bitkom

Cyberversicherung und -sicherheit

Herausgeber
Bitkom e. V.
Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Gustav Spät | Referent Digital Insurance & InsurTech
T 030 27576-137 | g.spaet@bitkom.org

Verantwortliches Bitkom-Gremium
AK Digital Insurance & InsurTech

Autorinnen und Autoren
Gisa Kimmerle | Hiscox SA
Falko Knöfler | Computacenter AG & Co. ohg
Sebastian Kokott | CONET Solutions GmbH
Christian Parschik | Markel Insurance SE
Hanno Pingsmann | Cyber Direkt GmbH
Axel Saß | Red Hat GmbH

Layout
Lea Joisten | Bitkom e.V.

Inhalt

1 Motivation

Aktuelle Bedrohungslage: Herausforderungen und Gründe für schlechten Schutz

Die aktuelle Bedrohungslage im Bereich der Cybersicherheit zeigt einen stetigen Anstieg in Bezug auf die Anzahl und Schwere von Cyberangriffen. Haben 2021 noch 9 Prozent der Unternehmen der Aussage zugestimmt, dass Cyberangriffe ihre wirtschaftliche Existenz bedrohen, waren es 2023 bereits 52 Prozent und damit erstmals mehr als die Hälfte der Unternehmen. Auch der finanzielle Schaden für die betroffenen Unternehmen wächst. 2023 haben Cyberattacken einen Schaden von insgesamt 148,2 Milliarden Euro verursacht.[1] Das Thema Cybersicherheit ist bei allen angekommen. Mit diesem Leitfaden wollen wir deshalb einen Überblick über das Thema und insbesondere über die Option einer Cyberversicherung sowie zu ihren Beiträgen in der Risikominimierung und Unterstützung im Falle einer Cyberattacke geben. Denn hier herrscht noch Nachholbedarf: Was können Cyberversicherungen leisten, warum sind sie als Teil einer holistischen Sicherheitsstrategie wichtig und wie kann man sich den Ernstfall exemplarisch vorstellen? Wir wollen ebenso aufzeigen, welche Mythen es rund um Cyberversicherungen gibt.

Die Bedrohungen sind vielfältig und nehmen zu. Sie stammen sowohl aus externen als auch internen Quellen. Einige Schlüsselfaktoren und Gründe für die verschärfte Bedrohungslage sowie den mangelhaften Schutz in Unternehmen haben wir im Folgenden zusammengefasst.

Externe Bedrohungen: Aus welchen Richtungen sind Unternehmen gefährdet?

Externe Akteure nutzen Schwachstellen in der Cybersicherheit aus, um beispielsweise an sensible Daten zu gelangen oder durch Lösegelderpressung Gewinne zu erzielen. Nationale Regierungen und staatliche Akteure engagieren sich in Cyberoperationen, um politische, wirtschaftliche oder strategische Vorteile zu erlangen, was zu hochentwickelten und gezielten Angriffen führen kann. Unternehmen sehen sich zudem zunehmend Angriffen von Wettbewerbern ausgesetzt. Diese wollen sensible Informationen stehlen oder versuchen, Geschäftsprozesse zu beeinträchtigen. Dies wird mehr und mehr durch die Bereitstellung von Cyberkriminalität als Dienstleistung (Cybercrime-as-a-Service) erleichtert, die es auch weniger versierten Angreifern ermöglicht, Werkzeuge und Dienstleistungen zu nutzen, was die Angriffslandschaft weiter diversifiziert. Erschaffen und ebenfalls genutzt wird Cyberkriminalität von gut organisierten kriminellen Gruppen, die finanzielle Gewinne aus Datendiebstahl, Erpressung und anderen kriminellen Aktivitäten erzielen.

Doch nicht nur Unternehmen als solche werden angegriffen. Auch die Lieferkette von Softwarekomponenten (Software Supply Chain) ist vermehrt Ziel von Cyberangriffen, nicht nur bei großen Konzernen, sondern auch bei kleinen und mittleren Unternehmen (KMU), die oft als weniger gut geschützte Zulieferer für größere Organisationen fungieren. KMU könnten aufgrund begrenzter

1 Bitkom Wirtschaftsschutz- Studie 2023 (↗ Wirtschaftsschutz 2023 (bitkom.org))

Ressourcen und geringerer Sicherheitsvorkehrungen (siehe Interne Bedrohungen) anfälliger für Angriffe sein, was die gesamte Lieferkette gefährdet. Unabhängig von der Größe des Unternehmens ist die Abwehr von **Software-Supply-Chain-Attacken** erheblich schwieriger als bei anderen Angriffen. Hier wird meist eine existierende Vertrauensbeziehung zwischen Zulieferer und Empfänger genutzt, um Komponenten in das Unternehmen einzuschleusen. Die schadhafte Komponente wird dabei in Produkte des Zulieferers eingeschleust, ohne Schaden anzurichten. Durch die Verteilung an die empfangenden Unternehmen innerhalb von zum Beispiel Dateibibliotheken wird es somit vereinfacht, die Schadkomponenten einzuschleusen. Die Erkennung eines derartigen Angriffs ist schwierig, wenn die Komponenten aktuell nicht als Schwachstellen bekannt sind. Hier helfen »normale« Scanner nicht weiter. Es muss das normale Verhalten mit dem Verhalten mit der Schadkomponente verglichen werden. Bei auffälligem Verhalten muss eingegriffen werden. Nach Bekanntwerden der Schwachstelle ist es dann wichtig zu wissen, ob und wenn ja wo die betroffenen Komponenten zu finden sind. Mithilfe einer Software Bill of Materials (SBOM) erfolgt eine Auflistung von verwendeten Klassen, die dann schnell isoliert werden können. Die Verteidigung gegen derartige Angriffe wird einfacher, je früher der Angriff erkannt wird, und je sicherer die Entwicklungsprozesse der Zulieferer abgesichert sind. Offene, nachvollziehbare und gesicherte Entwicklungsprozesse können hier frühzeitig Schaden vermeiden.

Es lassen sich verschiedene Arten von Angriffen differenzieren. Die wichtigsten Typen, und was man unter ihnen versteht, beschreiben wir im Folgenden. **Malware** wird breit gegen Regierungs- oder Unternehmenswebsites eingesetzt, um sensible Informationen zu sammeln oder den Betrieb zu stören. **Ransomware** bleibt eine Hauptbedrohung mit erheblichen finanziellen Kosten. **Phishing** als Form von Social Engineering zielt darauf ab, Menschen dazu zu bringen, sensitive Informationen preiszugeben oder Malware zu installieren. **Man-in-the-Middle-Angriffe** ermöglichen es einem Angreifer, heimlich die Kommunikation zwischen zwei Parteien zu belauschen und möglicherweise zu verändern. **Denial-of-Service-Angriffe** streben an, Maschinen oder Netzwerkressourcen unzugänglich zu machen, indem sie die Dienste eines Hosts stören. Zero-Day-Exploits nutzen unbekannte Software-Schwachstellen aus, die denjenigen, die für ihre Minderung verantwortlich sind, zuvor unbekannt waren. **Zero-Day-Exploits**, Malware und Ransomware haben gemein, dass dafür Komponenten in das Unternehmensnetzwerk eingeschleust werden müssen, um die Wirkung zu erzielen. Diese Angriffsmethoden machen die Abwehr von Bedrohungen zu einer komplexen Herausforderung für Unternehmen.

Interne Bedrohungen: Was bedingt schlechten Schutz, insbesondere für KMUs?

Vor allem die begrenzten Ressourcen von kleinen und mittleren Unternehmen (KMU) stellen eine Herausforderung dar, da sie häufig mit eingeschränkten Budgets, Personalmangel und Zeitdruck konfrontiert sind. Diese Faktoren erschweren die Implementierung umfassender Sicherheitsmaßnahmen, was KMU anfälliger für interne Bedrohungen macht. Während der Coronazeit haben überstürzte Änderungen in der Firmen-IT zu unsystematischen Veränderungen geführt. So wurden potenzielle Sicherheitslücken geschaffen und die Angriffsfläche vergrößert. Ein Mangel an Awareness-Trainings erhöht das Risiko von unvorsichtigem Mitarbeiterverhalten, was wiederum die Angriffsfläche erweitert. Das Fehlen einer umfassenden Sicherheitsstrategie, einschließlich eines Information Security Management Systems (ISMS) und klarer Richtlinien, führt zu einer unstrukturierten und ungeschützten IT-Landschaft. Zudem tragen meist zeitliche und finanzielle

Restriktionen dazu bei, dass Cybersicherheitsmaßnahmen durch die Geschäftsführung oft nicht angemessen priorisiert werden.

Diese internen und externen Bedrohungen führen insgesamt zu einer unübersichtlichen Bedrohungslandschaft. Unbekannte Assets und Datenverluste durch unbedachte SaaS-Nutzung nehmen zu. Die Anzahl der Schwachstellen und Advanced Persistent Threats (APTs) steigt. Die Nutzung von KI als Beschleuniger für Angriffe erschwert die Erkennung und Abwehr von Bedrohungen zusätzlich.

Risiken für Unternehmen: Finanzielle und operationelle Bedrohungen

Wie oben aufgezeigt, sind die Bedrohungen in der Cybersicherheit vielfältig und können erhebliche Auswirkungen auf Unternehmen haben. Die größten Risiken resultieren aus der Komplexität und Dynamik der oben erwähnten Cyberbedrohungen. Unternehmen stehen vor der Herausforderung, sich proaktiv mit präventiven Maßnahmen und einem effektiven Krisenmanagement auseinanderzusetzen, um die finanziellen und operationellen Auswirkungen von Cyberangriffen zu minimieren.

