud Provider oder etwa bei einem „wide spread virus" (Gespräch mit der Erichsen GmbH am 27. Juni 2016) und hat solche Szenarien modelliert.

Einige Versicherer reduzieren das Kumulrisiko, indem sie als Versicherungsfall nur einen zielgerichteten Angriff versichern wollen. Andere beschränken ihre Kapazitäten für bestimmte Branchen oder insgesamt.

Vertrieb

Cyber-Versicherungen sind für alle Marktteilnehmer zurzeit überwiegend Neuland. Erfahrungen im Vertrieb müssen erst noch gesammelt werden. Neue Begrifflichkeiten kommen hinzu. Die Risikosituation ist komplex. Die Gesprächsinhalte der Vertriebsmitarbeiter mit (potenziellen) Kunden müssen entsprechend angepasst werden.

So neu Cyber-Versicherungen sind – die Situation ist der Assekuranz aber nicht gänzlich unbekannt. So war es auch in anderen Sparten zu Beginn, zum Beispiel bei der D&O-Versicherung in den 90er-Jahren: Strukturell bedarf es keiner separaten Vertriebsorganisation, wie es sie etwa bei Kredit- oder Lebensversicherungen gibt. Soweit Cyber-Risiken als betriebliches Risiko analog der etablierten Sach- oder Haftpflichtrisiken behandelt werden, sollte der Markt mit der bestehenden, allerdings speziell für die Cyber-Risiken und -Versicherungsprodukte geschulten, Vertriebsorganisation bearbeitet werden können.

Aneignen sollten sich interne wie externe Cyber-Vertriebsmitarbeiter aber nicht nur das Vokabular der Cyber-Sparte. Sie müssen lernen, Cyber-Risiken einzuschätzen, passende Versicherungsbausteine zu identifizieren und sie dem Kunden zu erläutern. Dazu können die Versicherer auch auf spezialisierte Makler zurückreifen oder den Vertrieb an sie abgeben.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Handlungsfeld 3: Schadenregulierung/Case Management

Obwohl sich das Feld möglicher Cyber-Schäden vom Grundsatz her in Eigen- und Fremdschäden unterteilen lässt, wäre es ein Trugschluss anzunehmen, dass sich Cyber-Schäden mit dem klassischen Repertoire an Schadenregulierungs-Skills aus der Sach- bzw. Haftpflichtversicherung bearbeiten ließen. Aufgrund der neuen cyberspezifischen Risiken und Schadenarten gibt es wenig Erfahrungswerte hinsichtlich der Schadenregulierung. Welche aktuellen Schadenbilder gibt es? Wie gehen die Versicherer damit um?

Schadenabwicklung

Die Schadenabwicklung als solche bleibt bisher in den Händen des Versicherers, aufgehängt in der Schadenabteilung des Bereichs, der auch für das Underwriting verantwortlich ist. Dort wird die eigentliche Regulierung der wirtschaftlichen Folgen bearbeitet – die Abrechnung der Schäden. Das Case Management, also die technische Aufarbeitung vor Ort oder auch die Beratung in Datenschutzvorfällen, und das Krisenmanagement werden an spezialisierte Beratungs- und IT-Dienstleister ausgelagert. Entweder hat der Versicherer mit solchen Unternehmen ein stabiles Netzwerk aufgebaut oder der Versicherer überlässt die Auswahl des Dienstleisters dem Kunden: In diesen Fällen verfügt der Versicherer aber zumindest über eine Liste von Ansprechpartnern, die der Kunde nutzen kann, wenn er keinen eigenen Provider hat oder findet.

Case Management

Ein professionelles Case Management ist bei Cyber-Schäden von herausragender Bedeutung. Bei der Aufnahme der Schäden muss sehr schnell verstanden werden, was genau passiert ist, und welche Maßnahmen angezeigt sind.

Auf Cyber-Schäden spezialisierte Case Management Services finden sich insbesondere in den folgenden Bereichen:

IT-Forensik

- Aufgabe: Fehlersuche und Fehlerbehebung.
- Von einem Cyber-Schaden betroffene Unternehmen, aber auch Cyber-Versicherer haben häufig präferierte Partnerunternehmen, die sie im Schadenfall zur schnellen Schadenbehebung beim Kunden einsetzen.
- Die Höhe der Schadenkosten hängt entscheidend davon ab, wie schnell IT-Forensik-Dienstleister eingeschaltet werden.

Krisenberatung

- Bei größeren Schadenfällen ist ein professionelles Krisenmanagement notwendig, bei dem alle Handlungsschritte zentral organisiert und gesteuert werden.

„Maßgeblich für die Höhe eines Cyber-Schadens sind häufig ein unmittelbar und professionell umgesetztes Krisenmanagement beim geschädigten Kunden und der unverzügliche Einsatz von Cyber-Forensic-Dienstleistern zur Schadeninvestigation, -behebung und Wiederherstellung der Betriebsfähigkeit."

Michael Sauermann,
Partner, Cyber Forensic,
KPMG AG Wirtschaftsprüfungsgesellschaft

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

– Die Qualität und Professionalität des organisatorischen Krisenmanagements spielen ebenfalls eine wesentliche Rolle dabei, den Schadenherd unverzüglich zu eliminieren.
– Hierzu zählen unter anderem vorab detaillierte und mit allen Verantwortlichen abgestimmte Zuständigkeiten, Routinen und Aktivitäten für einen Krisenfall einschließlich des Einsatzes von externen Spezialisten sowie der internen und externen Krisenkommunikation.

Rechtsberatung

– Cyberspezifische Rechtsberatung ist insbesondere notwendig, um die Pflichten aus Benachrichtigungs- und Compliance-Vorschriften zu erfüllen. Ebenso ist sie Grundlage für die Prüfung und den Umgang mit Schadensersatzansprüchen Dritter.

PR-Beratung

– Bei Schadenfällen mit großem medialen Interesse und dem Risiko eines Reputationsverlusts empfiehlt sich der Einsatz von PR-Beratern, um größeren Schaden für Reputation und Marke zu vermeiden.

Case Management bezieht sich bislang nur auf Cyber-Schäden bei Unternehmen. Für Privatpersonen existieren praktisch keine entsprechenden Angebote.

Auch wenn es sich bei den Cyber-Schadenmanagement-Spezialisten um eine knappe Ressource handelt, gibt es bereits eine Reihe von Dienstleistern, die eng mit Versicherungsunternehmen zusammenarbeiten. Das erforderliche Anforderungsprofil weicht ab von dem der klassischen Call-Center-Mitarbeiter bei Versicherungen. Je nach Schaden sind unterschiedliche Qualifikationen gefragt:

– Spezialisierte Mitarbeiter einer Cyber Claims Management Unit können einige Schäden selbst bearbeiten. Hierunter fallen beispielsweise die Abstimmungen mit den Herausgebern von Kreditkarten im Falle eines Kreditkartenmissbrauchs.
– Externe Spezialisten wie Rechtsanwälte oder Forensiker werden gebraucht, wenn Schadenersatzansprüche an den Versicherungsnehmer gerichtet werden bzw. komplexe, schwer durchschaubare Schadenbilder zu bearbeiten sind.

Claims Management und externe Spezialisten stehen für 60 Prozent der Schadenkosten

Einer Vielzahl von Expertengesprächen folgend schätzen wir, dass 25 bis 30 Prozent der Gesamtschadenkosten auf die eigene Claims Management-Funktion entfallen. Weitere 25 bis 30 Prozent sollten für externe Spezialisten eingeplant werden, während die Entschädigung für am Ende nicht zu verhindernde Sach-, Betriebsunterbrechungs- und Fremdschäden bei, im Vergleich zu anderen Sparten, vergleichsweise geringen 40 bis 50 Prozent der Gesamtschadenaufwände liegen dürfte.

Ein Team mit zwei bis drei forensischen IT-Experten kostet im Schnitt mindestens 4.000 Euro pro Tag. Spezialisierte und internationale Anwaltskanzleien verlangen im Schadenfall etwa 500 Euro pro Stunde. Die Stundensätze von Krisenberatern liegen bei rund 250 bis 350 Euro. Vor diesem Hintergrund wird deutlich, warum sich die Beratungskosten in den uns bekannten Fällen schnell auf sechs- oder siebenstellige Beträge summierten.

Versicherer werden dauerhaft auf externe Experten bei der Schadenregulierung angewiesen sein. Daneben muss es Mitarbeiter geben, die die Deckungsfrage beim Schaden klären, die finanziellen Auswirkungen von Cyber-Schäden einschätzen und die Experten bei der Behebung des Schadens steuern. Solche Mitarbeiter sollten ferner in der Lage sein, zeitnah die Erfahrungen aus der Schadenregulierung mit den Underwritern zu teilen und mit ihnen gemeinsam die Konsequenzen für das Underwriting auszuarbeiten. Sprich: Die Lernkurve muss hier sehr viel steiler sein als für die etablierten Sparten. Dies bedingt einen institutionalisierten ständigen Austausch zwischen den Abteilungen für Schaden und Betrieb. Machbar ist dies nur mit spezialisierten Schadenregulierern, die auch den kontinuierlichen Austausch mit den IT-Forensikern pflegen.

