Cyber-Risk-Insurance

Einstiegsübersicht

Autor: Thomas Werth

Version: 1.0

Inhaltsverzeichnis

Allianz für Cybersicherheit

“Die Allianz für Cyber-Sicherheit ist eine Initiative des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die im Jahr 2012 in Zusammenarbeit mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) gegründet wurde.

Ziele und Angebote der Allianz
Als Zusammenschluss aller wichtigen Akteure im Bereich der Cyber-Sicherheit in Deutschland hat die Allianz das Ziel, die Cyber-Sicherheit in Deutschland zu erhöhen und die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. Zur gemeinsamen Förderung der Cyber-Sicherheit arbeitet das BSI dabei im Rahmen der Allianz intensiv mit Partnern und Multiplikatoren zusammen.
Zur Erreichung dieser Ziele verfolgt die Allianz die folgenden Maßnahmen:

- Erstellung und Pflege eines aktuellen Lagebilds
- Bereitstellung von Hintergrundinformationen und Lösungshinweisen
- Intensivierung des Erfahrungsaustausches zum Thema Cyber-Sicherheit
- Ausbau von IT-Sicherheitskompetenz in Organisationen mit intensivem IT-Einsatz

Die Allianz für Cyber-Sicherheit baut hierfür eine umfangreiche Wissensbasis auf und initiiert und betreibt Erfahrungs- und Expertenkreise zur Cyber-Sicherheit. Ergänzt werden diese Angebote durch weitere Beiträge der Partner z.B. in Form von Schulungen, zusätzlichen Informationsveranstaltungen oder der kostenlosen Bereitstellung von Sicherheitsprodukten.”
(Quelle: ACS-Homepage https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Ueber_uns/Einfuehrung/einfuehrung.html)

Als Partner der Allianz für Cyber-Sicherheit veröffentlicht die Werth IT dieses Dokument.

Was ist eine Cyber-Risk-Versicherung?

Die Cyber-Risk-Versicherung ist eine weitere Versicherungssparte für Unternehmen. Diese spezialisierte Versicherungssparte ist noch recht jung und besitzt noch keinen einheitlichen Namen. So wird sie auch Data Protect, Data-Risk, Cyber-Versicherung, Cyber-Deckung, Datenschutz-Versicherung oder Hacker-Versicherung genannt.

Sie besteht aus einer (Dritt-)Vermögensschadenhaftpflicht- und einer Eigenschadenversicherung. Versichert sind damit Vermögensschäden (Schäden finanzieller Natur) gegenüber Dritten, beispielsweise aufgrund von Datenrechtsverletzungen.
Zudem wird der Eigenschaden abgedeckt. Dabei wird nicht nur der direkte Schaden beglichen, sondern auch die Kosten, die für eine vollständige Wiederherstellung benötigt werden oder durch Leistungsausfall entstehen.
Die Höhe der Zahlungen richtet sich dabei nach dem entstandenen Schaden oder nach einer festgelegten Deckungssumme, je nachdem welcher Betrag niedriger ist.

Somit stellt die Cyber-Risk-Versicherung eine Absicherungsmöglichkeit für Unternehmen gegen Schäden dar, die generell gesehen aus mit IT-Sicherheit zusammenhängenden Risiken entstehen. Die neue Sparte Cyber-Risk ist insbesondere deswegen besonders sinnvoll, da die Betriebshaftpflichtversicherungen eher geringe Vermögensschäden und nicht immer IT-Schäden abdecken. Diese Deckungslücken können mit dieser Zusatzversicherung gezielt geschlossen werden.

Überschneidung mit anderen Versicherungssparten

Zur besseren Übersicht erfolgt an dieser Stelle eine Darstellung von potentiellen Überschneidungen mit anderen Versicherungssparten. Anhand dieser Übersicht lassen sich Doppel-Deckungen und Anpassungspotential erkennen, um die eigenen Beiträge zu minimieren.

Tabelle 1: Eigenschäden

Schaden	Sach / TV	Haftpflicht	Epressung / K&R	Vertrauens-schaden	Cyber-Risk
Wiederherstellung Daten / Programme	bedingt	✗	✗	✗	✓
Benachrichtigungskosten	✗	✗	✗	✗	✓
Betriebsunterbrechung	bedingt	✗	✗	✗	✓
Kosten IT-Forensik	✗	✗	✗	✓	✓
Wiederherstellung nach Hackerangriff	bedingt	✗	✗	✓	✓
Kosten Sicherheitsberater	✗	✗	✗	bedingt	✓
Kosten PR-Berater	✗	✗	✗	bedingt	✓
Diebstahl Vermögenswerte in elektronischer Form	✗	✗	✗	bedingt	bedingt
Erpressung Bedrohung	✗	✗	✓	✗	✓

Tabelle 2: Drittschäden

Anspruch / Schaden	Sach / TV	Haftpflicht	Epressung / K&R	Vertrauens-schaden	Cyber-Risk
Datenverlust	✗	✓	✗	✗	✓
Datenschutz	✗	✓	✗	✗	✓
Forderung PaymentCard-Industrie	✗	✗	✗	✗	✓
Persönlichkeitsrechts-verletzung	✗	bedingt	✗	✗	✓
Verletzung der Rechte an geistigen Eigentums	✗	bedingt	✗	✗	bedingt

Damit wird deutlich, dass zur Vorbereitung des Abschlusses einer Cyber-Risk-Versicherung auch die Kontrolle der bestehenden Versicherungen und deren Leistungsumfang gehört.