Dabei umfassen die monetären Auswirkungen zum einen die direkten Kosten, die durch den potenziellen Ausfall der Produktion bzw. Wegfall der Dienstleistungen, mit denen das Unternehmen Umsätze erzielt, entstehen. Nach einem Cyberangriff bringt dann die Wiederherstellung der Assets beträchtliche Kosten für forensische Analysen, Datenwiederherstellung und Sicherheitsverbesserungen mit sich. Zudem gibt es die Möglichkeit von finanziellen Sanktionen durch Aufsichtsbehörden und Regierungen aufgrund von Datenschutzverletzungen oder Nichteinhaltung von Sicherheitsvorschriften. Zuletzt stellt die zunehmende Verbreitung von Ransomware eine erhebliche Bedrohung dar, da Unternehmen erpresserischen Forderungen ausgesetzt sind, was zu erheblichen finanziellen Verlusten führen kann.

Neben den monetären sind auch nichtmonetäre Auswirkungen von großer Bedeutung. Cyberangriffe können zu erheblichem Reputationsverlust führen, insbesondere, wenn Angreifer Informationen an Aufsichtsbehörden weitergeben oder im Internet zur Verfügung stellen. Der Wert dieses Reputationsverlusts ist zwar nicht immer monetär quantifizierbar, kann jedoch langfristige Auswirkungen auf Kundenvertrauen und Geschäftsbeziehungen haben. Einen solchen nicht-quantifizierbaren Schaden kann auch eine Cyberversicherung nicht abdecken.

Regulatorische Anforderungen an Cybersicherheit

Verschiedene Gesetze und Vorschriften verpflichten Unternehmen dazu, angemessene Sicherheitsvorkehrungen zu treffen und im Falle von Sicherheitsvorfällen bestimmte Maßnahmen zu ergreifen. Erkennbar ist, dass der Gesetzgeber die Wichtigkeit von Cybersicherheit begriffen hat und versucht, mit den verschiedenen Regeln einen regulatorischen Rahmen zu schaffen. Welche dazugehören und wofür diese da sind, stellen wir im Folgenden vor.

Cyber Security Act:[2]

Mit diesem Europäischen Rechtsakt wird ein Zertifizierungsregelwerk einführt, um einheitliche Vorschriften und Verfahren bei sicherheitskritischen Vorfällen zu schaffen. Darüber hinaus werden die Kompetenzen der europäischen Agentur für Cybersecurity erweitert, um ein derartiges Regelwerk aufzusetzen.[3]

Cyber Resilience Act:[4]

Der CRA gilt für Produkte und Software, die einen digitalen Anteil haben. Diese dürfen nur dann auf den Markt gebracht werden, wenn sie bestimmte grundlegende Cybersicherheitsanforderungen über den Lebenszyklus der Produkte erfüllen, um Kundinnen und Kunden vor Schaden zu schützen. Als Ergänzung zum Cybersecurity Act zielt der CRA darauf ab, digitale Produkte sicherer zu machen, indem horizontale Cybersicherheitsregeln für Wirtschaftsakteure eingeführt werden. So sollen ein kohärenter Rahmen auf europäischer Ebene geschaffen und sich überschneidende oder gar widersprechende Vorschriften abgeschafft werden (New Legislative Framework).[5]

Netz- und Informationssicherheitsrichtlinie 2 (NIS2):

Die NIS2-Richtlinie legt harmonisierte Mindestsicherheitsanforderungen für Betreiber wesentlicher Dienste sowie digitale Diensteanbieter fest. Unternehmen müssen sich bei nationalen Aufsichtsbehörden registrieren, Sicherheitsmaßnahmen implementieren und im Falle von Sicherheitsvorfällen entsprechende Meldungen machen.[6] So sollen die Resilienz und die Fähigkeiten für Gegenmaßnahmen im Bereich der Cybersicherheit und beim Schutz von kritischer Infrastruktur gesteigert werden.[7] In Deutschland wird NIS2 durch das Gesetz zur Umsetzung von EU NIS2 und Stärkung der Cybersicherheit implementiert.[8]

2 ↗ https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
3 Bitkom Stellungnahme zum Cybersecurity Act, Dezember 2017, URL: ↗ 2017-12-20Stellungnahme-Cybersecurity-Act.pdf (bitkom.org)
4 ↗ https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
5 Bitkom Stellungnahme zum CyberResilience Act, Mai 2022, URL: ↗ 20220519_CRA_Bitkom_Positionspapier_de_final.pdf
6 ↗ https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
7 Bitkom Positionspapier zur NIS Directive 2.0, Januar 2022, URL: ↗ 03.01.22_bitkom_nis2_positionspapiertrilog.pdf
8 ↗ https://www.bitkom.org/Bitkom/Publikationen/Nationale-Umsetzung-NIS-2-Richtlinie

Datenschutz-Grundverordnung (DSGVO)[9]:

Die DSGVO legt strenge Anforderungen an den Schutz personenbezogener Daten fest. Unternehmen, die personenbezogene Daten verarbeiten, müssen sicherstellen, dass angemessene technische und organisatorische Maßnahmen ergriffen werden, um Datenschutzverletzungen zu verhindern. Ziel der DSGVO ist es, ein umfassendes, ausgewogenes und einheitliches Regelwerk für den Schutz personenbezogener Daten auf der einen und gleichzeitig einen Rahmen für den Austausch und das Nutzen von Daten für die Entwicklung neuer Innovationen auf der anderen Seite zu schaffen.[10] [11]

Branchenspezifische Vorschriften:

In einigen Branchen existieren spezifische regulatorische Anforderungen, wie zum Beispiel DORA (Digital Operational Resilience Act) für den Finanzsektor. Diese schreiben vor, dass Unternehmen angemessene Maßnahmen zur Gewährleistung der Cybersicherheit ergreifen müssen, um ihre Verfügbarkeit sicherzustellen.[12]

Die in Kürze vorgestellten Regelwerke sind lediglich ein Auszug der bestehenden Regelungen. An dieser Stelle erheben wir keinen Anspruch auf Vollständigkeit, sondern geben lediglich einen Überblick.

9 ↗ https://www.bmwk.de/Redaktion/DE/Artikel/Digitale-Welt/europaeische-datenschutzgrundverordnung.html
10 Bitkom Positionspapier: GDPR Review – Recommendations for the EUS's Data Protection Framework, Mai 2020, URL: ↗ 20200520-bitkom-position-paper-gdpr-review.pdf
11 Bitkom Publikationen aus dem Bereich Datenschutz sind hier zu finden ↗ Mediathek | Bitkom e. V.
12 Bitkom Positionspapier: DORA – Regulation on Digital Operational Resilience for the Financial Sector, Mai 2021, URL: ↗ 210521_bitkom-position-paper_dora.pdf

2 Anwendungsfall

Im Folgenden wird ein möglicher Anwendungsfall beschrieben, der selbst für große IT-Unternehmen eine Herausforderung darstellt.

Szenario

Unternehmen A ist im produzierenden Gewerbe tätig. Im Rahmen einer Digitalisierungsoffensive wurde ein Onlineportal eingeführt, um Lieferanten und Endkunden ebenfalls die Möglichkeit zu geben, Produkte des Unternehmens zu kaufen und Komponenten zu liefern. Die neue Ausrichtung hat dazu geführt, dass zahlreiche neue Softwareprodukte eingeführt und andere auf den neuesten Stand gebracht worden sind. In den Entwicklungsprozess wurde ein Scanner eingeführt, der verwendete Softwarekomponenten und darin enthaltene Bibliotheken auf veraltete Klassen oder Komponenten mit bekannten Schwachstellen prüft. Die Mitarbeitenden werden jedes Jahr geschult, um das Verhalten bei dem Umgang mit E-Mails und daran angehängte Anhänge etc. zu sensibilisieren.

Vor dem Vorfall

Unternehmen A hat sich dafür entschieden, eine Cyberversicherung abzuschließen. Was heißt das nun konkret? Üblicherweise setzt die Cyberversicherung Vorbereitungsmaßnahmen des Unternehmens voraus, die auf die Prävention und (frühzeitige) Detektion von Vorfällen abzielen. Eine Cyberversicherung entbindet das Unternehmen also nicht von der Verantwortung, sicherheitssteigernde Maßnahmen im Unternehmen umzusetzen. Vielmehr wird durch die Cyberversicherung aufgezeigt, was die wichtigsten Sicherheitsmaßnahmen im Unternehmenskontext sind und mindestens berücksichtigt werden sollten – auch um überhaupt eine Cyberversicherung abschließen zu können. Der Vorteil ist, dass durch diesen proaktiven Prozess die unternehmensspezifischen Handlungsbedarfe offengelegt werden.

Beispielsweise wird die Notwendigkeit identifiziert, das genutzte Authentifizierungsverfahren zu verbessern oder die Backup-Strategien zu überprüfen. Darüber hinaus wird versucht, dem Unternehmen einen tieferen Einblick in die Geschehnisse der IT-Infrastruktur zu geben. Dies umfasst z. B. das zentralisierte Vorfiltern, Sammeln und Auswerten wichtiger Log-Dateien aus Systemen und Netzwerkkomponenten sowie das Aufstellen von Intrusion Detection und Prevention-Systemen. Dabei ist nicht nur entscheidend, einen Angriff zu identifizieren, sondern auch, dessen Zeitpunkt bestimmen zu können, um bei der Suche nach einem sauberen Backup das Richtige zu wählen.

Vorfallbehandlung

Im Rahmen des regelmäßigen Updates von Komponenten wird am 13. März eine neue Version der serverbasierten Produktionssteuerungssoftware des Softwarezulieferers Y installiert. Die Software und deren Komponenten bzw. Klassen werden durch den Scanner untersucht. Es wird aber keine Unregelmäßigkeit festgestellt. Die neuen Komponenten werden produktiv geschaltet.

Am 1. Mai wird ein kaskadierender Ausfall der Produktionslandschaft festgestellt. Auf den betroffenen Servern taucht eine Ransomware-Meldung auf, die zur Zahlung eines Lösegelds aufruft.