Schadenhistorie

Nach wie vor basiert die Ermittlung der Schadenaufwände zu einem großen Teil auf Expertenwissen. Empirische Auswertungen aus dem In- und Ausland existieren dagegen kaum. Die einzige substanzielle Auswertung versicherter Schäden stammt aus den USA. Die Cyber Claims Study wertet seit 2012 in den USA versicherte und regulierte Schäden aus, indem die Schadenbearbeiter beim Versicherer um anonyme Informationen zu konkreten Schadenfällen gebeten werden (vgl. NetDiligence, 2016).

Der Bericht fasst die Informationen zu bisher 160 sogenannten „data breach insurance claims", also Versicherungsansprüche aus Datenschutzverletzungen zusammen. Davon beinhalten 155 den Verlust sensitiver persönlicher Daten. Nur zwei dieser Schäden hatten eine Betriebsunterbrechung zur Folge.

Geschwindigkeit wird zum Erfolgsfaktor

Noch viel mehr als in den klassischen Versicherungssparten wird der Erfolg eines Versicherers im Bereich der Cyber-Versicherung davon abhängen, wie schnell er auf Veränderungen reagieren kann. Die Veränderungsgeschwindigkeit im Bereich der Digitalisierung und des damit einhergehenden Cyber-Risikos ist so hoch, dass nur eine kontinuierlich lernende Organisation erfolgreich sein kann. Da sich die Risiken permanent weiterentwickeln, muss auch das Know-how zu Deckungen, Auflagen für den Kunden, Schadenhöhen etc. permanent angepasst werden. Für die Versicherungsbranche, die bislang eher in längeren Lernzyklen funktioniert hat, ist dies eine enorme Herausforderung.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Exkurs: Schadenregulierung mit Cyber-Forensic von KPMG

Kommt es zu einem Sicherheitsvorfall in einem Unternehmen, unterstützt der Forensic-Dienstleister bei der professionellen Aufarbeitung des Vorfalls, beim Krisenmanagement und der Wiederherstellung des normalen Geschäftsbetriebs.

Oftmals sehen sich Unternehmen bei Sicherheitsvorfällen großen Schäden ausgesetzt. Neben den Kosten zur Wiederherstellung des Geschäftsbetriebs und der IT-Infrastruktur kommt es durch das Entwenden von Geschäftsdaten oder geistigem Eigentum wie Mitarbeiter- und Kundendaten, Strategiepapieren, Finanzdaten, Rezepturen oder Konstruktionszeichnungen oftmals zu großen Schadensummen.

Im Rahmen einer Cyber-Police wird nach dem Vorfall auch der Cyber-Versicherer Fragen zur Reaktionsfähigkeit des Unternehmens stellen, wobei deren präzise Beantwortung unter Umständen Auswirkungen auf die Deckung des entstandenen Schadens hat.

Wichtig ist, aus jedem Vorfall zu lernen und sich durch Optimierungsmaßnahmen für weitere Angriffe besser aufzustellen. Nicht selten werden im Zusammenspiel zwischen Versicherungsnehmer, Versicherer und externen Forensik-Beratern die Eckpunkte des jeweiligen Vorfalls erörtert und mögliche Schwachstellen identifiziert. Hierbei schafft der Dialog bei allen Beteiligten Transparenz im Hinblick auf die Effektivität der Maßnahmen sowie die Bewertung der Reaktionsfähigkeit.

Unterstützung durch Cyber-Experten

Die zügige und qualifizierte Reaktion auf IT-Sicherheitsvorfälle mit Unterstützung externer Fachleute bereits in der Anfangsphase eines Vorfalls bzw. eines Angriffs ist von entscheidender Bedeutung. Kompetente und erfahrene Dienstleister können die Lage zügig einschätzen und effektive Sofortmaßnahmen zur Eindämmung der Auswirkungen vorschlagen und umsetzen. Im Schadenfall übernehmen Experten die forensische Sicherung und Analyse von Daten, Identifikation von Angriffsvektoren, das Stoppen etwaiger Datenlecks und die Wiederherstellung des Normalzustands sowie die fachgerechte Dokumentation. Abschließende Empfehlungen zur Vermeidung künftiger Vorfälle runden die Aufarbeitung ab.

Beispiel: Hacking-Angriff (sog. „Advanced Persistent Threat", APT)

Ein nicht aktualisierter Webserver war das erste Einfallstor für den Angriff. Mangelhafte Sicherheit bei der Administration von IT-Systemen ermöglichte zudem den Einbruch in das digitale Herz des Unternehmens. Nur durch Zufall wurde der Einbruch entdeckt. KPMG als externer forensischer Dienstleister stand dem betroffenen Unternehmen mit der Erfahrung aus vergleichbaren Fällen bei der koordinierten Aufarbeitung zur Seite. Auch wenn die Angreifer sich in diesem konkreten Fall zuvor bereits einige Zeit unentdeckt im IT-Netzwerk aufhalten konnten, sind die ersten Stunden und Tage kritisch, da die Täter auf Abwehrmaßnahmen reagieren und beispielsweise Spuren verwischen.

Bei APT-Angriffen ist das Verständnis für die eingesetzte Schadsoftware von großer Bedeutung, da diese Aufschluss über Motivation, Ziele und Reichweite des Angreifers zulassen. Im vorliegenden Fall waren mehr als 100 Systeme im Fokus der Untersuchung, und der Schaden belief sich auf mehrere Millionen Euro, einschließlich der Kosten für Betriebsunterbrechung, dem Neu-Aufsetzen betroffener Systeme sowie dem Schadenmanagement. Eine der Untersuchung nachgelagerte Dokumentation sowie konkrete Empfehlungen zur Vermeidung künftiger Vorfälle vervollständigen die Aufarbeitung.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Handlungsfeld 4:
Systemseitige Anforderungen

Schließlich stellt sich die Frage nach der Ausgestaltung der Aufbauorganisation inklusive eines Sourcing-Ansatzes: Über welche technischen Kompetenzen muss ein Versicherer verfügen, um erfolgreich in der Cyber-Sparte zu agieren? Das Cyber-Geschäft ist vor allem vor und nach der Dokumentierung des Versicherungsschutzes (Risikobewertung und Schadenregulierung) deutlich anders als andere Sparten, nicht aber in der klassischen Vertragsverwaltung.

Man könnte nun zu dem Schluss kommen, dass es systemseitig nur geringe spezifische Anforderungen durch die Cyber-Sparte gibt. Doch es reicht nicht, bestehende Produkt-IT-Lösungen aus Sach- und Haftpflicht in einigen wenigen cyberproduktspezifischen Punkten anzupassen und Cyber-Versicherungen und -Schadenfälle dann von bestehenden Systemlösungen verwalten zu lassen – auch wenn es im Einzelfall erfolgreich sein mag.

Für das Gros der uns bekannten Versicherersysteme gilt dies so nicht. Die Cyber-Sparte ist hochdynamisch: Sie wird sich in ihren Deckungselementen und im Pricing schneller als irgendeine andere Sparte verändern. Statt des üblichen Release-Zyklus von zwölf, sechs oder drei Monaten geht es hier um Reaktionszeiten von wenigen Tagen oder gar Stunden. Die Cyber-Sparte stellt drei Anforderungen an Versicherersysteme:

- Selbstlernende Systeme, die ein Maximum an underwriting relevanten Erkenntnissen aus Schadenbildern generieren
- Maximal flexible Schnittstellen zu Partnersystemen
- Produkt-Update-Zyklen eher in Echtzeit als in klassischen Release-Zyklen, um auf laufende Veränderungen der Risikobeschaffenheit und des Absicherungsbedarfs von Kunden eingehen zu können.

Für das individuelle Cyber-Geschäft mit Industriekunden sind Systeme mit diesen Fähigkeiten der berühmte Punkt auf dem „i". Für das Cyber-Massengeschäft im standardisierten Segment ist dies schlicht eine Frage des wirtschaftlichen Überlebens.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Make or Buy?

Der Umgang mit Cyber-Schäden weist ein anderes Bild auf, als wir es aus den traditionellen Versicherungssparten gewohnt sind. Die Behebung von Cyber-Schäden wird maßgeblich bestimmt durch den Einsatz der richtigen Spezialisten, sowohl im Management als auch in der Bearbeitung der Schadenfälle.

