LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

MRIC MUNICH RISK AND INSURANCE CENTER

OKTOBER 2017

CYBER RISK AGENCY

MRIC EXECUTIVE REPORT

VERSICHERUNG ALS INSTRUMENT DES CYBER-RISIKOMANAGEMENTS

MIT FOKUS AUF KLEINE UND MITTLERE UNTERNEHMEN

ZUSAMMENFASSUNG

Cyber-Angriffe verursachen in der deutschen Wirtschaft jährlich 55 Mrd. EUR an Schäden.

Aufgrund geringerer IT-Sicherheitsstandards und geringerer finanzieller Möglichkeiten stellen Cyber-Angriffe insbesondere für die schlechter geschützten kleineren Unternehmen ein existenzbedrohendes Risiko dar.

Durch die erhebliche Anzahl existenter Systemschwachstellen ist kein Unternehmen völlig sicher. Außerdem wird die Angriffsfläche durch die voranschreitende Digitalisierung (Stichwörter: Internet of Things und Industrie 4.0) weiter zunehmen.

Um sich auf Cyber-Attacken gezielt vorzubereiten, müssen Unternehmen ein umfassendes Cyber-Risikomanagement implementieren. Dies beinhaltet die folgenden Maßnahmen:

1. **Risikoadäquate IT-Sicherheitsstandards**
2. **Organisatorische Mindeststandards und geschulte Mitarbeiter**
3. **Notfallmanagement zum Schutz von Bilanz und sensiblen Daten**

Nur 11 Prozent der deutschen Unternehmen nutzen für ihr Cyber-Risikomanagement die Möglichkeiten der Cyber-Versicherung. Cyber-Versicherung bietet sowohl finanziellen Schutz als auch integrierte Unterstützungsleistungen der Cyber-Assistance für den Ernstfall.

ABSTRACT

Diese Studie analysiert den Bedarf nach Cyber-Versicherung und bietet einen Überblick über die Entwicklung und den aktuellen Stand des deutschen Cyber-Versicherungsmarktes.

In Deutschland ist mittlerweile jedes zweite Unternehmen von Cyber-Angriffen und Spionage betroffen. Besonders kleine und mittlere Unternehmen sind dabei attraktive Ziele für Cyber-Angriffe, da sie im Vergleich zu großen Unternehmen über geringere Sicherheitsstandards verfügen. Aber auch Großunternehmen können aufgrund von IT-Schwachstellen, der Professionalisierung der Cyber-Kriminalität und des sich ständig verändernden Risikos Angriffe selbst durch umfangreiche Investitionen in die IT-Sicherheit nicht gänzlich ausschließen.

Unternehmen sollten daher neben präventiven Maßnahmen durch entsprechend hohe IT-Sicherheitsstandards den Aufbau digitaler Kompetenz der Belegschaft sowie eines Notfallmanagements fördern. Bestimmte Schäden eines Cyber-Vorfalls können darüber hinaus durch den Abschluss einer Cyber-Versicherung abgedeckt werden. Kernelement und Mehrwert einer Cyber-Versicherung ist dabei neben entsprechendem finanziellen Schutz, der dem spezifischen Unternehmensrisiko angemessen sein muss, eine hochwertige Cyber-Assistance, die eine signifikante Reduktion der Schäden ermöglicht.

Trotz zunehmender Qualität der Cyber-Versicherungslösungen nutzen deutsche Unternehmen das Instrument der Cyber-Versicherung häufig nicht. Ein wichtiger Grund hierfür ist sicher die mangelnde Kenntnis des Cyber-Versicherungs-Angebots. Deshalb soll im Folgenden Cyber-Versicherung als Maßnahme eines sinnvollen Cyber-Risikomanagements diskutiert und die Bedeutung von Cyber-Assistance-Leistungen herausgestellt werden.

CYBER RISK AGENCY

AUTOREN

Verena Heisz
Tobias Huber
Stephanie Müller
Oliver Lehmeyer
Andreas Richter

DISCLAIMER

CYBER RISK AGENCY

ZUSAMMENFASSUNG

Die jüngsten Angriffe (z.B. „Locky“, „WannaCry“ und „Petya“) haben gezeigt, welche erhebliche Schäden durch Cyber-Kriminelle angerichtet werden können.

Bedingt durch die Nutzung automatisierter Tools hat sich nicht nur die absolute Zahl erfolgreicher Cyber-Attacken erhöht, sondern es sind auch immer häufiger kleine und mittlere Unternehmen von den Angriffen betroffen.

1. ENTWICKLUNG DER CYBER-KRIMINALITÄT

NEUE GEFÄHRDUNGSSITUATION

Mit dem Beginn des neuen Jahrtausends hat das Internet unter dem Stichwort „Web 2.0“ einen signifikanten Aufschwung hinsichtlich des Nutzungsverhaltens im privaten und im geschäftlichen Kontext erfahren. Allerdings bringt diese Entwicklung auch eine rasante Zunahme von Internetkriminalität (Cyber-Kriminalität) mit sich. Auch wenn die Gefahr durch Cyber-Kriminelle nicht ganz neu ist, hat sie insbesondere dadurch eine neue Dimension erhalten, dass Cyber-Kriminelle mittlerweile mithilfe von Hacking-Tools automatisierte und damit breit angelegte Angriffe auf identifizierte IT-Schwachstellen von Unternehmen durchführen. „Locky“, „Dyn“, „WannaCry“ und „Petya“ sind nur eine Auswahl der Cyber-Angriffe, die in den Jahren 2016 und 2017 weltweit immensen Schaden angerichtet haben.

Insbesondere Angriffe über sogenannte „Ransomware”[1] haben seit dem Einsatz des ersten Verschlüsselungstrojaners mit kombinierter Bitcoin[2]-Zahlung namens „Cryptowall” im Jahr 2013 signifikant zugenommen. Die hohe Zahlungsbereitschaft der Opfer beflügelt die Cyber-Kriminellen zu immer neuen Angriffsvarianten. Die Folge sind steigende Preise für die Entschlüsselung und eine zunehmende Professionalisierung des Angebotes an Hacking-Tools und Dienstleistungen über das sogenannte „Darknet“[3], durch die es mittlerweile keiner besonderen IT-Kenntnisse mehr bedarf, um Angriffe auf Unternehmen und Privatpersonen durchzuführen.

Bedingt durch diese Entwicklung steigen sowohl die Anzahl als auch die Streuung der durchgeführten Cyber-Angriffe. Im geschäftlichen Kontext können Cyber-Attacken hohe Verluste und Reputationsschäden bedeuten, die letztlich sogar zur Insolvenz von Unternehmen führen können. Entgegen der verbreiteten Meinung stellen derartige Angriffe nicht mehr ausschließlich eine Gefahr für große Unternehmen dar. Cyber-Kriminelle haben mittlerweile auch kleine und mittlere Unternehmen in ihr Visier genommen.

[1] Unter „Ransomware“ versteht man Schadprogramme, die Daten auf fremden Computern verschlüsseln und somit einen Zugriff ohne Entschlüsselung unmöglich machen. Für die Entschlüsselung ist ein Passwort erforderlich, das der Nutzer nur gegen Zahlung von Lösegeld (meist in Bitcoins) erhält.
[2] „Bitcoin“ ist eine digitale Währung, die im Jahre 2009 ihren Ursprung hat. Bitcoins werden in komplizierten Rechenprozessen erzeugt und auf Plattformen im Internet gehandelt. Im Gegensatz zu herkömmlichen Währungen unterliegen Bitcoins keiner Kontrolle durch Staaten oder Notenbanken.
[3] Das sogenannte „Darknet“ ist ein Teil des Internets, der nicht über Suchmaschinen und gängige Webbrowser zugänglich ist, sondern nur mithilfe spezieller Software erreicht werden kann. Es fungiert insbesondere als virtueller Schwarzmarkt für Kriminelle.

CYBER RISK AGENCY

ZUSAMMENFASSUNG

In den letzten zwei Jahren wurde jedes zweite Unternehmen Opfer von Cyber-Spionage, Sabotage oder Datendiebstahl.

Auch bei Unternehmen mit weniger als 100 Mitarbeitern waren über die Hälfte von Informationssicherheitsverstößen betroffen. Bei etwa der Hälfte der Unternehmen dieser Größenordnung ist ein geringer Reifegrad der Informationssicherheit vorzufinden.

Insbesondere kleinere Unternehmen haben erheblichen Handlungsbedarf.

Eine aktuelle Unternehmensbefragung des Digitalverbands Bitkom zeigt beispielsweise, dass jedes zweite befragte Unternehmen mit weniger als 100 Mitarbeitern innerhalb von zwei Jahren Opfer von Datendiebstahl, Industriespionage oder Sabotage geworden ist (vgl. Abbildung 1).

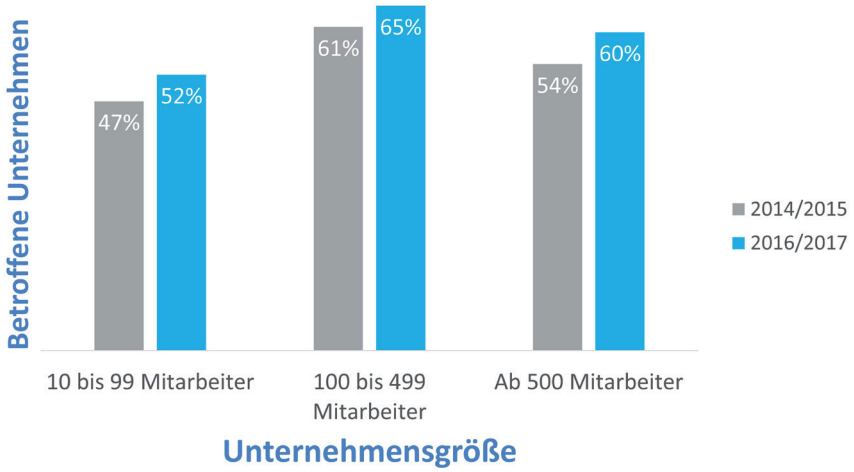

Abbildung 1: Von Cyber-Angriffen betroffene Unternehmen in Deutschland nach Unternehmensgröße[4]

Kleinere Unternehmen sind insbesondere deshalb attraktive Ziele für Cyber-Angriffe, da sie im Vergleich zu großen Unternehmen über geringere Sicherheitsstandards verfügen. So ist bei 48 Prozent der Unternehmen mit weniger als hundert Mitarbeitern der Reifegrad der Informationssicherheit als „Gering“ zu bewerten (vgl. Abbildung 2).

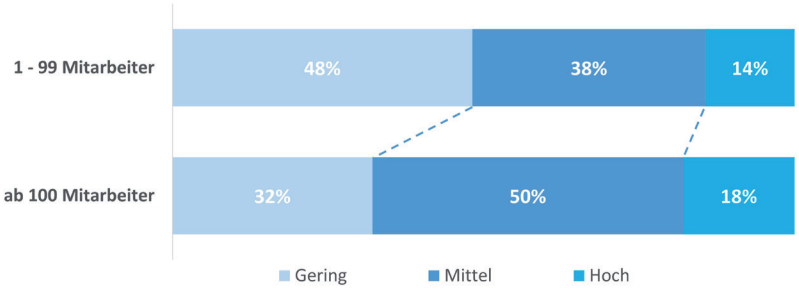

Abbildung 2: Reifegrad der Informationssicherheit nach Unternehmensgröße[5]

[4] Vgl. Bitkom (2016, 2017). Der Stichprobenumfang beträgt jeweils knapp über 1.000 Unternehmen.
[5] Bzgl. der Einordnung in die Kategorien „Gering“, „Mittel“ und „Hoch“ sowie bzgl. der Erhebung der Daten siehe Seite 12. Der Stichprobenumfang beträgt für die Kategorie „1-99 Mitarbeiter“ 56 Unternehmen und für die Kategorie „ab 100 Mitarbeiter“ 28 Unternehmen.