Das sofort einberufene Krisenteam bespricht das weitere Vorgehen. Schritt 1 ist die Abarbeitung der Notfallcheckliste des BSI.[13] Parallel werden die Ansprechpartner bei der Cyberversicherung alarmiert, die dann in kurzer Zeit ein Incident Response Team einschaltet. Gemeinsam werden die vom BSI aufgezeigten 3 Phasen der Reaktion auf einen derartigen Vorfall bearbeitet (siehe S. 8 des BSI-Papiers):

- Analyse
  - Es müssen die betroffenen Systeme ermittelt und diese dann vorerst von dem Netzwerk getrennt werden, um eine weitere Ausbreitung zu verhindern.
  - Danach muss ermittelt werden, um welchen Befall es sich handelt. Ist er bekannt?
- Übergangsbetrieb
  - Klärung der Fragen, welche Systeme betroffen sind: Welche sind notwendig für eine Aufrechterhaltung des weiteren Betriebs?
  - Entscheidung, wie weiter vorgegangen werden soll: Rumpfbetrieb, oder komplette Abschaltung, um sicherzustellen, dass es zu keiner weiteren Ausbreitung kommt.
- Bereinigung
  - Definition der weiteren Schritte:
    - Feststellung der schadhaften Komponenten, des Infektionszeitpunktes und des Zugangswegs.
    - Abhängig von den anderen Lösungsoptionen und der Schwere des Befalls muss entschieden werden, ob eine Zahlung in Betracht kommt.
    - Definition von erweiterten Sicherheitsprozessen und -verfahren.

Unter Mithilfe des Incident Response Teams, das durch die Cyberversicherung bereitgestellt wurde, wird mit der Analyse begonnen. Es stellt sich heraus, dass es sich um keine bekannte Ransomware-Attacke handelt. Deswegen konnten die Standardwerkzeuge und Virenscanner den Befall nicht frühzeitig erkennen. Nach Ermittlung des ersten Auftretens des Befalls innerhalb eines Serversystems im Produktionssteuerungssystem werden dieser Server und seine Offline-Backups einer intensiveren Untersuchung unterzogen.

Zur weiteren Evaluation der Lösungsoptionen wird ermittelt, wann der Befall stattgefunden hat. Die regelmäßig durchgeführten Backups des befallenen Systems werden in isolierten Servern analysiert und es wird festgestellt, dass eine Klasse der Produktionssteuerungssoftware des Anbieters Y der ursprüngliche Ausgangspunkt des Befalls war. Folgende Entscheidungsoptionen stellen sich:

13 ↗ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.pdf?__blob=publicationFile&v=3

- Systeme komplett herunterfahren und Verbindung der IT-Infrastruktur zum Internet trennen. Konsequenz ist die vorübergehende Nicht-Erreichbarkeit der Unternehmenswebsite und den damit verbundenen Shops bzw. Kundeninteraktionen. Dadurch kann verhindert werden, dass die Angreifer weitere Befehle an die eingeschleuste Schadsoftware senden. Die Verschlüsselung der Infrastruktur kann im besten Falle verhindert oder zumindest eingegrenzt werden.
- Systeme weiterlaufen lassen, wohlwissend, dass die Angreifer aktiv werden könnten. Die Notwendigkeit der Aufrechterhaltung des Geschäftsbetriebs wird höher priorisiert. Trennung der möglichen Zugangswege der Angreifer und Weiterbestehen der Shopsysteme und ihrer Erreichbarkeit aus dem Internet. Gleichzeitig wird versucht, die Systeme während des Betriebs zu bereinigen.

Es wird entschieden, die Systeme herunterzufahren, um eine weitere Ausbreitung und den Befall anderer Systeme und vor allem wichtiger Daten zu verhindern. Das führt dazu, dass es keinen Übergangsbetrieb gibt, und sich auf die Bereinigung konzentriert wird.

Im 3. Schritt wird die Bereinigung organisiert. Hierbei werden alle Systeme noch einmal genau untersucht und es wird geprüft, ob eine Infektion stattgefunden hat. Wenn ja, wird versucht, die Daten so zu sichern, dass ein Neuaufsetzen der Software möglich wird. Schritt für Schritt wird so die Gesamtinfrastruktur wieder aufgebaut. Hierbei zahlt es sich aus, dass die Strategie des Neuaufbaus anstatt des Updates umgesetzt wurde. Für jede Server-Komponente gibt es Skripte, die ein System von Null aufbauen.

Nach dem Vorfall

Nach der Meldung des Befalls bei dem Zulieferer wurde ermittelt, dass der schadhafte Code im Rahmen des Entwicklungsprozesses eingefügt worden ist und somit Signierung etc. nicht zu einem Erkennen des Problems geführt haben. Das Unternehmen versichert glaubhaft, dass die Prozesse angepasst werden und die sofort zur Verfügung gestellte neue Version der Software frei von schadhaften Komponenten ist.

Nach erfolgreicher Wiederherstellung des Regelbetriebs und Abschluss der Analysehandlungen fertigt der Incident Response-Dienstleister einen Bericht über den Sachverhalt und die Untersuchungsergebnisse an. Der Bericht beinhaltet hilfreiche Maßnahmenvorschläge für die Verbesserung der Sicherheitslage des Unternehmens, darunter bspw.:

- Verfeinerung der Backupstrategien und Verlängerung des Vorhaltens der Backups, um z. B. die Spanne zum Nachvollziehen eines unerkannten Befalls zu vergrößern.
- Weitergehende Umsetzung der Installations-Automatisierung, um jede Komponente gezielt durch Automatisierungsskripte von Grund auf neu aufzusetzen.
- Einführung eines Monitorings von der normalen Ausführung von Server-Prozessen und der Abweichung von dieser Norm, um frühzeitig unbekannte Schadsoftware zu

entdecken. Es wird zum Beispiel darauf geachtet, dass bestimmte Serverprozesse keine neuen Prozesse starten, die es bisher nicht bei der Ausführung gab.
- Überprüfung der Sicherheitsvorkehrungen der Zulieferer und setzen von Standards.
  - Darstellung der Entwicklungsprozesse, um Chancen eines Befalls zu minimieren.
  - Bereitstellung von Software Bills of Material (SBOM) der Komponenten der Zulieferer zum einfacheren Auffinden von Komponenten bei bekanntem Befall um Software Supply Chain Attacken vorzubeugen.

Vorteile der Vorfallbehandlung mittels der Dienstleister einer Cyberversicherung

Cyberversicherungen halten in der Regel mehrere Dienstleister vor, die im Fall eines Cyberangriffs mit Sofortmaßnahmen reagieren können und rund um die Uhr erreichbar sind (Incident Response). Das Risiko für die Auswahl eines (ungeeigneten) Dienstleisters ist somit nicht mehr in der Entscheidungssphäre der Unternehmen. Die Dienstleister verfügen über Spezialisten-Erfahrung aus vergleichbaren Fällen und durch die fortwährende Beschäftigung mit dem Themenkomplex. Für die Beweismittelsicherung und -analyse sind Spezial-Hard- und Software vorhanden, über die IT-Abteilungen, handwerkliche Betriebe, Kleinstunternehmen oder Arztpraxen üblicherweise nicht verfügen. Die Expertinnen und Experten sind zudem vertraut mit den einschlägigen Standards und Vorgehensweisen in den relevanten Kompetenzbereichen:

- IT-Sicherheit
- Forensik
- Krisenmanagement
- Kommunikation nach innen und außen

Das Unternehmen profitiert somit unmittelbar von der durch die Versicherung fachkundig getroffene Vorauswahl der Dienstleister sowie von deren aufgebautem Vertrauensverhältnis, das im Zuge verschiedener Extremsituationen bei früheren Einsätzen gewachsen ist.

Die Dienstleister sind zudem unterstützend tätig. Beispielsweise bei der Beratung über regulatorische Anforderungen, der initialen Beurteilung des Stands der Cybersicherheit eines Versicherungsnehmers oder bei Plausibilitätschecks von Questionnaire-Antworten der Versicherungsnehmer.

Im Vorfeld des Vertragsabschlusses einer Cyberversicherung ist es essenziell, dass das Unternehmen die vereinbarten Leistungsbausteine und die Leistungstiefe genau prüft und versteht. Vertraglich sind die Parteien angehalten, die Verfügbarkeiten der Dienstleister, die Meldewege, sowie die Kosten festzulegen.

3 Einführung Cyberversicherung: Wieso und was ist drin?

Heutzutage gibt es kaum ein Berufsbild, das nicht einen Computer oder ein mit dem Internet verbundenes technisches Hilfsmittel nutzt. Je größer die Abhängigkeit von der Technik ist, desto gravierender können die Folgen eines Hackerangriffs sein. Gefahren reichen von Daten-Diebstahl über Schadsoftware-Attacken bis hin zur digitalen Sabotage. Die Corona-Pandemie hat zusätzlich verdeutlicht, wie anfällig Unternehmen für Cyber-Angriffe sind. Hinzu kommt, dass die Komplexität der Software und IT-Lösungen in Unternehmen seit Jahren konstant ansteigt. Die Marktfähigkeit Künstlicher Intelligenz (KI) wird sich hierbei noch als zusätzlicher Treiber langfristig auswirken. Diese absehbare Entwicklung führt unweigerlich zu mehr Schwachstellen in der Unternehmens-IT. Nicht nur im Bereich der Hard- und Software, sondern auch im Umgang der eigenen Mitarbeitenden mit den eigenen oder Daten Dritter. Cyber-Attacken geschehen besonders abseits der großen Unternehmen nach dem Zufallsprinzip und haben zunächst kein spezielles Unternehmen im Visier. Daher kann jedes Unternehmen, welches Schwachstellen offenbart, zum Ziel eines Angriffs werden. Viele Unternehmen stellen sich deshalb die Frage, ob Sie eine Cyberversicherung benötigen.

Im ersten Teil dieses Leitfadens haben wir dargelegt, welche Gefahren durch Cyberattacken drohen, welche Regularien beim Ergreifen von Schutzmaßnahmen eine Rolle spielen und wie ein Ernstfall ablaufen kann. Doch warum ist eine Cyberversicherung sinnvoll, welche deckungsauslösenden Ereignisse werden üblicherweise von einer Cyberversicherung umfasst, und welche Leistungen sollte eine Cyberversicherung umfassen, um Unternehmen vor, während und nach einem Cybervorfall umfassend unterstützen zu können?

