Benchmark
28 Cyberversicherungen für kleine und mittlere Unternehmen (KMU)

infodas
connect more. be secure.

© infodas Juli 2020

Autoren: Moritz Durdel, Simon Ewers, Tobias Krauss

Die Studie wurde im Rahmen des Moduls IT-Management der Universität der Bundeswehr München unter der Betreuung von infodas (Sebastian Dännart, Dr. Alexander Schellong) erstellt.

Die in diesem Studiendokument veröffentlichten Inhalte, Werke und bereitgestellten Informationen unterliegen dem deutschen Urheberrecht. Der Urheber infodas GmbH erlaubt eine Vervielfältigung und Verlinkung der Inhalte - auch in Auszügen - solange deren Urheberschaft ausreichend deutlich gemacht wird. Jede Bearbeitung, Veränderung oder Verwertung außerhalb der Grenzen des Urheberrechts bedarf der vorherigen schriftlichen Zustimmung des jeweiligen Rechteinhabers.

Vorwort

Wir arbeiten seit vielen Jahren eng mit Universitäten und anderen Forschungseinrichtungen zusammen. Einige unserer Mitarbeiter haben an der Universität der Bundeswehr in München studiert. Insofern haben wir uns gefreut mit den Studententeams aus dem Modul IT-Management unterschiedliche Themen in der Cybersicherheit genauer zu untersuchen.

Im Rahmen unserer Beratungsprojekte im Bereich der IT-Sicherheit werden wir zunehmend auch mit Fragen zu Cyberversicherungen konfrontiert. Dies gilt für Großunternehmen wie für kleine und mittelständische Unternehmen gleichermaßen. Neben Cybersicherheitsprodukten, Prozess- und Verhaltensänderungen, stellen derartige Policen ein weiteres Element in einem ganzheitlichen Ansatz zum Umgang mit Cyberrisiken dar.

Interessenten stehen jedoch vor der Herausforderung die passende Wahl aus einer Vielzahl an Angeboten zu treffen. Diese Studie versucht einen strukturierten Überblick über den Abschlussprozess und die jeweiligen Produktbestandteile aus der Sicht zweier fiktiver Unternehmen zu geben. Wie bei jedem Benchmark, hängt das Ergebnis von der gewählten Methode und der Bewertung der Durchführenden ab. Entsprechend sollten die Ergebnisse interpretiert werden.

Wir wünschen Ihnen Freude beim Lesen und hoffen, dass Sie neue Erkenntnisse gewinnen können.

Carsten Schulz
Managing Director
INFODAS GmbH

Severin Quell
Director IT Security Consulting
INFODAS GmbH

Zusammenfassung

Das Ziel der vorliegenden Studie war Cyberversicherungen für kleine und mittlere Unternehmen (KMU) in Deutschland einheitlich auf Basis eines Bewertungsbogens und fiktiver Musterfirmen zu vergleichen. Die Ergebnisse der Studie richten sich an relevante Vertreter der Versicherungswirtschaft und Entscheider bei KMU.

Die Fähigkeiten zur Selbstwahrnehmung der eigenen Bedrohungslage und Gefahrenabwehr scheint bei vielen KMU nicht oder nur eingeschränkt vorhanden zu sein. Warum sollte man sich für sie interessieren? Dementsprechend gibt es auch nur eine geringe Bereitschaft in eine Cyberversicherung zu investieren.

Wenn sich ein Unternehmen (KMU) für eine Cyberversicherungen entscheidet, steht es vor der Herausforderung das passende Angebot aus einer wachsenden Anzahl von Versicherungstarifen zu identifizieren.

Für die Musterfirmen konnten keine signifikanten Unterschiede in den Tarifen festgestellt werden. Es gab nur leichte Abweichungen, welche durch Umsatz und gewünschter Versicherungssumme beeinflusst wurden, jedoch nicht durch den Industriesektor.

Im Bereich „Abschluss" liegt der Fokus auf dem Onlinekanal. 72% der Versicherungsunternehmen erlauben die vollständige Onlineabwicklung. Mit steigender Größe, Umsatz und der Versicherungssumme von KMU dürfte der persönliche Vertragsabschluss vorgezogen werden. Insgesamt sollten die Informationsseiten zu den Cyberpolicen noch weiter im Hinblick auf Nutzerfreundlichkeit und Informationsvermittlung verbessert werden.

Im Bereich Risikobetrachtung und Leistungsumfang sind die Versicherer gut und breit im Sinne der AVB Cyber aufgestellt. Lediglich in Hinblick darauf, wie gut man ein KMU in den Versicherungsbedingungen abbilden kann, treten deutliche Unterschiede auf, die sich auch stark auf die Gesamtbewertung auswirkten.

Im Bereich Leistungskategorien sind Schäden, sowohl Eigenschäden als auch Drittschäden, deutlich besser als Serviceleistungen wie die Krisenkommunikation in den Policen abgedeckt. Ob Versicherungsangebote auch ohne diese Leistungen erfolgreich wären, müsste geprüft werden.

Die Cyberpolice Cyber Clear der Hiscox belegt den ersten Rang. Allianz, AXA, Condor, Ergo, Signal Iduna sowie VHV teilen sich Rang Zwei. Auf dem dritten Rang sind Gothaer und Württembergische gefolgt von der R+V auf Rang Vier.

Für zukünftige Studien wäre nicht nur eine regelmäßige Wiederholung eines Benchmarks interessant, sondern auch detailliert die Anforderungen und Ansichten der Versicherten zu den Cyberpolicen zu erfassen.

Es ist davon auszugehen, dass der Markt für Cyberversicherungen analog zu den steigenden Cybervorfällen weiterwachsen und an Bedeutung gewinnen wird. Die Versicherten werden weiterhin die Herausforderung haben den passenden Tarif aus einer Vielzahl von Angeboten auszuwählen und im Vorfeld ihre Cybersicherheit oder -risiken zu verstehen.

1 Inhalt

Vorwort 3

Zusammenfassung 5

Abbildungsverzeichnis 7

Tabellenverzeichnis 8

1. Ziel der Studie 9

1.1 Abgrenzung KMU 11

2. Ergebnisse aktueller Forschung 12

2.1 Cyberversicherungen als Beitrag zur IT-Sicherheit 12

2.2 Wirtschaft: Optimism Bias 2.0 14

3 Benchmarking 18

3.1 Methode 18

3.1.1 Musterfirma Maschinenbau 19

3.1.2 Musterfirma Gesundheitswesen 20

3.1.3 Typische Cyberrisiken der Musterfirmen 20

3.1.4 Herleitung der Benchmarking-Kriterien 25

3.2 Anbieterübersicht 29

3.3 Produkteigenschaften Versicherung 30

3.4 Ergebnisse 36

3.4.1 Abschluss 36

3.4.2 Risikobetrachtung 37

3.4.3 Leistung 38

3.4.4 Bewertung 43

Abbildungsverzeichnis

Abbildung. 1: Zunahmen der Gefährdungsbewertung „Cyber Incidents“ im Allianz Risk Barometer. 14

Abbildung 2: (Lechner, 2017)): Schätzung der derzeitigen Bedrohungslage im Bereich IT-Sicherheit für die eigene Organisation, Branche und Wirtschaftsraum Deutschland. 15

Abbildung. 3: (nach (Lechner, 2017)): Einschätzung der Fähigkeit der eigenen Organisation / der eigenen Branche / des Wirtschaftsraums Deutschland, Cyberattacken abzuwehren. 16

Abbildung 4: Erfolgreiche Cyberangriffe 21

Abbildung 5: Übersicht Bandbreite DDoS-Angriffe 2018 22

Abbildung 6: Exemplarischer Aufbau Ratingbogen 25

Abbildung 7: Ratingbogen (Bausteine „Preis“ & „Gesamtbewertung“) 28

Abbildung 8: Exemplarischer Aufbau Firmenwebsite Signal Iduna 36

Abbildung 9: Exemplarischer Aufbau Corporate Website Hiscox 37

Abbildung 10: Verteilung der Bewertungen des Bausteins „Systemwiederherstellung“ 38

Abbildung 11: Verteilung der Bewertungen des Bausteins „Datenwiederherstellung“ 39

Abbildung 12: Verteilung der Bewertungen des Bausteins „Wirtschaftliche Schäden durch Betriebsunterbrechung“ 39

Abbildung 13: Verteilung der Bewertungen des Bausteins „Lieferverzug“ 40

Abbildung 14: Verteilung der Bewertungen des Bausteins „Datenmissbrauch“ 40

Abbildung 15: Verteilung der Bewertungen des Bausteins „Serviceausfall“ 41

Abbildung 16: Verteilung der Bewertungen des Bausteins „Rechtsschutz“ 41

Abbildung 17: Verteilung der Bewertungen des Bausteins „IT-Forensik-Experten“ 42

Abbildung 18: Verteilung der Bewertungen des Bausteins „Krisenkommunikation“ 42

Tabellenverzeichnis

Tabelle 1: Überblick Musterfirma Werkzeug GmbH 19
Tabelle 2: Überblick Arztpraxis Dr. Schröder 20
Tabelle 3: Versicherer und ihre Produkte 29
Tabelle 4: Produktbestandteile und Erläuterung 31
Tabelle 5: Versicherungsunternehmen und Produktbestandteile 1/4 32
Tabelle 6: Versicherungsunternehmen und Produktbestandteile 2/4 33
Tabelle 7: Versicherungsunternehmen und Produktbestandteile 3/4 34
Tabelle 8: Versicherungsunternehmen und Produktbestandteile 4/4 35
Tabelle 9: Ranking der Versicherungsunternehmen und Cyberpolicen 43

1. Ziel der Studie

Spätestens seitdem Mitte 2017 der Cyberangriff *WannaCry* weltweit die mediale Berichterstattung dominierte, ist der Begriff Ransomware[1] auch außerhalb von Fachkreisen weit verbreitet. In über 150 Ländern infizierte *WannaCry* mehr als 230.000 Rechner[2], Schätzungen des insgesamt verursachten Schadens liegen zwischen einigen Hundert Millionen und vier Milliarden Dollar[3].

Welche konkreten Folgen ein derartiger Cyberangriff für betroffene Firmen haben kann, zeigte sich erneut Ende des Jahres 2018 am Beispiel des Münchner Anlagenbauers Krauss Maffei: an zwei Standorten in Deutschland musste die Produktion des Unternehmens infolge einer Ransomware-Attacke auf Fertigungsanlagen gedrosselt werden[4].

Doch damit ist Krauss Maffei bei Weitem kein Einzelfall. Eine im Frühjahr 2018 für den Gesamtverband der Deutschen Versicherungswirtschaft (GDV) durchgeführte Forsa-Befragung mit dem Titel „Cyberrisiken im Mittelstand" ergab u. a., dass 30 % der befragten Unternehmen von wirtschaftlichen Schäden durch Cyberattacken betroffen waren[5]. Von den betroffenen Unternehmen mussten wiederum 43 % den Betrieb zeitweise stilllegen[6].

Vor diesem Hintergrund erscheint es folgerichtig, dass vor allem kleine und mittlere Unternehmen (KMU)[7] daran interessiert sind, Cyberrisiken durch eine Cyberversicherung abzudecken. Erfolgreiche IT-Governance beginnt jedoch erst dort, wo betriebliches Risikomanagement die Dimension „Cyber" entsprechend ihrer hohen Bedeutung vollumfänglich integriert. Einzelmaßnahmen, wie z. B. die Einführung eines Information Security Management Systems (ISMS), können dabei lediglich Teilschritte auf dem Weg zu ganzheitlich gelebter IT-Sicherheit in Unternehmen sein.

Laut Angaben des GDV bieten zum Zeitpunkt der Veröffentlichung dieses Dokuments 38 Versicherer in Deutschland eine Cyberversicherung an[8]. Dennoch ergab die bereits erwähnte Forsa-Befragung, dass über 85 % der KMU bisher keine Cyberversicherung abgeschlossen haben. Ein Ergebnis der im Jahr 2018 von KPMG durchgeführten Studie „Clarity on Cyber Security"[9] bestätigt dies. Als Grund für das nicht Abschließen einer Cyberversicherung[10] gaben

68 % der befragten Unternehmen an, keine den eigenen Bedürfnissen entsprechenden Versicherungstarife zu finden. Die vorliegende Studie widmet sich eben diesem Spannungsfeld.

---

[1] „Ransomware sind Schadprogramme, mit deren Hilfe ein Eindringling eine Zugriffs- oder Nutzungsverhinderung einzelner Daten oder des gesamten Computersystems erwirkt. Meist dient dies dazu, Lösegeld (ransom) zu erpressen." (Bundeskriminalamt (BKA), 2018)
[2] (Bundeskriminalamt (BKA), 2018)
[3] (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018)
[4] (vgl. u. a. (Dose, 2018))
[5] (Gesamtverband der Deutschen Versicherungswirtschaft e. V., 2018)
[6] (a. a. O., S. 4)
[7] Der Empfehlung 2003/361/EG der Europäischen Union folgend, arbeiten in solchen Unternehmen höchstens 250 Mitarbeiterinnen und Mitarbeiter; der Jahresumsatz darf nicht über 50 Millionen Euro und die Bilanzsumme nicht über 43 Millionen Euro liegen. (Kommission der Europäischen Gemeinschaften, 2003)
[8] (Gesamtverband der Deutschen Versicherungswirtschaft e. V.)
[9] (KPMG, 2018)
[10] (a. a. O., S. 12)

Auf der einen Seite steht die unstrittige Tendenz, dass Cyberrisiken mehr denn je für wirtschaftliche Schäden verantwortlich sind. Auf der anderen Seite stehen die Versicherer mit Angeboten, die vom Großteil der KMU noch nicht angenommen werden.

Die Studie will daher grundlegende Fragen im Zusammenhang mit der Entscheidung gegen eine Cyberversicherung näher beleuchten:

- Warum schließt eine so große Zahl von Unternehmen keine Cyberversicherung ab, obwohl das wirtschaftliche Risiko durch Cyberschäden deutlich wahrgenommen wird?
- Wo liegen gegenwärtig noch Hemmungen und Hürden beim Abschluss einer Cyberversicherung?
- Welche Merkmale zeichnen typische Cyberversicherungen aus?
  Passen diese Merkmale zum tatsächlichen Bedarf der Unternehmen?

Nicht zuletzt verfolgt die Studie dabei das Ziel, jene Tarife für Cyberversicherungen hervorzuheben, die für Unternehmen aufgrund ihres Gesamtpakets aus Leistungsumfang, Kundenkontakt und Preis als möglicher Einstieg in den Versicherungsschutz gegen Cyberrisiken besonders relevant sind.

Eine einführende Betrachtung aktueller Veröffentlichungen aus Wissenschaft und Wirtschaft dient als Rahmen, um die Versicherungen in das Unternehmensgeschehen einzuordnen. Den Schwerpunkt bilden hierbei die subjektive Risikoeinschätzung und Selbstwahrnehmung zahlreicher KMU, die oftmals nicht mit objektiv messbaren Indikatoren übereinstimmen.

Auf dieser Basis entstehen Studiendesign und Methodik, der Fokus liegt insbesondere auf der Entwicklung instruktiver Ratingkriterien für das Benchmarking.

Insgesamt soll die Studie vor allem der großen Masse der KMU, die bisher nicht gegen Cyberrisiken versichert sind, eine erste Orientierung auf dem Markt der Cyberversicherungen ermöglichen. Anhand zweier fiktiver Musterfirmen, die typisch für diese Zielgruppe sind, erfolgt dazu der Vergleich relevanter Cyberversicherungen. Abschließend werden angebotsübergreifende Trends identifiziert und die Ergebnisse diskutiert. Die Resultate sind auch für Anbieter von Cyberversicherungen aufschlussreich, um die Anforderungen potenzieller Versicherungsnehmer besser einordnen zu können.