Es gibt eine Vielzahl von Spezialisierungen im Kontext von Cyber-Schadenfällen, die Versicherer voraussichtlich nicht selbst werden vorhalten können oder wollen. Der Zugang zu einem gut entwickelten Spezialistennetzwerk wird für Cyber-Versicherer damit von entscheidender Bedeutung sein. Bei den Spezialgebieten Forensik und Krisenmanagement ist dies offensichtlich, aber auch im aktuariellen Bereich werden Versicherer in Zukunft vermutlich auf externe Spezialisten zurückgreifen.

Auch White Label-Einkauf denkbar

Dies kann so weit gehen, dass sich einzelne Versicherer – insbesondere kleine und mittelgroße Unternehmen – die Administration einschließlich Schadenbearbeitung von spezialisierten Dienstleistern „White Label" zuliefern lassen und deren Cyber-Produkte dann über ihre eigenen Vertriebskanäle unter ihrer Marke vertreiben. Eine Reihe von Gesellschaften hat uns in den Marktgesprächen gesagt, dass Cyber-Versicherungen in Zukunft mit Sicherheit zu ihrem Angebot gehören. Sie glauben aber nicht, alle Funktionalitäten für diese neue Sparte selbst aufbauen zu wollen.

Auch für größere Versicherungsgesellschaften, die sich ein Outsourcing der Cyber-Sparte alleine schon aus Gründen ihres Selbstverständnisses so nicht vorstellen können, ist die Zusammenarbeit mit Spezialisten-Netzwerken sowohl wegen der Erweiterung ihrer fachlichen Skills als auch wegen Skaleneffekten sinnvoll – und nicht zuletzt auch wegen der geforderten Reaktionszeiten, die mit einem auf solche Fälle fokussiert arbeitenden Spezialisten-Team verkürzt werden können.

Eine pauschale Empfehlung, welche Fähigkeiten und Kapazitäten ein Versicherer für das Cyber-Geschäft selbst aufbauen und welche er von spezialisierten Dienstleistern hinzukaufen sollte, würde der Unterschiedlichkeit der im Markt agierenden Versicherungsunternehmen nicht gerecht. Wohl aber lässt sich festhalten, dass es eine Reihe spezieller Aspekte im Cyber-Geschäft gibt. Dies gilt insbesondere für den Schadenfall, zu dessen Bewältigung alle Versicherer auf Spezialisten zurückgreifen sollten (Rechtsberatung, Forensik, Krisenmanagement etc.). Für alle anderen cyberspezifischen Fähigkeiten ist abzuwägen, inwieweit sich der Aufbau dieser Skills hausintern lohnt oder ein Dienstleisterangebot attraktiver ist.

Weiterhin gibt es cyber-spezifische Kumulrisiken, die in zweierlei Hinsicht eine Herausforderung für einen Versicherer darstellen: Einerseits gilt es, diese Risiken beim Underwriting sachgerecht zu beurteilen, preislich und im Sinne der eingesetzten Zeichnungskapazität. Andererseits kann ein Massenphänomen auf der Schadenseite sehr schnell zu einer Überlastung der eigenen Schadenabteilung führen. Die Frage von Kumulrisiken ist also auch ein Aspekt, der bei der Abwägung von interner und externer Lösung eine Rolle spielen sollte.

Es ist am Ende eine individuelle Entscheidung, welcher Mix von eigenen Fähigkeiten und externen Dienstleistungen am besten zum eigenen Unternehmen passt. Grundsätzlich sollten Versicherer aber offen sein für die Unterstützung von externen Spezialisten für das Cyber-Geschäft.

Unser Fazit: Investitionen in das Claims Management und das Partnernetzwerk zahlen sich bei der Cyber-Versicherung in zweierlei Hinsicht aus: Einerseits bei den Gesamtkosten eines Schadens, andererseits bei der Kundenzufriedenheit.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Abbildung 14: Abdeckung typischer Cyber-Schadenleistungen über klassische Schaden-/Unfall-Versicherungssparten

	Sach	Haftpflicht	Vertrauens-schaden
Wiederherstellungskosten Daten/Programme	Teilweise Deckung	Keine Deckung	Teilweise Deckung
Benachrichtigungskosten im Datenschutzvorfall	Keine Deckung	Keine Deckung	Keine Deckung
Cyberbedingte Betriebsunterbrechungsschäden	Teilweise Deckung	Keine Deckung	Teilweise Deckung
Kosten für IT-Forensik	Keine Deckung	Keine Deckung	Teilweise Deckung
Kosten für PR-Berater bei Cyber-Vorfall	Keine Deckung	Keine Deckung	Teilweise Deckung
Cyberbezogene Erpressung/Bedrohung	Keine Deckung	Keine Deckung	Keine Deckung
Belohnungsgelder für sachdienliche Hinweise im Erpressungsfall	Keine Deckung	Keine Deckung	Keine Deckung
Diebstahl von Geld oder Vermögenswerten in elektronischer Form	Keine Deckung	Keine Deckung	Teilweise Deckung
Haftpflichtansprüche Dritter aus Datenschutzrechtsverletzung	Keine Deckung	Vollständige Deckung	Keine Deckung
Forderungen der PaymentCard-Industrie	Keine Deckung	Keine Deckung	Keine Deckung
Ansprüche Dritter wegen Persönlichkeitsrechtsverletzungen	Keine Deckung	Teilweise Deckung	Keine Deckung
Ansprüche Dritter aus der Verletzung von Rechten des geistigen Eigentums	Keine Deckung	Teilweise Deckung	Keine Deckung

Keine Deckung — Teilweise Deckung — Vollständige Deckung

Quelle: Dr. Sven Erichsen, 2017

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

3.7 Fachliche und organisatorische Abbildung der Cyber-Versicherungssparte

Alles spricht für eine eigenständige Cyber-Sparte

Das Cyber-Geschäft sollte unserer Meinung nach aufgrund der Vielzahl seiner Besonderheiten als eigene Sparte geführt werden. Die Diskussion hierzu scheint beim Gesamtverband der Deutschen Versicherungswirtschaft noch nicht abgeschlossen zu sein. Allerdings zeichnet sich aus unserer Sicht auch hier die Tendenz zu einer eigenen Cyber-Sparte ab. Hier sind insbesondere die im Folgenden aufgeführten fachlichen und organisatorischen Gründe zu nennen, die dafür sprechen, Cyber-Versicherungen als eigenständige Versicherungssparte zu etablieren.

Unzureichende Abdeckung durch andere Versicherungssparten

Cyber-Risiken werden bisher nur ausschnittsweise und sehr begrenzt über bestehende Haftpflicht-, Sach- oder Vertrauensschaden-Versicherungen abgedeckt (siehe Abbildung 14). Der Versicherungsschutz für Cyber-Risiken in diesen Sparten ist nach unserer Auffassung unzureichend, da

- die Versicherungsfalldefinition Cyber-Vorfälle nicht erfasst,
- genannte Ausschlüsse einschlägig sind und
- im Schadenfall häufig mehrere Versicherer zu involvieren wären.

Sachversicherungen

Sachversicherungen (Feuer, Elektronik- oder Maschinenversicherungen etc.) gehören zu den Standardversicherungen von Unternehmen. Insbesondere auf eine Feuerversicherung kann kein Unternehmen verzichten. In allen Sachversicherungen wird der Versicherungsfall als ein Sachschaden definiert, das heißt der Versicherer entschädigt nur, wenn Sachen durch Eingriff in die Sachsubstanz zerstört oder beschädigt werden (siehe beispielsweise § 1 Abs. 1 Allgemeine Bedingungen für die Feuerversicherung [AFB 2010] Version 01.04.2014 GDV 0100).

Fazit: Ein Cyber-Vorfall stellt in der Regel keinen Eingriff in die Sachsubstanz dar. Diese Vorfälle sind Vermögens- und keine Sachschäden. Unter den Sachversicherungen besteht ohne Weiteres kein Versicherungsschutz.

Haftpflichtversicherungen

Haftpflichtversicherungen bieten Versicherungsschutz für gesetzliche Schadenersatzansprüche privatrechtlicher Natur, die durch Dritte gegen den Versicherungsnehmer erhoben werden (Quelle: § 1 Allgemeine Bedingungen für die Haftpflichtversicherung AHB).

Oft enthalten Haftpflichtversicherungen Klauseln, nach denen Schadenersatzansprüche auch aus der Nutzung des Internets,

„Swiss Re Corporate Solutions befürwortet es, wenn das Thema Cyber(Versicherung) professionell als eigene Sparte behandelt wird, mit den entsprechenden Spezialisten in Underwriting, Aktuariat, Risk Engineering und der Schadenbehandlung, um die Herausforderungen der Zukunft zu bewältigen."

Philippe Aerni,
Head of Financial & Professional Lines und Managing Director,
Swiss Re Corporate Solutions

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

aus Datenschutzverletzungen oder Übertragungen von Schadsoftware eingeschlossen sind. Nicht versichert sind jedoch sogenannte Schadenminderungskosten, das heißt Kosten, die entstehen, um einen drohenden Schadenersatzanspruch nicht erst entstehen zu lassen oder abzuwehren. In einem Schadenfall ist jedoch eine schnelle und professionelle Reaktion entscheidend.