Warum eine Cyberversicherung sinnvoll ist

Viele Unternehmen wiegen sich in falscher Sicherheit, wenn das Audit positiv verlaufen ist oder weil eine eigene IT-Security vorhanden ist. Doch zahlreiche Firmen haben für den Ernstfall, wenn ein Cyberangriff erfolgt ist, keinen Notfallplan.

- Wie muss ich mich verhalten, wenn ich eine Kompromittierung festgestellt habe?
- Wie stelle ich fest, was in meinen Systemen vorgefallen ist?
- Wer ist mein erster Ansprechpartner im Notfall?

Das sind nur drei Fragen, die Unternehmen beantworten können sollten, die aber gerade kleine Betriebe nur selten beantworten können. Anders sieht es bei Unternehmen aus, die eine Cyberversicherung haben. Versicherungsnehmer einer solchen Police können auf ein ganzes Netzwerk des Versicherers zugreifen. So bieten in der Regel alle Versicherer eine 24h-Hotline an, bei der dem Unternehmen sofort geholfen wird. Es werden per Telefon erste Maßnahmen ergriffen, um eine Ausweitung der Cyberattacke zu verhindern. Die Dienstleister des Versicherers kümmern sich auch um die weiteren Abläufe, je nach Art und Umfang des Schadens werden umgehend weitere Dienstleister involviert.

Zum Beispiel:

- ein IT-Forensik-Team, das ermittelt, welche Systeme letztlich befallen worden sind und durch welche Schwachstellen der Angreifer in das IT-System gelangt ist,
- einen auf die Datenrettung und -wiederherstellung spezialisierten Dienstleister,
- Rechtsanwälte, die bei der Verletzung von Datenschutzrechten unterstützen,
- PR-Berater, die versuchen, den Schaden am Ruf des Unternehmens so klein wie möglich zu halten.

Was bietet eine Cyberversicherung neben dem Zugriff auf spezialisierte Dienstleister und welche Aspekte sollte man als Unternehmen in die Überlegungen einbeziehen, ob ein Abschluss sinnvoll ist?

- **Präventive Maßnahmen:** Unternehmen und deren Mitarbeitende können mit einer Cyberversicherung auf bestimmte Schulungsmöglichkeiten zugreifen. So werden z. B. Online-Trainings für Cybersicherheit und Datenschutz angeboten. Auch kann das Unternehmen auf laufende Phishing-Tests, einen Online-Konten-Check, E-Mail-Scanner und viele weitere Dienstleistungen zurückgreifen.
- **Risiko-Transfer:** Eine Cyberversicherung ermöglicht Unternehmen, einen Teil des finanziellen Risikos im Falle von Cyberangriffen auf den Versicherer zu übertragen. Dieser Risiko-Transfer ist entscheidend, um potenziell verheerende finanzielle Auswirkungen auf das eigene Budget zu minimieren.
- **Reaktiv und proaktiv:** Die Cyberversicherung bietet sowohl reaktive als auch proaktive Vorteile. Im reaktiven Sinne greift die Versicherung bei einem Sicherheitsvorfall, um die finanziellen Folgen zu mildern. Proaktiv wird die Prämie der Cyberversicherung oft durch die Implementierung von Security-Maßnahmen beeinflusst. Je höher ein Mindestmaß an Security-Hygiene eingehalten wird, desto niedriger kann die Risiko-Prämie ausfallen.
- **»ROI« – Weitreichende Schäden verhindern:** Der Return on Investment (ROI) einer Cyberversicherung liegt nicht nur in der finanziellen Entschädigung nach einem Angriff, sondern auch in der Verhinderung weitreichender Schäden. Durch den Einsatz von 24/7-Security-Analysten kann eine Cyberversicherung frühzeitig auf Sicherheitsvorfälle reagieren, wodurch potenziell größere Schäden vermieden werden.

Insgesamt bietet die Cyberversicherung somit nicht nur einen finanziellen Schutzmechanismus, sondern fördert auch proaktive Sicherheitsmaßnahmen. Unternehmen, die ein höheres Maß an Sicherheitsvorkehrungen implementieren, können nicht nur ihre Risiko-Prämien minimieren, sondern auch die Effizienz der Versicherung in der Verhinderung und Begrenzung von Cyberangriffen maximieren.

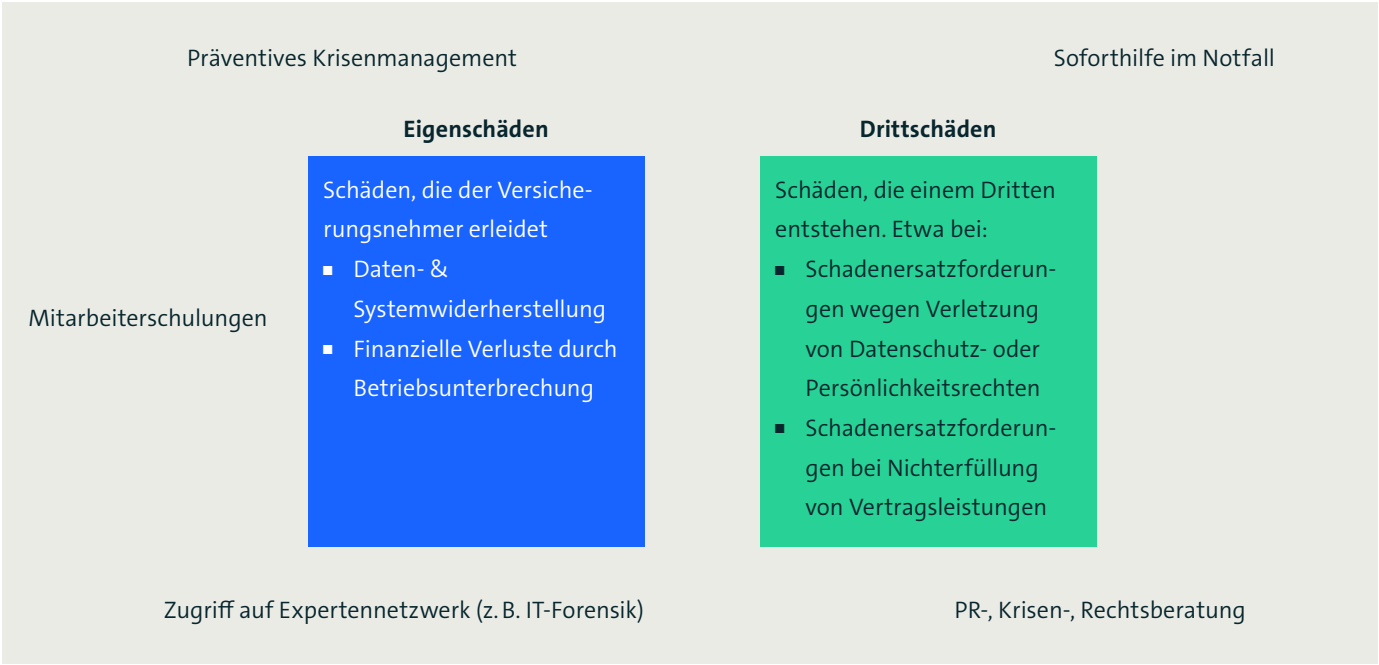
Deckungsauslösende Ereignisse

Eine Cyberversicherung soll Unternehmen gegen die Folgen von Netzwerksicherheitsverletzungen, Datenrechtsverletzungen und Erpressung absichern. Bei einer Netzwerksicherheitsverletzung oder auch Informationssicherheitsverletzung handelt es sich gemäß gängiger Definition um jede Form von unzulässigen Zugriffen oder Nutzungen

des IT-Systems eines versicherten Unternehmens. Umfasst sind insbesondere Hacker-Angriffe, Täuschung von Mitarbeitenden beispielsweise über Phishing sowie Schadprogramme, die sich im Netzwerk eines Unternehmens ausbreiten. Eine Erweiterung des Deckungsumfangs umfasst bei gängigen Versicherungsprodukten zudem Bedien- und Programmierfehler, welche auch Schäden durch unsachgemäße Bedienung des IT-Systems durch eigene Mitarbeitende absichern soll, sowie Cyber-Erpressung, welche Deckungsschutz bei Androhung einer Informationssicherheitsverletzung bietet.

Leistungsumfang einer Cyberversicherung: Was beinhaltet eine Cyberversicherung?

Wie bei allen Versicherungsprodukten gibt es auch für die Cyberversicherung eine Empfehlung des GDV (Gesamtverband der Versicherer), welche Mindestleistungen in einem Bedingungswerk des Versicherers enthalten sein sollten.[14] Sie sind speziell für Unternehmen mit einem Umsatz bis 50 Millionen Euro und einer Größe bis 250 Mitarbeitenden zugeschnitten und wurden im Frühjahr 2024 angepasst. Informationssicherheitsverletzungen, die während des Fernzugriffs erfolgen (mobiles Arbeiten), sind in den aktualisierten Musterbedingungen ebenfalls abgedeckt.[15] Um sich einen Überblick über die wesentlichen Elemente einer Cyberversicherung zu verschaffen, kann das 3-Säulen-Modell hilfreich sein. Hierbei klassifizieren die drei Säulen die wesentlichen Deckungsinhalte in drei Kategorien: Übergreifenden Service-Leistungen sowie die beiden Schadenkategorien Eigenschäden und Drittschäden.