1.1 Abgrenzung KMU

Diese Studie befasst sich mit Cyberversicherungen im Sinne der unverbindlichen Musterbedingungen des GDV[11]. „Sie sind speziell auf die Bedürfnisse von kleinen und mittleren Unternehmen zugeschnitten und richten sich sowohl an Arztpraxen [...] als auch an [...] Industriezulieferer."[12]

Solche Versicherungen übernehmen bei Eintritt des Versicherungsfalls nicht nur die Kosten durch Datendiebstähle, Betriebsunterbrechungen und für den Schadenersatz an Dritte, sondern stehen den Kunden darüber hinaus auch mit einem umfangreichen Serviceangebot zur Seite. Dieses Serviceangebot umfasst je nach Einzelfall Experten für IT-Forensik, spezialisierte Anwälte oder Krisenkommunikatoren[13].

[11] (Gesamtverband der Deutschen Versicherungswirtschaft e. V., 2018)
[12] (a. a. O., S. 11)
[13] (vgl. ebd.)

Das Zusammenwirken dieser unterschiedlichen Versicherungsleistungen trägt dazu bei, das Ausmaß des Schadens für betroffene Unternehmen möglichst minimal zu halten.

Angesichts der Tatsache, dass der stark wachsende Markt für Cyberversicherungen ständigen Veränderungen unterliegt, existieren zahlreiche verschiedene Angebote, deren trennscharfe Abgrenzung nicht immer leichtfällt.

Dies gilt vor allem für Cyberversicherungen, die als Erweiterung oder Ergänzung zu privaten Haftpflicht- oder Hausratversicherungen angeboten werden. Deren Leistungsumfang beschränkt sich i. d. R. auf die typischen Anwendungsfälle von IT im privaten Umfeld, oft am Beispiel einer Kleinfamilie illustriert[14]. In vielen Fällen umfassen Cyberversicherungen dieser Art zudem Leistungen, die für Unternehmen prinzipiell nicht anwendbar sind[15].

Cyberversicherungen dieser Art werden in dieser Studie nicht behandelt, da die u. a. hinsichtlich Zielgruppe, Leistungsumfang und Preis vorhandenen Unterschiede quantitativ und qualitativ zu gravierend sind, um einen sinnvollen Vergleich zuzulassen.

Für den zielgerichteten Vergleich von Cyberversicherungen ist es zunächst erforderlich, diese mit ihren Besonderheiten im Hinblick auf Risiken und Leistungen zu verstehen. Außerdem ist die Einstellung der KMU bezüglich des Nutzens solcher Versicherungen von Interesse. Daran schließt sich die Beschreibung von Methodik, Design und Ratingkriterien der Studie an.

2. Ergebnisse aktueller Forschung

Die bereits angeführten Statistiken sind ein kleiner Teil der umfangreichen internationalen Forschung auf dem Themengebiet der Cyberversicherungen. Das Spektrum der Veröffentlichungen reicht dabei von generellen Fragestellungen der Versicherbarkeit von Cyberrisiken[16], über allgemeine Grenzen der Cyberversicherung[17] bis zur Analyse konkreter Fragebögen für den Abschluss solcher Policen[18].

2.1 Cyberversicherungen als Beitrag zur IT-Sicherheit

Cyberversicherungen unterscheiden sich in vielerlei Hinsicht von Versicherungen für klassische Domänen, die bereits seit langer Zeit von einer großen Anzahl von Firmen versichert werden. Beispielhaft sei die Gebäudeversicherung genannt, diese schützt vor wirtschaftlichen Folgen bei Schäden an Betriebsgebäuden, welche häufig durch Elementargefahren wie Feuer, Sturm oder Überschwemmung verursacht werden.

Da Cyberrisiken für Wirtschaft und Wissenschaft vor einigen Jahren vergleichsweise neu waren, bildeten bereits die Modellierung von IT-Sicherheitsrisiken sowie deren Bewertung ein eigenständiges Forschungsgebiet[19]. Hinzu kam, dass das Konzept der Cyberversicherung anfangs mit dem Wunsch nach mehr IT-Sicherheit verbunden wurde[20], die Schadensregulierung

[14] Dazu zählen z. B. bei der IT-Nutzung durch Kinder häufig verursachte Schäden wie illegale Musik- oder Videodownloads.
[15] Beispielhaft hierfür ist die psychologische Beratung bei Cyber-Mobbing (vgl. z. B. (VERIVOX, 2019) und (BavariaDirekt)).
[16] (vgl. z. B. (Biener, et al., 2015))
[17] (vgl. (Böhme, et al., 2006) und (Biener, et al., 2015))
[18] (vgl. wegweisend erstmals (Woods, et al., 2017))
[19] (vgl. früh (Wawrzyniak, 2006), aktueller (Eling, 2018))
[20] (vgl. (Böhme, et al., 2006))

sollte z. B. mittels IT-Sicherheitsdaten zu weltweiten Standards und Best Practices beitragen[21]. Gänzlich neu war jedoch die Komplexität der Wechselwirkungen[22] auf globaler sowie lokaler Ebene, da einerseits voneinander unabhängige Firmen zur gleichen Zeit vom selben Cyberschaden betroffen sein können (*global*)[23], währenddessen andererseits ein einzelner kompromittierter Rechner in einem Unternehmen ausreichen kann, um das gesamte Unternehmen zu schädigen (*lokal*)[24].

Diese neue Komplexität stellt Anbieter von Cyberversicherungen vor enorme Herausforderungen; abgesehen davon, dass auch diese Opfer derselben Cyberschäden werden können. Vor diesem Hintergrund kommen Biener et al. nach Auswertung von nahezu 1000 versicherten Cyberschäden zu dem Schluss, dass die Entstehung eines stabilen Marktes für Cyberversicherungen durch die der Dimension Cyber innewohnenden besonderen Charakteristika fundamental behindert wird[25]; dabei sind vor allem unzureichende Daten und informationelle Asymmetrien von Bedeutung[26].

Neben den grundlegenden theoretischen Konzepten hat auch die Cyberversicherungspraxis wissenschaftliche Beachtung erfahren. Wodds, et Al. (2017) haben einen Vergleich von 24 Fragebögen zum Abschluss von Cyberversicherungen in Großbritannien und den USA vorgelegt, um festzustellen, inwiefern Cyberversicherungen die Verbreitung von Best Practices mit Bezug zur IT-Sicherheit fördern.[27]

Im deutschsprachigen Raum gilt Choudry (2014) als Standardwerk zur Einführung in die Thematik.[28] Zu praktisch bedeutsamen Aspekten und der typischen Tarifstruktur von Cyberversicherungen gibt Lomen (2017) einen zusammenfassenden Überblick.[29]

Eine Bewertung von gewerblichen Cyber-Policen im deutschen Markt wurde von Franke und Bornberg[30] durchgeführt und wurde für die Entwicklung dieses Benchmarks berücksichtigt.

---

[21] Mittlerweile ist das Anstreben einer ausgeglichenen Balance zwischen Risikominimierung durch eigenverantwortliche Schutzmaßnahmen und Risikoübertragung auf den Versicherer Konsens, vgl. dazu (Martinelli, et al., 2018).
[22] (vgl. dazu (Meland, et al., 2017))
[23] Einen Spezialfall dieser globalen Komplexität stellen Cyberversicherungen für Anbieter elektronischer Zahlungsdienstleistungen dar, vgl. dazu (Franke, 2018).
[24] (vgl. (Böhme, et al., 2006))
[25] (vgl. z. B. (Biener, et al., 2015))
[26] (Baban, et al., 2018) gehen auf die konzeptionell notwendigen Unterschiede zwischen Cyberversicherungen und klassischen Versicherungsangeboten ein, sodass theoretische Grenzen deutlich werden.
[27] (Woods, et al., 2017)
[28] (Choudhry, 2014)
[29] (Lomen, 2017)
[30] (vgl. (Franke und Bornberg GmbH, 2018))

2.2 Wirtschaft: Optimism Bias 2.0

Auch auf globaler Ebene ist die unternehmensseitige Wahrnehmung der Dimension Cyber als Risiko unstrittig. Dies belegt das „Allianz Risk Barometer" für das Jahr 2019[31]. Seit 2014 gehören Cyberrisiken zu den Top 10 der globalen Risiken (Abbildung. 1). „Cyber Incidents" belegen den zweiten Platz bei prozentualer Gleichheit mit „Business Interruption" auf dem ersten Platz[32].

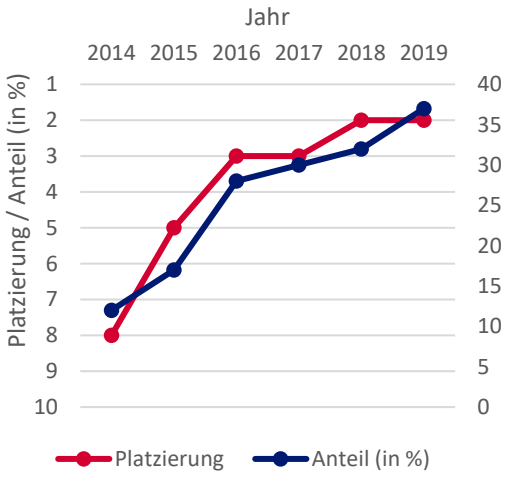


Abbildung. 1: Zunahmen der Gefährdungsbewertung „Cyber Incidents" im Allianz Risk Barometer.

Somit können Cyberbedrohungen momentan weltweit als das entscheidende Risiko für Unternehmen verstanden werden – noch vor Naturkatastrophen (28 %). In Deutschland drückt sich die prozentuale Zustimmung im Vergleich zu 37 % auf globaler Ebene noch deutlicher aus: 44 % für „Cyber Incidents" gegenüber 48 % Zustimmung für „Business Interruption"[33].

Insbesondere im Sektor professioneller Dienstleistungen, der z. B. Rechts- und Steuerberatung umfasst, wird das Cyberrisiko mit 40 % Zustimmung und Platz 1 sehr ernstgenommen. Ähnliches gilt für den Gesundheitssektor, der Cyberrisiken bei 41 % Zustimmung prozentgleich mit sich ändernden gesetzlichen Rahmenbedingungen auf Platz 1 sieht.

Interessant erscheint ferner der Umstand, dass einzig die Kleinunternehmen[34] das Cyberrisiko als für ihre Gruppe relatives Hauptrisiko, Platz 1, identifizieren[35]. Dieser Umstand widerspricht offenbar der durch die mediale Berichterstattung geprägten Intuition, dass Großkonzerne durch Cyberangriffe besonders schwer getroffen werden. Folglich sind sich Kleinunternehmen ihrer Verwundbarkeit durch Cyberangriffe durchaus bewusst. Da zudem in den meisten Fällen kein Cyberversicherungsschutz besteht, ist die fatale Einschätzung der Wirkung erfolgreicher Cyberangriffe zutreffend.

[31] (Allianz, 2019)
[32] (Allianz, 2019)
[33] (a. a. O., S. 6)
[34] Das Allianz Risk Barometer bezeichnet Unternehmen, deren Jahresumsatz 250 Mio. € nicht überschreitet, als klein. Man beachte den definitorischen Unterschied zum Begriffsverständnis dieser Studie (vgl. Fn. 7).
[35] (vgl. (Allianz, 2019), S. 33 f.)

Eine mögliche Erklärung dieses vermeintlichen Widerspruchs zwischen Risikoeinschätzung und unternehmerischem Handeln, hier dem (Nicht-)Abschluss einer Cyberversicherung, liefert das sog. Optimism Bias, auch als „Unrealistic Optimism" bezeichnet.

Kleine Unternehmen gehen dem Anschein nach davon aus, nicht Ziel von Cyberangriffen zu werden. Die gefährlich-trügerische Logik lautet in etwa: Wer gar nicht Ziel ist, benötigt – trotz mangelhaftem Schutz – keine Versicherung.

Diese Einstellung lässt sich aus unterschiedlichsten statistischen Erhebungen rekonstruieren. Hier werden zwei Studien mit ihren für diese Thematik relevanten Ergebnissen näher vorgestellt[36]. Als erstes artverwandtes Beispiel folgt die auszugsweise Betrachtung der Ergebnisse des Projekts „Monitor IT-Sicherheit Kritischer Infrastrukturen".

Die zugehörige erste Umfrage im Rahmen des Projekts „Vernetzte IT-Sicherheit Kritischer Infrastrukturen (VeSiKi)" als Teil des Förderschwerpunkts IT-Sicherheit für Kritische Infrastrukturen[37] (ITS|KRITIS) fand im zweiten Halbjahr 2016 statt[38]. 46 % der befragten Unternehmen sind KMU im Sinne der auch dieser Studie zugrunde liegenden Definition[39], die übrigen Unternehmer sind nach Beschäftigten oder Umsatz größer.

Für die Darstellung des Optimism Bias sei lediglich auf folgende Ergebnisse verwiesen, die in (Lechner, 2017) veröffentlicht wurden. Je höher die Abstraktionsebene, d. h. je größer der Abstand von der befragten Organisation, desto häufiger wurde die derzeitige Bedrohungslage als „sehr hoch" eingeschätzt. Dazu passend sinkt die Häufigkeit der Einschätzung „gering" deutlich von „Organisation", über „Branche", bis hin zu „Wirtschaftsraum Deutschland". Die befragten Organisationen halten sich jeweils selbst für am wenigsten betroffen während die Branche und der Wirtschaftsraum Deutschland relativ stark betroffen sind. Da die deutliche Mehrheit der

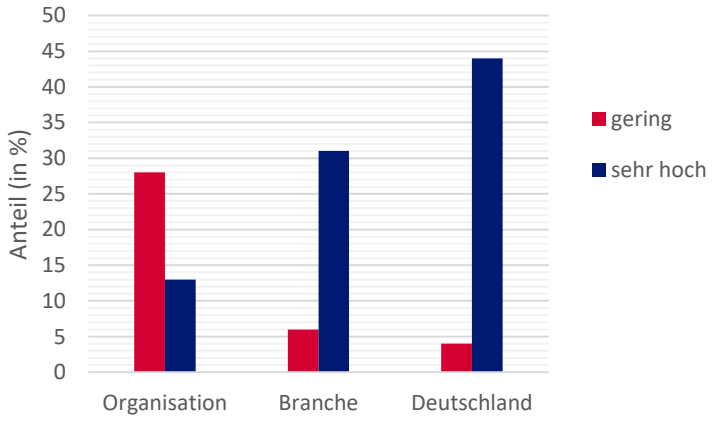


Abbildung 2: (Lechner, 2017)): Schätzung der derzeitigen Bedrohungslage im Bereich IT-Sicherheit für die eigene Organisation, Branche und Wirtschaftsraum Deutschland.

[36] Darüber hinaus finden sich weitere Studien, deren Ergebnisse in eine ähnliche Richtung weisen, z. B. (Deloitte, 2017): 65 % der befragten Führungskräfte benannten Diebstahl von Know-how als Gefahr für die deutsche Wirtschaft. Eine Gefahr für das eigene Unternehmen sahen darin nur 34 %.

[37] Gem. der Definition des Bundesministeriums des Innern bezeichnet man „Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden[,]" als „Kritische Infrastruktur" (Lechner, 2017).