CYBER RISK AGENCY

BEISPIELE FÜR VERLETZUNGEN DER SCHUTZZIELE:

Vertraulichkeit:
Verletzung u.a. durch das Entwenden von Unternehmensgeheimnissen durch ehemalige Mitarbeiter oder durch Cyber-Spionage im Auftrag der Konkurrenz möglich.

Verfügbarkeit:
Störung des Zieles u.a. durch die Verweigerung des Zugriffes auf Daten durch Verschlüsselung (vgl. Ransomware-Attacke).

Integrität:
Manipulation von Unternehmensdaten (z.B. in Finanzsystemen) durch unautorisierte Dritte.

BEGRIFFSDEFINITION

Cyber-Risiken entstehen aus der Möglichkeit, unautorisiert, steuernd in virtuell vernetzte Computersysteme eingreifen zu können. Hieraus ergibt sich die Gefahr, dass Steuerungsimpulse nicht im Sinne der Eigentümer der Systeme und Daten erfolgen und diesen in der Folge ein Schaden entsteht. In einer weiter gefassten Definition sind damit alle Verstöße gegen die Ziele der Informationssicherheit zum Schutz der Vertraulichkeit, Verfügbarkeit und Integrität von Informationen gemeint (vgl. Abbildung 3). Cyber-Risiken umfassen somit alle Schutzverletzungen von Informationen, unabhängig davon, ob diese durch einen externen Angreifer oder durch einen mit der Verarbeitung und Bearbeitung von Daten beauftragten „Internen“ (zum Beispiel durch einen Mitarbeiter) verursacht werden.

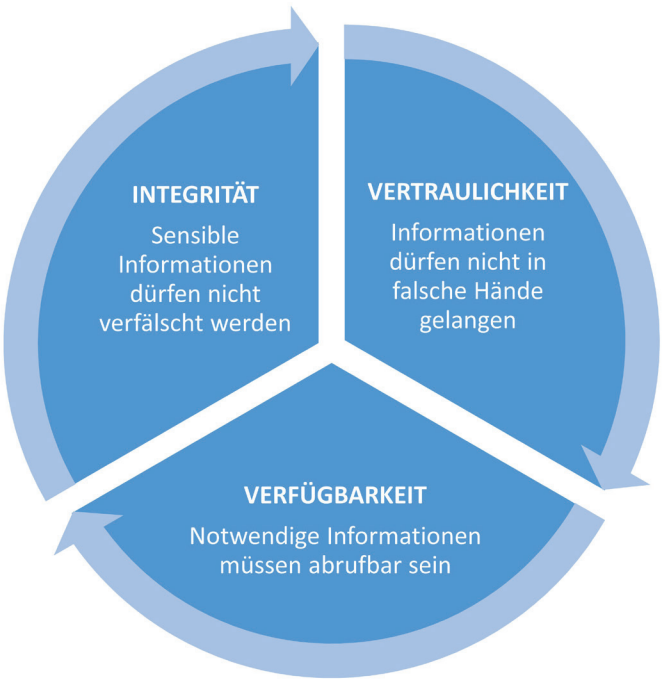

Abbildung 3: Die Schutzziele der Informationssicherheit[6]

[6] *Vgl. Bundesamt für Sicherheit in der Informationstechnik (2016).*

CYBER RISK AGENCY

ZUSAMMENFASSUNG

Cyber-Kriminelle verursachen in Deutschland jährlich Schäden von ca. 55 Mrd. EUR.
Davon entstehen 16 Mrd. EUR durch Ermittlungsaufwände, Kosten für Wiederherstellung der IT und durch Betriebsstillstand.

Der Gesamtschaden von 55. Mrd. EUR beträgt somit ca. 1,8 Prozent des deutschen Bruttoinlandsprodukts (Quelle: Statistisches Bundesamt).

Die Schäden übersteigen somit die Summe der jährlichen Leistungen deutscher Schaden- und Unfallversicherer in Höhe von ca. 49,5 Mrd. EUR (Quelle: GDV).

SCHÄDEN IN DEUTSCHLAND

Laut dem Digitalverband Bitkom entstehen der deutschen Wirtschaft durch Cyber-Kriminalität pro Jahr fast 55 Mrd. Euro an Schäden (vgl. Abbildung 4). Die Aufteilung der jährlichen Gesamtschäden für die deutsche Wirtschaft nach operativen Folgeschäden und direkten Schäden durch Spionage zeigt insbesondere die erheblichen Schäden, die der deutschen Wirtschaft im Zusammenhang mit Ermittlungen, Wiederherstellungen und Betriebsunterbrechungen entstehen. Diese machen 29 Prozent (16 Mrd. EUR) der Gesamtschäden aus. Die genannte Gesamtschadenhöhe kann hier jedoch nur als Anhaltspunkt gelten, da viele Delikte entweder nicht zur Anzeige kommen oder erst gar nicht entdeckt werden.

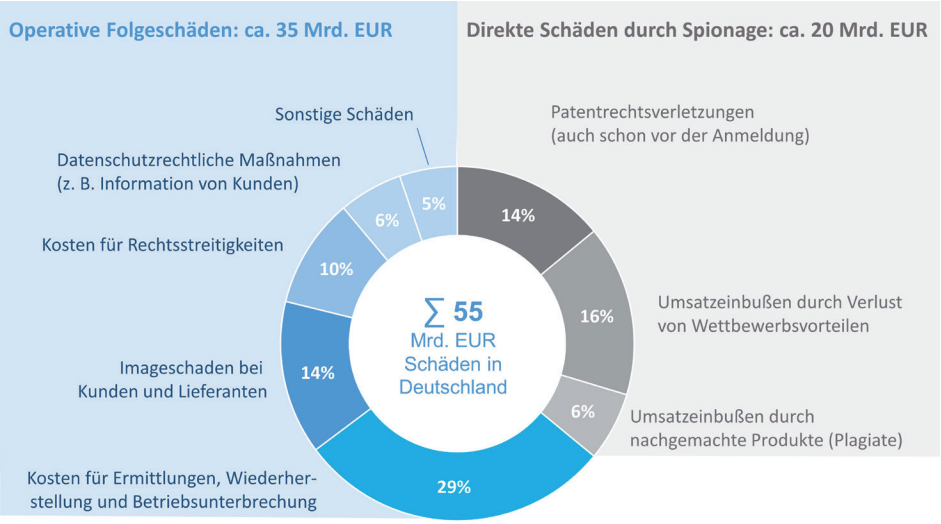

Abbildung 4: Cyber-Schäden in Deutschland[7]

IT-SCHWACHSTELLEN

Cyber-Kriminelle nutzen für ihre Angriffe die Schwachstellen von Anwendungen und IT-Sicherheitssystemen gezielt aus. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Jahr 2016 1.000 kritische Schwachstellen[8] in gängiger Standardsoftware identifiziert (vgl. Abbildung 5).

[7] *Vgl. Bitkom (2017).*
[8] *Das Bundesamt für Sicherheit in der Informationstechnik beschreibt kritische Schwachstellen als leicht ausnutzbare Schwachstellen in weit verbreiteten Systemen.*

CYBER RISK AGENCY

ZUSAMMENFASSUNG

Schwachstellen in gängiger Standardsoftware begünstigen die Angriffe durch Cyber-Kriminelle.

Das BSI hat alleine in Standardsoftware über 1.000 kritische Schwachstellen identifiziert.

Für Cyber-Kriminelle stellt jede dieser Lücken ein potentielles Einfallstor dar.

Eine absolute IT-Sicherheit kann daher in keinem Unternehmen erreicht werden.

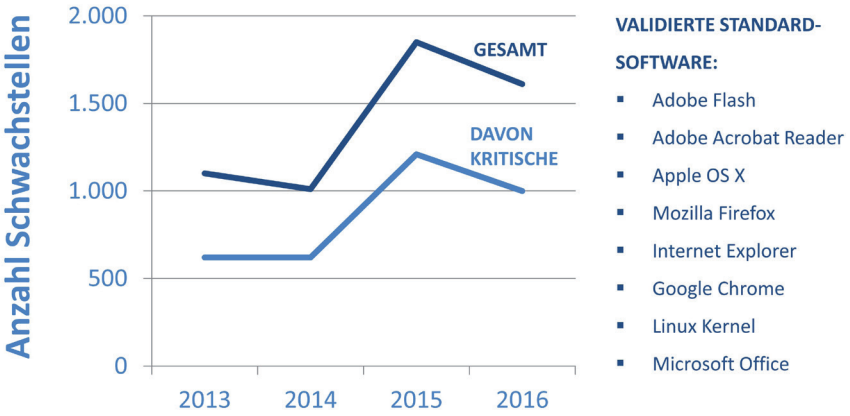

Abbildung 5: Anzahl der Schwachstellen in Standardsoftware[9]

Ebenso mussten auch die Anbieter gängiger IT-Sicherheitsanwendungen Schwachstellen in ihren Lösungen einräumen. Eben solche Schwachstellen bieten Cyber-Kriminellen ein Einfallstor, um in Computersysteme einzudringen. Derartige Lücken werden in der Hacker-Community kommerziell verbreitet und für breit angelegte Angriffe wie im Falle von „WannaCry“ und „Petya“ genutzt. Zwar sind die Anbieter von Software nach Bekanntwerden solcher Lücken bemüht, diese durch Updates zu schließen, doch werden diese Updates oft nicht konsequent und schnell genug auf der Nutzerseite eingespielt. Bei gewachsenen Altsystemen lassen sie sich oft nicht ohne nennenswerte Anpassungen und größere Investitionen in die Unternehmens-IT implementieren.

Nach Bekanntwerden stellen derartige nicht geschlossene Sicherheitslücken für Unternehmen ein erhöhtes Risiko dar, denn auch Cyber-Kriminelle erlangen durch die Veröffentlichung Kenntnis über potentielle Einfallstore.
Hinzu kommen weitere Herausforderungen durch die voranschreitende Digitalisierung. Die Anzahl vernetzter Geräte wird sowohl im privaten Umfeld als auch in Unternehmen erheblich steigen (Stichwörter: Internet of Things und Industrie 4.0). Einen derzeitigen Trend stellt auch das sog. „Smart Home“ dar, bei dem beispielsweise Kühlschränke, Fernseher und Heizungen via Smartphone oder Tablet gesteuert werden können. Anbieter sammeln Verbraucherdaten und werten diese aus. Auch Produktionsanlagen arbeiten künftig verstärkt standortübergreifend, indem sie über elektronische und webbasierte Steuerungslösungen vernetzt werden.
Unzureichende Schutzmechanismen und die Nutzung veralteter Betriebssysteme und Software mit Sicherheitslücken sind hierbei nur ein Teil des Problems. Im Rahmen der Digitalisierung kommen insbesondere durch

[9] *Vgl. Bundesamt für Sicherheit in der Informationstechnik (2016).*

CYBER RISK AGENCY

EXKURS ZUM „NEED-TO-KNOW"-PRINZIP

In 62 Prozent der Fälle sind aktuelle oder ehemalige Mitarbeiter für Informationssicherheitsverletzungen verantwortlich. Insbesondere in kleinen und schnell gewachsenen mittleren Unternehmen haben oftmals selbst Praktikanten uneingeschränkten Zugang zu sensiblen Unternehmensdaten.

Mitarbeiter sollten generell nur zu solchen Informationen Zugriff erhalten, die diese unmittelbar für die Erfüllung ihrer übertragenen Aufgaben benötigen. Erforderlich sind insbesondere:

- Ein abgestuftes Rechtesystem für den Zugriff auf und die Verschlüsselung von Daten
- Systemseitige Schutzmechanismen zum eingeschränkten Export und/ oder Druck von sensiblen Daten (zum Beispiel Kundendatenbanken).