Ferner enthalten diese Versicherungen oft Ausschlüsse oder Obliegenheiten, die es für den Versicherungsnehmer schwierig machen, auch tatsächlich Versicherungsschutz zu erhalten. Ein Beispiel dafür ist ein Ausschluss für den Fall, dass die Sicherheitseinrichtungen nicht dem Stand der Technik entsprechen.

Fazit: Haftpflichtversicherungen bieten nur eingeschränkten Schutz gegen Cyber-Vorfälle.

Vertrauensschadenversicherungen

Das Eigentum von Unternehmen – egal ob materiell oder immateriell – kann durch kriminelle Machenschaften von Mitarbeitern oder außenstehenden Dritten auch ohne Cyber-Attacken geschädigt werden. Daran können häufig auch die besten Sicherheitsvorkehrungen nichts ändern.

Die Vertrauensschadenversicherung ersetzt den Unternehmen Vermögensschäden, die von Mitarbeitern oder Dritten vorsätzlich verursacht werden. Die Vertrauensschadenversicherung greift bei Schäden durch Diebstahl, Unterschlagung, Betrug, Untreue, Computerbetrug oder sonstigen vorsätzlichen Handlungen, die nach den gesetzlichen Bestimmungen über unerlaubte Handlungen zum Schadensersatz verpflichten. Ersetzt werden Schäden im Rahmen der Versicherungssumme, die dem Versicherungsnehmer durch Vertrauenspersonen selbst oder von Dritten zugefügt werden.

Für Schäden, die dem Versicherungsnehmer von außen stehenden Dritten durch unmittelbare und rechtswidrige Eingriffe in seine elektronische Datenverarbeitung zugefügt werden, beispielsweise durch Cyber-Angriffe, besteht Deckungsschutz, soweit Dritte sich dabei am Vermögen des Versicherungsnehmers bereichert haben.

Fazit: Vertrauensschaden- und Cyber-Versicherungen überschneiden sich in einigen Aspekten. In beiden Versicherungen werden Kosten von IT-Forensik, Rechtsberatung oder Krisenmanagement übernommen. Die Cyber-Versicherung übernimmt darüber hinaus auch fahrlässig verursachte Schäden sowie Betriebsunterbrechungen. Ferner werden die teilweise sehr hohen Kosten für die Benachrichtigung der durch einen Datenschutzvorfall Betroffenen übernommen.

Abhängig von der Risikosituation beim zu versichernden Unternehmen sollte individuell geprüft werden, ob neben der Vertrauensschadenversicherung auch eine explizite Cyber-Versicherung sinnvoll ist.

Organisatorische Notwendigkeit einer eigenständigen Cyber-Sparte

Wie anfänglich erwähnt, haben die meisten Versicherer, mit denen wir gesprochen haben, sich dazu entschieden, das Cyber-Geschäft mittel- bis langfristig als eigenständige Sparte zu organisieren. Dafür sprechen insbesondere folgende Argumente:

- Schwierigkeiten der Tarifierung und der Schadenbehandlung. Beides unterscheidet sich bei Cyber-Vorfällen deutlich von anderen Sparten.
- Bewertung des Kumulrisikos wäre bei einer Aufteilung von Cyber-Schutz auf mehrere Sparten kaum möglich.
- Notwendigkeit einer einheitlichen Assistance-Leistung.

Eine adäquate Tarifierung kann nur mit entsprechendem Fachwissen und speziellen Tools sichergestellt werden. Mit der Brille der klassischen Versicherungssparten wird der Blick für die Besonderheiten dieses Risikos verstellt.

Ferner, und das ist das entscheidende Argument, müssten im Schadenfall zunächst aus verschiedenen Policen Deckungsinhalte geprüft und Ansprechpartner identifiziert werden. Das kostet Zeit und verhindert eine schnelle Eindämmung von Schäden.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Eigene Cyber-Sparte kommt

Die Cyber-Versicherung wird sich voraussichtlich als eigene Hauptsparte neben Feuer-, Kfz- und Haftpflichtversicherung etablieren. Diese Entwicklung kann deutlich schneller vonstattengehen als bei der letzten größeren Neuerung, der D&O-Versicherung. Wir gehen davon aus, dass sie schon in fünf bis sieben Jahren abgeschlossen sein könnte.

Auch wenn es sich für einzelne Versicherer heute noch nicht zu lohnen scheinen mag, auch für das Cyber-Privatgeschäft die Funktionalitäten einer eigenen Sparte aufzubauen, der fachliche und technische Anspruch dieses Geschäftes macht dies wohl unausweichlich. Klassische Privatkundenprodukte mit Cyber-Elementen „aufzuladen", halten wir für einen riskanten Weg. Die Dynamik im Cyber-Geschäft und dessen technischer Anspruch sind derart hoch, dass er im Rahmen einer Hausratversicherung oder ähnlicher Produkte auf Dauer nicht erfüllt werden kann. Außerdem werden voraussichtlich auch die Privatkunden eine deutlich weitergehende Absicherung und entsprechende Dienstleistungen nachfragen.

„Mit zunehmender Digitalisierung nehmen auch die Cyber-Risiken zu. Der Bedarf an qualifiziertem Versicherungsschutz wird nach der Großindustrie nun auch im großen wie mittleren Gewerbesegment spürbar. Wir haben uns hierauf durch Bereitstellung geeigneter Cyber-Versicherungslösungen für alle Kundensegmente eingestellt."

Dr. Norbert Rollinger,
Vorstandsvorsitzender der R+V Versicherungs AG

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

4. Schlusswort

Das KPMG-Marktmodell „Cyber"

Unabhängig davon, welches der vorgestellten KPMG-Szenarien man für am realistischsten hält, werden Cyber-Versicherungen aller Voraussicht nach sehr bald von einer Randerscheinung im deutschen Markt zu einer der zentralen Versicherungssparten heranwachsen.

Unter Berücksichtigung des bisher kaum entwickelten Kundensegments der kleineren Unternehmen und der privaten Haushalte erwarten wir bis 2036 in unserem Modell mit neutraler Prognose die folgenden Cyber-Prämienvolumina (Jahresprämie) für den deutschsprachigen Raum:

- DACH gesamt – 19,6 Milliarden Euro,
  davon in
  - Deutschland – 15,2 Milliarden Euro
  - Österreich – 2,2 Milliarden Euro
  - Schweiz – 2,2 Milliarden Euro

Den deutlich größten Teil dieses Prämienvolumens erwarten wir mit 78 Prozent im Segment der standardisierten Versicherungslösungen, also dem Geschäft mit den kleineren Unternehmen (36 Prozent) und den privaten Haushalten (42 Prozent).

Wer als Versicherer in dem volumenstärksten Cyber-Segment anbieten möchte, sollte sich darüber im Klaren sein, dass der Erfolg hier zu einem Großteil davon abhängt, ob es gelingt, das Geschäft extrem standardisiert und automatisiert abzuwickeln. Auch ist dieses Segment geprägt von den – nach heutigem Stand – am schlechtesten geschützten Risiken. Ein weiteres wichtiges Kriterium, insbesondere in diesem Segment, dürfte das Kumulrisiko sein.

Die Herausforderung für Versicherer dürfte also darin liegen, die in der Cyber-Versicherung liegenden Chancen konsequent und zügig zu ergreifen, dabei aber nicht zu vergessen, dass es sich um ein weitgehend neues, durchaus risikobehaftetes Geschäft handelt.

Ausgestaltung der Cyber-Wertschöpfungskette

Der Markt der Cyber-Risiko-Dienstleister insgesamt ist deutlich weiterentwickelt als der Cyber-Versicherungsmarkt im deutschsprachigen Raum. Diese Spezialisten verfügen über eine ganze Reihe von Fähigkeiten, die auch für einen Versicherer im professionellen Umgang mit Cyber-Risiken von großer Bedeutung sind. Dies bezieht sich schwerpunktmäßig auf die Felder:

- Risiko-Prävention
- Underwriting, insbesondere Pricing
- Schadenregulierung/Case Management

In der Frage der Zusammenarbeit mit diesen Dienstleistern ist grundsätzlich die gesamte Bandbreite vorstellbar, vom Zukauf einer umfänglichen White Label-Lösung bis hin zu einem gezielten Einsatz von Spezialisten in besonders komplexen Aufgabenstellungen. In zwei Feldern dürfte in diesem Sinne aber bei jedem Versicherer Kooperationsbedarf mit externen Dienstleistern bestehen:

- Risikoanalyse und Bewertung von Maßnahmen zur Risiko-Prävention
- Case Management im Schadenfall

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Insgesamt sind bei der Ausgestaltung des Sourcing-Ansatzes und der organisatorischen Abbildung des Cyber-Geschäfts im eigenen Haus folgende Aspekte zu berücksichtigen:

- Es lassen sich Modelle mit stark unterschiedlichem Sourcing-Ansatz erfolgreich betreiben.
- Das Modell kann zwecks Kompetenzaufbau und initialer Risikovermeidung temporär auch stärker extern betrieben werden.
- Unabhängig von dem avisierten Zielmodell ist der intensive und laufende Austausch mit ausgewiesenen Experten aus IT/Forensic etc. von enormer Bedeutung, da sich das Underwriting- und schadenrelevante Wissen laufend verändert und über Erfolg und Misserfolg in der Sparte entscheidet.
- Die organisatorische Abbildung der Cyber-Operations zentral als eigenständige Sparte stellt die wahrscheinlich sinnvollste Form dar.
- Während der Aufbauphase der Cyber-Sparte könnte es eine Zwischenlösung sein, die bestehende Organisationseinheit temporär an einer Hauptsparte anzusiedeln.