[38] (Lechner, 2017)

[39] (vgl. Fn. 7)

Befragten diese Einschätzung teilt, ist das Resultat insgesamt nicht stimmig, wenn man die Zusammensetzung von Branchen aus einzelnen Organisationen bedenkt. Selbiges gilt für den Wirtschaftsraum Deutschland, der in diesem Sinne aus einzelnen Branchen besteht. Der Widerspruch in Selbstwahrnehmung und Risikoeinschätzung besteht demzufolge in der weitverbreiteten Überzeugung, trotz allgemein hoher Gefährdung selbst kaum gefährdet zu sein.

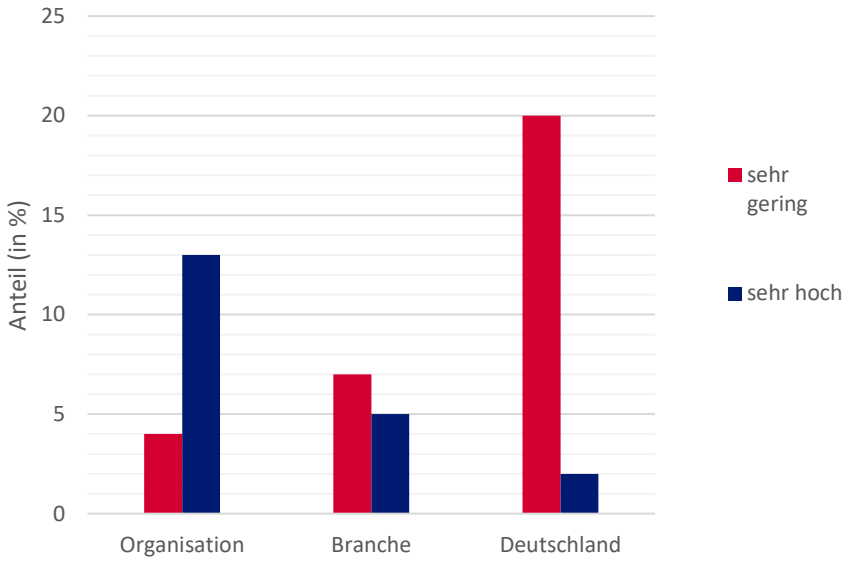


Abbildung. 3: (nach (Lechner, 2017)): Einschätzung der Fähigkeit der eigenen Organisation / der eigenen Branche / des Wirtschaftsraums Deutschland, Cyberattacken abzuwehren.

Der sinngemäß analog verlaufende Trend zeigt sich bei der Einschätzung der Fähigkeit zur Abwehr von Cyberattacken. Beide Aussagen zusammen lassen den Schluss zu, dass die befragten Organisationen zu unbegründetem Optimismus neigen, der sich in einer unrealistisch positiven Selbstwahrnehmung widerspiegelt. Die Wiederholung der zugrunde liegenden Befragung im Jahr 2018 bestätigte diesen Umstand explizit[40]. Es handelt sich somit nicht um einzelne Fehleinschätzungen der befragten Akteure, sondern um ein systematisch verzerrtes Bild der Realität. Diese Abweichung gewinnt weiter an Bedeutung, wenn man sich in Erinnerung ruft, dass der zwischen den Befragungen liegende Zeitraum keineswegs frei von verheerenden Cyberattacken auf Unternehmen jeder Größenordnung war.

Das zweite Beispiel zur Verdeutlichung des Widerspruchs in der Selbst- und Risikowahrnehmung zahlreicher Unternehmen ist die im Auftrag des GDV durchgeführte Forsa-Befragung „Cyberrisiken im Mittelstand".

Unter der Überschrift „Prinzip Hoffnung" stellt der GDV[41] fest, dass 72 % der befragten KMU das Risiko von Cyberkriminalität für KMU in Deutschland als „eher bzw. sehr hoch" einschätzen[42]. Dem gegenüber steht ein vergleichsweise geringer Anteil von 34 % der befragten KMU, die das

[40] (vgl. (Lechner, 2018))
[41] (vgl. Fn. 5, 6)
[42] (Gesamtverband der Deutschen Versicherungswirtschaft e. V., 2018)

Risiko von Cyberkriminalität für das eigene Unternehmen als „eher bzw. sehr hoch" bewerten[43]. Folglich schätzen bis zu 38 % der Befragten das Risiko für ihr eigenes Unternehmen geringer ein als das Risiko für vergleichbare Unternehmen in Deutschland. Die Zusammenfassung des GDV, „Das Risiko gibt es – aber mein Unternehmen betrifft es nicht!", bringt diese Diskrepanz deutlich auf den Punkt.

Die Frage, ob ein Unternehmen bislang von Cyberattacken betroffen war[44]. 46 % der Unternehmen, die bereits betroffen waren, verfügen über eine Cyberversicherung oder sind daran interessiert. Bei den Unternehmen, die bisher noch nicht von einer Cyberattacke betroffen waren, sind lediglich 4 % an einer Cyberversicherung interessiert, 96 % sind nicht interessiert.

Die Unternehmensgröße[45].Je kleiner das Unternehmen, desto geringer wird das eigene Risiko und desto besser wird der eigene Schutz eingeschätzt[46]. Erschwerend gilt jedoch ebenso, dass die Investitionsbereitschaft in IT-Sicherheit mit der Unternehmensgröße abnimmt. Als Resultat dieser Kombination aus der Fehleinschätzung des eigenen Risikos und Schutzes sowie mangelnder Investitionsbereitschaft ergibt sich, dass kleinere Unternehmen schlechter geschützt sind. Dasselbe gilt für die Anfälligkeit gegenüber mehrfachen Cyberangriffen: je kleiner das Unternehmen, desto wahrscheinlicher die mehrmalige Betroffenheit.

Ein Großteil der Unternehmen schätzt das eigene Cyberrisiko zu niedrig ein. Dieser Irrtum wird ergänzt durch die Überbewertung des eigenen IT-Schutzes. Aus beiden Fehleinschätzungen wird gefolgert, weder weiter in Schutzmaßnahmen investieren zu müssen noch eine Cyberversicherung zu benötigen[47]. Diese Gesamteinschätzung ändert sich offenbar erst dann, wenn das Unternehmen selbst Opfer einer Cyberattacke geworden ist.

---

[43] (a. a. O., S. 6)
[44] (vgl. a. a. O., S. 7)
[45] (vgl. a. a. O., S. 8 f.)
[46] (vgl. dazu instruktiv ein Ergebnis von (de Smidt, et al., 2018): die Einschätzung der Cyberfähigkeiten des eigenen Unternehmens beeinflusst u. a. die Einschätzung der *Wahrscheinlichkeit* eines Cyberangriffs.)
[47] Diese Erkenntnis ist nicht auf den deutschsprachigen Raum beschränkt, vgl. (de Smidt, et al., 2018). Vielmehr scheint gegenwärtig international eine generelle Ablehnung gegenüber Cyberversicherungen feststellbar.

3 Benchmarking

3.1 Methode

Die Methodik dieser Studie verwendet die Methodentriangulation im Sinne einer Mixed-Methods-Studie[48]. Ziel ist es, unterschiedliche Perspektiven auf Cyberversicherungen in Deutschland, einzunehmen.

Dies bedeutet, dass qualitative und quantitative Ergebnisse in das Benchmarking einfließen. Ergänzend werden darüber hinaus zentrale Aussagen eines Experteninterviews (Meuser, et al., 2009) einbezogen, die den Blick aus Sicht eines Anbieters von Cyberversicherungen einbringen.

Franke und Bornberg veröffentlichte im Jahr 2018 ein erstes Rating für gewerbliche Cyberversicherungen im deutschen Markt[49]. Verglichen wurden 34 Tarife. Ziel war das Aufzeigen von Deckungsunterschieden und das Schaffen von Transparenz für Anbieter und Interessenten gleichermaßen. Sie bezeichnen das Rating als „Benchmark für das detaillierteste Produktrating in Deutschland"[50] und geht davon aus, dass ein Anstieg von „Leistungsniveau und [...] Präzision der Formulierungen in dieser noch jungen Sparte" auf das Rating zurückzuführen sein wird[51].

Das Benchmarking erfolgt aufgeteilt in drei Bewertungskategorien (Kontakt zur Versicherung, Leistungsumfang, Preis) mit jeweils maximal sechs Unterkategorien. Kriterien werden dabei je nach Merkmal entweder in zwei („Trifft zu", „Trifft nicht zu") oder in vier Stufen („Trifft nicht zu", „Trifft kaum zu", „Trifft zu", „Trifft besonders zu") bewertet. Die abschließende Bewertung in vier Abstufungen beinhaltet neben diesen Merkmalen auch einen übergreifenden Gesamteindruck mit Hinblick auf die betrachteten Musterfirmen.

Zur Vergleichbarkeit der Policen, wurden zwei fiktiven KMU Kunden aus dem Gesundheitswesen (Praxis Allgemeinmediziner) und Maschinenbau (Werkzeugfertigung) erstellt und deren typischen Cyberrisiken analysiert.

[48] (vgl. (Pickel, 2009))
[49] (vgl. (Franke und Bornberg GmbH, 2018))
[50] (Franke und Bornberg GmbH, 2018)
[51] (a. a. O., S. 4)

3.1.1 Musterfirma Maschinenbau

Werkzeug GmbH	
Gründung	1891
Mitarbeiter	360
Umsatz	38 Mio €
Produkt	Qualitätswerkzeug
Vertriebsart	Business to Business
Rechenzentrum	Betriebseigen
IT-Abteilung	4 Personen
Cyberversicherungssumme	5 Mio €

Tabelle 1: Überblick Musterfirma Werkzeug GmbH

Die seit ihrer Gründung 1891 im Familienbesitz befindliche Werkzeug GmbH entwickelt und produziert in Deutschland an drei Standorten Qualitätswerkzeug mit einem hohen Fokus auf Innovation. Mit rund 360 Mitarbeitern und einem Jahresumsatz von 36 Millionen Euro werden die Produkte zu 100 % unter strengen Qualitätskontrollen an je einem der drei Standorte hergestellt.

Dazu kauft das Unternehmen Rohstoffe und Komponenten bei Zulieferern aus dem In- und Ausland ein. Die Werkzeug GmbH betreibt keinen Vertrieb an Endkonsumenten, sondern sämtliche Produkte werden ausschließlich von externen Distributoren und Fachhändlern vertrieben.

Deshalb besteht der Hauptanteil der Daten im Unternehmen aus Buchhaltungsdaten, sowie Daten aus der Entwicklung. Ausgelagerte Prozesse gibt es hierbei keine. Die IT-Infrastruktur beinhaltet unter anderem drei physische Server, welche in einem kleinen Rechenzentrum betrieben werden. Der Personalaufwand hierbei liegt bei vier Mitarbeitern.

Hellhörig bezüglich der Thematik Cyberangriffe und eventuellen Präventivmaßnahmen ist die Geschäftsführung durch einen Angriff auf das Konkurrenzunternehmen „Metabo" im Jahre 2018 geworden. Die Schadsoftware wurde durch einen Hacker, der im Team des Softwareherstellers der verwendeten Buchhaltungssoftware saß, eingeschleust[52]. Grundsätzlich ist es einem Hacker dadurch möglich, Daten zu verschlüsseln und dem Unternehmen so zu schaden oder sogar Lösegeld für ebendiese zu fordern. Das Unternehmen brauchte ganze fünf Tage Zeit, bis erste Teilbereiche wieder einsatzbereit waren und sogar neun Tage, bis die Produktion wieder aufgenommen werden konnte[53].

Als erste Präventionsmaßnahme hat sich die Werkzeug GmbH deshalb dazu entschieden, eine Cyberversicherung mit einer Versicherungssumme von fünf Millionen Euro abzuschließen.

[52] (Gann, 2018)
[53] (a. a. O.)

3.1.2 Musterfirma Gesundheitswesen

Arztpraxis Dr. Schröder	
Unternehmen	Praxis Allgemeinmediziner
Arzthelferinnen	3
Administrationsmitarbeiter	1
Patienten	1500
Umsatz	350 T €
IT-Wartung	Über Dienstleister
IT-Abteilung	5 Arbeitsrechner und Server
Cyberversicherungssumme	1 Mio €

Tabelle 2: Überblick Arztpraxis Dr. Schröder

Der Allgemeinmediziner Dr. Schröder führt seine eigene Arztpraxis mit einem Patientenstamm von ca. 1.500 Patienten. Zur Behandlung dieser stehen Dr. Schröder 3 Arzthelferinnen zur Seite. Darüber hinaus beschäftigt sich ein weiterer Mitarbeiter mit sämtlicher Administration.

Der Jahresumsatz der Praxis lag im letzten Jahr bei 350.000 Euro. Die IT-Infrastruktur setzt sich aus 5 Arbeitsplatzrechnern und einem Server zusammen. Die Wartung der Systeme ist durch einen Supportvertrag mit einem Dienstleister sichergestellt. Besonders vor dem Hintergrund der sensiblen Patientendaten, ist Herrn Dr. Schröder der Risikostatus seiner Praxis in Bezug auf einen Cyberangriff bewusst.

Vor dem Hintergrund beispielgebender Folgen hat sich Dr. Schröder für eine Cyberversicherung entschieden. Die Versicherungssumme soll hierbei 1 Million Euro betragen.

3.1.3 Typische Cyberrisiken der Musterfirmen

Doch ist eine Absicherung hinsichtlich informationstechnischer Risiken immer zwangsweise mit einer hohen Investition verbunden? Dieser Frage hat sich der GDV im Jahre 2018 angenommen und eine Übersicht über die wichtigsten Cyberrisiken für den Mittelstand erstellt[54].

Eine wichtige Erkenntnis war, dass Cyberkriminelle durchaus Hintertüren in Spezialsoftware nutzen, Passwörter ausspähen oder Tastaturanschläge mitschneiden können, dies jedoch in Anbetracht der Angriffe der letzten Jahre gar nicht müssen. Die Statistik zeigt, dass fast 60 % aller erfolgreichen Angriffe über das E-Mail-Postfach erfolgen. Der Mensch bleibt die größte Schwachstelle.

Mitarbeiter öffnen E-Mail-Anhänge häufig im Vertrauen darauf, dass die betriebliche Firewall und Virenscanner eventuelle Malware bereits vorher identifizieren. Bereits 2017 warnte GDV-Cyberversicherungsexperte Peter Graß vor Fahrlässigkeit: „Die technischen Hilfsmittel können den gesunden Menschenverstand und eine gewisse Skepsis nicht ersetzen". Genau deshalb empfiehlt er regelmäßige Schulungen und verbindliche Vorsichtsmaßnahmen.

Dass ein Hacker durch den Einsatz spezieller Software oder das Erspähen von Passwörtern keinen großen Aufwand betreiben muss, zeigt auch die weitere Betrachtung der GDV-Übersicht. So kommen bei nur ca. jedem vierten Angriff ebendiese zum Einsatz (s. Abbildung 4).