14 ↗ Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung (gdv.de)
15 ↗ Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung (gdv.de)

1. Eigenschäden

Eigenschäden sind Schäden, die der Versicherungsnehmer selbst oder sein Vermögen erleidet. Im Bereich der Cyberversicherung sind Eigenschäden zum Beispiel:

- Wirtschaftliche Schäden durch Betriebsunterbrechungen, die durch einen Cyberangriff oder eine technische Störung verursacht werden. Wenn z. B. die Maschinen stillstehen und nicht mehr produziert werden kann, oder wenn der Online-Shop auf einmal nicht mehr erreichbar ist. In solchen Situationen springt die Versicherung ein und zahlt einen vereinbarten Tagessatz oder kompensiert den entstandenen Ertragsausfall, bis alles wieder funktioniert. Die Kompensation von Ertragsausfällen ist die gängige Variante.
- Kosten für die Datenwiederherstellung, die anfallen, wenn die IT-Infrastruktur durch einen Cyberangriff oder eine technische Störung beeinträchtigt oder zerstört wird. Sind beispielsweise die Daten nach einem Hackerangriff vollständig gelöscht worden, ist die Wiederherstellung sehr kosten- und zeitintensiv.
- Kosten für die Systemwiederherstellung, die anfallen, wenn die IT-Infrastruktur durch einen Cyberangriff oder eine technische Störung beeinträchtigt oder zerstört wird.

2. Drittschäden

Drittschäden sind Schäden, die einem Dritten entstehen, wenn das Unternehmen durch einen Cyberangriff oder eine technische Störung seine vertraglichen oder gesetzlichen Pflichten verletzt. Im Bereich der Cyberversicherung sind Drittschäden zum Beispiel:

- Schadensersatzforderungen, die durch die Verletzung von Datenschutzrechten oder Persönlichkeitsrechten von Kunden, Geschäftspartnern oder anderen Dritten entstehen. Beispielsweise, wenn Hacker sensible Daten wie Kreditkartennummern, Passwörter oder Gesundheitsdaten stehlen und missbrauchen. In der Regel machen die Betroffenen nach solch einem Vorfall Schadensersatzansprüche gegen das Unternehmen geltend.
- Schadensersatzforderungen, die durch Nichterfüllung von Vertragsleistungen oder die Verletzung von Schutzrechten des Unternehmens oder eines Dritten entstehen. Beispielsweise, wenn ein Online-Shop lahmgelegt wird und dringend bestellte Ware nicht ausgeliefert werden kann.

3. Service-Leistungen

Service-Leistungen sind Leistungen, die eine Cyberversicherung zusätzlich zu den reinen Schadensersatzleistungen anbietet. Sie sollen dem versicherten Unternehmen helfen, die Folgen eines Cyberangriffs zu bewältigen und zu begrenzen. Zu den Service-Leistungen können zum Beispiel gehören:

- IT-Forensik-Experten, die zur Analyse, Beweissicherung und Schadensbegrenzung herangezogen werden.
- Anwältinnen und Anwälte für IT- und Datenschutzrecht, die über die rechtlichen Konsequenzen eines Cyberangriffs informieren (Informationspflicht).
- PR-Experten, die bei der Wiederherstellung des guten Rufs des versicherten Unternehmens helfen und eine Kommunikationsstrategie entwickeln.

Abgrenzung zu anderen Versicherungssparten

Die Cyberversicherung deckt eine wesentliche Deckungslücke bei Unternehmen jeder Größe. Dennoch gibt es für dieses – noch recht junge Versicherungsprodukt – immer wieder Fragen der Abgrenzung vor allem im Vergleich zur Vertrauensschadenversicherung und einer IT-Haftpflichtversicherung.

Eine Vertrauensschadenversicherung sichert die Folgen einer vorsätzlich unerlaubten Handlung durch eine Vertrauensperson oder einen Dritten ab. Damit ergeben sich zwar Überschneidungen mit der Cyberversicherung, insbesondere bei Spionage und Veruntreuung, welche auch durch die Cyber-Police im digitalen Raum gedeckt sein kann. Jedoch ist ein Zugriff auf ein Expertennetzwerk im Falle eines Schadens ein typischer Baustein der Cyberversicherung und in der Vertrauensschadenversicherung nicht enthalten.

Insbesondere Unternehmen im Bereich der Informationstechnik besitzen überwiegend eine IT-Haftpflicht. Auch hier zeigen sich Überschneidungen: Ansprüche Dritter durch Verlust von Daten oder Schäden aufgrund von versehentlich übermittelten Schadprogrammen können im Deckungsumfang beider Produkte enthalten sein. Jedoch beinhaltet die IT-Haftpflicht keine Kostenposition für Eigenschäden, Soforthilfe im Notfall und Betriebsunterbrechung durch einen Cyber-Angriff. Die IT-Haftpflicht stellt allerdings nicht rein auf eine Netzwerksicherheitsverletzung ab, sondern schützt auch vor Ansprüchen aufgrund selbstverschuldeter Fehler.

Festzuhalten ist, dass sich zwar Überschneidungen mit anderen Versicherungsprodukten ergeben, sich die Cyberversicherung jedoch durch weiten Deckungsumfang, ihre Vorrangigkeit vor anderen Produkten sowie die Expertenunterstützung im Notfall deutlich von anderen Produkten abhebt und in den meisten Fällen eine sinnvolle Ergänzung zu bereits bestehenden Versicherungen darstellt.

Die (5) größten Irrtümer: Was sind die häufigsten Einwände gegen eine Cyberversicherung?

Irrtum	Aufklärung
Wir sind ein kleines Unternehmen – Hacker werden sich nicht für uns interessieren.	Die überwiegende Anzahl von Cyber-Attacken erfolgt nicht gezielt auf bestimmte Unternehmen, sondern wird über E-Mails an eine breite Anzahl von Empfängern (z. B. durch Phishing-E-Mails) gestreut.
Ich habe ein Backup meiner Daten. Wenn ich von einer Verschlüsselungssoftware betroffen bin, spiele ich die Daten einfach wieder ein.	Hacker wissen, dass die angegriffenen Unternehmen über ein Daten-Backup verfügen. Die meisten Schadsoftware-Varianten sind daher so programmiert, dass Sie die Wiedereinstellung von Backups erschweren bzw. das Backup ebenfalls verschlüsselt wird. Letzteres tritt insbesondere in jenen Fällen ein, wo das Backup nicht als Offline-Datensicherung bzw. physisch getrennt von den IT-Systemen des Unternehmens angelegt ist. Darüber hinaus gehen die Angreifer mittlerweile dazu über, die betroffenen Daten im Darknet zu veröffentlichen, wenn die Unternehmen der Lösegeldforderung nicht nachkommen.
Bei uns gibt es keine geheimen Daten, mit denen ein Hacker etwas anfangen kann. Cyberkriminelle werden uns daher nicht angreifen.	Das Hauptziel von organisierter Cyberkriminalität ist die Erpressung der betroffenen Unternehmen. Mittels sog. Ransomware-Angriffe werden dabei die auf den IT-Systemen befindlichen Kundendaten verschlüsselt und unbrauchbar gemacht. Für Entschlüsselung und Rückgabe der Daten wird Lösegeld in unterschiedlicher Höhe verlangt. Auf diesem Wege ist praktisch jedes Unternehmen erpressbar und für Cyberkriminelle ein geeignetes Ziel.
Wir haben sehr viel in unsere IT-Sicherheit investiert und Hacker haben keine Chance mehr, bei uns einzudringen.	Cyber-Angriffe werden oft erst dadurch ermöglicht, dass ein Mensch im entscheidenden Moment eine falsche Entscheidung trifft. Es gibt grundsätzlich keine hundertprozentige Sicherheit gegen Hackerangriffe und eine Cyberversicherung dient der Absicherung dieses Restrisikos.
Ich habe meine Daten an einen externen Dienstleister ausgelagert, der die Verantwortung für die Datensicherheit trägt.	Die rechtliche Verantwortung für Datensicherheit kann nicht vollständig ausgelagert werden. Verantwortliche Stelle im Sinne der DSGVO ist das Unternehmen, welches die Daten erhebt und z. B. den Vertrag mit den Kunden hat.

4 Einordnung Cyberversicherungen – Voraussetzungen, Ausschlüsse und erste Schritte

Damit ein Unternehmen vom Schutz einer Cyberversicherung profitieren kann, muss eine IT ein Mindestmaß an Sicherheit aufweisen. Diese »Mindestanforderungen« finden wir auch in vielen anderen Versicherungen, wie z. B. in der Hausrats- oder Inhaltsversicherung, wo als Voraussetzung für einen Versicherungsabschluss ein bestimmtes Schloss in der Eingangstür vorhanden sein muss.

Betriebe müssen zum Beispiel einen Virenschutz und eine Firewall installiert haben, oder es muss eine regelmäßige Datensicherung vorgenommen werden. Je nach Größe des Unternehmens und Umfang des Versicherungsschutzes variieren die Anforderungen von Versicherer zu Versicherer. Gleichzeitig gibt es eine Reihe von Ausschlüssen sowie Unterschiede in der Prämienkalkulation (je nach Branche des Unternehmens).

Mindestanforderung für den Abschluss einer Cyberversicherung

Die dynamische Risikoentwicklung im Bereich der Cyber-Angriffe hat insbesondere in den letzten Jahren bei Versicherern zu erhöhten Anforderungen und Mindestkriterien geführt, die Unternehmen für den Abschluss einer Deckung erfüllen müssen. Ziel ist es, eine gute Cyber-Hygiene und Resilienz zu fördern, welche maßgeblichen Einfluss auf die Eintrittswahrscheinlichkeit und Schadenhöhe von Cyber-Schäden haben kann.

Dabei unterscheiden sich die Mindestanforderungen je nach Umsatz und Branche des Unternehmens. Im Folgenden soll daher auf die wesentlichen technischen und organisatorischen Anforderungen eingegangen werden, die ein Unternehmen erfüllen muss. Aufgrund des jungen Alters der Sparte hat sich noch kein einheitlicher Standard etabliert, welcher herangezogen werden kann. Daher sind die genannten Anforderungen lediglich als grobe Richtlinien zu verstehen und nicht abschließend.