Was für den einzelnen Versicherer die richtige Ziel- und Zwischenlösung ist, lässt sich pauschal nicht beantworten.

Relevanz für das eigene Unternehmen und idealer Zeitpunkt des Markteinstiegs

Insgesamt bietet die Cyber-Versicherung für Versicherer enorme Chancen für die Zukunft. Das Wachstum in der traditionellen Schaden-Unfallversicherung ist begrenzt. Von den klassischen Sparten ist auf Sicht kein Wachstum zu erwarten. Gleichzeitig birgt die Digitalisierung enorme Herausforderungen, die tendenziell eher dämpfend auf das Geschäftsvolumen der Versicherer wirken werden.

Vor diesem Hintergrund kann es eigentlich für keinen Versicherer eine ernsthafte Option sein, sich nicht mit der Cyber-Versicherung zu beschäftigen. Dabei ist die zögerliche Haltung vieler Anbieter verständlich: Nach einigen schmerzhaften Erfahrungen mit Spezialrisiken in der Vergangenheit ist die Bereitschaft, erneut ein womöglich schwer einschätzbares Risiko einzugehen, begrenzt. Also erst einmal abwarten, andere die Fehler machen lassen und dann einsteigen, wenn die Sicht klarer ist?

Angesichts der beschriebenen Herausforderungen in der Cyber-Versicherung erscheint dies ein verlockender Weg zu sein. Für den überwiegenden Teil der Versicherer halten wir dies aber nicht für zielführend. So schnell wie möglich Erfahrungen und vor allem Daten in dieser Sparte zu sammeln, wird in absehbarer Zeit ein wesentlicher Wettbewerbsvorteil sein – in der Produktgestaltung, im Underwriting und auch im Schadenmanagement. Diese Erfahrungen gilt es so schnell wie möglich zu machen, um sich Wettbewerbsvorteile zu sichern. Insbesondere im Vorgriff auf den Zeitpunkt, wenn die Marktnachfrage dann deutlich anzieht.

Das Versicherungsgeschäft ist zu einem wesentlichen Teil ein Erfahrungsgeschäft. Erfahrungen sind manchmal schmerzhaft, aber immer wertvoll. Wer sich jetzt in Richtung Cyber-Versicherung aufmacht, verschafft sich die Option auf überdurchschnittliches Wachstum in den nächsten Jahren. Wer dabei schnell lernt, wird auch in der Lage sein, die am Ende überlegenen Produkte zu entwickeln und eine gute Profitabilität sicherstellen zu können.

Selten hatten wir bei der Bearbeitung eines Themas so sehr das Gefühl, die Assekuranz an der Schwelle zu einer neuen Zeit zu sehen. Ohne Zweifel ist es ein langer Weg, der vor allen Beteiligten liegt. Skills müssen erworben, Organisationen aufgebaut und Risiken akzeptiert werden. Aber am Ende wird sich diese Reise für alle Beteiligten gelohnt haben. Daran haben wir nach einem Jahr intensiver Befassung mit dem Thema Cyber keinen Zweifel. Wir freuen uns sehr darauf, diesen Weg der Assekuranz zu begleiten, Ansätze mit Ihnen zu entwickeln, auszuprobieren und anzupassen. Lassen Sie uns miteinander sprechen, wir freuen uns darauf.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Ihre Ansprechpartner

Jörg Wälder

Jörg Wälder ist Senior Executive im Bereich Financial Services bei KPMG. Er verfügt über mehr als 30 Jahre Expertise im Bereich der Schaden-/Unfallversicherung. Rund 20 Jahre C-Level, 15 Jahre in internationalen Rollen. Ein besonderer Fokus seiner Tätigkeiten liegt auf der digitalen Transformation des Versicherungsgeschäfts sowie auf Cyber. Vor KPMG war er unter anderem als Chief Underwriting Officer Zurich Deutschland sowie als Global CEO Versicherungen bei Volkswagen tätig.

Markus Heyen

Markus Heyen ist als Partner im Bereich Financial Services auf die strategische Beratung von Versicherern und weiteren Finanzdienstleistern spezialisiert. Er verfügt über 12 Jahre Erfahrung in der Beratung von Versicherern und Banken. Sein Fokus liegt auf der digitalen Transformation des Versicherungsgeschäfts und der Entwicklung zukünftiger Versicherungsmodelle. Vor KPMG war er unter anderem für AXA, Accenture und PwC tätig.

Hendrik C. Jahn

Hendrik C. Jahn ist als Partner im Bereich Financial Services auf die strategische Beratung von Versicherern und weiteren Finanzdienstleistern spezialisiert. Hier verfügt er über 23 Jahre Erfahrung. Seine Schwerpunkte liegen in der Strategieentwicklung, Prozessoptimierung sowie der Transformation der Kernversicherungsfunktionen. Zuvor war er Partner bei PwC und Accenture sowie Principal bei BCG.

Christian Sagawe

Christian Sagawe arbeitet als Senior Manager im Bereich Financial Services bei KPMG und ist auf die strategische Beratung von Versicherern spezialisiert. Seine Schwerpunkte sind die strategische Neuausrichtung des Schadenmanagements und die Digitalisierung der Versicherungsindustrie. Vor KPMG war Christian Sagawe 8 Jahre als Managementberater für Insurance bei Accenture Strategy und anschließend bei PwC tätig.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Methodik

Die Studie basiert auf über 100 Marktgesprächen von Oktober 2015 bis Dezember 2016 mit Versicherern, spezialisierten Versicherungsmaklern, Dienstleistern, aufstrebenden Insur-Techs sowie den Erkenntnissen von zahlreichen KPMG-Fachexperten. Diese Unternehmen wurden in iterativen Gesprächen in den Erstellungsprozess der Studie mit einbezogen. Ergänzend wurden Sekundärliteratur, externe Datenbanken sowie Unternehmensinformationen und Pressemittleitungen hinzugezogen.

Mit freundlicher Unterstützung von:

Allianz SE, Arvato AG, Avira, AXA Versicherung AG, Bundesamt für Verfassungsschutz, Control€xpert, ERGO Versicherungsgruppe, Erichsen GmbH, etventure, Finanzchef24, Gothaer Versicherungsbank VVaG, Grazer Wechselseitige Versicherung AG, Hiscox Ltd., kreait GmbH, Frau Dr. Anastassia Lauterbach, LVM Versicherung, Marsh GmbH, Precire Technologies GmbH, R+V Allgemein Versicherungs-AG, Swiss Re Corporate Solutions, Toyota Insurance Management, UNIQA Insurance Group, Vienna Insurance Group, Virado, Wiener Städtische Versicherung AG, Zurich Insurance Group

Über KPMG

KPMG ist ein Firmennetzwerk mit mehr als 189.000 Mitarbeitern in 152 Ländern.

Auch in Deutschland gehört KPMG zu den führenden Wirtschaftsprüfungs- und Beratungsunternehmen und ist mit rund 10.200 Mitarbeitern an mehr als 20 Standorten präsent. Unsere Leistungen sind in die Geschäftsbereiche Audit, Tax, Consulting und Deal Advisory gegliedert. Im Mittelpunkt von Audit steht die Prüfung von Konzern- und Jahresabschlüssen. Taxt steht für die steuerberatende Tätigkeit von KPMG. Die Bereiche Consulting und Deal Advisory bündelen unser hohes fachliches Know-how zu betriebswirtschaftlichen, regulatorischen und transaktionsorientierten Themen.

Für wesentliche Branchen unserer Wirtschaft haben wir eine geschäftsübergreifende Spezialisierung vorgenommen. Hier laufen die Erfahrungen unserer Experten weltweit zusammen und tragen zusätzlich zur Beratungsqualität bei.