[54] (Gesamtverband der Deutschen Versicherungswirtschaft e. V., 2018)

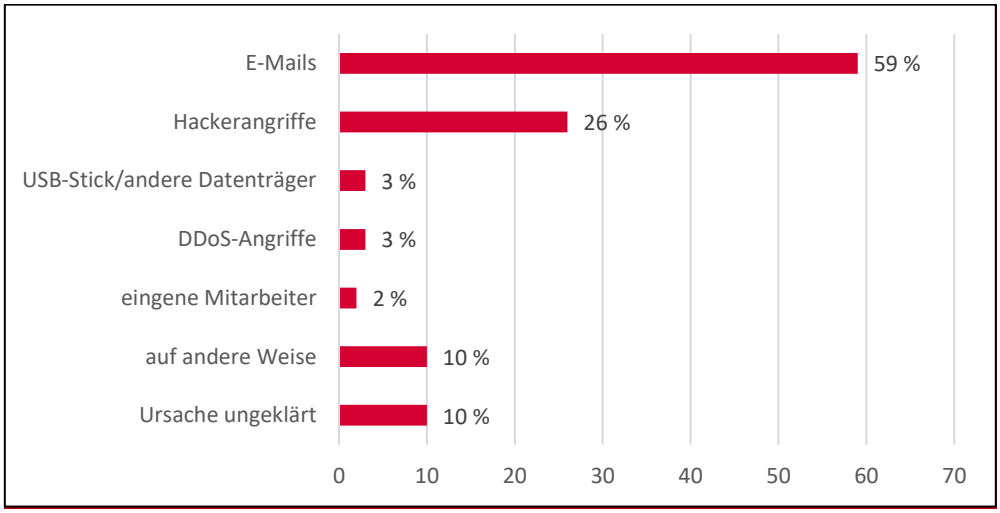


Abbildung 4: Erfolgreiche Cyberangriffe

DDoS-Angriffe machen nur etwa 3 % aller Angriffe aus. Anteilig auf einem ähnlichen Level befinden sich die eigenen Mitarbeiter. Mit dieser Kategorie sind nicht die eingangs erwähnten fälschlicherweise geöffneten E-Mails gemeint, sondern beispielsweise die Fehlbedienung eines Systems. Auch hierdurch können Versicherungsfälle für Cyberversicherungen entstehen. Boshafte Intentionen seitens eigener Mitarbeiter fallen ebenfalls in diese Sparte.

Nachdem ein Überblick über die Einfallstore für Cyberangriffe gegeben wurde, werden nachfolgend die bereits angeschnittenen Angriffsmethoden und -mittel eines Cyberkriminellen in Kürze dargestellt. Dadurch werden die verschiedenen Möglichkeiten eines Hackers verdeutlicht und es lassen sich Trends und Tendenzen erkennen, die beim Aufbau einer erfolgreichen Abwehr berücksichtigt werden sollten. Das Bundesamt für Sicherheit in der Informationstechnik liefert hierzu jährlich „Die Lage der IT-Sicherheit in Deutschland". In diesem Bericht werden neben anderen Thematiken die folgenden Angriffsmöglichkeiten aufgeführt[55]:

1. **Advanced Persistent Threats (APTs)**
   Unter APTs versteht man zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer persistenten[56] Zugriff zu einem Netzwerk verschafft und diesen auf weitere Systeme ausweiteten kann.
   Hierbei wird oftmals in der initialen Phase der Angriffe ein Installer- und Update-Hijacking verwendet. Dafür werden beispielsweise auf den Webseiten von Software-Herstellern Installationsarchive mit Schadcode versehen. Wenn die Nutzer die Programme herunterladen und installieren, wird dadurch auch ein eingeschleustes Schadprogramm ausgeführt, das wiederum weitere Module nachladen kann[57].

2. **Angriffe auf Industrial Control Systems**
   Angriffe auf Produktionssysteme finden oftmals durch Phishing-Mails oder Wechsel-datenträger statt. Gründe, für die oftmals einfach zugänglichen Einfallstore sind jedoch

[55] (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018)
[56] dauerhaften
[57] (vgl. (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018), Kap. 1.4.1)

anderer Natur. Zum Beispiel die zum Teil sehr alten Systeme, für die es oftmals keine Updates mehr gibt oder bei denen für vorhandene Updates keine Freigabe durch den Hersteller der Maschine vorhanden ist.
In solchen Fällen ist ein Separieren von Systemen und Segmentieren von Netzwerken wichtig, damit unberechtigte Zugriffe vermieden werden können. Hierbei sei für explizite Maßnahmen auf die IT-Grundschutz-Bausteine für industrielle Systeme und das ICS-Security-Kompendium verwiesen[58].#

3. **DDoS-Angriffe**

Der Distributed-Denial-of-Service ist ein „Verteilter" Denial-of-Service (DoS), der wiederum eine Dienstblockade darstellt. Diese liegt vor, wenn ein angefragter Dienst nicht mehr bzw. nur noch stark eingeschränkt verfügbar ist. Auslöser ist in den meisten Fällen eine Überlastung der IT-Infrastruktur. Angreifer nutzen diese Art der Cyber-Kriminalität, um beispielsweise von ungeschützten Unternehmen Lösegelder zu erpressen[59].

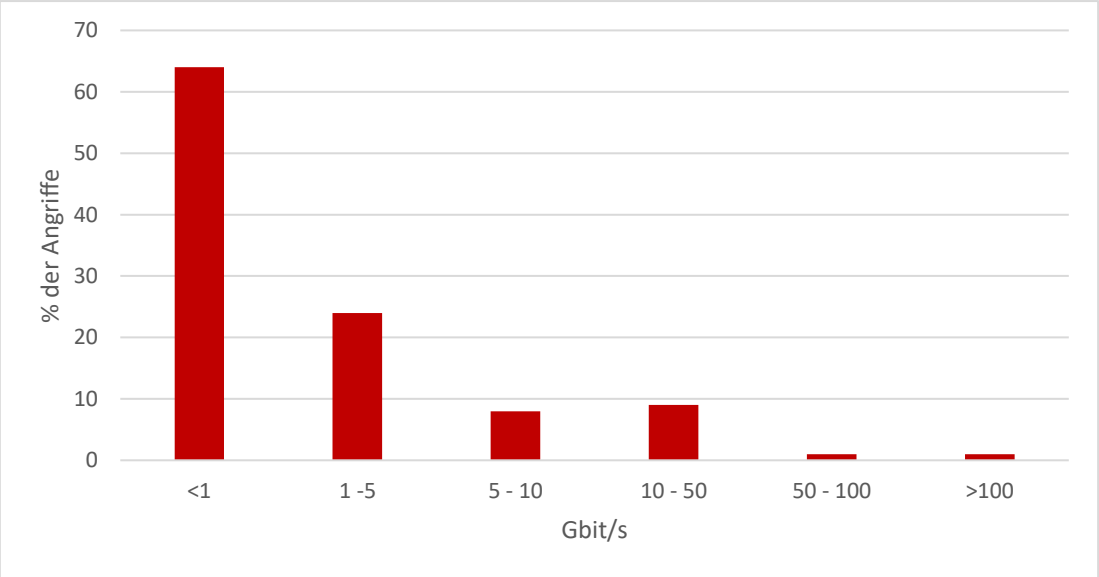


Abbildung 5: Übersicht Bandbreite DDoS-Angriffe 2018

Die Statistik über das gesamte Jahr zeigt, dass die Mehrheit aller Angriffe Bandbreiten von maximal 5 Gbit/s aufweisen[60] (s. Abb. 5). Auf der technischen Ebene könnten sich Unternehmen also bereits vor einem signifikanten Anteil aller durchgeführten DDoS-Angriffe schützen, indem relevante Systeme in einem solchen Maße überdimensioniert werden, dass deren Funktionsfähigkeit selbst nach dem Angriff noch gewährleistet ist[61].

[58] (vgl. a. a. O., Kap. 1.4.2)
[59] (vgl. (Myra Security GmbH, 2019))
[60] (vgl. (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018), 1.4.4)
[61] (vgl. a. a. O.)

4. **Kryptografie**

Kryptografische Mechanismen sind die Grundbausteine für die Wirksamkeit vieler IT-Sicherheitsprodukte. Heutzutage häufig verwendete Verfahren sind beispielsweise das symmetrische Verschlüsselungsverfahren AES oder der asymmetrische Diffie-Hellman-Schlüsselaustausch.

Das BSI empfiehlt in der Technischen Richtlinie TR-02102 eine Reihe von kryptografischen Algorithmen und Protokollen, die aufgrund von eingehenden mathematischen Analysen allgemein als sicher angesehen werden. Bei diesen Analysen wird jedoch eine Reihe von Annahmen getroffen. Für den sicheren praktischen Einsatz muss daher überprüft werden, ob diese Annahmen erfüllt sind. In der Praxis können hierbei verschiedene Aspekte dazu führen, dass ein System versagt.

Gemäß dem Bundesamt für Sicherheit in der Informationstechnik gehören dazu mitunter:

- Sicherheitslücken der Hardware
- Fehler in Implementierungen
- Fehler auf Protokollebene
- Verwendung veralteter Standards
- Schwächen in der Schlüsselerzeugung
- unzureichende Zufallszahlengeneratoren

Die neuste Entwicklung in diesem Bereich ist der Einsatz des Maschinellen Lernens. Während dies in anderen Bereichen der IT bereits breitflächig unter Namen wie Data Mining, Pattern Recognition oder Artificial Intelligence bekannt ist, steht die Etablierung als Teil von Sicherheitsbetrachtungen für IT-Systeme noch aus[62].

5. **Ransomware**

Software, die den Zugriff auf einen Rechner verwehrt oder einschränkt, nennt man Ransomware. Erst durch Zahlung eines Lösegeldes[63] werden diese Ressourcen dann wieder freigegeben. Neben der Einschränkung von Systemen kann Ransomware auch dazu genutzt werden, um gezielt Daten zu verschlüsseln. Das Format der Daten, sprich Text-, Audio-, Video- und Präsentations-Inhalte, oder auch Tabellenkalkulationen und Datenbanken, ist hierbei irrelevant.

Die Einfallstore sind auch hier vielfältiger Natur – dazu gehören SPAM-Mails, Exploits, Passwort-Schwachstellen oder Wartungs-Schwachstellen. Um als Unternehmen gegen eine solche Angriffsart vorbereitet zu sein, hilft ein regelmäßiges, ausgelagertes Backup. Die Verbindung zwischen Backup-Medien und Originalsystem sollte hierbei keinesfalls permanent sein. Darüber hinaus sind regelmäßige Updates und das Monitoring verwendeter Software hinsichtlich Schwachstellen und Expositionen[64] von großer Bedeutung[65].

[62] (vgl. (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018), Kap. 1.4.5)
[63] Lösegeld = Ransom (engl.)
[64] Gem. (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018)
[65] (vgl. (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018), Kap. 1.4.6)

6. Schadprogramme

Unter dem Begriff Schadprogramme[66] werden alle Arten von Computerprogrammen zusammengefasst, die unerwünschte und schädliche Funktionen auf einem Computersystem ausführen. Als Synonym werden hierbei oftmals die Begriffe Trojaner, Viren, Würmer usw. genutzt.

In letzter Zeit zeichnete sich ein verstärkter Wandel des Infektionswegs ab. Während anfangs die Schadsoftware im E-Mail-Anhang enthalten war, befindet sich diese nun zunehmend in verlinkten E-Mail-Texten. Auf diese Weise wird die Schadsoftware nicht direkt auf dem Mailserver gespeichert, wo entsprechende Sicherheitsmaßnahmen diese entdecken und entfernen könnten, sondern die Schadsoftware wird durch diese Methode beispielsweise durch einen direkten Download zum Client transportiert[67]. Diesbezügliche Bewusstheit seitens aller Mitarbeiter ist hierbei essenziell für ein Unternehmen.

7. Schwachstellen in Software und Hardware

Während der Berichterstattung seitens des BSI im Jahre 2018 zeigte sich eine zum Vorjahr kaum veränderte und zugleich hohe Anzahl an bekannt gewordenen Schwachstellen in Softwareprodukten.

Zwar werden Softwareentwicklungswerkzeuge, wie Compiler oder IDEs, ständig verbessert und können Softwareentwickler dadurch auf potenzielle Fehlerquellen hinweisen, gleichzeitig aber werden diese durch die folgenden Trends untergraben:

- massiv gestiegene Komplexität von Endanwendungen
- ungeprüfte Integration von zunehmend mehr externen Abhängigkeiten
- Geschwindigkeitsoptimierungen zu Lasten der Sicherheit
- Verzicht auf Fehlerbehebung mit Verweis auf Mitigation-Maßnahmen
- Verweigerung von Sicherheitsupdates und -aufklärung seitens vieler Hersteller

Dazu kommt die eigene Firmenpolitik: halbjährliche Wartungszyklen ziehen eine Verzögerung der Installation von Sicherheitsprogrammen mit sich, da diese mit betrieblichen Prozessen abgestimmt werden müssen und in einigen Fällen zusätzlichen regulatorischen Anforderungen unterliegen[68].

[66] (engl.: malware)
[67] (vgl. (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018), Kap. 1.4.7)
[68] (vgl. (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018), Kap. 1.4.9)

3.1.4 Herleitung der Benchmarking-Kriterien

Um die quantitativen Daten für eine Bewertung zu erfassen, wurde ein einheitlicher Fragebogen entwickelt, welcher in drei Hauptkategorien untergliedert ist. Diese Kategorien sind: „Kontakt zur Versicherung", „Leistungsumfang" und „Preis". Weiterhin verfügt der Ratingbogen über einen Kopf, indem grundlegende Daten wie der Versicherer oder der Name des Cyberversicherungstarifs erfasst werden können.

Ratingbogen Cyberversicherung Datum: _____

Musterfirma: _____

Versicherung: _____

Produktname: _____

Bemerkung: _____

Ratingkriterien	Bewertung			
Kontakt zur Versicherung				
Angaben vor Police-Abschluss (z. B. Fragebogen)				
	Trifft nicht zu	Trifft kaum zu	Trifft zu	Trifft besonders zu
Erfassung Unternehmen in repräsentativem Umfang				
Umfassende Risikoerfassung				
Analyse Abschlussverfahren				
	Trifft nicht zu		Trifft zu	
Vertragabschluss online möglich				
Vertragabschluss offline möglich				
Betreuung in Form eines persönlichen Beraters				
Betreuung unpersönlich (z.B. Service-Hotline)				
Leistungsumfang				
Eigenschäden				
Abdeckung von ...	Trifft nicht zu	Trifft kaum zu	Trifft zu	Trifft besonders zu
Wirtschaftlichen Schäden durch Betriebsunterbrechung				
Kosten der Datenwiederherstellung				
Kosten der Systemwiederherstellung				
Drittschäden **Abdeckung von Schadensersatzforderung von Kunden wegen ...**				
Datenmissbrauch				
Lieferverzug				
Serviceausfall oder -verzug				

Abbildung 6: Exemplarischer Aufbau Ratingbogen
(Bausteine: „Kontakt zur Versicherung" & „Leistungsumfang")

Der Kontakt zur Versicherung wurde als wesentlicher Faktor für die Güte einer Cyberversicherung bewertet. Hierfür gibt es ein breites Spektrum an Gründen. Zuerst soll hierzu darauf eingegangen werden, wie jung der Markt für Cyberversicherungen ist. Einige Versicherer

deklarieren ihre Cyberversicherungen in diesem Zusammenhang nicht einmal als solche[69]. Hieraus folgt, dass aus Unternehmenssicht ein intensiver Kontakt zum Versicherer unerlässlich ist, um das für sie passendste Angebot zu erhalten.

Neben den Schwierigkeiten bei der Namensfindung, gestaltet sich auch das Angebot von Cyberversicherungen als vielfältig. Die Schäden, die ein Unternehmen versichern kann, sind so umfangreich, dass auch hier eine intensive Beratung durch den Versicherer notwendig ist[70].

Letztlich dienten auch die Erkenntnisse aus dem Experteninterview als weiteres Argument für die Auswahl von „Kontakt zur Versicherung" als wesentliches Kriterium für das Rating von Cyberversicherungen. Insbesondere die Aussage, dass der Markt einem ständigen Wandel unterliegt, deckt sich mit den Erkenntnissen der Literaturrecherche und unterstreicht somit noch einmal die Bedeutung eines umfangreichen Kontakts zum Versicherer.