Meist sind solche Maßnahmen auf Basis gängiger IT-Lösungen ohne großen Implementierungsaufwand umsetzbar.

immer kürzer werdende Innovationszyklen und fehlende Entwicklungsstandards immer mehr Anbieter mit internetbasierten Lösungen auf den Markt, die nicht über die notwendigen Sicherheitsstandards verfügen. Sowohl die Zunahme an Schwachstellen in mobilen Endgeräten (vgl. Abbildung 6) als auch diverse aktuelle Warnungen der Verbraucher- und Datenschützer vor Sicherheitslücken in vernetzten Endgeräten sind Indikatoren für eine Vergrößerung der Angriffsfläche für Cyber-Kriminelle.

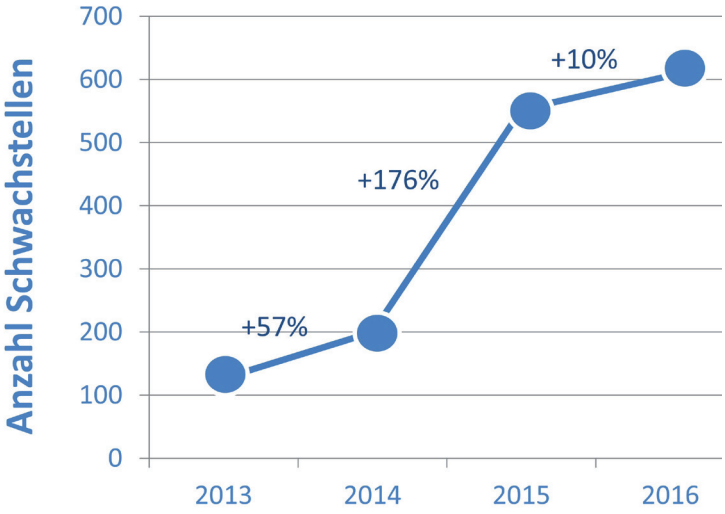

Abbildung 6: Summe der bekannten Sicherheitslücken in mobilen Endgeräten[10]

TÄTERKREISE UND ANGRIFFSARTEN

Neben den Delikten durch innerdeutsche Tätergruppen (37 Prozent) haben 23 Prozent der lokalisierten Attacken auf deutsche Unternehmen ihren Ursprung in Osteuropa. 20 Prozent der Angriffe stammen aus China und 18 Prozent aus Russland.[11] Die geographische Streuung der Cyber-Angriffe führt zu einer erschwerten Rück- und Strafverfolgung der Vergehen. Die Gefahr, Opfer von Cyber-Angriffen zu werden, geht dabei keinesfalls ausschließlich von externen Täterkreisen aus. In 62 Prozent der Fälle der letzten zwei Jahre waren es aktuelle oder ehemalige Mitarbeiter, die diese Taten verübten.[12] In 41 Prozent der Fälle kommen die Täter aus dem Wettbewerber-, Kunden-, Lieferanten- oder Dienstleisterumfeld. Hierdurch wird die Relevanz von Zugriffsrechten für Mitarbeiter nach dem sogenannten „Need-To-Know"-Prinzip deutlich, welches Mitarbeitern ausschließlich Zugriff auf Informationen ermöglicht, welche zur Erfüllung ihrer Aufgaben benötigt werden. Betrachtet man die Altersstruktur der Täter, so wird deutlich, dass hierbei jugendliche

[10] *Vgl. Symantec (2016, 2017).*
[11] *Vgl. Bitkom (2017). Der Stichprobenumfang beträgt 571 Unternehmen. Mehrfachnennungen waren dabei möglich.*
[12] *Vgl. Bitkom (2017). Der Stichprobenumfang beträgt 571 Unternehmen. Mehrfachnennungen waren dabei möglich.*

CYBER RISK AGENCY

ZUSAMMENFASSUNG

Die Professionalisierung von Cyber-Kriminellen durch den Zusammenschluss in Netzwerken und Arbeitsteilung nimmt zu. Zudem verfügen sie über ausreichend Erfahrung, denn nach einer aktuellen Statistik des Bundeskriminalamtes (BKA) sind 86 Prozent der Tatverdächtigen über 20 Jahre alt.

Bei ihren Angriffen nehmen sie dabei sowohl sensible Daten und vertrauliche Informationen als auch die Verfügbarkeit der Unternehmens-IT oder wichtige Systeme und Anwendungen in ihr Visier.

Täter nur einen geringen Anteil aller Tatverdächtigen ausmachen. Über die Hälfte (54 Prozent) der registrierten Delikte von Cyber-Kriminellen wurde von über 30-Jährigen begangen. Dabei reicht das Täterspektrum vom Einzeltäter bis hin zu international organisierten Gruppen.

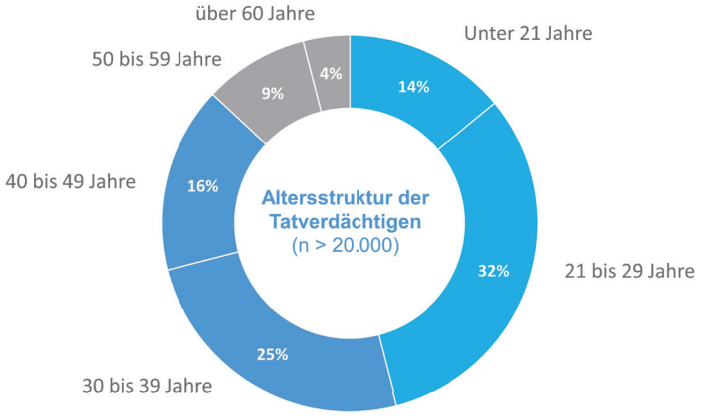

Abbildung 7: Altersstruktur der gemäß Bundeskriminalamt unter Tatverdacht stehenden Cyber-Kriminellen im Jahr 2016[13]

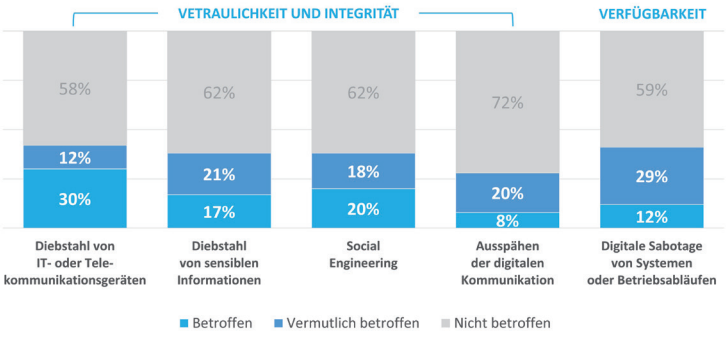

Abbildung 8: Angriffsarten auf deutsche Unternehmen[14]

Neben Angriffen auf die Vertraulichkeit und Integrität von Informationen durch Diebstahl von IT- oder Telekommunikationsgeräten, Spionage durch sogenanntes „Social Engineering“[15] und Diebstahl sensibler Unternehmensdaten werden immer wieder auch Angriffe auf die Verfügbarkeit von Systemen und Betriebsabläufen verübt. Cyber-Kriminelle starten hierbei nicht nur direkte individuelle Hackerangriffe auf Daten und Systeme, sondern auch breit angelegte Angriffe mit Hilfe automatisierter Hacking-Tools und Angriffe auf die Verfügbarkeit der Unternehmens-IT durch sog. „DDoS-Attacken“[16].

[13] Vgl. Bundeskriminalamt (2016). Die Stichprobe umfasst dabei 20.920 Tatverdächtige.
[14] Vgl. Bitkom (2017).
[15] Social Engineering wird als Versuch von Cyber-Kriminellen verstanden, mittels E-Mails, sozialer Netzwerke und anderer Formen elektronischer Kommunikation Mitarbeiter zu manipulieren und dadurch vertrauliche Informationen zu erhalten oder die Opfer im Rahmen eines Angriffs zu bestimmten Handlungen zu motivieren.
[16] Unter einer Distributed Denial of Service (DDoS)-Attacke versteht man den erpresserischen Versuch, die Verfügbarkeit der Unternehmens-IT (Computer, Server, Netze) durch Überlastung außer Kraft zu setzen.

CYBER RISK AGENCY

ZUSAMMENFASSUNG

Um sich auf Cyber-Attacken gezielt vorzubereiten, müssen Unternehmen ein umfassendes Cyber-Risikomanagement implementieren. Dies beinhaltet die folgenden Maßnahmen:

1. **Risikoadäquate IT-Sicherheitsstandards**
2. **Organisatorische Mindeststandards und geschulte Mitarbeiter**
3. **Notfallmanagement zum Schutz von Bilanz und sensiblen Daten**

Sowohl in der IT-Security als insbesondere auch bei der Vorbereitung der Organisation und ihrer Mitarbeiter auf den Ernstfall besteht in vielen Unternehmen noch Nachholbedarf.

Auch nutzen derzeit nur wenige deutsche Unternehmen Cyber-Versicherungen als Instrument des Notfallmanagements. Das geschätzte weltweite Prämienvolumen von ca. 4,1 Mrd. Dollar bezieht sich zu beinahe 70 Prozent auf Policen, die im US-Markt gezeichnet wurden (Quelle: KPMG (2017)).

2. BEDARF FÜR CYBER-RISIKOMANAGEMENT

INSTRUMENTE DES CYBER-RISIKOMANAGEMENTS

Um den vielfältigen Risiken eines Geschäftsbetriebs zu begegnen, sollten Unternehmen ein umfassendes Risikomanagement betreiben, welches Strategien zur Vermeidung, Reduktion, Übertragung und Selbsttragung von Risiken umfasst. Während im Kontext von Cyber-Risiken eine vollständige Vermeidung aufgrund fortlaufend neu identifizierter Sicherheitslücken nicht möglich ist und eine reine Selbsttragung der Risiken zu weitreichenden Konsequenzen für ein Unternehmen führen kann, ist der Reduktion und Übertragung von Cyber-Risiken besondere Bedeutung beizumessen.

Zum Schutz des Unternehmens kombiniert eine bestmögliche Abwehrstrategie gegen Cyber-Risiken daher verschiedene Instrumente des Risikomanagements.

Unternehmen sollten neben einer Basisabwehr durch präventive Maßnahmen der IT-Sicherheit vor allem auch den Aufbau digitaler Kompetenz der Belegschaft und eines effektiven Notfallmanagements fördern sowie bestimmte finanzielle Risiken eines Cyber-Vorfalls durch den Abschluss einer Cyber-Versicherung abdecken (vgl. Abbildung 9).

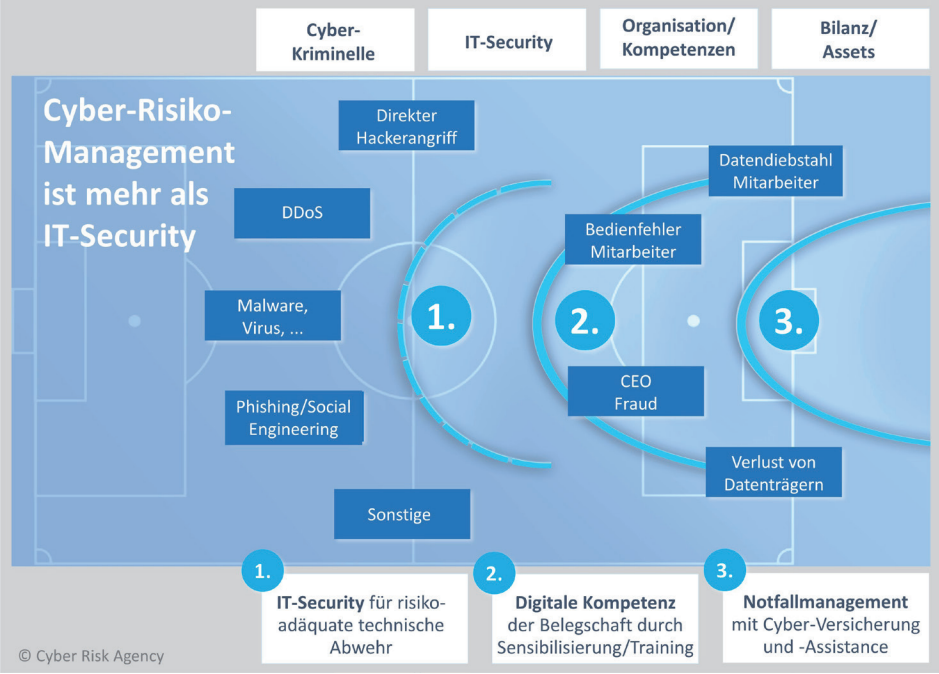

Abbildung 9: Instrumente des Cyber-Risikomanagements

CYBER RISK AGENCY

ZUSAMMENFASSUNG

Cyber-Risikomanagement ist über drei Abwehrreihen zu implementieren:

IT-Security sorgt für eine solide technische Abwehrarbeit durch gute Basisabwehr und risikoadäquate IT-Sicherheitsmaßnahmen in sensiblen Bereichen. Da Angreifer immer neue Angriffsstrategien wählen, muss IT-Security als dynamische Unternehmens-aufgabe verstanden werden.