Abbildungen:

Titel: NASA/JPL/MPS/DLR/IDA; S. 2: NASA/JPL-Caltech; S. 4: NASA/JPL, NASA/JPL/MPS/DLR/IDA; S. 6: NASA/JPL-Caltech/Space Science Institute, NASA/JPL/MPS/DLR/IDA; S. 9: 2010 bielmeier/Photocase; S. 10, 11: by-studio/Fotolia; S. 12: NASA/SDO; S. 39, 40: ERGO Versicherung AG, Quirin Leppert, München; S. 60: NASA's Scientific Visualization Studio, NASA, NASA/JPL/MPS/DLR/IDA

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Quellen

Accenture, 2014. The Cyber Security Leap: From Laggard to Leader (online). Zu finden unter: https://www.accenture.com/au-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Local/au-en/PDF/1/Accenture-Laggard-to-Leader-PoV-%20FINAL.pdf (Stand: 10.03.2016)

ACE, 2014. Emerging Risk Barometer 2015 (online). Zu finden unter: http://www.acegroup.com/global-assets/documents/Europe-Corporate/Risk-Briefing/2015-07-07-Emerging-Risks-Barometer-final--PUBLISHED.pdf (Stand: 09.06.2016)

Allianz, 2014. Allianz Risk Barometer (online). Zu finden unter: http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf (Stand: 09.06.2016)

Allianz, 2015. A Guide to Cyber Risk – Managing the Impact of Increasing Interconnectivity (online). Zu finden unter: http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf (Stand: 27.05.2016)

Allianz, 2016. Cyber Risiken und deren Versicherbarkeit (online). Zu finden unter: http://www.nik-nbg.de/uploads/tx_seminars/Jens-Krickhahn-Allianz.pdf (Stand: 02.06.2016)

AON, 2014. Marktprognose 2016 (online). Zu finden unter: http://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0ahUKEwj65s7D-pjQAhVJchQKHV27Ar4QFggtMAM&url=http%3A%2F%2Ffinanzwirtschaft.fuerstenberg-forum.de%2Fattachment.php%3Fattachmentid%3D184%26d%3D1453922767&usg=AFQjCNHUENdt2a5TinjuclOumbEoO89mYA&sig2=bcvVn1_ZdkI7aoEtTRx_lA (Stand: 08.06.2016)

AON, 2014. Marktreport 2015 Der deutsche Versicherungsmarkt (online). Zu finden unter: http://www.aon.com/germany/publikationen/risk-solutions/marktreport-2015.jsp (Stand: 10.06.2016)

AT Kearney, 2015. Information Security: It's all about Trust (online). Zu finden unter: https://www.atkearney.de/documents/856314/5891973/Information+Security-+It's+All+About+Trust.pdf/83fc5e88-4fdb-4f53-8380-9b7d56a432d9 (Stand: 10.03.2016)

Betterley Report, 2014. Cyber/Privacy Insurance Market Survey 2014 (online). Zu finden unter: http://betterley.com/samples/cpims14_nt.pdf (Stand: 10.06.2016)

Bitkom, 2015. Nachfrage nach IT-Sicherheit wächst kräftig (online). Zu finden unter: https://www.bitkom.org/Presse/Presseinformation/Nachfrage-nach-IT-Sicherheit-waechst-kraeftig.html (Stand: 10.06.2016)

Bitkom, 2015. Digitale Angriffe auf jedes zweite Unternehmen (online). Zu finden unter: https://www.bitkom.org/Presse/Presseinformation/Digitale-Angriffe-auf-jedes-zweite-Unternehmen.html (Stand: 18.05.2016)

Bitkom, 2015. Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz im digitalen Zeitalter (online). Zu finden unter: https://www.bitkom.org/noindex/Publikationen/2015/Studien/Studienbericht-Wirtschaftsschutz/150709-Studienbericht-Wirtschaftsschutz.pdf (Stand: 27.05.2016)

Bitkom, 2015. Studie „Internet-Sicherheit" (online). Zu finden unter: https://www.bitkom.org/noindex/Publikationen/2010/Studie/Studie-Internet-Sicherheit/BITKOM-Internet-Sicherheit-Extranet.pdf (Stand: 10.03.2016)

Bitkom, 2016. Anteil Cyber-Versicherungen mit Schäden (online). Zu finden unter: https://www.hisolutions.com/_Downloads/Leitfaden/Leitfaden_Bitkom_Kosten_Cyber-Schadensfall.pdf (Stand: 12.09.2016)

Bitkom, 2016. Kosten eins Cyber-Schadenfalles (online). Zu finden unter: https://www.bitkom.org/noindex/Publikationen/2016/Leitfaden/Kosten-eines-Cyber-Schadensfalles/160426-LF-Cybersicherheit.pdf (Stand: 27.05.2016)

BMWi, 2014. Der IT-Sicherheitsmarkt in Deutschland (online). Zu finden unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Studien/it-sicherheitsmarkt-in-deutschland (Stand: 02.06.2016)

Bundesamt für Sicherheit der Informationstechnik, 2015. Die Lage der IT-Sicherheit in Deutschland 2015 (online). Zu finden unter: https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf?__blob=publicationFile&v=4 (Stand: 09.06.2016)

Bundeskriminalamt, 2014. BKA_Definition Cybercrime (online). Zu finden unter: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html (Stand: 07.06.2016)

Bundeskriminalamt, 2014. Cybercrime - Bundeslagebild 2013 (online). Zu finden unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2013.html (Stand: 10.03.2016)

Bundeskriminalamt, 2015. Cybercrime - Bundeslagebild 2014 (online). Zu finden unter: https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0ahUKEwjXtfOu8JjQAhWHbxQKHTUNCr0QFggqMAM&url=https%3A%2F%2Fwww.bka.de%2FSharedDocs%2FDownloads%2FDE%2FPublikationen%2FJahresberichteUndLagebilder%2FCybercrime%2FcybercrimeBundeslagebild2014.pdf%3F__blob%3DpublicationFile%26v%3D2&usg=AFQjCNHCWSdi-POxsujaZIhkwYKfNo6Sow&sig2=__soQ-9ImCVq4R6YJYdsCQ (Stand: 06.07.2016)

Capgemini, 2014. Staying Ahead in the Cyber Security Game (online). Zu finden unter: https://www.capgemini.com/resource-file-access/resource/pdf/staying_ahead_in_the_cybersecurity_game_-_what_matters_now.pdf (Stand: 10.03.2016)

Capgemini, 2016. Securing the Internet of Things Opportunity (online). Zu finden unter: https://www.capgemini-consulting.com/resource-file-access/resource/pdf/securing_the_internet_of_things.pdf (Stand: 10.03.2016)

CB Inside, 2014. From IIoT Security to Quantum Encyrption: 106 Cybersecurity Startups In A Market Map (online). Zu finden unter: https://www.cbinsights.com/blog/cybersecurity-market-map (Stand: 22.09.2016)

Cebr, 2014. Konsequenzen unzureichender Cyber-Sicherheit für Unternehmen und Wirtschaft in Deutschland (online). Zu finden unter: https://www.veracode.com/sites/default/files/Resources/AnalystReports/business-and-economic-consequences-of-inadequate-cybersecurity-the-case-of-germany-de.pdf (Stand: 12.09.2016)

Choudhry, Umar, 2014: Der Cyber-Versicherungsmarkt in Deutschland, 1. Auflage. Gabler-Verlag, Wiesbaden 2014.

Chubb, 2016. Identity theft als Annex (online). Zu finden unter: https://www2.chubb.com/us-en/individuals-families/identity-management.aspx (Stand: 12.08.2016)

com-magazin.de, 2014. So lassen sich IT-Risiken im Unternehmen versichern (online). Zu finden unter: http://www.com-magazin.de/dl/6/0/9/9/3/5/Cyberversicherungen.pdf (Stand: 07.06.2016)

Computerwoche, 2015. IT-Security – Wann zahlt die Versicherung (online). Zu finden unter: http://www.computerwoche.de/a/wann-zahlt-die-versicherung,2553102 (Stand: 01.04.2016)

CRO Forum, 2015. Big Datat & Analytics (online). Zu finden unter: https://www.munichre.com/site/corporate/get/documents_E571900048/mr/assetpool.shared/Documents/0_Corporate%20Website/1_The%20Group/Focus/Emerging%20Risks/CRO-Forum-Cyber-Risk.pdf (Stand: 11.08.2016)

cybersecurityventures.com, 2014. Top10 cybersecurityfirmen Weltweit (online). Zu finden unter: http://cybersecurityventures.com/cybersecurity-500 (Stand: 07.06.2016)

Cybersecurity Ventures, 2015. Announcing the Cybersecurity 500 List (online). Zu finden unter: http://cybersecurityventures.com/press-release-cybersecurity-500-q2-2016-edition (Stand: 13.06.2016)

Deutsche Telekom/ T-Systems, 2014. Cybersecurity Report 2014 (online). Zu finden unter: http://www.cybersecuritysummit.de/downloads/CyberSecurityReport_2014.pdf (Stand: 10.06.2016)