Diese Bedeutung nimmt sich der Ratingbogen in der Kategorie „Kontakt zum Versicherer" in Form von fünf Unterpunkten an. Eingangs wird hier die Risikoerfassung betrachtet. Hierbei soll ermittelt werden, wie genau der Versicherer das Unternehmen in seinem Fragebogen bzw. seiner Risikoerfassung abbildet und somit ein auf das Unternehmen zugeschnittenes Angebot vorschlagen kann. Bieten der Fragebogen und die Risikoerfassung ausreichend Möglichkeit, das eigene Unternehmen abzubilden, wird diese Fähigkeit mit „Trifft zu" bzw. „Trifft besonders zu" bewertet. Wird eine nicht ausreichende Erfassung vorgenommen, wird das Kriterium mit „Trifft kaum zu" bzw. „Trifft nicht zu" bewertet.

Um den Zugang zum Versicherer ganzheitlich abzubilden, werden weiterhin Serviceleistungen zur Kontaktaufnahme bewertet. Hierbei wird beurteilt, ob ein Vertragsabschluss online oder offline möglich ist oder beides. Weiterhin wird zwischen einer persönlichen und einer unpersönlichen Betreuung durch den Versicherer unterschieden. Mit „persönlich" ist in diesem Zusammenhang ein persönlicher Betreuer gemeint, der sich im Idealfall in räumlicher Nähe des Unternehmens befindet. Mit „unpersönlich" sind alle anderen Betreuungsmöglichkeiten, die keinen persönlichen Betreuer bereitstellen, gemeint. Hierunter können beispielsweise eine Service-Hotline oder ein Abschlussverfahren, das in Gänze online erfolgt, fallen.

Der zweite Block des Ratingbogens legt den Fokus auf den Leistungsumfang einer Cyberversicherung.
Die Grundlage für diesen Bewertungsbaustein setzt sich wieder aus mehreren Quellen zusammen.

Erster Anhaltspunkt sind hier die „Allgemeinen Versicherungsbedingungen für die Cyberrisiko-Versicherung", kurz „AVB Cyber", des GDV. Dieses Whitepaper umfasst wesentliche Bausteine zum Aufbau einer Cyberversicherung und soll als Anhaltspunkt für den Leistungsumfang dieser gelten.

Im Folgenden soll in Kürze auf die Grundstruktur des Whitepapers eingegangen werden. Das Whitepaper gliedert sich in zwei Teile, „A" und „B". Teil A beschäftigt sich mit den Regeln zur Ausgestaltung des Versicherungsschutzes, in einer Cyberversicherung. Diesem Teil sind im Wesentlichen die Ratingbausteine für die spätere Evaluation im Ratingbogen entnommen. Teil B

[69] Vgl. Choudhry 2014, S.5
[70] Vgl. Choudhry 2014, S.6

beschreibt Rechte und Pflichten der Vertragspartner einer Cyberversicherung. Dieser Baustein findet im Ratingbogen keine Beachtung[71].

Die essenziellen Punkte, die aus den AVB Cyber in den Ratingbogen eingeflossen sind, umfassen:

- Abschnitt A2: Service-/Kosten-Baustein,
- Abschnitt A3: Drittschaden-Baustein,
- Abschnitt A4: Eigenschaden-Baustein.
  Hieraus sind wiederum folgende Punkte speziell im Ratingbogen abgebildet:
  - A4-1 Betriebsunterbrechung/Ertragsausfall,
  - A4-2 Wiederherstellung von Daten,
  - A3-3 Ansprüche außerhalb der gesetzlichen Haftpflicht,
  - A3-4.3 Vertragliche Schadensersatzansprüche,
  - A2-1 Forensik Schadensfeststellungskosten,
  - A3-6.5 Prozesskosten bei Übersteigen der Versicherungssumme,
  - A2-2.2 Krisenkommunikation und PR-Maßnahmen[72].

Die Auswahl der im Ratingbogen abgebildeten Kriterien erfolgte nach der Gesamtevaluation des Versicherungsmarkts. Angebotspunkte die sowohl im Versicherungsangebot als auch im Portfolio des GDV häufig Erwähnung finden, wurden in den Ratingbogen aufgenommen. Weiterhin sind auch Bewertungskriterien wie „Kosten der Systemwiederherstellung" aufgeführt, da diese häufig im Leistungsportfolio der Versicherer zu finden sind. Zusammengefasst bietet das Whitepaper des GDV eine erste Grundlage für die Sinnhaftigkeit des im Ratingbogen analysierten Leistungsumfangs.

Letztlich bieten Studien wie das „Allianz Risk Barometer 2019" einen Überblick darüber, welchen Stellenwert der Leistungsumfang einer Cyberversicherung einnimmt. In diesem Bericht ist übersichtlich aufgeschlüsselt, welche Risiken für Unternehmen von Bedeutung sind, aber auch inwiefern bestimmte Risiken an Bedeutung gewonnen bzw. verloren haben[73]. Es lässt sich hieraus schlussfolgern, dass sich auch der Leistungsumfang der Versicherer einer stetigen Veränderung unterworfen sieht, weshalb eine Evaluation der unterschiedlichen Versicherungsleistungen zweckmäßig ist.

Für die Beurteilung der o. g. Kriterien wurde, ähnlich wie im Block „Kontakt zum Versicherer", wieder ein vierstufiges System verwendet.

Den letzten Baustein vor der Gesamtbeurteilung bildet der Preis – oder präziser ausgedrückt: der Preis nach Anforderung. Hiermit ist gemeint, dass bei der Auswertung der Versicherungsunternehmen mehrmals Versicherer die Cyberversicherung in Kombination mit anderen Versicherungsleistungen angeboten haben. Weiterhin gab es auch Fälle, in denen die Anforderungen des Musterunternehmens nicht mit einer Versicherung abgedeckt werden konnten, sondern mehrere Pakete erforderlich waren. Der Schwerpunkt dieser Kategorie liegt darauf, abzubilden, wer für die Anforderungen des Musterunternehmens das beste Paket und hiermit verbunden auch den besten Preis sicherstellen kann.

[71] Vgl. Gesamtverband der Deutschen Versicherungswirtschaft e.V. 2017, S.1
[72] Vgl. Gesamtverband der Deutschen Versicherungswirtschaft e.V. 2017 S.2 f.
[73] Vgl. Allianz 2019 S.5 ff.

Service-Leistungen				
Abdeckung von Kosten für ...	**Trifft nicht zu**	**Trifft kaum zu**	**Trifft zu**	**Trifft besonders zu**
IT-Forensik-Experten				
Rechtsschutz (Anwälte aus dem Bereich IT- und Datenschutzrecht)				
PR-Spezialisten für Krisenkommunikation				
Preis				
Preis für die Abdeckung der Anforderungen setzt sich aus mehreren Paketen/Angeboten zusammen				
Paketpreis deckt Anforderungen genau ab				
Paketpreis enthält nicht benötigte Zusatzangebote				
	A - -	**A -**	**A +**	**A + +**
Gesamtbewertung				

Abbildung 7: Ratingbogen (Bausteine „Preis“ & „Gesamtbewertung“)

Abschließend werden alle gewonnenen Erkenntnisse in einer Gesamtwertung zusammengefasst. Diese Wertung unterscheidet sich im Wesentlichen nicht von der Art der Bewertung in den Blöcken „Preis“ oder „Leistungsumfang“. Einziger Unterschied ist, dass bei der Gesamtbewertung Noten von „A++“ bis „A--" vergeben werden.

3.2 Anbieterübersicht

Um Teil dieser Studie zu werden benötigt ein Versicherungsunternehmen grundsätzlich ein Angebot über eine Cyberversicherung für KMU. Der Umfang, der in der Studie von Franke und Bornberg betrachteten Versicherungen wurde als Grundbaustein für die hier vorliegende Studie verwendet. Die 34 verglichenen Tarife stammten von insgesamt 25 Versicherungsunternehmen[74]. Diese wurden nach einer erneuten Überprüfung der einzelnen Angebote übernommen.

Da am volatilen Markt für Cyberversicherung stets neue Versicherungen mit einem Produkt an den Markt kommen und das Rating von Franke und Bornberg bereits knapp ein Jahr zurück liegt, wurde der vorhandene Stamm an Versicherungen aktualisiert. Grundlage hierzu war die online verfügbare Übersicht über Cyberversicherungen des Gesamtverbandes der Deutschen Versicherungswirtschaft[75]. Gelistet sind zum Zeitpunkt der Erstellung dieser Arbeit 38 Versicherer. Sämtliche nicht bereits im Stamm vorhandenen Versicherungen wurden ebenfalls hinsichtlich Ihres Angebotes einer Cyberversicherung für KMU geprüft. Nach Abschluss dieser Maßnahmen blieben insgesamt 28 Versicherungen übrig, welche für den vorliegenden Anwendungsfall in Betracht gezogen werden müssen.

Unternehmen	Produkt	Unternehmen	Produkt
AIG	CyberEdge	Helvetia	Business Cyber
Allianz	CyberSchutz	Hiscox	CyberClear
Arag	CyberSchutz	Interfloyd	CyberSchutz PLUS
Axa	ByteProtect	Markel	Pro Cyber
Badische BGV	BGVFIRM Cyber	Provinzial (Nord)	Cyber-Versicherung
Basler	Cyber-Police	Provinzial (Westf.)	Cyber-Versicherung
CNA Hardy	Netprotect	QBE	Cyber-Response
Condor	CyberRiskPolice	R+V	CyberRisk Police
Die Bayerische	Cyber Multi Risk	Signal Iduna	CyberPolice
Dual Deutschland	AVB Cyber Defence	SV Sparkassen	SV CyberSchutz
Ergo	Cyber-Versicherung	VGH	CyberSchutz
Gothaer	Cyber-Versicherung Gewerbe	VHV	Cyber Protect
HDI	Cyberversicherung Firmen	Württembergische	Cyber-Versicherung
HDI Global SE	Cyber+ Smart	XL Insurance	Cyberschaden-Vers.

Tabelle 3: Versicherer und ihre Produkte

[74] (Franke und Bornberg GmbH, 2018)
[75] (Gesamtverband der Deutschen Versicherungswirtschaft e. V.)

3.3 Produkteigenschaften Versicherung

Im nächsten Schritt wurden für alle Versicherungen über die unternehmenseigenen Webseiten, Dokumente über die Versicherungstarife, Vermittlerplattformen, etc. die jeweiligen Versicherungsmerkmale und -eigenschaften herausgearbeitet. Mit jeder neuen behandelten Versicherung wurde das Portfolio an Produkteigenschaften um weitere Eigenschaften erweitert oder bestimmte Definitionen für bereits vorhandene Eigenschaften angepasst beziehungsweise erweitert.

Basis-Bestandteile, die von jeder betrachteten Versicherung abgedeckt sind:

- Betriebsunterbrechung
- Cyber-Erpressung
- Datenmanipulation
- Datenwiederherstellung
- Schadenhotline.

All diese Bestandteile gehören zu den oftmals in der Literatur benannten Eigenschäden[76] und sind damit elementarer Bestandteil einer Cyberversicherung.

Mindestens 91 % der betrachteten Versicherungen decken zusätzlich behördliche Datenschutzverfahren, Funktionswiederherstellung, Kostenübernahme IT-Spezialisten, Kostenübernahme Rechtsberatung und Rettungsaufwendungen ab. Etwa 80 % erweitern das Angebot zusätzlich um eine Abdeckung von Fehlbedienung, Krisenkommunikation, Telefon-Hacking und Verlust durch Schäden bei externen Dienstleistern. Neben den bereits benannten Eigenschäden spiegeln sich in diesen Produktbestandteilen zusätzlich die Abdeckung von Fremdschäden[77] und Service-Leistungen[78] wider, wodurch sämtliche nach Umar Choudry in „Der Cyber-Versicherungsmarkt in Deutschland" genannten Merkmale zumindest bereits einen Vertreter haben[79].

Selten finden sich die letzten drei Bestandteile in den Versicherungsangeboten. Während die Policen zwar etwa über 60 % eine Systemverbesserung beinhalten, konnte eine Abdeckung von Softwareproblemen und Vertragsstrafen bei nur 13 von 28 Versicherungen festgestellt werden. Damit sind diese zwei Bestandteile bei weniger als 50 % aller am Markt vertretenen Cyberversicherungen abgesichert.

[76] (vgl. (Choudhry, 2014), Kap. 2.7)
[77] Bspw. Rettungsaufwendungen
[78] Bspw. Funktionswiederherstellung
[79] (Choudhry, 2014)

Produktbestandteil	Erläuterung
Datenschutzverfahren	Kosten für Rechtsanwälte und Sachverständige bei Einleitung von Straf-, Ordnungswidrigkeits- oder sonstiges behördliches Verfahren
Betriebsunterbrechung	Entgangener Gewinn fortlaufende Kosten bei Netzwerkeingriffen oder behördlichen Stilllegungsverfügungen bei Datenschutzverletzung
Cyber-Erpressung	Abdeckung von Cybererpressungen, wie z.B. Ransomware, welche Daten verschlüsselt und nur gegen Zahlung wieder entschlüsselt.
Datenmanipulation	Eigenschaden aufgrund der irrtümlichen Überweisung von Geld infolge einer Manipulation des Computersystems.
Datenwiederherstellung	Wiederherstellung der Daten bei Netzwerkeingriffen oder behördlichen Stilllegungsverfügungen wegen Datenschutzverletzungen
Externe Dienstleister	Mitversicherung eigener BU durch Ausfall von externen Dienstleistern
Fehlbedienung	Schadenbegrenzung aufgrund eines internen Systemausfalls, der aufgrund von Fehlbedienung entstanden ist
Funktionswiederherstellung	Wiederherstellung der IT nach Netzwerkeingriffen oder behördlichen Stilllegungsverfügungen nach Datenschutzverletzungen
Kostenübernahme IT-Spezialisten	Kosten eines IT-Forensikers im Falle tatsächlicher oder vermuteter Anhaltspunkte einer Cybervorfalls (Schaden)
Rechtsberatung	Aufwendung des VN z.B. für Rechtsanwälte
Krisenkommunikation	Kosten eines Krisenkommunikators in einem Schadensfall zur Abwehr und Minderung eines Reputationsschadens
Rettungsaufwendungen	Mit dem Versicherer abgestimmte Aufwendungen zur Vermeidung von Drittansprüchen, z.B. Gutscheine für Anspruchsteller
Schadenhotline	24 / 7 - Hotline im Schadensfall
Softwareprobleme	Schadensbegrenzung bei Systemausfällen wg. Softwareproblemen
Systemverbesserung	Kosten zur Schließung der für den Cyber-Angriff ursächlichen Sicherheitslücke, um künftige Angriffe zu vermeiden
Telefon-Hacking	Telefonmehrkosten infolge eines Angriffs auf das Telefonsystem
Vertragsstrafen	PCI-DSS Vertragsstrafen bei Kreditkartenbetrug oder -datendiebstahl.