Organisatorische Maßnahmen inkl. der Sensibilisierung und Schulung von Mitarbeitern sind neben dem zielgerichteten Einsatz von IT-Security unbedingt erforderlich. So müssen Mitarbeiter zum Beispiel auf „Social Engineering"-Angriffe wie Ausspähversuche durch Anrufer sensibilisiert werden.

Notfallmanagement zur Vorbereitung auf den Ernstfall inkl. der finanziellen Absicherung und eines professionellen CERT-Services sind bei der signifikanten Anzahl erfolgreicher Angriffe unabdingbar. Cyber-Versicherungen umfassen beide Komponenten.

1. IT-Security

Investitionen in die IT-Sicherheit sind zwingend erforderlich, um die Hürde für Cyber-Kriminelle hinreichend hoch zu setzen. Über eine solide technische Basisabwehr hinaus, die die Unternehmens-IT generell schützen soll, sind kritische Prozesse und sensible Daten wegen der besonders weitreichenden Folgen, die ein Angriff hier haben kann, gezielt nach aktuellem Stand der Technik zu schützen. Da Cyber-Kriminelle vor allem auf die Schwachstellen gängiger Lösungen abzielen und immer neue Angriffsstrategien entwickeln, müssen Unternehmen hier auch zukünftig kontinuierlich und sehr flexibel auf die sich verändernden Angriffsstrategien reagieren.

2. Digitale Kompetenz der Belegschaft

Als zweite „Line of Defense" sollte durch gezielte Mitarbeiterschulungs- und Sensibilisierungsmaßnahmen die Belegschaft mit entsprechender Kompetenz ausgestattet und somit eine „Human Firewall" im Unternehmen aufgebaut werden. Dies ist insbesondere deshalb wichtig, weil Hacker zunehmend auf sogenanntes „Social Engineering" setzen. Darunter versteht man das gezielte Ausspionieren der Unternehmen und seiner Mitarbeiter über Recherche in sozialen Netzwerken und durch gezielte Telefonanrufe in der Belegschaft. Des Weiteren sind Wechseldatenträger und E-Mails beliebte Einfallstore, um schädliche Software in der Firmen-IT zu platzieren. Entsprechend geschulte und sensibilisierte Mitarbeiter können solche Gefahren erkennen, im Ernstfall richtig handeln und das Unternehmen so vor größerem Schaden schützen.

3. Notfallmanagement mit Cyber-Versicherung

Neben den genannten Abwehrstrategien muss auch ein professionelles Notfallmanagement etabliert werden, da die Schäden aus erfolgreichen Angriffen trotz guter IT-Sicherheitsmaßnahmen erheblich sein können (vgl. Kapitel 1). Unternehmen können dies mittels des Abschlusses einer Cyber-Versicherung[17] mit professionellen Serviceleistungen wie einer 24/7-Notfall-Hotline und einem Experteneingriffsteam (sog. „CERT[18]-Service") erreichen. Eine solche Versicherung stellt eine Alternative zum Zukauf der erforderlichen Expertise für den Notfall dar, bietet die Chance auf einen schnellen Wiederanlauf der IT und deckt die Kosten für die Wiederherstellung und sonstige durch den Cyber-Angriff entstandenen Aufwände, inklusive der Ertragsausfälle während einer Betriebsunterbrechung.

[17] Im Folgenden bezieht sich der Begriff der Cyber-Versicherung ausschließlich auf Cyber-Versicherungsprodukte für Firmenkunden.
[18] CERT = Computer Emergency Response Team.

CYBER RISK AGENCY

EXKURS ZUR IT-SICHERHEIT NACH DEM „STAND DER TECHNIK“

In der IT-Sicherheit wird oft von Standards nach “Stand der Technik” gesprochen. Eine absolute Sicherheit kann aber aufgrund von Schwachstellen und sich ständig verändernden Angriffsstrategien nie garantiert werden. Neben eines Basisschutzes der Unternehmens-IT ist ein individuelles Vorgehen auf Basis einer Schutzbedarfsfeststellung sinnvoll.

REIFEGRAD DERZEITIGER ABWEHRMASSNAHMEN

Große Unternehmen verfügen in der Regel über die Ressourcen, beträchtliche Summen in IT-Sicherheit und Experten investieren zu können. Kleine und mittlere Unternehmen können dies in der Regel intern nicht abbilden und können somit beim „technischen Wettrennen“ gegen Cyber-Kriminelle oft nicht mithalten. Nicht zuletzt aus diesem Grund werden kleine Unternehmen immer häufiger Opfer solcher Angriffe. Der Reifegrad der Schutzmaßnahmen in kleinen und mittleren Unternehmen ist hierbei zumeist nicht risikoadäquat. Dies zeigt sich insbesondere in den nachstehenden Abbildungen 10 bis 14. Die Resultate beziehen sich dabei auf Daten, die durch das Online-Tool CyberRiskRadar© der Cyber Risk Agency in den Jahren 2016 und 2017 gewonnen wurden,[19] mittels dessen Entscheidungsträger kleiner und mittelständischer Unternehmen den Reifegrad ihrer Schutzmaßnahmen vor Cyber-Risiken testen können.

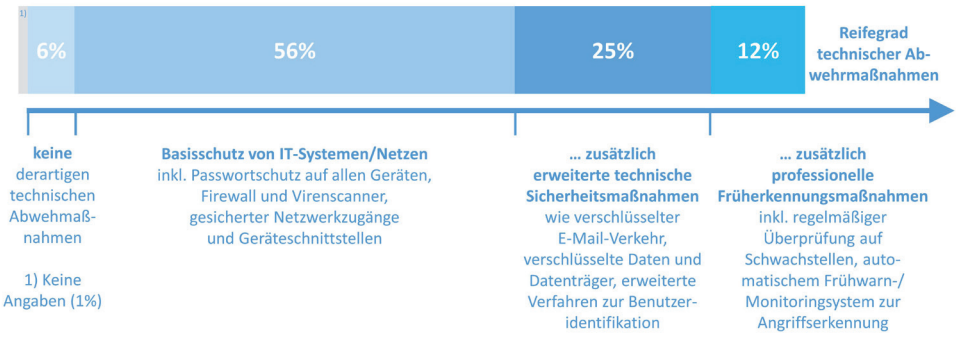

Abbildung 10: Technische Abwehrmaßnahmen kleiner und mittlerer Unternehmen

REIFEGRAD TECHNISCHER ABWEHRMASSNAHMEN

Mit 56 Prozent investiert der Großteil der kleinen und mittleren Unternehmen mindestens in einen Basisschutz für IT-Systeme und Netze (vgl. Abbildung 10). Ein Schutz nach dem „Stand der Technik“ enthält unter anderem einen umfassenden Passwortschutz sowie stets aktualisierte Firewalls und Virenscanner. 25 Prozent der Unternehmen treffen darüber hinaus erweiterte technische Sicherheitsmaßnahmen, weitere 12 Prozent unternehmen zudem professionelle Maßnahmen zur Früherkennung von Cyber-Gefahren.

[19] *Siehe www.CyberRiskAgency.de. Die Stichprobe umfasst 84 Unternehmen.*

CYBER RISK AGENCY

ZUSAMMENFASSUNG

In den meisten Unternehmen existiert ein ausreichender Basisschutz der Daten und es erfolgt eine Sicherung der Unternehmensdaten. Jedoch überprüfen nur wenige Unternehmen, ob ihre Datensicherungen auch tatsächlich funktionieren (Verwendbarkeit des Daten-Backups) und proben auch den Wiederanlauf der IT nicht.

Über 60 Prozent der Unternehmen haben keinen internen Experten für Fragen der Informationssicherheit und nur 14 Prozent verfügen über eine Zertifizierung ihrer Informationssicherheit.

REIFEGRAD DER DATENSICHERUNG

Die Hälfte der befragten Unternehmen investiert neben physischem und technischem Schutz der Daten in zusätzliche Maßnahmen des Informationsschutzes, welcher beispielsweise eine regelmäßige externe Datensicherung einschließen (vgl. Abbildung 11). Jedoch verfügen nur 21 Prozent der Unternehmen über ein Wiederanlaufkonzept. Dieses beinhaltet üblicherweise regelmäßige Tests des Wiederanlaufs bzw. das erfolgreiche Wiedereinspielen der Backup-Daten in die Systeme.

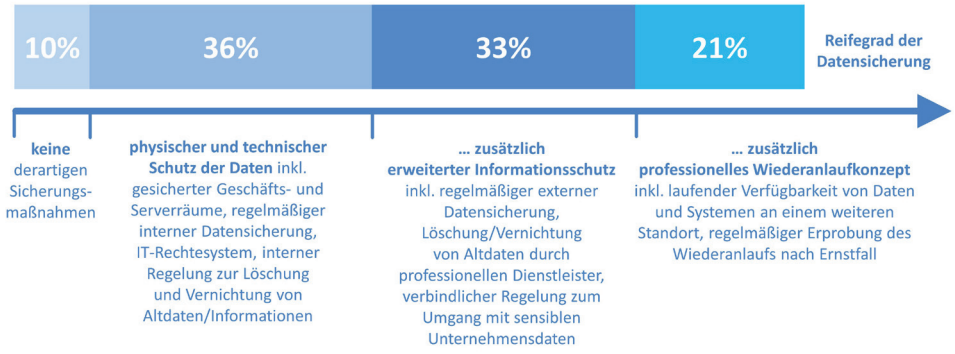

Abbildung 11: Datensicherungsmaßnahmen in kleinen und mittleren Unternehmen

REIFEGRAD ORGANISATORISCHER SICHERHEIT

Über technische Sicherheitsmaßnahmen hinaus haben 35 Prozent der kleinen und mittleren Unternehmen weder einen Datenschutzbeauftragten noch einen Informationssicherheitsexperten (vgl. Abbildung 12). Während 27 Prozent der Unternehmen ausschließlich einen Datenschutzbeauftragten einsetzen, beschäftigen 24 Prozent zusätzlich einen Experten für IT-Sicherheit und weitere 14 Prozent verfügen über eine Zertifizierung ihrer Informationssicherheit.

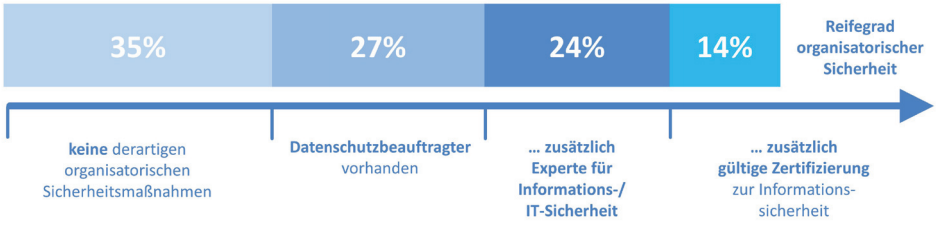

Abbildung 12: Organisatorische Sicherheitsmaßnahmen in kleinen und mittleren Unternehmen

CYBER RISK AGENCY

ZUSAMMENFASSUNG

Aktuell bereiten sich nur wenige Unternehmen ausreichend auf einen Ernstfall vor.