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Die Welt, 2014. Feind in der eigenen Firma (online). Zu finden unter: https://www.welt.de/print/welt_kompakt/print_wirtschaft/article155987412/Feind-in-der-eigenen-Firma.html (Stand: 23.06.2016)

Die Welt, 2014. Wie Telekom-Experten das Internet überwachen (online). Zu finden unter: https://www.welt.de/wirtschaft/webwelt/article129201672/Wie-Telekom-Experten-das-Internet-ueberwachen.html (Stand: 10.03.2016)

DIW, 2016. Tatort Internet: Kriminialität verursacht Bürgern Schäden in Milliardenhöhe (online). Zu finden unter: https://www.bitkom.org/Presse/Presseinformation/Erst-jedes-zehnte-Industrieunternehmen-gegen-Cybercrime-versichert.html (Stand: 25.05.2016)

DVS, 2014. Sonderheft Cyber-Versicherungen (online). Zu finden unter: http://www.gvnw.de/fileadmin/user_upload/Publikationen/Wolters_Kluwer_Cyber-Versicherung_Leseprobe.pdf (Stand: 10.06.2016)

enterpreneur.com, 2014. 5 Fundamentals for Protecting your identity and your privacy (online). Zu finden unter: https://www.entrepreneur.com/article/275463 (Stand: 30.06.2016)

Evolita, 2016. Connected Medical Devices (online). Zu finden unter: http://beta.evolita.com/explore/connected-medical-devices-total-worldwide-between-2013-and-2018/7rlbx/ (Stand: 24.09.2106)

FAZ, 2015. Deutsche Bank warnt vor Cyber-Angriffen (online). Zu finden unter: http://www.faz.net/aktuell/wirtschaft/wirtschaftskriminalitaet-deutsche-bank-warnt-vor-cyber-angriffen-14424706.html (Stand: 22.09.2016)

Focus, 2014. Warum Gangster auf Autos abfahren (online). Zu finden unter: http://www.focus.de/finanzen/news/wirtschaft-und-geld-warum-gangster-auf-vernetzte-autos-abfahren_id_5548613.html (Stand: 09.06.2016)

fortune.com, 2014. SWIFT Discloses More Cyber Thefts (online). Zu finden unter: http://fortune.com/2016/08/30/swift-discloses-more-cyber-thefts (Stand: 22.09.2016)

fortune.com, 2015. Employees Are the Weakest Link in Computer Security (online). Zu finden unter: http://fortune.com/2016/06/20/employees-computer-security (Stand: 27.06.2016)

futurezone, 2015. Cybercrime-Versicherungen erwarten Boom in Europa (online). Zu finden unter: https://futurezone.at/b2b/cybercrime-versicherungen-erwarten-boom-in-europa/161.304.311 (Stand: 23.06.2016)

cybersecuritysummit.de, 2014. A new approach to risk assessment for cyber insurance (online). Zu finden unter: http://www.cybersecuritysummit.de/downloads/CyberSecurityReport_2014.pdf (Stand: 10.03.2016)

Gründerszene, 2015. Hacker könnten Bremsen manipulieren (online). Zu finden unter: http://www.gruenderszene.de/automotive-mobility/interview-arne-schoenbohm-cyber-angriffe?utm_source=rss&utm_medium=rss&utm_campaign=rss&utm_source=rss&utm_medium=rss&utm_campaign=interview-arne-schoenbohm-cyber-angriffe (Stand: 10.06.2016)

Handelsblatt, 2014. Cebit warnt vor Sicherheitsrisiken: Cyberangriffe verursachen Milliardenschäden (online). Zu finden unter: http://www.handelsblatt.com/technik/it-internet/cebit2016/cebit-warnt-vor-sicherheitsrisiken-cyberangriffe-verursachen-milliardenschaeden/11510724.html (Stand: 10.03.2016)

Handelsblatt, 2015. Mehr Cyber-Attacken auf Regierung und Wirtschaft (online). Zu finden unter: http://www.handelsblatt.com/technik/sicherheit-im-netz/bundesamt-fuer-sicherheit-mehr-cyber-attacken-auf-regierung-und-wirtschaft/14504788.html (Stand: 22.09.2016)

Hiscox, 2015. Berechnungsgrundlagen Prämienkalkulation Cyberversicherung (online). Zu finden unter: https://www.hiscox.de/geschaeftskunden/cyber-versicherung (Stand: 12.09.2016)

Hiscox, 2015. Schadenbeispiele (online). Zu finden unter: https://www.hiscox.de/geschaeftskunden/cyber-versicherung (Stand: 12.09.2016)

Insurance Information Institute, 2014. Cybersecurity And Identity Theft Coverage: The State of the Industry (online). Zu finden unter: http://www.iii.org/article/cybersecurity-and-identity-theft-coverage-the-state-of-the-industry (Stand: 09.08.2016)

it-daily.net, 2014. Datenschutz im „smarten" Business Industrie 4.0 darf nicht zum Monitoring 4.0 werden (online). Zu finden unter: https://www.it-daily.net/it-sicherheit/datenschutz/10855-datenschutz-im-smarten-business-industrie-4-0-darf-nicht-zum-monitoring-4-0-werden (Stand: 07.06.2016)

iX Magazin, 2014. Abgrundtief – Einblicke in die dunkle Seite des Internets (online). Zu finden unter: https://www.heise.de/ix/inhalt/2016/5/40 (Stand: 09.06.2016)

Jung, Marcus, 2013: Virtuelle Kampfzone, in: JUVE Rechtsmarkt, 11/13, S.54–60.

Kaspersky, 2014. IT-Sicherheit – eine Frage des Budgets (online). Zu finden unter: http://www.kaspersky.com/de/about/news/business/2013/IT-Sicherheit-eine_Frage_des_Budgets (Stand: 12.08.2016)

Keith Kirkpatriok, 2014. Cyber Policies on the Rise (online). Zu finden unter: http://cacm.acm.org/magazines/2015/10/192376-cyber-policies-on-the-rise/abstract (Stand: 12.05.2016)

KPMG, 2015. e-crime – Computerkriminalität in der deutschen Wirtschaft 2015 (online). Zu finden unter: https://www.kpmg.com/DE/de/Documents/e-crime-studie-2015.pdf (Stand: 01.06.2016)

KPMG, 2015. IT-Sicherheit in Deutschland (online). Zu finden unter: http://bdi.eu/media/presse/publikationen/KPMG_IT-Sicherheit_in_Deutschland.pdf (Stand: 09.06.2016)

Liberty Mutual, 2014. Indentity Theft Insurance (online). Zu finden unter: https://www.libertymutual.com/identity-theft-insurance (Stand: 12.08.2016)

LinkedIn, 2015. The Globality Quotient: Cybersecurity (online). Zu finden unter: https://www.linkedin.com/pulse/global-quotient-cybersecurity-ludmila-morozova-buss (Stand: 07.06.2016)

Linus Neumann, 2016. Preisliste laut einer Darknetrecherche von Linus Neumann, MWV Seminar 15.Juni 2016

MARSH, 2016. Monitor Das Magazin der Marsh Gmbh November 2015.

MARSH, 2016: Marsh Cyber-Risiko-Befragung 2016 (online). Zu finden unter: https://www.marsh.com/content/dam/marsh/Documents/PDF/de/de/Marsh%20Cyber-Risiko-Befragung%202016.pdf (Stand: 11.01.2017)

McAfee, 2015. Net Losses: Estimating the Global Cost of Cybercrime (online). Zu finden unter: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf (Stand: 12.09.2016)

MLP, 2015. Umfangreiche Kooperation von MLP mit FinTech massUp (online). Zu finden unter: https://mlp-ag.de/presse/pressemitteilungen/2015/umfangreiche-kooperation-von-mlp-mit-fintech-massup (Stand: 12.08.2016)

Munich Re, 2016. Gefahr aus dem Netz (online). Zu finden unter: https://www.munichre.com/site/corporate/get/documents_E-2068517148/mr/assetpool.shared/Documents/5_Touch/_Publications/302-08481_de.pdf (Stand: 09.06.2016)

Krebs on Security, 2016. The value of a Hacked Company (online). Zu finden unter: https://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company (Stand: 22.07.2016)

Nationwide, 2014. Identity Theft Insurance (online). Zu finden unter: https://www.nationwide.com/identity-theft-protection.jsp (Stand: 12.08.2016)

NetDiligence, 2016. Cyber Claims Study (online). Zu finden unter: https://netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf (Stand: 09.01.2017)

networkasia, 2015. Next-generation data security will rely on silicon and artificial intelligence (online). Zu finden unter: http://www.networksasia.net/article/next-generation-data-security-will-rely-silicon-an (Stand: 23.06.2016)

Norton by Symantec, 2012. 2012 Norton Cybercrime Report (online). Zu finden unter: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf (Stand: 10.03.2016)