Tabelle 4: Produktbestandteile und Erläuterung

	VERSICHERUNGSUNTERNEHMEN						
PRODUKTBESTANDTEILE	AIG Europe S.A. *Cyber Edge*	Allianz AG *Cyber Schutz*	ARAG *Cyber Schutz*	AXA Vers. AG *Byte Protect*	BGV AG *BGVFIRM Cyber*	Basler AG *Cyber-Police*	CNA Hardy *Netprotect*
Datenschutzverfahren	✓	✓	✓	✓	✓	✓	✓
Betriebsunterbrechung	✓	✓	✓	✓	✓	✓	✓
Cybererpressung	✓	✓	✓	✓	✓	✓	✓
Datenmanipulation	✓	✓	✓	✓	✓	✓	✓
Datenwiederherstellung	✓	✓	✓	✓	✓	✓	✓
Fehlbedienung	✓	✓	✓	✓	×	✓	✓
IT-Wiederherstellung	✓	✓	✓	✓	×	✓	✓
IT-Forensiker	✓	✓	✓	✓	✓	✓	✓
Rechtsberatung	✓	✓	✓	✓	✓	✓	✓
Krisenkommunikation	✓	✓	✓	✓	✓	✓	✓
Rettungsaufwendungen	✓	✓	✓	✓	✓	✓	✓
Schadenhotline	✓	✓	✓	✓	✓	✓	✓
Softwareprobleme	✓	×	×	×	×	✓	×
Systemverbesserung	✓	✓	✓	✓	×	✓	✓
Telefon-Hacking	✓	✓	✓	✓	×	✓	✓
Externe Dienstleister	✓	✓	✓	✓	✓	×	×
Vertragsstrafen	×	✓	×	×	✓	✓	×

Tabelle 5: Versicherungsunternehmen und Produktbestandteile 1/4

	VERSICHERUNGSUNTERNEHMEN						
PRODUKTBESTANDTEILE	Condor *CyberRisk Police*	Die Bayerische *Cyber Multi Risk*	DUAL GmbH *Cyber Defence*	ERGO Group AG *Cyber-Vers.*	Gothaer VVaG *Cyber-Vers.*	HDI Vers. AG *Cybervers.*	HDI Global SE *Cyber + Smart*
Datenschutzverfahren	✓	✓	✓	✓	✓	✓	✓
Betriebsunterbrechung	✓	✓	✓	✓	✓	✓	✓
Cybererpressung	✓	✓	✓	✓	✓	✓	✓
Datenmanipulation	✓	✓	✓	✓	✓	✓	✓
Datenwiederherstellung	✓	✓	✓	✓	✓	✓	✓
Fehlbedienung	✓	×	✓	✓	✓	✓	✓
IT-Wiederherstellung	✓	✓	✓	✓	✓	✓	✓
IT-Forensiker	✓	✓	✓	✓	✓	✓	✓
Rechtsberatung	✓	✓	✓	✓	✓	✓	✓
Krisenkommunikation	✓	✓	✓	✓	✓	✓	✓
Rettungsaufwendungen	✓	✓	✓	✓	✓	✓	✓
Schadenhotline	✓	✓	✓	✓	✓	✓	✓
Softwareprobleme	×	✓	×	✓	×	✓	✓
Systemverbesserung	×	✓	✓	✓	✓	✓	✓
Telefon-Hacking	✓	✓	✓	✓	×	✓	✓
Externe Dienstleister	✓	✓	×	×	×	×	✓
Vertragsstrafen	×	✓	✓	✓	✓	✓	✓

Tabelle 6: Versicherungsunternehmen und Produktbestandteile 2/4

	VERSICHERUNGSUNTERNEHMEN						
PRODUKTBESTANDTEILE	Helvetia *Business Cyber*	HISCOX *Cyber Clear*	Interlloyd *Cyber Schutz+*	Markel *Pro Cyber*	Provinzial Nord *Cyber-Vers.*	Provinzial WF *Cyber-Vers.*	QBE *Cyber Response*
Datenschutzverfahren	✓	✓	×	✓	×	×	✓
Betriebsunterbrechung	✓	✓	✓	✓	✓	✓	✓
Cybererpressung	✓	✓	✓	✓	✓	✓	✓
Datenmanipulation	✓	✓	✓	✓	✓	✓	✓
Datenwiederherstellung	✓	✓	✓	✓	✓	✓	✓
Fehlbedienung	✓	✓	×	✓	✓	✓	✓
IT-Wiederherstellung	×	✓	✓	✓	✓	✓	✓
IT-Forensiker	✓	✓	✓	✓	✓	✓	✓
Rechtsberatung	✓	✓	✓	✓	✓	✓	✓
Krisenkommunikation	✓	✓	×	✓	×	×	✓
Rettungsaufwendungen	✓	✓	×	✓	✓	✓	×
Schadenhotline	✓	✓	✓	✓	✓	✓	✓
Softwareprobleme	×	×	✓	✓	✓	✓	×
Systemverbesserung	×	×	×	✓	✓	✓	×
Telefon-Hacking	✓	✓	×	×	✓	✓	×
Externe Dienstleister	✓	✓	✓	✓	✓	✓	✓
Vertragsstrafen	×	✓	×	✓	×	×	×

Tabelle 7: Versicherungsunternehmen und Produktbestandteile 3/4

	VERSICHERUNGSUNTERNEHMEN						
PRODUKTBESTANDTEILE	R + V *Cyber Risk Police*	Signal Iduna *Cyber Police*	Sparkassen Vers. *SV Cyberschutz*	VGH *Cyber Schutz*	VHV *Cyberprotect*	Württemberg. *Cyber-Vers.*	XL Insurance *cyber insurance*
Datenschutzverfahren	✓	✓	✓	✓	✓	✓	✓
Betriebsunterbrechung	✓	✓	✓	✓	✓	✓	✓
Cybererpressung	✓	✓	✓	✓	✓	✓	✓
Datenmanipulation	✓	✓	✓	✓	✓	✓	✓
Datenwiederherstellung	✓	✓	✓	✓	✓	✓	✓
Fehlbedienung	✓	×	×	✓	✓	✓	✓
IT-Wiederherstellung	✓	✓	✓	✓	✓	✓	✓
IT-Forensiker	✓	✓	✓	✓	×	✓	×
Rechtsberatung	✓	✓	✓	✓	✓	✓	×
Krisenkommunikation	✓	×	×	✓	✓	✓	×
Rettungsaufwendungen	✓	✓	×	✓	✓	✓	✓
Schadenhotline	✓	✓	✓	✓	✓	✓	✓
Softwareprobleme	×	✓	×	×	✓	×	✓
Systemverbesserung	×	×	×	×	×	✓	✓
Telefon-Hacking	✓	✓	✓	✓	✓	×	✓
Externe Dienstleister	✓	✓	✓	✓	✓	✓	✓
Vertragsstrafen	×	×	×	×	×	✓	✓

Tabelle 8: Versicherungsunternehmen und Produktbestandteile 4/4

3.4 Ergebnisse

Im Folgenden werden die Ergebnisse des Benchmarks präsentiert. Dazu werden in drei Spotlights „Abschluss", „Risikobetrachtung" und „Leistungen" die Versicherungen vorgestellt, die in ihrer jeweiligen Kategorie das beste Rating erzielen konnten. Sinn und Zweck dieser Spotlights ist es, Tendenzen auf dem Markt aufzuzeigen und diese anhand herausragender Versicherer zu illustrieren.

3.4.1 Abschluss

Versicherer erhielten ein positives Rating, die ein besonders transparentes Abschlussverfahren anbieten. Weiterhin war auch eine intuitive Bedienbarkeit der Firmenwebsite sowie eine persönliche Beratung in Form einer Hotline oder eines Versicherungsberaters ein positiver Ratingfaktor.

Alle Versicherungsanbieter beschreiben bereits auf ihren Websites die Möglichkeit zum Offline-Vertragsabschluss. 72 % der Anbieter stellen dem Kunden den Abschluss auch online zur Verfügung. In Bezug auf die Digitalisierung des Abschlussverfahrens ist hier der einzige potenzielle Handlungsbedarf zu erkennen. Es muss allerdings berücksichtigt werden, dass hinsichtlich der Komplexität des Cyberversicherungsmarktes nicht grundsätzlich klar ist, ob bei einem Online-Vertragsabschluss die ganzheitliche Erfassung eines Unternehmens gewährleistet werden kann. Dementsprechend ist der Handlungsbedarf nur bedingt gegeben.

Auch in Bezug auf die Kundenbetreuung schneiden die Versicherer überwiegend positiv ab. 81 % der Versicherer bieten eine direkte Betreuung durch einen Versicherungsberater auf ihren Websites an. Weiterhin bieten 72 % eine Betreuung in Form einer Kunden-Hotline an.

Hier sollen Versicherer vorgestellt werden, die in Bezug auf den Abschluss einer Cyberversicherung im Rating besonders gut abgeschnitten haben.

Die Cyberpolice der Signal Iduna erfüllt alle geforderten Kriterien und schneidet in dieser Kategorie „Abschluss" mit Bestnote ab. Die Website der Signal Iduna besticht durch gute Bedienbarkeit. Es besteht die Möglichkeit sich umgehend persönlich beraten zu lassen.

Abbildung 8: Exemplarischer Aufbau Firmenwebsite Signal Iduna

Kontaktfelder sind durchgängig auf der Website zu finden. Es besteht die Möglichkeit eine Cyberpolice entweder direkt auf der Website abzuschließen oder nach dem Gespräch mit einem persönlichen Berater. Weiterhin wird der potenzielle Kunde auf der Website direkt und unkompliziert mit Informationsmaterial zur Cyberpolice versorgt. Dies geschieht in Form von PDF-Downloads zu den Cyberpolicen und weiterem Informationsmaterial.

Neben der Signal Iduna erfüllte nur die Ergo Cyberversicherung alle Anforderungen in der Kategorie „Abschluss". Auch hier tat sich die Website durch eine intuitive Bedienbarkeit, einen verständlichen Aufbau und einen unkomplizierten Zugang zu einem Kundenberater oder einer Hotline hervor.

Zusammenfassend bietet der überwiegende Teil der 28 Versicherer seinen potenziellen Kunden einen unkomplizierten Zugang zu Kundenberatung und Informationsmaterial. Die Websites sind übersichtlich und bieten alle Informationen zur Cyberversicherung in komprimierter Form. Der Trend geht eindeutig zum Versicherungsabschluss über das Internet.

3.4.2 Risikobetrachtung

Das zweite Spotlight geht der zentralen Frage nach, wie gut sich ein KMU in der Versicherung wiederfindet. Dazu wurden Risikobetrachtung und Leistungsumfang der Versicherungen evaluiert.

54 % der Versicherer erfassen auf ihren Websites die fiktiven Musterunternehmen in Form eines Fragebogens. Zwei Versicherer haben besonders umfangreiche Fragebögen zur Analyse der Musterunternehmen und erhielten die Bewertung „Trifft besonders zu".

72 % der Versicherer erfüllten die Anforderungen an die Erfassung von Risiken. Zwei Versicherer übertrafen die Anforderungen. Sowohl bei der Erfassung von Unternehmen als auch der umfassenden Risikoerfassung konnte nur jeweils ein Versicherer die Anforderungen nicht erfüllen.

Die Überführung der relevanten Kennzahlen in den Leistungsumfang der Versicherung gelingt den meisten Versicherern. Bis auf Ausnahmen im Bereich Softskills, bildet die Mehrheit der Versicherer die in den AVB Cyber geforderten Leistungen ab. Näheres hierzu in Spotlight 3.

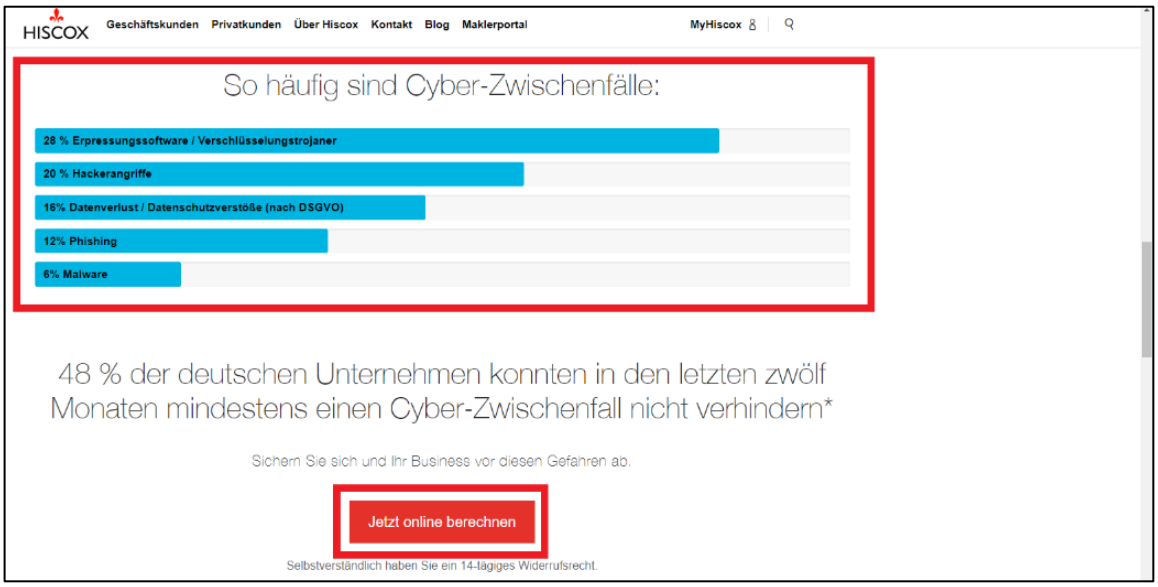


Abbildung 9: Exemplarischer Aufbau Corporate Website Hiscox

Insgesamt erhalten 59 % der Versicherer das Rating „Trifft zu“ bei der Evaluation ihres Leistungsumfangs.

Spitzenreiter in der Risikobetrachtung und Überführung in den Leistungsumfang ist Hiscox. Der Tarif „CyberClear“ erzielt im Benchmark die besten Ergebnisse. Hiscox informiert als einziger Versicherer umfassend über Cyberrisiken von Unternehmen. Kunden können ihre Prämie in einem detaillierten Fragebogen berechnen. Hiscox erfasst die umfassendsten Kundendaten und kann somit die Frage, wie gut sich ein Unternehmen im Versicherungstarif wiederfindet, am besten beantworten. Dieser ganzheitliche Ansatz findet sich auch im Angebot der Hiscox wieder. Die Kombination aus umfassender Risikoerfassung sowie der Unternehmenserfassung und einem breiten Leistungsportfolio, verschafft der Hiscox insgesamt die Bestnote A++.

Zusammengefasst kann auch im Spotlight 2 eine positive Bilanz zum Cyberversicherungsmarkt gezogen werden. Der Großteil der Versicherer ist sowohl in Risikoerfassung als auch in Leistungsumfang solide aufgestellt und erfüllt die Forderungen des Ratingbogens.

3.4.3 Leistung

In Spotlight 3 werden die einzelnen Leistungen der Versicherungen zueinander in Bezug gesetzt, um so einen Überblick darüber zu verschaffen, welche dieser Leistungen besonders häufig oder ausgesprochen selten und in welcher Qualität durch die Versicherer abgedeckt werden.

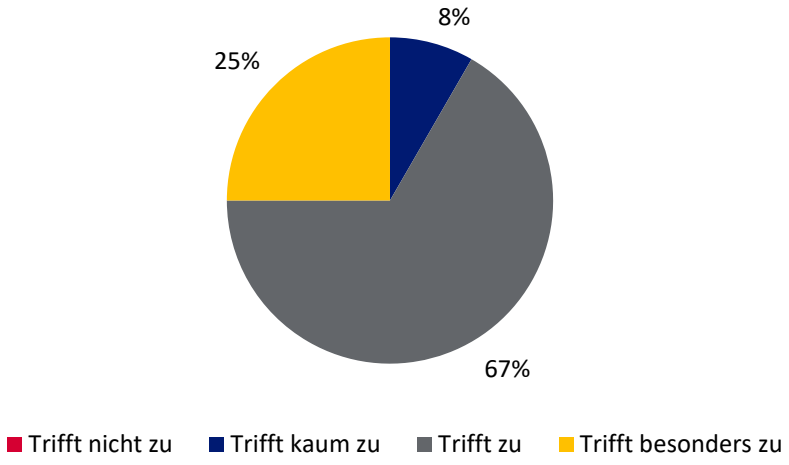


Abbildung 10: Verteilung der Bewertungen des Bausteins „Systemwiederherstellung“

Die Bausteine „Systemwiederherstellung“ und „Datenwiederherstellung“ werden von den Versicherern als jeweils eigenständige Inhalte der Police verstanden, jedoch gleich bewertet. Auch der GDV weist beide Bausteine einzeln aus. Eine Systemwiederherstellung beinhaltet sehr wahrscheinlich auch die Widerherstellung von Daten, umgekehrt kann aber ein System funktionieren, Daten aber verloren sein.