Kleine und mittelständische Unternehmen

- Virenschutz mit automatischer Aktualisierung
- Firewalls an allen Übergängen in das Internet
- Regelmäßige Ransomware-sichere Backups (z. B. Offline-Backups auf externen Festplatten oder unveränderliche Online-Backups)
- Regelmäßiger Patch-Management-Prozess sowie sicherer Betrieb bzw. das Ablösen von Altsystemen
- Abgestuftes Rechtekonzept mit administrativen Zugängen ausschließlich für IT-Verantwortliche

- Absicherung von Fernzugriffen und Admin-Zugängen durch den Einsatz von Mehrfaktorauthentifizierung
- Passwort-Richtlinien mit definierten Anforderungen an Passwortlänge und Passwortstärke
- Datenschutzbeauftragter (intern oder extern) sowie verbindliche Richtlinien zum Datenschutz
- Regelmäßige Sensibilisierung und Schulungen von Mitarbeitenden für IT-Sicherheit

Industrieunternehmen zusätzlich

- Weitergehende Sicherung der Backups über Anwendung einer 3-2-1-Backup-Strategie und durch regelmäßige Rücksicherungstests
- Maßnahmen zur Angriffserkennung und Einsatz von »Endpoint Detection and Response Systems« (SIEM, EDR / XDR)
- Implementierung und regelmäßige Überprüfung eines Business Continuity Plans inkl. Richtlinien zum Umgang mit Informationssicherheitsverletzungen
- Durchsetzung von IT-Mindestanforderungen auch bei Dienstleistern
- Einsatz regelmäßiger Schwachstellentests und / oder Penetrationstests
- Regelungen zur Nutzung privater Geräte
- Physischer Schutz der IT-Systeme vor unbefugten Zugriffen
- Einsatz eines dezidierten IT-Sicherheitsbeauftragten
- Netzwerk-Segmentierung, z. B. zwischen Standorten oder zwischen Büro-IT und Produktions-IT
- Verschlüsselung von Endgeräten

Prämienkalkulation

Die Versicherungsprämien der einzelnen Anbieter für vergleichbare Risiken unterscheiden sich teilweise sehr deutlich. Hierbei ist auch zu berücksichtigen, dass die Grundlagen für die Prämienkalkulation nicht einheitlich sind.

Standardisierte Prämien

Für mittelständische Unternehmen geben die Versicherer vorberechnete Prämien heraus, welche primär auf dem Netto-Jahresumsatz, der Branche des Kunden, der gewünschten Versicherungssumme und dem Selbstbehalt basieren. Diese Tarife sind über Vergleichsrechner für Cyberversicherungen im Internet zugänglich, welche eine schnelle Orientierung hinsichtlich der zu erwartenden Jahresprämie ermöglichen. Die Umsatzgrenzen für eine standardisierte Prämienkalkulation können sehr unterschiedlich sein. Zahlreiche Versicherer bieten diese für Unternehmen mit bis zu 10 Mio. Euro Jahresumsatz an, andere bis 25 Mio. Euro. Es werden meistens Versicherungssummen von bis zu 2 Mio. Euro angeboten. Zum Teil gehen Standardverträge auch bis 3 Mio. Euro Versicherungssumme. Der Antragsprozess ist in diesen Fällen ebenfalls standardisiert und es müssen nur wenige Risikofragen beantwortet werden, um die Cyberversicherung abzuschließen.

Individuelle Prämienkalkulation

Oberhalb dieser Umsatzgrenzen können die Versicherer eine Prämie nur dann kalkulieren, wenn der Antragstellende einen Fragebogen ausfüllt. Die darin abgefragten Risikoinformationen sind umfangreicher und detaillierter. Ein Unternehmen, welches sich aufgrund der Größe außerhalb der o. g. Umsatzbänder befindet, muss daher gegenüber dem Versicherer mehr Informationen zu IT-Systemen, IT-Organisation und IT-Sicherheit angeben. Der Einsatz von Fragebögen ist ebenso für höhere Versicherungssummen bzw. Unternehmen aus Hochrisikobereichen.

Optionale Bausteine

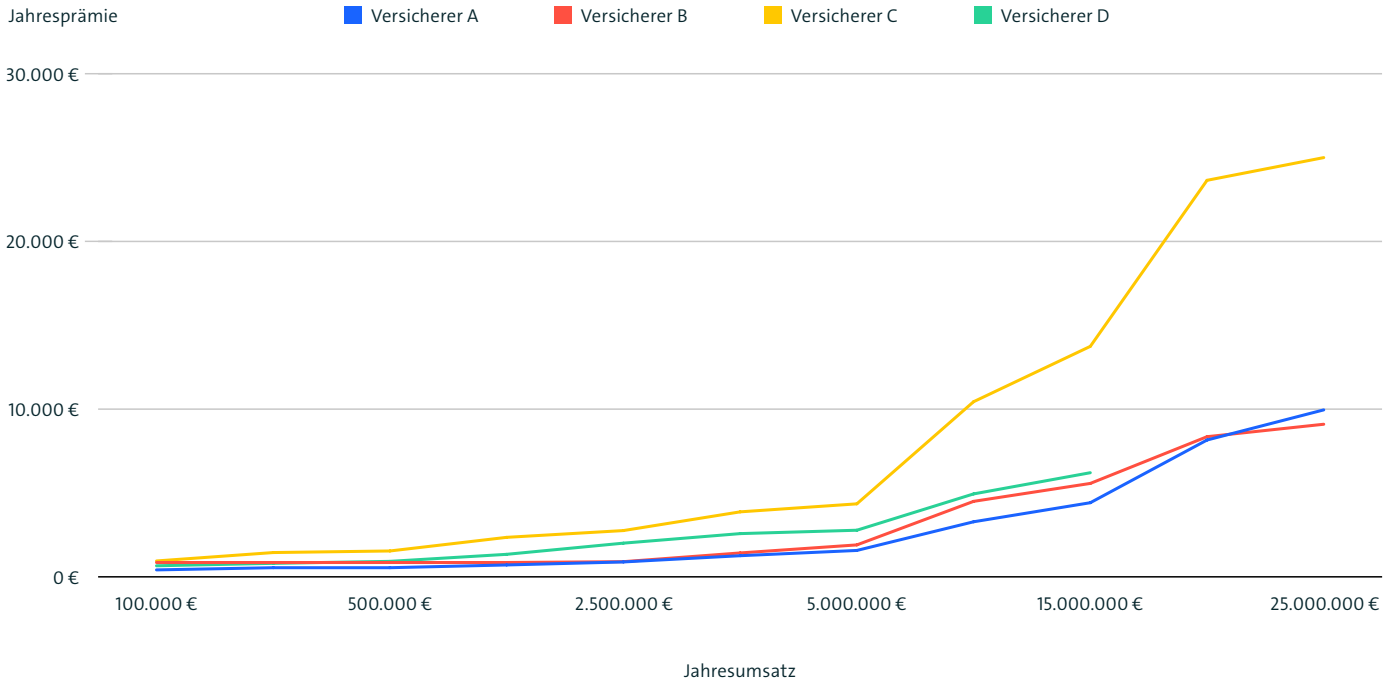
Einige Cyberversicherungen sind modular gestaltet, sodass bestimmte Leistungen an- und abwählbar sind. Die optionalen Deckungselemente werden in diesen Tarifen separat bepreist und auf die Prämie aufgeschlagen. Hier empfiehlt es sich, einen genauen Blick auf die zur Auswahl stehenden Tarife zu werfen. Teilweise sind die Leistungen, welche bei einem Versicherer gegen einen Aufpreis hinzugewählt werden können, in anderen Tarifen bereits im Standard enthalten. Grundsätzlich ermöglichen modulare Tarife dem versicherten Unternehmen jedoch, die Cyberversicherung auf die eigenen Bedürfnisse anzupassen. Gängige optionale Bausteine sind z. B. der Einschluss von Betriebsunterbrechung (inkl. einer Erweiterung auf den Ausfall von Cloud-Dienstleistern), Lösegeld oder Cyber-Betrug (Fake-President-Schäden).

Sublimite

Nur in wenigen Tarifen steht die Versicherungssumme für alle Leistungsbereiche der Cyberversicherung gleichmäßig zur Verfügung, da die Versicherer regelmäßig mit sog. Sublimiten für vorher definierte Teilrisiken arbeiten. Dies kann z. B. dazu führen, dass eine Police mit 1 Mio. Euro Versicherungssumme für Cyber-Betrug, Lösegeld oder Ersatz von Hardware nur 100.000 Euro leistet. Die Sublimite müssen in jedem Angebot sowie der Versicherungspolice transparent ausgewiesen werden. Durch diese monetäre Begrenzung der Leistungen im Schadenfall wird die Vergleichbarkeit von Angeboten zusätzlich erschwert und es empfiehlt sich die Beratung durch einen Versicherungsmakler einzuholen.