Zwei Drittel der Unternehmen verfügen über kein Notfallhandbuch und führen auch keine regelmäßigen Sensibilisierungs- und Trainingsmaßnahmen bei ihren Mitarbeitern durch.

Fast 70 Prozent haben keinen Versicherungsschutz für durch Cyber-Angriffe verursachte Eigenschäden und nur 11 Prozent haben eine Cyber-Versicherung mit entsprechender Cyber-Assistance zur schnellen Unterstützung im Ernstfall. Ein Grund hierfür ist vermutlich die mangelnde Kenntnis vieler Entscheidungsträger über Cyber-Versicherungsprodukte und ihre Möglichkeiten.

REIFEGRAD PERSONELLER SICHERHEIT

Hinsichtlich der personellen Sicherheitsmaßnahmen, die einen wichtigen Indikator für den Reifegrad der unternehmerischen Schutzmaßnahmen darstellen, ergreifen 23 Prozent der Unternehmen keine entsprechenden Schutzmaßnahmen. 43 Prozent der Unternehmen verfügen zwar über ein etabliertes Risikomanagement, aber nur 17 Prozent der Firmen schulen ihre Mitarbeiter auch regelmäßig, um Cyber-Angriffe erkennen und im Ernstfall richtig reagieren zu können (vgl. Abbildung 13).

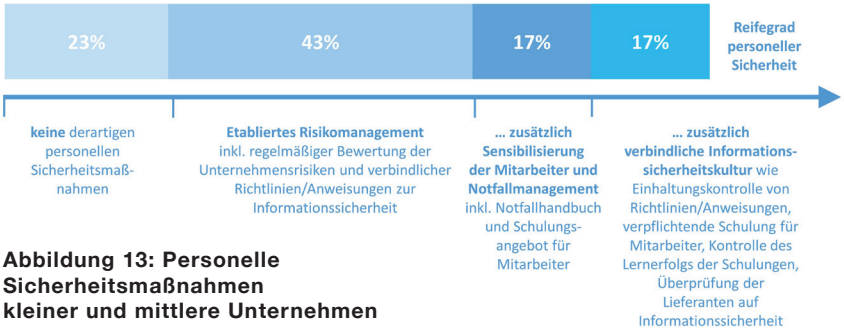

Abbildung 13: Personelle Sicherheitsmaßnahmen kleiner und mittlere Unternehmen

REIFEGRAD VERSICHERUNGS-TECHNISCHER ABSICHERUNG

Mit 11 Prozent nehmen nur sehr wenige der befragten kleinen und mittelständischen Unternehmen eine umfassende Absicherung und weiterführende Unterstützung durch Cyber-Versicherungslösungen in Anspruch (vgl. Abbildung 14). 31 Prozent der Unternehmen besitzen keine Versicherungslösung, und selbst wenn sie in Versicherungsschutz investieren, besteht dieser häufig nur aus der Deckung von Schadensersatzansprüchen von Kunden oder Partnern, nicht aber der Absicherung von entstehenden Eigenschäden.

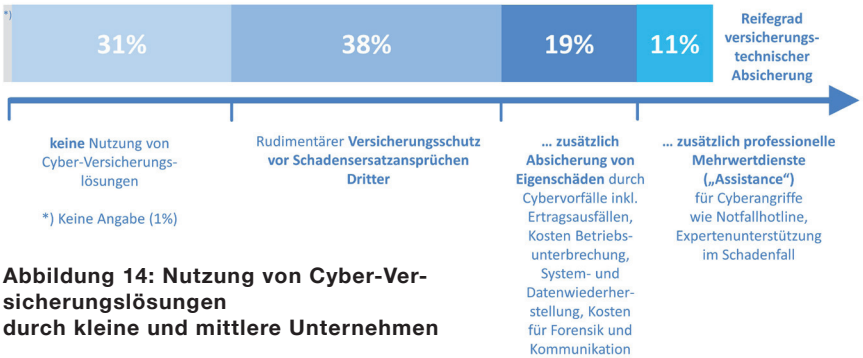

Abbildung 14: Nutzung von Cyber-Versicherungslösungen durch kleine und mittlere Unternehmen

CYBER RISK AGENCY

ZUSAMMENFASSUNG

Die Versicherbarkeit aus der Perspektive des...

Versicherungsunternehmens: Aufgrund wenig Datenerfahrung bezüglich Cyber-Vorfällen, eines sich ständig wandelnden technischen Umfelds, nur schwer quantifizierbaren Reputationsschäden und Kumul- und Ansteckungsgefahren stellt die Sicherstellung der Versicherbarkeit eine Herausforderung dar.

Versicherungsnehmers: Die bloße Existenz von Versicherungsdeckungen reicht nicht aus, um im Falle eines Cyber-Vorfalls einen adäquaten Versicherungsschutz zu besitzen. Ausschlüsse, Obliegenheiten und Selbstbehalte können in spezifischen Konstellationen dazu führen, dass der Versicherungsschutz unzureichend ist.

3. MERKMALE VON CYBER-VERSICHERUNGSDECKUNGEN

ASPEKTE DER VERSICHERBARKEIT

Vor der Betrachtung des deutschen Cyber-Versicherungsmarktes soll die Frage der Versicherbarkeit von Cyber-Risiken diskutiert werden.
Aus der Sicht des Versicherungsunternehmens werden zur Beantwortung dieser Frage die traditionellen Kriterien der Zufälligkeit, Eindeutigkeit, Schätzbarkeit, Unabhängigkeit und Größe herangezogen.[20]

Zufälligkeit
Die den Versicherungsfall auslösenden Ereignisse und ihre Konsequenzen sollen durch den Versicherungsnehmer (bzw. andere Begünstigte) nicht beeinflusst werden können. Jedoch ist denkbar, dass nach Abschluss einer Versicherungspolice Maßnahmen zur Reduktion des Schadeneintritts oder der Schadenhöhe (z.B. Mitarbeiterschulungen oder regelmäßige Sicherheitsupdates) vernachlässigt werden (internes moralisches Risiko) und somit der Eintritt oder die Höhe des Versicherungsfalles beeinflusst werden. Ebenso kann sich Versicherung auf Reparaturmärkte auswirken (externes moralisches Risiko).[21] Beispielsweise kann Cyber-Versicherung dazu führen, dass die Kosten für ein Notfallteam oder IT-Forensik steigen, falls Versicherungsverträge keine Anreize bieten, diese gering zu halten.

Eindeutigkeit
Eine eindeutige Festlegung von Versicherungsfällen und zugeordneten Versicherungsleistungen ist bei Cyber-Attacken oft nur schwer oder gar nicht möglich. So ist schon bei der Definition des versicherten Risikos die rasante Weiterentwicklung der technischen Möglichkeiten zu berücksichtigen. Darüber hinaus können z.B. die Auswirkungen eines Angriffes auf die Reputation eines Unternehmens monetär nur schwer beziffert werden und manche Angriffe bleiben unentdeckt. Zudem ist auch denkbar, dass internationale Rechtsstreitigkeiten aufgrund von Inkonsistenzen in Gesetzgebung und Rechtsprechung zu Unklarheiten führen.

Schätzbarkeit
Die Bestimmung einer Schadenverteilung auf Basis objektiver Wahrscheinlichkeiten für die Schäden durch Cyber-Attacken wird einerseits durch zu wenige Daten und andererseits durch die ständige Veränderung des Risikos beeinträchtigt. Zudem besteht die Gefahr, dass potentielle Versicherungskunden besser über ihr eigenes IT-Risiko informiert sind, was zu adverser Selektion führen kann.

[20] *Vgl. Karten (1972) sowie Karten, Nell, Richter und Schiller (2017).*
[21] *Vgl. Nell, Richter, Schiller (2009).*

CYBER RISK AGENCY

EXKURS ZUM KUMUL-POTENTIAL VON CYBER-RISIKEN

Der Verschlüsselungstrojaner „WannaCry“ nutzte im Mai 2017 eine bekannte Sicherheitslücke und befiel zahlreiche Windows-Betriebssysteme, bei denen zu diesem Zeitpunkt noch kein Sicherheitsupdate installiert wurde.

Dadurch konnten die Daten von weltweit mehr als 230.000 Systemen verschlüsselt werden.

Im November 2016 konnte ein Hacker ca. 1,25 Mio. Router eines deutschen Telekommunikationsanbieters mittels einer einzigen identifizierten Schwachstelle außer Funktion setzen.

Unabhängigkeit
Hacker können Sicherheitslücken in Standardsoftware ausnutzen und damit mittels des gleichen Angriffes weltweit viele Unternehmen gleichzeitig infizieren (Kumulrisiko). Ebenso führt die zunehmende Vernetzung von Computersystemen zu einer erhöhten Ansteckungsgefahr zwischen Unternehmen (Ansteckungsrisiko). Cyber-Versicherungsschäden können somit hochkorreliert sein.

Größe
Die Solvenz von Versicherungsunternehmen sollte nicht durch das Auftreten von sehr großen Gesamtschäden beeinträchtigt werden. Insbesondere die angesprochenen Kumulgefahren können im Hinblick auf dieses Kriterium die Grenzen der Versicherbarkeit aufzeigen.

Diese potentiellen Schwierigkeiten bedeuten jedoch nicht die prinzipielle Unversicherbarkeit von Cyber-Risiken. Einerseits ist davon auszugehen, dass nach Eintritt der neuen EU-Datenschutzverordnung mit dem Jahr 2018 die Meldung von Cyber-Attacken zunimmt und sich infolgedessen eine größere Datenbasis ergibt und andererseits zeigt die obige Diskussion Ansatzpunkte für die Gestaltung von Produkten und Services durch die Versicherer auf, durch die die Versicherbarkeit gewährleistet werden kann.[22]

Aus der Sicht der Versicherungsnehmer können so entstehende Ausschlüsse, Selbstbehalte, Obliegenheiten und Begrenzungen des Deckungsumfangs dazu führen, dass sie in bestimmten kritischen Schadenfällen nicht ausreichend geschützt sind. Ebenso werden Cyber-Versicherungspolicen, die sich auf rein monetäre Leistungen beschränken, in vielen Fällen nur einen Teil des Schadens decken bzw. das Risiko nur unzureichend absichern. Bei Schadeneintritt sind oft Assistance-Leistungen sowohl aus Kunden- als auch aus Versicherersicht entscheidend. So können insbesondere Betriebsunterbrechungsschäden durch ein schnelles und professionelles Eingreifen eines erfahrenen CERT-Services signifikant reduziert werden. CERT-Services sind jedoch zwingend mit entsprechenden Kapazitäten zu hinterlegen, die auch einem Kumulszenario mit einer Vielzahl betroffener Unternehmen standhalten. Hierfür wird in der Zukunft erforderlich sein, dass die entsprechenden Kapazitäten für Cyber-Assistance im Angebot vieler Versicherer weiter ausgebaut werden.