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

resilient systems, 2015. Incident Response-Herausforderungen und Chancen für europäiische Unternehmen (online). Zu finden unter: https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwjRl9LKg5nQAhUFwBQKHT9DAeIQFggdMAE&url=https%3A%2F%2Fwww.cirosec.de%2Ffileadmin%2Fpdf%2FPresse_2015%2FRS_PACExecSummary_German_A4.pdf&usg=AFQjCNELmfoWdRFXUvgqeTZETCvYVwPZ5Q&sig2=8bRelA-okCYk7gcBIpIEmA&bvm=bv.137904068,d.d24&cad=rja (Stand: 25.05.2016)

Roland Berger, 2015. Cyber-Security: Managing threat scenarios in manufacturing companies (online). Zu finden unter: https://www.rolandberger.com/publications/publication_pdf/roland_berger_tab_cyber_security_20150305.pdf (Stand: 10.03.2016)

State Farm, 2014. Identity Theft Insurance (online). Zu finden unter: https://www.statefarm.com/insurance/identity-restoration (Stand: 12.08.2016)

statista, 2015. Internetkriminalität in Deutschland – Statista-Dossier (online). Zu finden unter: https://de.statista.com/statistik/studie/id/7320/dokument/internetkriminalitaet-statista-dossier (Stand: 13.04.2016)

statista, 2017. Anzahl der Suchanfragen bei Google weltweit in den Jahren 2000 bis 2015 (in Milliarden). Zu finden unter: https://de.statista.com/statistik/daten/studie/71769/umfrage/anzahl-der-google-suchanfragen-pro-jahr/ (Stand: 11.01.2017)

Stern, 2015. Neuer Erpressungs-Trojaner sperrt Smartphones (online). Zu finden unter: http://www.stern.de/digital/smartphones/trojaner-dogspectus-sperrt-android-handys-6821916.html (Stand: 11.08.2016)

techcrunch, 2016. Cyber insurance is changing the way we look at risk (online). Zu finden unter: https://techcrunch.com/2016/06/13/cyber-insurance-is-changing-the-way-we-look-at-risk (Stand: 12.08.2016)

The Financial Express, 2014. Cyber security: 60% of digital businesses to suffer major service failures, say Gartner (online). Zu finden unter: http://computer.expressbpd.com/news/cyber-security-60t-of-digital-businesses-to-suffer-major-service-failures-say-gartner/17816 (Stand: 23.06.2016)

The Guardian, 2015. Car hacking is the future – and sooner or later you'll be hit (online). Zu finden unter: https://www.theguardian.com/technology/2016/aug/28/car-hacking-future-self-driving-security (Stand: 22.09.2016)

The New York Times, 2014. How Spy Tech Firms Let Governments See Everything on a Smartphone (online). Zu finden unter: http://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html?_r=0 (Stand: 22.09.2016)

The New York Times, 2015. A hacking of more than 50 Million Dollar Dashes Hopes in the World of Virtual Currency (online). Zu finden unter: http://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html?_r=0 (Stand: 23.06.2016)

Verizon, 2014. 2016 Data Breach Investigations Report (online). Zu finden unter: http://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwj3ubXN95jQAhUDOhQKHRviCL4QFggnMAE&url=http%3A%2F%2Fwww.verizonenterprise.com%2Fresources%2Freports%2Frp_DBIR_2016_Report_en_xg.pdf&usg=AFQjCNGO_-X9afKczCQUHfqqfh1pOSeA0g&sig2=EF-cL8e4v91kllpKt-67nw (Stand: 09.06.2016)

Verlag Versicherungswirtschaft GmbH, 2015. Cyber: Munich Re rechnet mit Milliarden-Volumen (online). Zu finden unter: http://versicherungswirtschaft-heute.de/koepfe/cyber-munich-re-rechnet-mit-milliarden-volumen (Stand: 11.08.2016)

Verlag Versicherungswirtschaft GmbH, 2014. Computerkriminelle kosten deutsche Wirtschaft 54 Milliarden (online). Zu finden unter: http://versicherungswirtschaft-heute.de/unternehmen/computerkriminelle-kosten-deutsche-wirtschaft-54-milliarden (Stand: 10.03.2016)

Verlag Versicherungswirtschaft GmbH, 2015. 6.000 Cyberangriffe gegen VW (online). Zu finden unter: http://versicherungswirtschaft-heute.de/schlagzeilen/6-000-cyberangriffe-gegen-vw (Stand: 22.09.2016)

Verlag Versicherungswirtschaft GmbH, 2015. Cyber-Experte für allgemeine Meldepflicht (online). Zu finden unter: http://versicherungswirtschaft-heute.de/unternehmen/cyber-experte-fur-allgemeine-meldepflicht (Stand: 10.03.2016)

Verlag Versicherungswirtschaft GmbH, 2015. Kritische Aspekte der Cyber-Versicherung (online). Zu finden unter: http://versicherungswirtschaft-heute.de/politics/kritische-aspekte-der-cyber-versicherung (Stand: 11.03.2016)

Verlag Versicherungswirtschaft GmbH, 2015. Lloyd's: „Explosion in the Potential of Cyber Risk" (online). Zu finden unter: http://versicherungswirtschaft-heute.de/dossier/lloyds-explosion-in-the-potential-of-cyber-risk (Stand: 22.09.2016)

Verlag Versicherungswirtschaft GmbH, 2015. Steigende Nachfrage bei Cyber- und Terrorversicherungen (online). Zu finden unter: http://versicherungswirtschaft-heute.de/maerkte/steigende-nachfrage-bei-cyber-und-terrorversicherungen (Stand: 22.09.2016)

Versicherungsjournal, 2014. Fünf neue Cyber Policen (online). Zu finden unter: http://www.versicherungsjournal.de/versicherungen-und-finanzen/fuenf-neue-cyber-policen-125691.php (Stand: 11.05.2016)

Versicherungsmagazin, 2014. Vernetzte Gebäude kaum gegen Cyberattacken geschützt (online). Zu finden unter: http://www.versicherungsmagazin.de/Aktuell/Nachrichten/195/22963/pr/print.html (Stand: 15.03.2016)

Verlag Versicherungswirtschaft GmbH, 2015. Cyber-Risiken: Versicherer bilden die zweite Linie der Verteidigung (online). Zu finden unter: http://versicherungswirtschaft-heute.de/unternehmen/cyber-risiken-versicherer-bilden-die-zweite-linie-der-verteidigung (Stand: 10.03.2016)

Willis, 2016. Insurance Cyberrisk (online). Zu finden unter: http://www.pwc.dk/da/arrangementer/assets/cyber-tineolsen.pdf (Stand: 07.06.2016)

Zurich, 2014. Cyber Risk – Report: Global cyber governance: preparing for new business risks (online). Zu finden unter: https://www.zurich.de/it/corporate/knowledge/articles/2015/04/global-cyber-governance-preparing-for-new-business-risks (Stand: 10.03.2016)

Zurich, 2014. Risk Nexus Global cyber governance: preparing for new business risks (online). Zu finden unter: http://itemsweb.esade.edu/wi/web/risk-nexus-april-2015-global-cyber-governance.pdf (Stand: 10.03.2016)

Zurich, 2015. Cyber Risk - The $445 billion cyber risk gap (online). Zu finden unter: https://www.zurich.com/en/knowledge/articles/2015/04/the-445-billion-cyber-risk-gap (Stand: 17.03.2016)

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft

Dr. Frank Ellenbürger
Partner, Bereichsvorstand Insurance
T +49 89 9282-1867
fellenbuerger@kpmg.com

Jörg Wälder
Senior Executive, Financial Services
T +49 221 2073-1349
jwaelder@kpmg.com

Markus Heyen
Partner, Financial Services
T +49 40 32015-4006
mheyen@kpmg.com

Hendrik C. Jahn
Partner, Financial Services
T +49 221 2073-1346
hjahn@kpmg.com

Christian Sagawe
Senior Manager, Financial Services
T +49 221 2073-1304
csagawe@kpmg.com

Cyber Services

Uwe Bernd-Striebeck
Partner, Cyber Security
T +49 201 455-6870
uberndstriebeck@kpmg.com

Michael Sauermann
Partner, Forensic
T +49 30 2068-4624
msauermann@kpmg.com

Ansprechpartner KPMG in der Schweiz

Dr. Anup Nastik
Director, Financial Services
T +41 58 249 54 62
anastik@kpmg.com

Ansprechpartner KPMG in Österreich

Andreas Tomek
Partner, Cyber
T +43 1 31332-3930
atomek@kpmg.at

www.kpmg.de

www.kpmg.de/socialmedia

Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation. Die Ansichten und Meinungen in Gastbeiträgen sind die des Verfassers und entsprechen nicht unbedingt den Ansichten und Meinungen der KPMG AG Wirtschaftsprüfungsgesellschaft.

© 2017 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Printed in Germany. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.