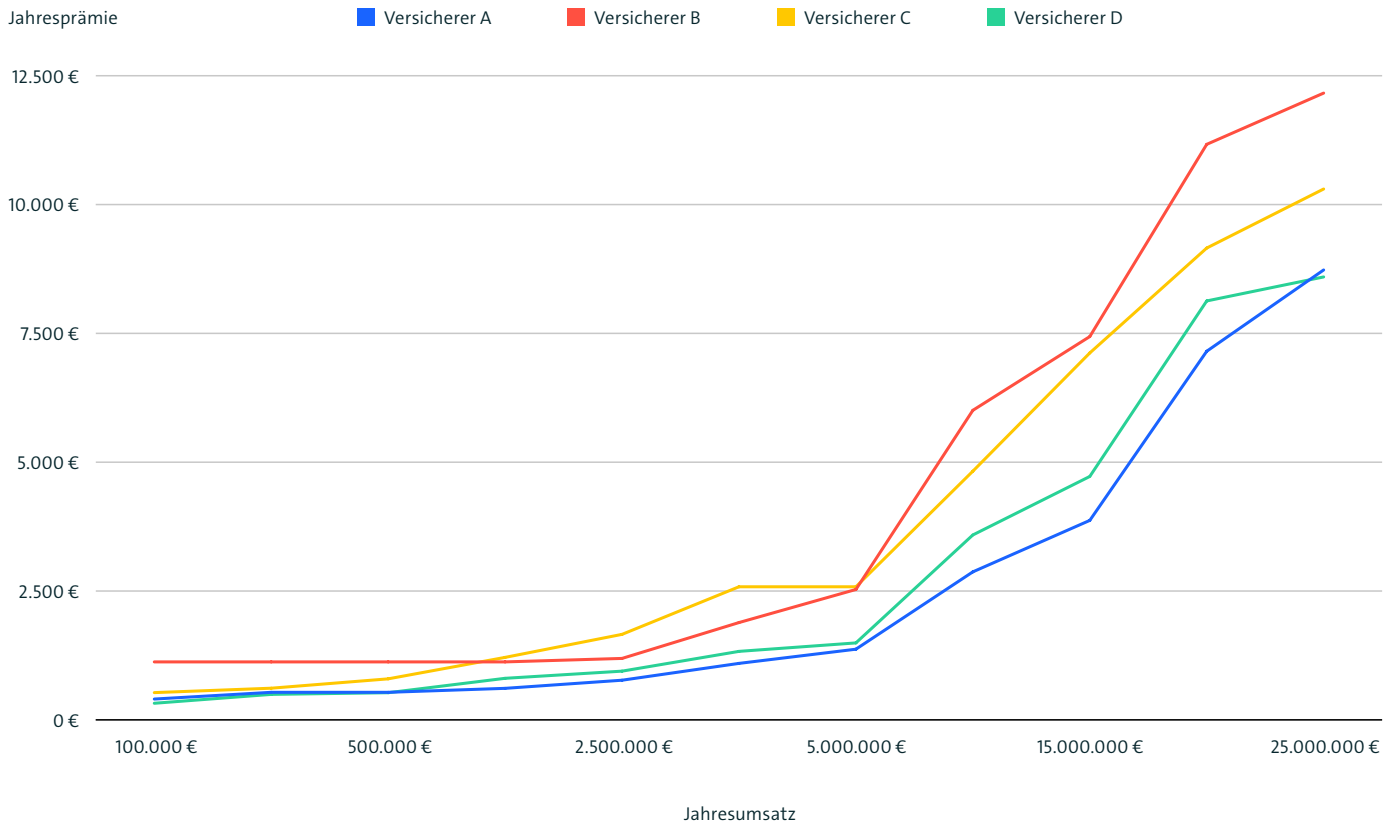
Die Heterogenität des Marktes führt insgesamt zu erheblichen Preisdifferenzen. Ein Vergleich mehrerer Angebote ist für Unternehmen aller Größenordnungen sinnvoll. Exemplarisch wurden die Preise (Y-Achse) standardisierter Tarife für unterschiedliche Umsatzgrößen (X-Achse) in unterschiedlichen Branchen in den nachfolgenden Grafiken veranschaulicht.

Benchmark IT-Unternehmen, SB 2.500 €



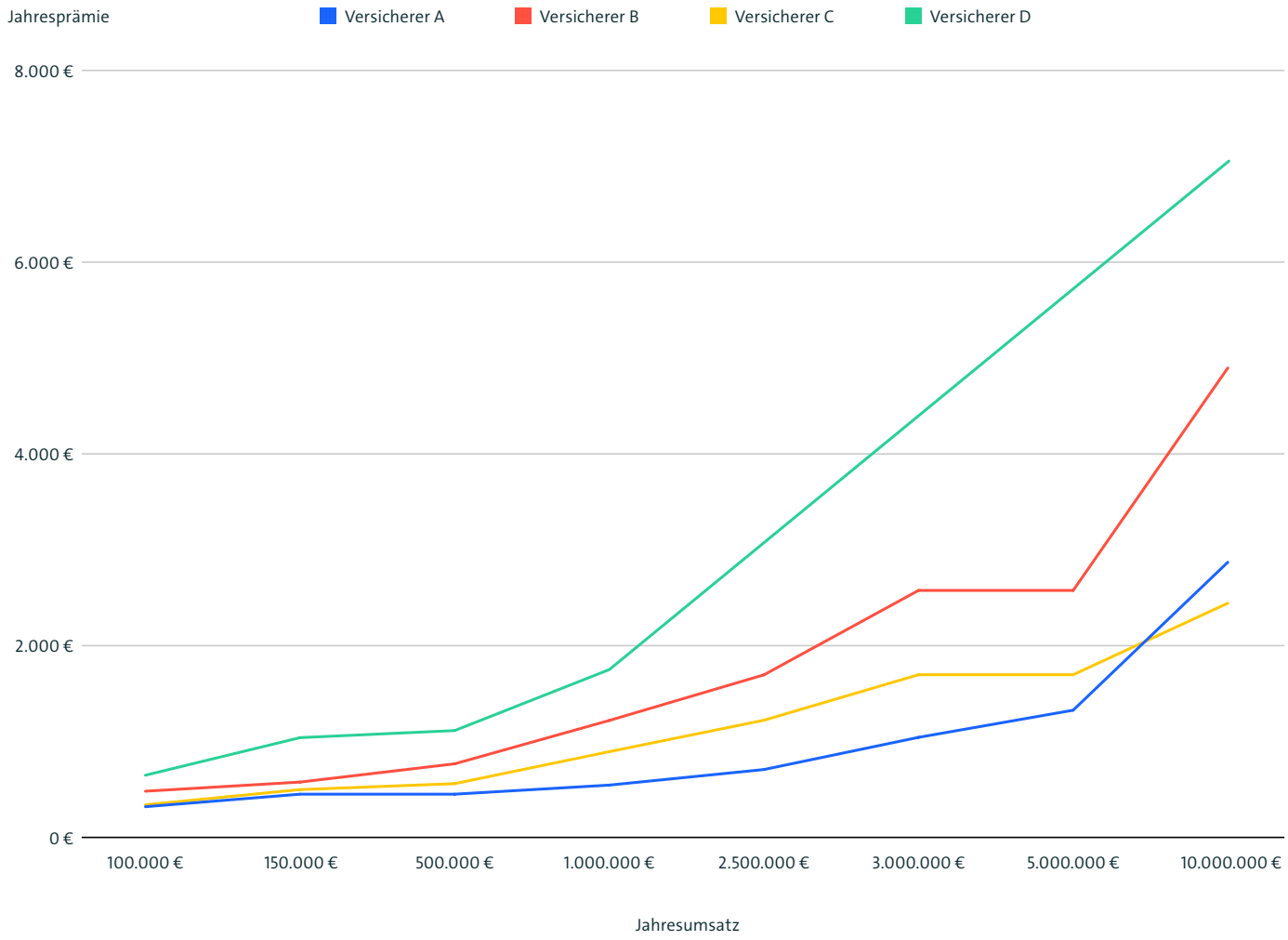
Quelle: CyberDirekt

Benchmark Produzierendes Gewerbe, SB 2.500 €



Quelle: CyberDirekt

Benchmark Kammerberufe, SB 1.000 €



Quelle: CyberDirekt

Ausschlüsse

Ausschlüsse in der Cyberversicherungen dienen dazu, den Umfang der Deckung klar zu definieren. Wie nahezu jedes Versicherungsprodukt kommt auch die Cyberversicherung nicht ohne den Ausschluss bestimmter Risikobereiche aus. Die Versicherungsgesellschaften versuchen sich auf diesem Wege vor schwerwiegenden Risiken zu schützen, welche die Kapazität der Versicherungswirtschaft zum Tragen von Risiken überschreiten. Durch die Definition von Ausschlüssen wird der Umfang der Deckung klarer abgegrenzt. Dies hilft sowohl dem Versicherungsunternehmen als auch dem Versicherungsnehmenden zu verstehen, welche Arten von Schäden abgedeckt sind und welche nicht. Bestimmte Schäden durch Cyberangriffe können extrem kostspielig sein. Durch den Ausschluss dieser Risiken kann das Versicherungsunternehmen die Prämien verlässlicher kalkulieren und die finanzielle Stabilität des Versicherungskollektivs sicherstellen. Die nachfolgende Auflistung umfasst gängige Ausschlüsse in der Cyberversicherung:

- Vorsatz
- Krieg & politische Gefahren
- Infrastruktur
- Hoheitliche Eingriffe
- Terror
- Finanzmarkttransaktionen
- Glücksspiel
- Produktrückruf
- Rechtswidrige Datenerfassung
- Produkthaftung
- Vertragsstrafen
- Vertragserfüllung
- Kernenergie

In der Neuauflage der Musterbedingungen sind Störungen bei externen Dienstleistern wie Cloud-Anbietern, Rechenzentren oder Software-as-a-Service-Lösungen größtenteils nicht mehr ausgeschlossen.

Im Folgenden werfen wir einen genaueren Blick auf die Ausschlüsse für Vorsatz, Krieg & politische Gefahren und Infrastruktur.

Der Ausschluss von Vorsatz ist in nahezu allen Versicherungen enthalten, weil Versicherungsschutz darauf abzielt, unvorhergesehene Risiken und Schäden abzudecken, nicht jedoch absichtliches Fehlverhalten oder gar kriminelle Handlungen der Versicherten. Der standardmäßige Vorsatzausschluss wird in der Cyberversicherung jedoch meist aufgeweicht, um auch vorsätzlichen Handlungen von Mitarbeiterinnen und Mitarbeitern des Versicherten einzuschließen. Konkret geht es um das Risiko des sog. »Innentäters«, welcher absichtlich IT-Systeme oder Daten des Versicherten schädigt.