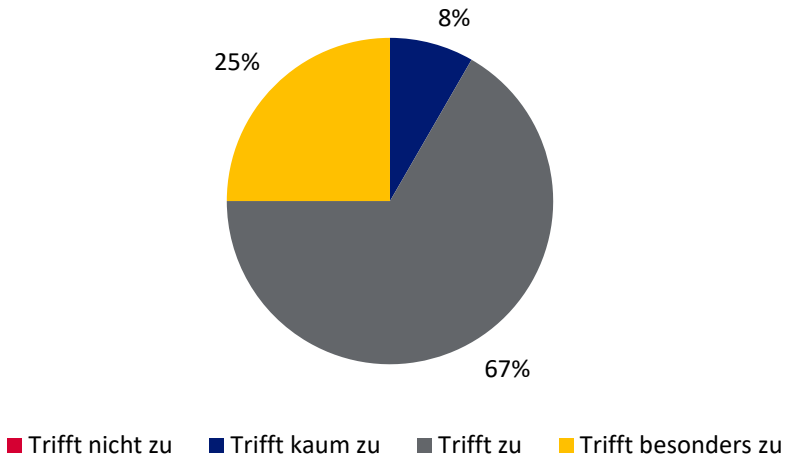


Abbildung 11: Verteilung der Bewertungen des Bausteins „Datenwiederherstellung“

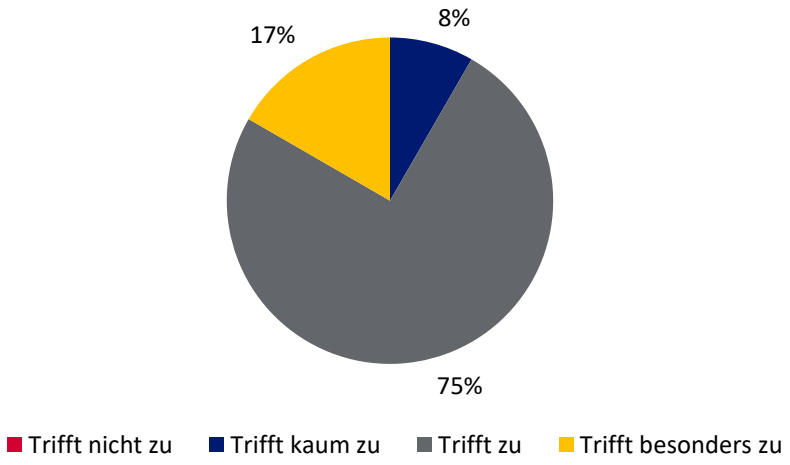


Abbildung 12: Verteilung der Bewertungen des Bausteins „Wirtschaftliche Schäden durch Betriebsunterbrechung“

Die Kostenübernahme von wirtschaftlichen Schäden durch Betriebsunterbrechungen infolge eines Cybervorfalls macht den größten Anteil des Spektrums aus. Diese werden in über 90 % der Fälle ausgeglichen. Insgesamt übernehmen alle untersuchten Versicherer mindestens einen Teil der hieraus entstandenen wirtschaftlichen Schäden.

Eigenschäden stehen im Fokus der unterschiedlichen Policen. Ein hoher Teil der untersuchten Versicherungen deckt Eigenschäden voll oder gar besonders ab während im Gegenzug in keinem der untersuchten Fälle eine Nichtabdeckung von Eigenschäden stattfindet. Dies hebt den Leistungsbereich der Eigenschäden deutlich von denen der Drittschäden und der Service-Leistungen ab.

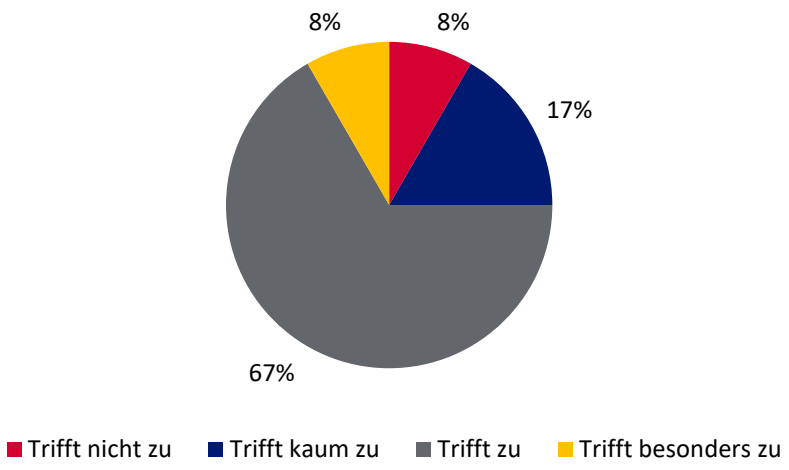


Abbildung 13: Verteilung der Bewertungen des Bausteins „Lieferverzug“

Der Baustein Lieferverzug erweitert den Baustein der wirtschaftlichen Schäden durch Betriebsunterbrechung Dritter (Kunden der Policeninhaber) dar. Dabei ist zu beobachten, dass hier immer noch ein starker Fokus auf der Abdeckung dieser Schäden liegt.

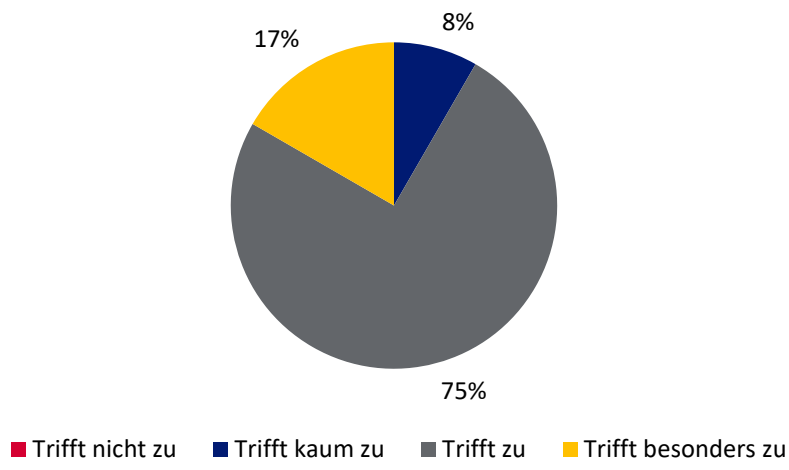


Abbildung 14: Verteilung der Bewertungen des Bausteins „Datenmissbrauch“

Über 90 % der untersuchten Policen decken Schäden für Dritte im Rahmen von Datenmissbrauch ab, welche gerade im Rahmen der restriktiveren Vorgaben und Haftungsbedingungen durch den Gesetzgeber wie die EU-Datenschutz-Grundverordnung (EU-DSGVO) an Bedeutung gewinnen.

Der Baustein „Schutze vor Serviceausfall bei Dritten“ wird von allen untersuchten Cyber-Versicherungen zumindest eingeschränkt angeboten. In 17 % der Fälle wird ein besonderer Wert auf die Abdeckung dieses Schadens gelegt.

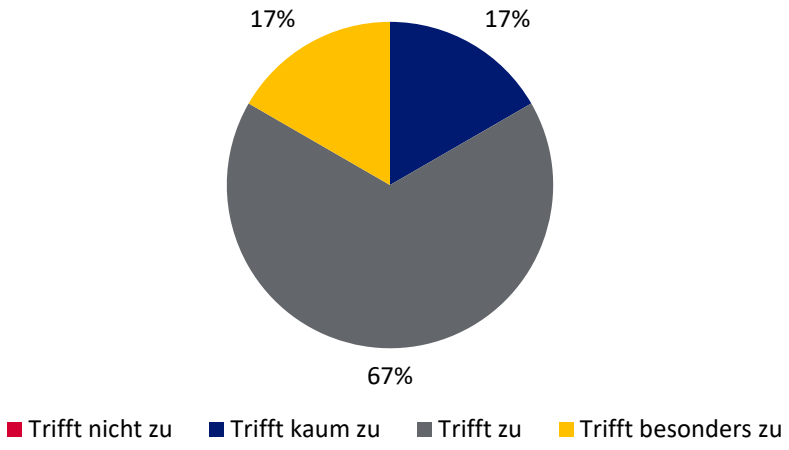


Abbildung 15: Verteilung der Bewertungen des Bausteins „Serviceausfall“

In der Gesamtbetrachtung haben Drittschäden ein ähnliches Gewicht wie Eigenschäden. Bis auf den Schaden „Lieferverzug“, erhalten Kunden bei allen Policen eine rudimentäre Abdeckung. Geht man davon aus, dass alle Teilnehmer einer B2B Wertschöpfungskette Cyberpolicen besitzen, ist eine doppelte Absicherung von Schäden durch Cybervorfälle vorhanden ist.

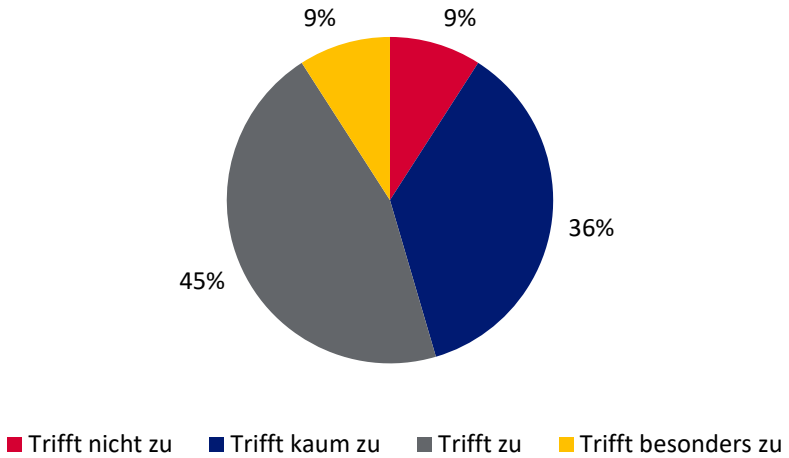


Abbildung 16: Verteilung der Bewertungen des Bausteins „Rechtsschutz“

Der Baustein „Rechtsschutz“ weicht von den übrigen Ergebnissen ab. Ein möglicher Grund für diese im Vergleich geringere Bereitschaft der Kostenübernahme durch die Versicherer könnte darin liegen, dass sie Umfang und Dauer von Rechtsstreitigkeiten im Zusammenhang mit Cyberangriffen unzureichend einschätzen können. Eine weitere Möglichkeit bestünde in der Vielfalt von Rechtsschutzversicherungsangebote deren Absatz man nicht kannibalisieren möchte.

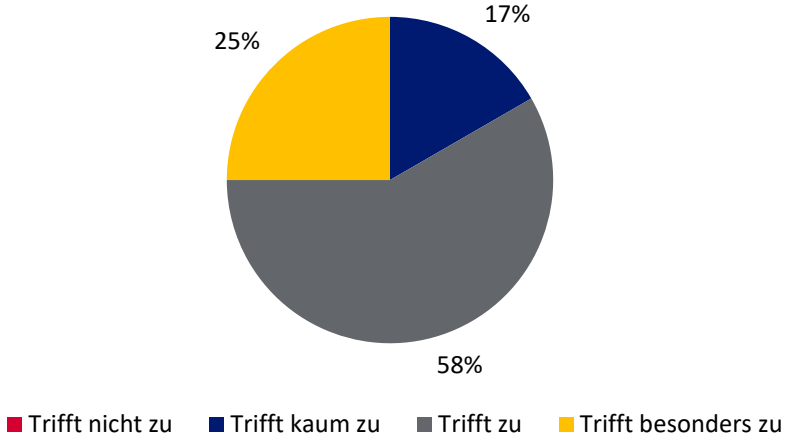


Abbildung 17: Verteilung der Bewertungen des Bausteins „IT-Forensik-Experten"

Alle Policen beinhalten den Baustein „Bereitstellung von IT-Forensik-Experten nach einem Cyberangriff". Die Versicherer schließen dazu Verträge mit einem oder mehreren Cybersecurity Consulting Anbietern. Maßnahmen der IT-Forensik nach einem Cyberangriff bieten die Möglichkeit, nicht nur den Angreifer zu identifizieren und den Schaden eingrenzen zu können, sondern auch die Schwachstellen im System, aufzuspüren und zu schließen. Dies dient dem Schutz vor erneuten Angriffen und der Kostenvermeidung durch weitere Auszahlungen der Versicherer. Andererseits könnten IT-Forensik-Experten eine ursächliche Fahrlässigkeit auf Versichertenseite nachweisen.

Je nach Aufstellung der Versicherungsbedingungen könnten durch diese nachgewiesene Fahrlässigkeit Ausschlussklauseln greifen, welche den Versicherer vor umfangreicheren Zahlungen und damit – aus seiner Sicht – Schäden schützt. Aus Sicht der Versicherten stellt der Baustein der IT-Forensik-Experten insbesondere für kleinere Unternehmen wie die, „Arztpraxis Dr. Schröder" möglicherweise ein attraktives Angebot dar. Schließlich verfügen KMU, wenn überhaupt, nur über geringe interne IT-Mitarbeiter-Ressourcen.

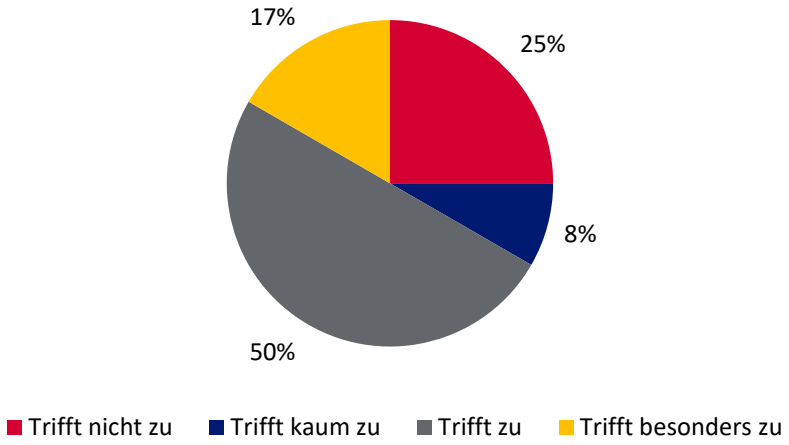


Abbildung 18: Verteilung der Bewertungen des Bausteins „Krisenkommunikation"

Der Baustein „Krisenkommunikation" bietet ein ähnliches Bild wie der Baustein „Rechtsschutz". Die Krisenkommunikation weist den höchsten Anteil des Nichtanbietens von allen untersuchten Komponenten der Policen auf.