[22] *Während sich diese Studie auf eine skizzenhafte Beschreibung der wesentlichen Aspekte der Versicherbarkeit beschränkt, diskutieren bereits Lesch und Richter (2000) die Versicherbarkeit von IT-Risiken in größerer Tiefe.*

CYBER RISK AGENCY

ZUSAMMENFASSUNG

Die typischen Deckungskomponenten einer Cyber-Versicherung umfassen

- Ertragsausfallschäden im Fall einer Betriebsunterbrechung
- Kosten der Wiederherstellung von Daten und Systemen
- Haftpflichtansprüche von Kunden und Geschäftspartnern
- Sonstige Krisenkosten

Die wesentlichen Cyber-Assistance-Leistungen umfassen

- Hotline für den Ernstfall
- Experten-Notfallteam (CERT Service)
- IT-Forensik-Services
- Rechtsberatung für IT- und Datenschutzrecht
- Krisenkommunikation (Public Relations Maßnahmen und Informationspflichten)
- Sonstige Assistance-Leistungen (unter anderem Präventionsberatung und Optimierungsmaßnahmen nach Schäden)

TYPISCHE KOMPONENTEN EINER CYBER-DECKUNG

Die Basiskomponenten einer Cyber-Versicherung umfassen die finanzielle Deckung von Eigen- und Fremdschäden aus Sicht des Unternehmens im Fall von Informationssicherheitsvorfällen. Eigenschäden sind hierbei primär die durch eine Betriebsunterbrechung entstandenen Ertragsausfälle und fortlaufenden Kosten sowie Kosten der System- und Datenwiederherstellung. Gedeckte Fremdschäden stellen vor allem Haftpflichtansprüche von Kunden und Geschäftspartnern dar, wobei auch vertragliche und behördliche Ansprüche inbegriffen sein können. Zusätzlich gewähren Cyber-Versicherungen Deckung für diverse sonstige Krisenkosten, unter anderem Aufwendungen für IT-Forensik, Krisenkommunikation und Rechtsberatung. Abgesichert werden können hierbei Cyber-Vorfälle durch Außen- sowie durch Innentäter. Im Schadenfall leisten Cyber-Versicherungen vorrangig, d.h. vor anderen Versicherungen.

CYBER-ASSISTANCE

Neben der finanziellen Absicherung im Schadenfall kann der Abschluss einer Cyber-Versicherung für ein Unternehmen eine effektive Maßnahme zum Aufbau eines leistungsfähigen Notfallmanagements darstellen. Gleichzeitig trägt der schnelle Wiederanlauf des Betriebs als ein wesentliches Instrument zum aktiven Schadenmanagement des Versicherers bei, da dieser im Schadenfall für jeden Tag des Betriebsstillstands die entstehenden Ertragsausfallschäden und Aufwendungen für die Wiederherstellung des Betriebes bis zur versicherten Höchstsumme entschädigen muss. Auf diese Weise profitieren sowohl Kunden als auch Versicherer von einer hohen Qualität der Notfall-Assistance-Leistungen.

CYBER RISK AGENCY

ZUSAMMENFASSUNG

Es wurden 20 Anbieter von Cyber-Versicherungslösungen im deutschen Markt identifiziert.

Cyber-Versicherungslösungen werden seit 6 Jahren im deutschen Markt angeboten.

Eine weitere Zunahme des Wettbewerbs und eine damit einhergehende weitere Zunahme der Expertise sowie der Vertriebsaktivitäten sind zu erwarten.

4. ANALYSE DES DEUTSCHEN CYBER-VERSICHERUNGSMARKTES

MARKTÜBERBLICK

Abbildung 16 bietet einen Überblick über die derzeitige Anbieterlandschaft für Cyber-Versicherungspolicen in Deutschland. Seit im Jahr 2011 die erste Cyber-Deckung in Deutschland angeboten wurde, ist die Zahl der verfügbaren Cyber-Policen kontinuierlich auf mittlerweile 20 gestiegen (vgl. Abbildung 17).[23] Der Angebotszuwachs innerhalb der Jahre 2016 und 2017 um jeweils vier neue Policen steht im Einklang mit dem Anstieg der Fälle von Cyber-Kriminalität in jüngster Vergangenheit und legt somit eine nachfrageinduzierte Angebotsausweitung nahe. Aktuellen Schätzungen zufolge erreichte das Prämienvolumen für Cyber-Versicherungen in Deutschland Ende 2016 ein Volumen von etwa 100 Mio. Euro.[24] Zum jetzigen Zeitpunkt planen zudem weitere Versicherer den Eintritt in den deutschen Markt für Cyber-Policen. Mit der Zunahme der Wettbewerber kann davon ausgegangen werden, dass auch die Erfahrung und die Expertise im Umgang mit Cyber-Risiken und dadurch deren Versicherbarkeit zunimmt.

Abbildung 16: Anbieter von Cyber-Versicherungsdeckungen in Deutschland[25]

[23] Im Rahmen unserer Analyse des deutschen Cyber-Versicherungsmarktes wurden weder Lösungen für Privatkunden noch Rückversicherungslösungen betrachtet.
[24] Vgl. KPMG (2017).
[25] Swiss Re und XL Catlin treten als Erstversicherer von Cyber-Versicherungen auf. Die Anzahl der Versicherer beinhaltet mit Allianz Deutschland und Allianz Global Corporate & Specialty zwei Unternehmen, die separate Cyber-Versicherungen anbieten. In dieser Darstellung sind diese allerdings unter dem Namen des Allianz Konzerns zusammengefasst.

CYBER RISK AGENCY

ZUSAMMENFASSUNG

Die 20 identifizierten Angebote wurden anhand definierter Bewertungskriterien auf ihren relativen Leistungsumfang hin verglichen. Bewertet wurde sowohl der Deckungsumfang gemäß Versicherungsbedingungen als auch die angebotenen Cyber-Assistance-Leistungen.

METHODIK

Um den somit noch relativ jungen Markt für Cyber-Versicherungsprodukte in Deutschland auch qualitativ beschreiben zu können, wird der Leistungsumfang aller 20 Policen, die derzeit am deutschen Markt angeboten werden, systematisch bewertet. Hierzu wurden im Zeitraum von Mai bis August 2017 die Bedingungswerke sämtlicher Policen gesammelt und deren Inhalte bezüglich ihres relativen Leistungsumfangs dezidiert bewertet.

Die Analyse umfasst hierzu alle im vorherigen Kapitel vorgestellten Leistungsaspekte der beiden Kategorien Deckungsumfang und Cyber-Assistance-Leistungen. Für jeden dieser Aspekte erfolgt die Einordnung der dazu in den Versicherungsbedingungen formulierten Inhalte in eine der folgenden fünf Leistungskategorien: (1): „nicht vorhanden“, (2): „kaum vorhanden“, (3): „beschränkt vorhanden“, (4): „hauptsächlich vorhanden“ und (5): „umfangreich vorhanden“. Abbildung 19 (siehe Seite 23) zeigt einen Gesamtüberblick über die herangezogenen Aspekte in beiden Leistungskategorien. Diese Einordnung erlaubt es folglich, ein Fazit über den relativen Gesamtleistungsumfang der Produkte des momentanen Marktportfolios zu ziehen (vgl. Abbildung 18). Für die Einordnung des gesamten Leistungsumfangs aus beiden Leistungskategorien wurden die einzelnen Leistungsaspekte jeweils gleich gewichtet.

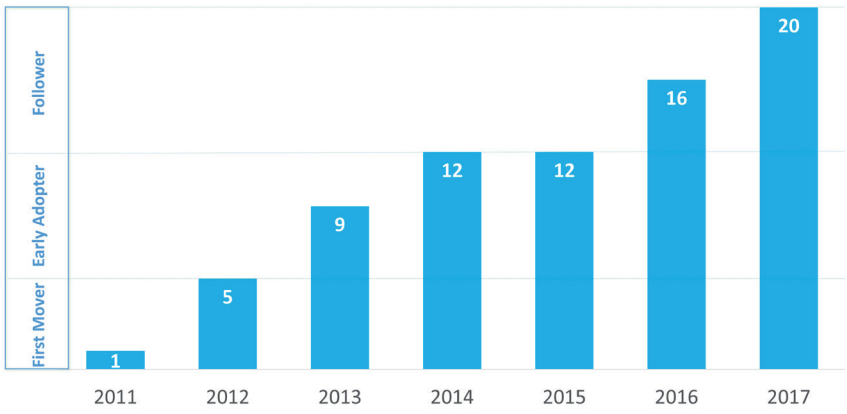

Abbildung 17: Anzahl der Anbieter im deutschen Cyber-Versicherungsmarkt nach Jahren

CYBER RISK AGENCY

ZUSAMMENFASSUNG

Cyber-Versicherungen sind sowohl bezüglich ihres Deckungsumfangs als auch bezüglich des Reifegrads ihrer Assistance-Leistungen zu bewerten.

Bei der Deckung von Eigen- und Fremdschäden unterscheiden sich die Deckungskonzepte kaum. Einzelne Anbieter bieten darüber hinaus die Deckung von Zusatzkosten wie die Aufwände interner Mitarbeiter, Sachkosten zur Kompensation von Ertragsausfällen und Vertragsstrafen.

Die Obliegenheiten der Cyber-Versicherungsprodukte unterscheiden sich stark. Besonders die zum Teil geforderten Sicherheitsstandards nach dem „Stand der Technik“ sind aufgrund ständiger Veränderungen der technischen Möglichkeiten nur schwer zu erreichen. Für Versicherungsnehmer sind diese Unterschiede daher besonders relevant.

Ein wesentliches Bewertungskriterium ist zudem der Reifegrad der Cyber-Assistance, wie z.B. die unmittelbare Handlungsfähigkeit der 24/7-Hotline und des CERT-Services.

Es zeigt sich, dass 6 der 20 untersuchten Policen sowohl in Bezug auf den angebotenen Deckungsumfang als auch bezüglich des Reifegrads der bereitgestellten Assistance-Leistungen einen relativ hohen Leistungsumfang aufweisen.
Während für den Deckungsumfang der Bedarf an Zusatzleistungen unternehmensindividuell sehr unterschiedlich sein kann, ist der Leistungsumfang der Assistance-Services insbesondere in Bezug auf die Notfallleistungen für kleine und mittlere Unternehmen ähnlich erfolgskritisch, da diese professionelle Notfallservices nur sehr schwierig in ähnlicher Effektivität aufbauen können. Entsprechend der regionalen Ausrichtung der Geschäftstätigkeit des Unternehmens bestimmt sich zudem der Bedarf nach nationalen oder internationalen CERT-Services.

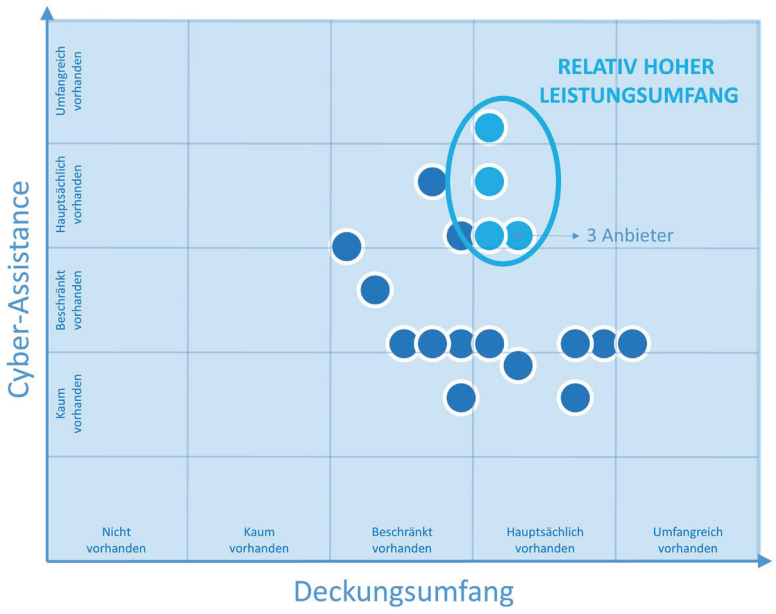

Abbildung 18: Relativer Leistungsumfang der Cyber-Policen im deutschen Markt

CYBER RISK AGENCY

BEWERTUNGSKRITERIEN DECKUNGSUMFANG (u.a.)