Seit Ende 2021 entstand in der Versicherungsbranche eine Diskussion um den Ausschluss von kriegsbedingten & politischen Gefahren und die Notwendigkeit, eine Klarstellung der Definition von Krieg aufzunehmen, die auch Krieg unter Einsatz digitaler Mittel umfasst. Hierbei soll der Leistungsausschluss zugunsten des Versicherers auch um einen möglichen »Cyberkrieg« erweitert werden, d. h. staatlich gesteuerte Cyber-Angriffe, welche auch zu einem Ausfall oder einer Beeinträchtigung von kritischen Infrastrukturen eines anderen Staates führen, sollen explizit von der Deckung ausgeschlossen werden. Der Gesamtverband der Deutschen Versicherungswirtschaft hat mit seiner kürzlichen Neuauflage der Cyber-Musterbedingungen und Aufnahme eines erweiterten Kriegsausschlusses einen Schritt in diese Richtung vorgenommen. So wurde beispielsweise klargestellt, dass ein Krieg ebenso mit digitalen Mitteln geführt werden kann.[16] Die – in vielen Fällen nicht ganz einfache – Beweisführung, ob ein staatlicher Akteur die Attacke zu verantworten hatte, obliegt hierbei dem Versicherer. Aktuell ist die Aufnahme des Kriegsausschlusses bei einer Mehrheit der Versicherer mit Cyberpolicen im KMU-Segment noch nicht erfolgt.

16 ↗ Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung (gdv.de)

Ebenso wie ein Krieg ist der Angriff bzw. Ausfall von Infrastrukturen (insb. Internet und Telekommunikation) durch einen Cyber-Angriff für den Versicherer ein Kumulrisiko, welches gleichzeitig bei mehreren oder vielen versicherten Unternehmen Schäden auslösen würde (Klumpenrisiko). Einige Cyber-Versicherer haben die Bedingungen insoweit gestaltet, dass jedoch Infrastruktur, welche vom versicherten Unternehmen selbst betrieben wird, weiterhin in die Deckung eingeschlossen ist.

Umgang mit Vorschäden

Alle Versicherer fordern bei Beantragung einer Cyberversicherung Auskünfte über eventuelle Vorschäden und bekannte Umstände, welche vom Gegenstand des Versicherungsschutzes erfasst sein könnten. Hierbei ist ein vorangegangener Vorfall kein Hindernis für die grundsätzliche Versicherbarkeit des Unternehmens. Vielmehr fordern die Risikoträger in diesem Fall mit dem Antrag auch detaillierte Informationen zum Vorschaden, wie z. B. die Schadenshöhe, Vorgehensweise zur Beseitigung oder den im Anschluss getroffenen Maßnahmen zur Sicherheitsverbesserung an. Ohne die Bereitschaft des Unternehmens, diese Details offenzulegen, kann i. d. R. kein Versicherungsschutz angeboten werden.

Obliegenheiten im Rahmen von Cyberversicherungen

Wie eingangs erwähnt, sind die Risikoerfassung sowie die Definition von Mindestanforderungen in der Cyberversicherung im Vergleich zu anderen Sparten umfangreich und dienen dem Zweck, nur versicherbare und kalkulierbare Risiken in das Portfolio eines Risikoträgers aufzunehmen.

Neben der Bestimmung von Mindestanforderung, die ein Unternehmen vor Beginn des Deckungsschutzes erfüllen muss, arbeiten Versicherungsunternehmen zunehmend auch mit der Definition von technischen Obliegenheiten, die während der Vertragslaufzeit zu jedem Zeitpunkt eingehalten werden müssen. Obliegenheiten dienen dem Zweck, Versicherungsnehmer von einem grob fahrlässigen Verhalten abzuhalten, welches möglicherweise einen Schadenfall auslösen könnte. Für den Umfang der technischen Obliegenheiten hat sich noch kein einheitlicher Marktstandard etabliert. In den meisten Fällen bilden die technischen Obliegenheiten einen Teil der oben genannten Mindestanforderungen ab. Dabei ist darauf zu achten, dass die Obliegenheiten möglichst transparent und abschließend formuliert sind. Interpretationsspielraum und Unschärfen sollten vermieden werden.

Sofern der Versicherungsnehmer die technischen Obliegenheiten nicht erfüllt und dies ursächlich für bzw. in einem kausalen Zusammenhang zu einem Schadenfall steht, liegt eine sogenannte Obliegenheitsverletzung vor. Der Versicherer ist dann berechtigt – je nach Schwere der Obliegenheitsverletzung – Leistungen im Schadensfall zu kürzen oder abzulehnen.

Der Umfang der technischen Obliegenheiten ebenso wie die deren Transparenz sollte bei Vertragsabschluss und während der Vertragslaufzeit Beachtung finden.

Zwar gibt es auch Anbieter, welche vollständig auf die Definition von technischen Obliegenheiten verzichten; dieser Verzicht bedeutet aber nicht zwangsläufig, dass ein Versicherungsnehmer keine Anforderungen an die IT-Sicherheit zu erfüllen hat. Auch die Angaben, die ein Unternehmen im Rahmen der Risikoerfassung gemacht hat, sollten im Verlauf der Vertragslaufzeit nicht nachteilig verändert werden. Auch hier können sich negative Veränderungen der IT-Sicherheit deckungsschädlich auf den Versicherungsschutz auswirken.

Erste Schritte zur Absicherung

Auch wenn Unternehmen der Ansicht sind, sie seien ausreichend gegen Cyberangriffe geschützt, macht ein Gespräch mit Fachberaterinnen und Fachberatern zum Thema Cyberversicherung Sinn. Denn Cyberversicherungen sind komplex, ebenso wie die individuelle Risikosituation von Unternehmen. Aus diesen Gründen ist der passgenaue Abschluss einer Cyberversicherung für die meisten Unternehmen ohne umfassende Beratung nicht sinnvoll bzw. gar nicht möglich. Diese Beratung können spezialisierte Versicherungsvermittler übernehmen, die verschiedene Lösungen und optionale Deckungsinhalte kennen und dem individuellen Risikoappetit eines Unternehmens entsprechend beraten können.

Je nach Unternehmensgröße haben Versicherer unterschiedliche Anforderungen. Während bei kleineren Unternehmen meist nur wenige Risikofragen gestellt werden, ist bei großen Unternehmen ein Cyber-Audit durch den Versicherer oder einen Dienstleister notwendig. In der Regel sind die Termine und Audit bei bekundetem Interesse kostenlos. Als Vorbereitung sollte sich ein Unternehmen bereits Gedanken über die individuelle Risikosituation machen. Dazu gehört neben der Identifikation von Unternehmensrisiken auch die Einschätzung der eigenen Abhängigkeit von IT-Systemen und das Zusammentragen von Informationen zum Umfang des IT-Systems und der IT-Sicherheit. Als Richtlinie können die obenstehenden Mindestanforderungen herangezogen werden.

Nach Bestimmung des Absicherungsbedarfs und Festlegen einer geeigneten Versicherungssumme kann eine Anfrage an Versicherer gestellt werden. In diesem Prozess werden Versicherer Informationen zu Art der Tätigkeit, zum Umfang des IT-Systems, zur IT-Sicherheit sowie zum Umgang mit sensiblen Daten und Zahlungsdaten abfragen, um eine präzise Risikoeinschätzung des Unternehmens vornehmen zu können. Je nach Umsatz und Branche erfolgt diese Abfrage über eine standardisierte Prämienkalkulation z. B. im Rahmen von Antragsmodellen, über die – nach positiver Beantwortung von Antragsfragen – sofortiger Deckungsschutz gewährt wird. Bei höheren Umsätzen oder bestimmten Branchen wird die Risikoerfassung über Fragebögen und Risikodialoge mit dem Versicherer erstellt. Sofern auch in diesem Prozess alle Mindestkriterien für den Abschluss einer Cyberversicherung erfüllt werden, erhält das Unternehmen ein individuell zugeschnittenes Angebot. Im Vorfeld des Vertragsabschlusses einer Cyberversicherung ist es essenziell, dass das Unternehmen die vereinbarten Leistungsbausteine und die Leistungstiefe genau prüft und versteht. Vertraglich sind die Parteien angehalten, die Verfügbarkeiten der Dienstleister, die Meldewege sowie die Kosten festzulegen.

Ein großer Vorteil für das Unternehmen ist, dass es sich während der Vorbereitung und Prüfung mit seiner eigenen IT-Infrastruktur auseinandersetzen muss. Bestehende Software und Hardware wird erfasst und dokumentiert. Das Unternehmen bekommt Einsicht in die Mindestanforderungen, die ein Versicherer erwartet und kann dies mit seiner bestehenden IT-Infrastruktur abgleichen. Viele Versicherer stellen auch einen kostenlosen Report zur Verfügung, der aufzeigt, welche Schwachstellen im Unternehmen vorhanden sind.

Mittlerweile gibt es auch einige Vergleichsportale im Netz, die einen umfangreichen Vergleich im Bereich Cyberversicherungen anbieten. Hier können sich in der Regel Unternehmen bis 25 Millionen Euro Umsatz einen guten Überblick über die Preise und Leistungen der Anbieter verschaffen. In Einzelfällen gibt es auch Vergleiche für bis zu 50 Millionen Euro Umsatz. Darüber hinaus erhält der Interessent auch eine Übersicht über die Sicherheitsanforderung, die von Versicherer zu Versicherer durchaus abweichen.

5 Schlusswort

In diesem Leitfaden haben wir uns der aktuellen Risiko- und Bedrohungslandschaft im Cyberraum sowie der Möglichkeit für Unternehmen gewidmet, sich gegen Angriffe abzusichern. Insbesondere aufgrund des stetig wachsenden Risikos ist es essenziell für Unternehmen jeglicher Größe, eine holistische Sicherheitsstruktur aufzubauen. Regulatorische Vorgaben an Cybersicherheit oder gute Schulung der Mitarbeiterinnen und Mitarbeiter können nicht ausschließen, dass ein Angriff zum Erfolg führt. Um das bestehende Risiko zu minimieren, kann eine Cyberversicherung ein elementarer Baustein sein. Das gilt nicht nur für die bloße Absicherung finanzieller Schäden, sondern insbesondere auch für die Prävention und für die Schadensbehebung im Anschluss an einen erfolgten Angriff.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bitkom e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

bitkom.org