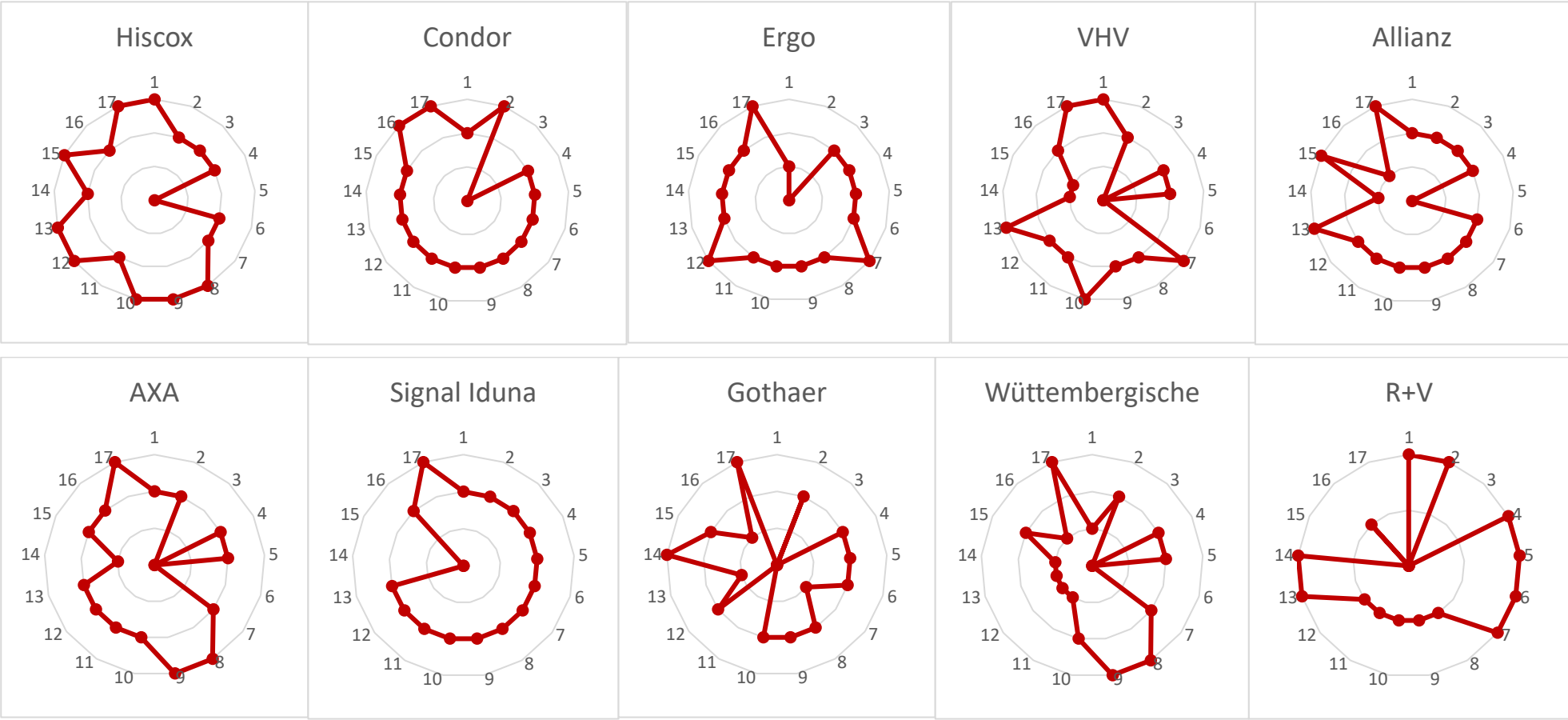
3.4.4 Bewertung

Die Cyberpolice Cyber Clear der Hiscox belegt den ersten Rang. Allianz, AXA, Condor, Ergo, Signal Iduna sowie VHV teilen sich Rang Zwei. Auf dem dritten Rang sind Gothaer und Württembergische gefolgt von der R+V auf Rang Vier.

Versicherung	Rang	%
Hiscox	1	≥ 75
Allianz	2	≥ 60
AXA		
Condor		
ERGO		
Signal Iduna		
VHV		
Gothaer	3	≥ 45
Württembergische		
R+V	4	< 45

Tabelle 9: Ranking der Versicherungsunternehmen und Cyberpolicen

Einzelbewertung von Cyberpolicen und Versicherungsunternehmen (Absteigender Rang)



1: Erfahrung Firma 2: Erfahrung Risiko 3: Vertrag online 4: Vertrag offline 5: Betreuung persönlich 6: Betreuung unpersönlich 7: Betriebsunterbrechungen 8: Datenwiederherstellung 9: System Wiederherstellung 10: Datenmissbrauch 11: Lieferverzug 12:Serviceausfall 13: Forensik 14: Rechtsschutz 15: PR 16: deckt genau 17: Zusatz

Quellenverzeichnis

Allianz. 2019. *Allianz Risk Barometer – Results Appendix.* München : Allianz Global Corporate & Specialty SE, 2019.

—. 2019. *Allianz Risk Barometer – Top Business Risks for 2019.* München : Allianz Global Corporate & Specialty SE, 2019.

Baban, Constance P., et al. 2018. Die Grenzen von Cyberversicherungen. *BIGS / Essenz.* April 2018, 17, S. 1-15.

BavariaDirekt. BavariaDirekt. *Cyber-Versicherung: Produktinfos.* [Online] https://www.bavariadirekt.de/versicherungen/rund-ums-haus/cyber-versicherung/produktinfos/.

Biener, Christian, Eling, Martin und Wirfs, Jan Hendrik. 2015. Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers.* 2015, 40, S. 131-158.

Böhme, Rainer und Kataria, Gaurav. 2006. On the Limits of Cyber-Insurance. [Hrsg.] Simone Fischer-Hübner, Steven Furnell und Costas Lambrinoudakis. *Trust, Privacy, and Security in Digital Business.* Krakau : Springer, 2006, Bd. Lecture Notes in Computer Science 4083, S. 31-40.

Bundesamt für Sicherheit in der Informationstechnik (BSI). 2018. *Cyber-Sicherheits-Exposition.* Bonn : s.n., 2018.

—. 2018. *Die Lage der IT-Sicherheit in Deutschland 2018.* Bonn : s.n., 2018.

Bundeskriminalamt (BKA). 2018. *Cybercrime – Bundeslagebild 2017.* Wiesbaden : s.n., 2018.

Choudhry, Umar. 2014. *Der Cyber-Versicherungsmarkt in Deutschland.* Wiesbaden : Springer Gabler, 2014.

de Smidt, Guido und Botzen, Wouter. 2018. Perceptions of Corporate Cyber Risks and Insurance Decision-Making. *The Geneva Papers.* 20. März 2018, 43, S. 239-274.

Deloitte. 2017. *Cyber-Security Report 2017 – Teil 2: Cyber-Risiken in Unternehmen.* 2017.

Dose, Jens. 2018. Das sagen Experten zur Ransomware-Attacke auf Krauss Maffei. *ChannelPartner.* [Online] IDG, 11. Dezember 2018. [Zitat vom: 10. Februar 2019.] https://www.channelpartner.de/a/das-sagen-experten-zur-ransomware-attacke-auf-krauss-maffei,3546268.

Eling, Martin. 2018. Cyber Risk and Cyber Risk Insurance: Status Quo and Future Research. *The Geneva Papers.* 15. März 2018, 43, S. 175-179.

Ferguson, Scott. 2018. Security Now. [Online] 03. August 2018. [Zitat vom: 2019. Februar 26.] https://www.securitynow.com/author.asp?section_id=613&doc_id=741202.

Franke und Bornberg GmbH. 2018. *Franke und Bornberg präsentiert erstes Cyber-Rating.* Hannover : s.n., 2018.

Franke, Ulrik. 2018. Cyber Insurance Against Electronic Payment Service Outages. [Hrsg.] Sokratis K. Katsikas und Cristina Alcaraz. *Security and Trust Management.* Barcelona : Springer, 2018, Bd. Lecture Notes in Computer Science 11091, S. 73-84.

Gann, Florian. 2018. Elektrowerkzeughersteller Metabo aus Nürtingen: Wie ein Cyberangriff das Unternehmen lähmte. *Stuttgarter Zeitung.* [Online] 17. Juli 2018. [Zitat vom: 25. Februar 2019.] https://www.stuttgarter-zeitung.de/inhalt.it-manager-erlebte-cyberangriff-man-wird-in-die-steinzeit-zurueckgebombt.21ffcde5-443a-4398-afbd-5d65dd69f726.html.

Gesamtverband der Deutschen Versicherungswirtschaft e. V. 2018. *Cyberrisiken im Mittelstand.* Berlin : s.n., 2018.

—. 2018. *Cyberrisiken im Mittelstand.* Berlin : s.n., 2018.

—. Die Versicherer – Das Verbraucherportal des GDV. *Entdecken: Wer versichert was.* [Online] [Zitat vom: 22. März 2019.] https://www.dieversicherer.de/service/wer-versichert-was/versicherer/14?p=Cyberversicherung.

—. 2019. Wer versichert was. *dieversicherer.* [Online] 2019. [Zitat vom: 28. Februar 2019.] https://www.dieversicherer.de/service/wer-versichert-was/versicherer/14?p=Cyberversicherung.

Hiscox SA. *hiscox.de.* [Online] [Zitat vom: 2019. 03 26.] https://www.hiscox.de/geschaeftskunden/cyber-versicherung/.

Kommission der Europäischen Gemeinschaften. 2003. *Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (Text von Bedeutung für den EWR).* [Amtsblatt Nr. L 124] Brüssel : s.n., 20. Mai 2003. K(2003) 1422.

KPMG. 2018. *Clarity on Cyber Security – Driving growth with confidence.* Zürich : KPMG AG, 2018.

Lechner, Ulrike, [Hrsg.]. 2018. *Monitor 2.0 IT-Sicherheit Kritischer Infrastrukturen.* Neubiberg : s.n., 2018.

—. 2017. *Monitor IT-Sicherheit Kritischer Infrastrukturen.* Neubiberg : s.n., 2017.

Lomen, Heinz. 2017. Die zweite Verteidigungslinie – Cyber-Versicherung – Versicherungsschutz für Risiken aus der Sphäre von Industrie 4.0. [Hrsg.] Volker P. Andelfinger und Till Hänisch. *Industrie 4.0.* Wiesbanden : Gabler, 2017, 9, S. 111-135.

Martinelli, Fabio, Uuganbayar, Ganbayar und Yautsiukhin, Artsiom. 2018. Optimal Security Configuration for Cyber Insurance. [Hrsg.] Lech Jan Janczewski und Mirosław Kutyłowski. *ICT Systems Security and Privacy Protection.* Poznan : Springer, 2018, S. 187-200.

Meland, Per Håkon, et al. 2017. Facing Uncertainty in Cyber Insurance Policies. [Hrsg.] Giovanni Livraga und Chris Mitchell. *Security and Trust Management.* Oslo : Springer, 2017, Bd. Lecture Notes in Computer Science 10547, S. 89-100.

Meuser, Michael und Nagel, Ulrike. 2009. Das Experteninterview – konzeptionelle Grundlagen und methodische Anlage. [Hrsg.] Susanne Pickel, et al. *Methoden der vergleichenden Politik- und Sozialwissenschaft.* Wiesbaden : VS Verlag für Sozialwissenschaft, 2009, S. 465-479.

Myra Security GmbH. 2019. Myracloud - Was ist ein DDoS-Angriff? [Online] 2019. [Zitat vom: 2019. Februar 26.] https://myracloud.com/de/was-ist-ein-ddos-angriff/.

Pickel, Susanne. 2009. Die Triangulation als Methode in der Politikwissenschaft. [Hrsg.] Susanne Pickel, et al. *Methoden der vergleichenden Politik und Sozialwissenschaft.* Wiesbaden : VS Verlag für Sozialwissenschaft, 2009, S. 517-542.

Pickel, Susanne, et al., [Hrsg.]. 2009. *Methoden der vergleichenden Politik- und Sozialwissenschaft.* Wiesbaden : VS Verlag für Sozialwissenschaften, 2009.

Rudel, Steffi und Lechner, Ulrike, [Hrsg.]. 2018. *IT-Sicherheit für Kritische Infrastrukturen – State of the Art: Ergebnisse des Förderschwerpunkts IT-Sicherheit für Kritische Infrastrukturen ITS|KRITIS des BMBF.* Neubiberg : s.n., 2018.

SIGNAL IDUNA Krankenversicherung a. G. *signal-iduna.* [Online] [Zitat vom: 2019. 03 26.] https://www.signal-iduna.de/technische-versicherung/cyber-versicherung.php.

Turek, Michael. 2016. Arzt ist Opfer einer Cyberattacke - Patientendaten gesperrt. *Neue Ruhr Zeitung.* [Online] 2016. [Zitat vom: 25. Februar 2019.] https://www.nrz.de/staedte/dinslaken-huenxe-voerde/arzt-ist-opfer-einer-cyberattacke-patientendaten-gesperrt-id11917990.html.

VERIVOX. 2019. VERIVOX. *Cyber-Versicherung.* [Online] 2019. https://www.verivox.de/privathaftpflicht/themen/cyber-versicherung/.

Wawrzyniak, Dariusz. 2006. Information Security Risk Assessment Model for Risk Management. [Hrsg.] Simone Fischer-Hübner, Steven Furnell und Costas Lambrinoudakis. *Trust, Privacy, and Security in Digital Business.* Krakau : Springer, 2006, Bd. Lecture Notes in Computer Science 4083, S. 21-30.

Woods, Daniel, et al. 2017. Mapping the coverage of security controls in cyber insurance proposal forms. *Journal of Internet Services and Applications.* 14. Juli 2017, Bd. 8, 8.

Über infodas

Gemeinsam die (digitale) Welt sicherer machen
Wir machen durch unsere Produkte und Dienstleistungen eine sichere, system- und domänenübergreifende Digitalisierung im öffentlichen Sektor und in der Wirtschaft möglich.

Wir sind ein unabhängiges und innovatives Familienunternehmen des deutschen Mittelstandes. Wir ermöglichen und leben die Grundsätze von Familie. Kunden, Partner und Mitarbeiter sind Teil dieser Familie. Für Sie stehen wir ein – heute, morgen, übermorgen. Informationssicherheit und modernste Technologien sind unsere Leidenschaft.

Was bedeutet unser Mission Statement?
Virtuelle Organisationen, verteilte Infrastrukturen und vernetzte Operationsführung – Das sind nur ein paar Begriffe, die unterstreichen, dass die Ende-zu-Ende-Digitalisierung von Prozessen und Systemen und damit eine zunehmende Vernetzung unabdingbar wird – **connect more.**

Mehr Vernetzung birgt jedoch auch mehr Angriffsmöglichkeiten. Folglich ist das Sichern der digitalen Verbindungen ein absolutes Muss, dies auch über die System- und Domänengrenzen hinweg. Zudem ist es erforderlich, dass die Informationssicherheit bei allen Projekten zu jedem Zeitpunkt konzeptionell und integriert berücksichtigt wird – **be secure.**

Unser Mission Statement greift genau das auf: Mit **connect more. be secure.** möchten wir unsere Verantwortung und Rolle im digitalen Zeitalter zum Ausdruck bringen.
Ob Domänenübergänge mit SDoT, ein solides ISMS mit SAVe und flankierendem Pentesting oder Digitalisierungskonzepte, wir tragen als Teil der infodas Familie gemeinsam dazu bei, unser Mission Statement jeden Tag zu leben.

Kontakt

INFODAS Gesellschaft für Systementwicklung und Informationsverarbeitung mbH
Rhonestr. 2 I 50765 Köln I Deutschland
T: +49 221 70912-0 I F: +49 221 70912-655 I E: vertrieb@infodas.de I www.infodas.de

Mehr zu Digitalisierung und Cybersicherheit auf www.infodas.de/blog oder folgen Sie uns auf

@INFODAS

de.linkedin.com/company/infodas

www.xing.com/companies/infodas

infodas
connect more. be secure.