Ertragsausfall:
Selbstbehalt, Haftzeit, Cloud-Nutzung, Ausfälle durch fehlerhafte Bedienung

Wiederherstellungskosten:
Kompensation externer und interner Aufwände, Daten/Systeme, Wiederbeschaffungskosten

Schadenersatzforderungen Dritter:
Abwehr und Ausgleich, Vertragsstrafen

Sonstige Krisenkosten:
Forensik, Krisenkommunikation, Erpressung/Lösegeld, unautorisierte Überweisungen/Zahlungen, Vermögensschaden durch Spionage, nachgelagerte Sicherheitsverbesserung

Obliegenheiten:
IT-Security nach dem „Stand der Technik“, Überprüfung/Dokumentation der Eignung der Systeme, Sicherheitsstandards externer Partner, Gefahrenerhöhung durch neue Umstände

BEWERTUNG DES DECKUNGSUMFANGS

Die Mehrheit der angebotenen Cyber-Policen deckt die wesentlichen finanziellen Risiken des Versicherungsnehmers ab. Bei 11 der untersuchten 20 Policen können alle wesentlichen Deckungskomponenten der Kategorie „hauptsächlich vorhanden“ zugeordnet werden. Die Police mit dem höchsten Leistungsumfang in der finanziellen Schadendeckung weist überwiegend Leistungsaspekte der Kategorie 5 „umfangreich vorhanden“ auf.

Während die meisten der Cyber-Versicherer umfassende Deckungskonzepte bei den Wiederherstellungskosten anbieten, sind Einschränkungen insbesondere im Bereich der Schadenersatzforderungen gegenüber Dritten vorzufinden. Bei 9 der analysierten Policen wurden außerdem zum Teil sehr umfassende und für kleine und mittlere Unternehmen nur bedingt erfüllbare Obliegenheiten identifiziert.

Während fast alle Versicherer eine grundsätzliche Deckung von Betriebsunterbrechungsschäden inklusive daraus entstehender Ertragsausfälle gewährleisten, bieten darüber hinaus nur einzelne Versicherer eine Deckung von Ertragsausfällen und Kosten an, die nach der Wiederaufnahme des Geschäftsbetriebs als Spätfolge entstehen. Außerdem decken nicht alle Versicherer Mehrkosten, die zur Vermeidung von weiteren Ertragsausfällen (zum Beispiel die vorübergehende Nutzung einer Fremdproduktionsstätte) erforderlich sind. Auch die Deckung der Kosten für Betriebsunterbrechungsschäden, welche von eigenen Mitarbeitern durch Fehlbedienung hervorgerufen werden, stellt einen wesentlichen Unterschied zwischen den Policen dar. Die Regelungen zur Deckung der Aufwendungen zur Wiederherstellung der Unternehmens-IT weisen ebenfalls wesentliche Unterschiede in den Bedingungswerken auf. Diese können zu relevanten Konsequenzen für das Unternehmen führen, wenn es auf den schnellen Wiederanlauf der durch einen Cyber-Vorfall angegriffenen Systeme und Programme angewiesen ist. Beispielsweise sind durch einen Teil der Policen ausschließlich die Aufwendungen eines externen Dienstleistungsunternehmens, nicht aber der interne und somit direkt verfügbare Wiederherstellungseinsatz durch eigene Mitarbeiter versichert. Durch einen Versicherungsfall entstandene Schadensersatzansprüche Dritter, z.B. von Kunden oder Geschäftspartnern, werden von allen Versicherern im deutschen Markt gedeckt. Einige der Versicherer leisten zusätzlich im Fall von Vertragsstrafen aus Verstößen gegen Kreditkartenverarbeitungsvereinbarungen. Einige wenige leisten sogar für Vertragsstrafen aus der Nichterfüllung von Liefer- oder Abnahmeverpflichtungen in Folge einer Betriebsunterbrechung. Neben weiteren Unterschieden hinsichtlich zusätzlich versicherter Krisenkosten stellen vor allem auch Obliegenheiten ein wichtiges Produktmerkmal dar. Die Obliegenheiten betreffende Formulie-

CYBER RISK AGENCY

rungsunterschiede können spürbare Auswirkungen auf den Versicherungsnehmer haben. So gibt es z.B. Versicherer, die die Einhaltung des Stands der Technik für die verwendeten Systeme und Programme fordern. Eine solche Forderung kann für versicherte Unternehmen durchaus bedeutend sein, da die damit einhergehende Verpflichtung zu einer ständigen Aktualisierung in der operativen Umsetzung anspruchsvoll und kostenintensiv ist.

BEWERTUNGSKRITERIEN ASSISTANCE-LEISTUNGEN (u.a.)

Handlungsfähigkeit der 24/7-Hotline

Kapazitäten des CERT-Teams

Assistance Services aus einer Hand vs. Dienstleister-Pools

Nationaler vs. internationaler Vor-Ort-Service

Direktmandat für sofortigen Einsatz des Krisenteams

IT-Sicherheitsberatung, IT-Workshops, Audits und Notfallprozess-Implementierung

BEWERTUNG DER CYBER-ASSISTANCE-LEISTUNGEN

Generell ist der Reifegrad der Cyber-Assistance-Leistungen im deutschen Markt als heterogen zu bezeichnen. So sind bei 9 der analysierten Policen die Assistance-Leistungen nur beschränkt, bei 3 weiteren Policen sogar kaum vorhanden. Jedoch sind im Bereich der erfolgskritischen Notfall-Assistance-Leistungen hochwertige Lösungen erhältlich, die ein effizientes Notfallmanagement mittels Notfallhotline und CERT-Team bieten.

Eine weitere wichtige Komponente der Assistance-Leistungen besteht in der Einräumung eines Ermessensspielraums für die Freistellung gewisser Kosten im Schadenfall. Beauftragte Dienstleister können dann, ohne erst eine Vertragssichtung und Bewertung durch den Versicherer abzuwarten, mit ihrer Arbeit beginnen und somit das Schadenausmaß eindämmen. Viele Policen beinhalten zudem sehr ausgeprägte Services im Bereich der IT-Forensik (Beweismittelsicherung) und der Beratungsleistungen im IT- und Datenschutzrecht für den Schadenfall. In diesem Bereich und für Krisenkommunikationsleistungen, die in der Regel ebenfalls Bestandteil der Bedingungswerke sind, arbeiten Versicherer oft mit spezialisierten Partnern zusammen.

Im Rahmen der sonstigen Serviceleistungen gewähren einige Anbieter unter anderem kostenlose Reviews im Rahmen des Geschäftsabschlusses, unterstützen ihre Kunden bei der Implementierung eines Notfallprozesses oder bieten Maßnahmen zur Verbesserung der IT-Sicherheit nach einem eingetretenen Schadenfall an. Das Serviceangebot ist insbesondere für diejenigen Unternehmen interessant, die über keine eigene Expertise im Bereich der Informations- und IT-Sicherheit verfügen (sog. „Smart-Sourcing“). Versicherungsnehmer profitieren dabei auch von Preisvorteilen, die der Versicherer durch die Bündelung vieler Kunden gegenüber einem individuellen Vertragsschluss erlangen kann.

CYBER RISK AGENCY

ZUSAMMENFASSUNG

Cyber-Versicherungslösungen müssen auf das spezifische Geschäftsmodell des Unternehmens zugeschnitten sein.

Einzelne Deckungskonzepte weisen noch Lücken auf und sind zum Teil im Bereich der Unterstützungsprozesse der Assistance noch nicht bedarfsgerecht.

Die Erfüllbarkeit der Obliegenheiten unterscheiden sich teilweise stark und sind für den Kunden entscheidend, um im Schadenfall nicht mit Ausschlüssen konfrontiert zu sein.

Einzelne Angebote im deutschen Markt übertreffen insbesondere durch attraktive Zusatzdeckungen und durch erfolgskritische Assistance-Leistungen den Marktstandard.

BEWERTUNGSKRITERIEN CYBER-VERSICHERUNG	↘	⇨	↗
1. DECKUNGSUMFANG	*Negative Einschränkungen*	***Erforderlicher Mindeststandard***	*Positive Ergänzungen*
1.1 BETRIEBSUNTERBRECHUNG/ ERTRAGSAUSFALL	❑ Einschränkung der Deckung auf spezifische Cyber-Delikte ❑ Deckung in Höhe einer definierten Tagespauschale (Risiko der Unterversicherung) ❑ Haftzeitende nicht eindeutig geregelt ❑ Selbstbehalt > 12 Stunden	❑ Deckung im Fall von Informationssicherheitsvorfällen ❑ Deckung von Ertragsausfällen und fortlaufenden Kosten ❑ Haftzeit bis Ende der Betriebsunterbrechung ❑ Selbstbehalt von 12 Stunden	❑ Deckung auch im Fall von ursächlicher fehlerhafter Bedienung ❑ Deckung von Mehrkosten/ Schadenminderungskosten ❑ Haftzeit über Betriebsunterbrechungszeit hinaus ❑ Selbstbehalt < 12 Stunden
1.2 WIEDERHERSTELLUNGSKOSTEN	❑ Ausschließliche Deckung von Datenwiederherstellungsaufwendungen	❑ Deckung von Daten-, Programm- und Systemwiederherstellungsaufwendungen externer Dienstleister	❑ Deckung von Aufwendungen zur Wiederherstellung von Individualprogrammen ❑ Deckung auch von internen Wiederherstellungsaufwendungen
1.3 SCHADENERSATZFORDERUNGEN DRITTER	❑ Eingeschränkte Deckung von bestimmten Verfahrenskosten ❑ Keine Deckung von Vertragsstrafen	❑ Abwehr unbegründeter und Ausgleich begründeter Schadenersatzansprüche ❑ Teilweise Deckung von Vertragsstrafen	❑ Deckung von Vertragsstrafen
1.4 SONSTIGE KRISENKOSTEN	❑ Keine Deckung im Fall von Cyber-Erpressungen	❑ Deckung von Aufwendungen für IT-Forensik, PR- und Rechtsberatung ❑ Deckung im Fall von Cyber-Erpressung	❑ Deckung von Schäden durch unautorisierte Überweisungen/Zahlungen ❑ Deckung von Vermögensschäden durch Cyber-Spionage ❑ Deckung von Aufwendungen für nachgelagerte Sicherheitsverbesserungen
1.5 OBLIEGENHEITEN	❑ Stand der Technik zum Schutz der Systeme ❑ Regelmäßige Überprüfung/Dokumentation der Eignung der eigenen Systeme ❑ Überprüfung der Informationssicherheitsstandards externer Partner ❑ Auswahl geeigneter Mitarbeiter ❑ Gegenmaßnahmen für Systeme mit bekannten Sicherheitslücken ❑ Im Schadenfall muss das Schadenbild in unverändertem Zustand belassen werden ❑ Unspezifische Auflage zur Anzeige von Gefahrenerhöhungen ❑ Hoher sonstiger Umfang der Obliegenheiten	❑ Betriebswirtschaftlich angemessener Schutz der Systeme und Daten inkl. einzelner Mindestanforderungen ❑ Mindeststandards für Outsourcing/ Cloud-Nutzung ❑ Spezifische Auflage zur Anzeige von Gefahrenerhöhungen	❑ Nennung spezifischer Mindestanforderungen an die IT-Sicherheit ❑ Spezifische Definition des Umgangs mit Risiken der Cloud-Nutzung
2. REIFEGRAD ASSISTANCE	*Negative Einschränkungen*	***Erforderlicher Mindeststandard***	*Positive Ergänzungen*
2.1 HOTLINE FÜR DEN ERNSTFALL	❑ Hotline ohne Schadenminderungs-Auftrag (z.B. reine Rechtsberatung) und kein Beauftragungsmandat für CERT-Service	❑ 24/7 Hotline mit Notfallmanagement-Leistungen (telefonische Erstberatung) inkl. Beauftragungsmandat für CERT-Service	❑ Voll handlungsfähige 24/7-Hotline mit Notfallmanagement-Leistungen inkl. Zuschaltung auf Systeme, Rechtsberatung und Mandat für die Beauftragung eines CERT-Service
2.2 EXPERTEN-NOTFALLTEAM (CERT-SERVICE)	❑ Nach Schadenmeldung erfolgt Qualifizierung und/oder CERT-Service-Dienstleister-Auswahl mit dem Versicherer ❑ Reiner Dienstleisterpool (Überprüfung Qualitätsstandards?) ❑ Nur geringe Notfall-Team-Ressourcen (Risiko von Kapazitätsengpässen im Kumulszenario)	❑ Eingeschränktes Leistungsmandat für CERT-Service ohne Freigabeerfordernis durch Versicherer ❑ Nationale Lösung zzgl. internationaler Ausweitungsoptionen ❑ Gebündelte Dienstleister-Ressourcen mit ausreichender Kapazität	❑ CERT-Service direkt per Notfallhotline mobilisierbar ❑ Internationaler Vor-Ort-Service ❑ Implementiertes Notfallmanagement (schon zum Vertragsabschluss) ❑ Skalierbare Ressourcen im Kumulszenario
2.3 WEITERE KRISENSERVICES	❑ Nur teilweise vorhanden und/oder nur über frei konfigurierbares Dienstleisterportfolio organisiert	Eingespieltes Expertenteam mit ... ❑ IT-Forensik-Service ❑ Rechtsberatung für IT- und Datenschutzrecht ❑ Krisenkommunikation	❑ Gebündelte Krisenmanagement-Services aus einer Hand
2.4 SONSTIGE LEISTUNGEN	❑ Kostenpflichtige Sicherheitsaudits vor Vertragsabschluss ❑ Keine Informations- und Awareness-Leistungen	❑ Bedarfsgerechte Sicherheitsaudits bei Vertragsabschluss (kostenfrei) ❑ Diverse Informations- und Awareness-Leistungen	❑ Schutzbedarfsfeststellung vor Vertragsabschluss (kostenfrei) ❑ Beratungsleistungen und Workshops zu Informationssicherheitsthemen ❑ Verbesserungsleistungen der IT-Sicherheit nach eingetretenem Schadenfall

Abbildung 19: Schematische Bewertung von Cyber-Versicherungslösungen im Vergleich zum erforderlichen Mindeststandard

CYBER RISK AGENCY

EXKURS ZUR EU-DATENSCHUTZ-GRUNDVERORDNUNG

Gesetzeseintritt: 2018

Inhalte (u.a.):
Bei Datenschutzverstößen müssen sowohl die Aufsichtsbehörden als auch die betroffenen Personen umgehend informiert werden.

Sanktionen (u.a.):
Die Aufsichtsbehörden können Geldbußen in der Höhe bis zu 2 Prozent des jährlichen weltweiten Umsatzes verhängen. Unter gewissen Umständen können sich diese sogar auf 4 Prozent des jährlichen weltweiten Umsatzes erhöhen (Art. 83). Zudem kann die Datenverarbeitung vorübergehend oder endgültig beschränkt werden (Art. 58(2)).

5. ZUSAMMENFASSUNG UND AUSBLICK

Diese Studie diskutiert Versicherung als Maßnahme des Risikomanagements für Cyber-Vorfälle und analysiert deren Komponenten.

Unter Berücksichtigung der dynamischen Entwicklung von Cyber-Risiken und existenter Schwachstellen von Informationstechnologien reichen Investitionen in IT-Sicherheit für das Management von Cyber-Risiken alleine nicht aus. Für Entscheidungsträger in Unternehmen bedeutet dies, dass verstärkt digitale Kompetenz im Unternehmen aufgebaut werden muss, um den mit der Digitalisierung einhergehenden Risiken begegnen zu können. Daneben kann der Abschluss einer Cyber-Versicherung sinnvoll sein, um einerseits den finanziellen Risiken eines Cyber-Angriffes Rechnung zu tragen und andererseits durch den Einkauf von Cyber-Assistance ein professionelles Notfallmanagement zu etablieren. Insbesondere kleine und mittlere Unternehmen haben hier Nachholbedarf, da sie in der Regel über geringere IT-Sicherheitsstandards als Konzerne verfügen.

Die Anzahl der Anbieter im deutschen Cyber-Versicherungsmarkt hat seit 2011 stark zugenommen und umfasst derzeit 20 Versicherungsunternehmen. Die 20 identifizierten Angebote wurden anhand definierter Bewertungskriterien auf ihren relativen Leistungsumfang hin verglichen. Bewertet wurde sowohl der Deckungsumfang gemäß Versicherungsbedingungen als auch die angebotenen Cyber-Assistance-Leistungen. Weiterentwicklungen bei den gedeckten Komponenten sind im Laufe der Zeit durch den Zugewinn von Erfahrung und Daten zu erwarten. Handlungsbedarf besteht allerdings bei der Hinterlegung von Notfall-Services mit entsprechenden Kapazitäten. Aufgrund der Gefahr von Kumul- und Ansteckungsrisiken können Cyber-Vorfälle bei vielen Unternehmen gleichzeitig auftreten, sodass Versicherungsunternehmen eine höhere Dienstleistungskapazität für ihr Notfallmanagement benötigen, um allen Versicherungskunden schnell Hilfe bereitstellen zu können. Zukünftig wird die Bedeutung von Cyber-Risikomanagement in der strategischen Unternehmensplanung noch weiter steigen. Es ist nicht nur von einer weiteren Professionalisierung der Cyber-Kriminalität auszugehen, sondern es wird auch die Anzahl der IT-Schwachstellen durch technologische Entwicklungen, wie z.B. das Internet of Things oder die Industrie 4.0, zunehmen. Ebenso sind Attacken auf die Verfügbarkeit von Cloud-Services denkbare Szenarien. Darüber hinaus werden im Jahr 2018 mit dem Inkrafttreten der neuen Datenschutz-Grundverordnung der Europäischen Union die Rechte der Verbraucher gestärkt. Unternehmen werden unter anderem dazu verpflichtet, ihre Kunden möglichst schnell über Datenschutzverstöße bzw. Cyber-Vorfälle zu informieren. Verstöße gegen diese Bestimmungen können mit empfindlichen Bußgeldern bestraft werden.

CYBER RISK AGENCY

Mit freundlicher Unterstützung von

- AIG
- Allianz
- AXA
- CNA Hardy
- CHUBB
- DUAL
- ERGO
- Gothaer
- HDI
- Hiscox
- Markel
- R+V Versicherung
- Provinzial
- SV Sparkassen Versicherung
- Swiss Re
- Tokio Marine
- W&W Württembergische
- XL Catlin
- Zurich Versicherung

QUELLENVERZEICHNIS

Bundesamt für Sicherheit in der Informationstechnik, 2016. Leitfaden Informationssicherheit – IT-Grundschutz kompakt. [online] unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf

Bundesamt für Sicherheit in der Informationstechnik, 2016. Die Lage der IT-Sicherheit in Deutschland 2016. [online] unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf

Bundeskriminalamt, 2016. Cybercrime – Bundeslagebild 2016. [online] unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.pdf

Bitkom, 2016. Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter. [online] unter: https://www.bitkom.org/noindex/Publikationen/2015/Studien/Studienbericht-Wirtschaftsschutz/150709-Studienbericht-Wirtschaftsschutz.pdf

Bitkom, 2017. Wirtschaftsschutz in der digitalen Welt. [online] unter: https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017.pdf

Karten, W., 1972. Zum Problem der Versicherbarkeit und zur Risikopolitik des Versicherungsunternehmens – betriebswirtschaftliche Aspekte. *Zeitschrift für die gesamte Versicherungswissenschaft*, 61, S. 279-299.

Karten, W., Nell, M., Richter, A. und Schiller, J., 2017. *Risiko und Versicherungstechnik – Eine ökonomische Einführung*. Wiesbaden: Springer.

KPMG, 2017. Neues Denken, Neues Handeln - Insurance Thinking Ahead - Versicherungen im Zeitalter von Digitalisierung und Cyber - Studienteil B: Cyber. [online] unter: https://home.kpmg.com/de/de/home/themen/2017/02/cyber-versicherungen-werden-zum-must-have.html

Lesch, T. und Richter, A., 2000. Risiken aus kommerzieller Nutzung des Internet – Möglichkeiten der Schadenverhütung und Versicherung. *Zeitschrift für die gesamte Versicherungswissenschaft*, 89(4), S. 605-633.

Nell, M., Richter A. und Schiller, J., 2009. When prices hardly matter – Incomplete insurance contracts and markets for repair goods. *European Economic Review*, 53(3), S. 343-354.

Symantec, 2016. Internet Security Threat Report. [online] unter: https://www.symantec.com/content/dam/symantec/docs/security-center/archives/istr-16-april-volume-21-en.pdf

Symantec, 2017. Internet Security Threat Report. [online] unter: https://www.symantec.com/de/de/security-center/threat-report

ÜBER DIE CYBER RISK AGENCY UND DAS MUNICH RISK AND INSURANCE CENTER

CYBER RISK AGENCY

Die Cyber Risk Agency ist Spezialmakler für Cyber-Versicherungen und Best-Practice-Lösungen im Bereich Informationssicherheit für kleine und mittlere Unternehmen. Sie bietet unabhängige Beratung und Vermittlung für:

- Cyber-Versicherungen inkl. außergerichtliche Vertretung von Interessen im Schadenfall
- IT-Security-Lösungen für risikoadäquaten Schutz
- Consultingleistungen zur Informationssicherheit (Audits, Zertifizierung, Penetration-Testing etc.) im Expertennetzwerk
- Mitarbeitertrainings für Prävention und Ernstfall

In einem sowohl angreifer- als auch anbieterseitig hoch dynamischen Umfeld analysiert die Cyber Risk Agency hierzu laufend den Markt und leistet individuell Beratung, um ihre Kunden bestmöglich vor Cyber-Kriminellen zu schützen.

Wie sicher ist Ihr Unternehmen? Machen Sie den kostenlosen Onlinetest mit dem CyberRiskRadar, der von der Initiative Mittelstand aktuell mit dem „Best of Innovationspreis 2017“ ausgezeichnet wurde.

MUNICH RISK AND INSURANCE CENTER

Das Munich Risk and Insurance Center (MRIC) an der Ludwig-Maximilians-Universität München fördert Forschung und Lehre im Bereich Risikomanagement und Versicherung am Standort München. Es bietet eine Infrastruktur für den aktiven Austausch zwischen Theorie und Praxis. Als interdisziplinäres Zentrum richtet das MRIC Konferenzen und ähnliche Veranstaltungen aus und initiiert und unterstützt Forschungsprojekte zum Thema Risikomanagement und Versicherung. Das MRIC bietet den beteiligten Forschern eine Plattform, um ihre Zusammenarbeit und insbesondere auch die Vernetzung mit Kooperationspartnern aus Theorie und Praxis weiter zu stärken. Darüber hinaus engagiert sich das Center in der Förderung von Studierenden und Nachwuchswissenschaftlern des Faches. Um Studierende mit Interesse an versicherungs- und risikomanagementbezogenen Themen gezielt zu unterstützen, steht das MRIC in intensiver Zusammenarbeit mit seinen Praxispartnern. Insbesondere gilt dies auch für den am Center beheimaten berufsbegleitenden Studiengang „Executive Master of Insurance“, der sich an hochmotivierte Young Professionals aus der Versicherungsbranche richtet (www.EMInsurance.de).

CYBER RISK AGENCY

CYBER RISK AGENCY

Versicherungsmakler gem. §34d Abs. 1 GewO

Gründung: 2016

Geschäftsführung:
Oliver Lehmeyer

Kontakt:
info@cyberriskagency.de

Homepage:
www.CyberRiskAgency.de

MUNICH RISK AND INSURANCE CENTER

Gründung: 2010

Direktor:
Prof. Dr. Andreas Richter

Geschäftsführung:
Dr. Stephanie Müller

Kontakt:
s.mueller@bwl.lmu.de

Homepage:
www.mric.lmu.de