Um letztlich beurteilen zu können welche Deckungslücken die Cyber-Risk-Versicherung schließen muss oder an welchen Stellen eine bessere Deckung durch diese geboten werden kann.

Grundstruktur einer Cyber-Risk-Versicherung

Damit die Cyber-Risk-Versicherung die in den Tabellen aufgeführte Abdeckung erreichen kann, hat sie in der Regel immer diese Grundstruktur:

Haftpflicht/ Schadensersatzansprüche Dritter:

- Rechtschutzfunktion / Anspruchsabwehr
- Befriedigung berechtigter Ansprüche

Eigenschäden

- Wiederherstellungskosten Daten/Programme/Netzwerk/IT
- Ertragsausfall durch Umsatzverluste
- Kosten provisorischer Betrieb oder Beschleunigte Wiederherstellung
- Optional: Betriebsunterbrechung
- Optional: Cyber-Diebstahl (Außentäter)
- Optional: Erpressung

Kostenpositionen

- Kosten zur Information der Betroffenen nach Datenschutzvorfall
- Kosten der IT-Forensik
- Kosten der Rechtsberatung
- Kosten des PR-Beraters
- Kosten Forderungen der PaymentCard-Industrie

Wann ist eine Cyber-Risk-Versicherung sinnvoll?

Cyber-Delikte steigen kontinuierlich an. Die e-crime Studie der KPMG [1] belegt dies anschaulich. So sind 2015 bereits 40% aller befragten Unternehmen Opfer von e-crime geworden. Im Vergleich zur Vorstudie von 2013 ist das ein Zuwachs von 50%. Ebenso sehen 89% e-crime als sehr hohes Risiko und 95% der Unternehmen haben große Schwierigkeiten Vorfälle aufgrund deren Komplexität aufzuarbeiten und zu verfolgen.

Es gilt somit für Unternehmen auf das berühmte Katz- und Mausspiel zwischen Angreifer und Verteidiger vorbereitet zu sein. Eine Cyber-Risk-Versicherung kann hier Schutz vor finanziellen Folgen und Unterstützung in Vorfallbewältigung liefern.

Zu erkennen ob derartige Unterstützung benötigt wird, kann durch Beantwortung der folgenden Fragen [4] erkannt werden:

- Wie verhält sich das Unternehmen, wenn es Opfer eines Cyberangriffs wird? Werden die richtigen Maßnahmen getroffen?
- Wie reagiert das Unternehmen bei einem Erpressungsversuch mittels Veröffentlichung von sensiblen Daten?
- Wie setzt sich der Krisenstab bei Datenrechtsverletzungen zusammen und welche Pressemeldungen werden abgegeben?
- Wie lange kann das Unternehmen einen Ausfall seiner geschäftskritischen IT-Systeme verkraften? Wie ist der Notfallplan bei unerwarteten Betriebsunterbrechungen?

Jedes Unternehmen, das wichtige Geschäftsprozesse IT- oder Web-gesteuert nutzt oder sensible Daten (vertraulich, personenbezogen) seiner Mitarbeiter, Kunden, Partner digital speichert oder verarbeitet, muss zufriedenstellende Antworten auf diese Fragen finden und abwägen ob eine Cyber-Risk-Versicherung sinnvoll ist.

Insbesondere da bei einem akuten Sicherheitsvorfall eine schnelle Reaktion entscheidend ist, unterstützt eine Cyber-Risk-Versicherung konkret durch:

Professionelle Hilfe im Krisenfall
- Minderung des Reputationsschadens
- Kostenreduzierung
- Schnellere Krisenbewältigung

Reduzierung des finanziellen Risikos
- Betriebsunterbrechung
- Mehrkosten
- Sachverständigenkosten
- Aufwendungen bei Datenschutzverletzungen
- Vermögensverlust durch Betrug

Haftpflichtansprüche
- Abwehr unberechtigter Ansprüche
- Ausgleich des Schadens
- Strafrechtsschutz

Schadensbeispiel

Ein einfaches Schaubeispiel hilft sicherlich die Sinnhaftigkeit einer Cyber-Risk-Versicherung am praktischen Beispiel zu veranschaulichen. Das folgende Schadensbeispiel stammt von der Webseite der Firma Hiscox und zeigt einen Vorfall in einem mittelständischen Unternehmen, wie man ihn immer wieder in den Medien liest:

Ein mittelständisches Unternehmen der Onlinebranche ist aufgrund eines Hackerangriffes Opfer von Datenmissbrauch geworden. Über mehrere Wochen konnten sich Hacker rechtswidrigen Zugang zu dem eigentlich streng gesicherten online-basierten Abrechnungssystem für Bezahlkarten verschaffen (Payment Processing Tool). Während dieser Zeit konnten die Hacker über 100.000 Kundendaten kopieren und unrechtmäßig nutzen. Das Schadenausmaß ist immens, es entsteht neben dem sehr hohen finanziellen Schaden auch ein nicht zu beziffernder Imageschaden.

Der Schaden: Forensische Dienstleistungen 15.000 €, Rechtsberatung und Rechtsbeistand 35.000 €, gesetzliche Informationspflichten 25.000 €, Media- und PR-Arbeiten 19.500 €, geltend gemachter Vermögensschaden der Payment Card Industry 495.000 €.Gesamtkosten 589.500 €

Quelle: Hiscox [4]

Man sieht an diesem Beispiel gut welche Kosten in einem solchen Vorfall auf ein Unternehmen zukommen und welche Gesamtkosten entstehen können. Dabei bleibt der entstandene Imageschaden jedoch unberücksichtigt. Ebenso wird anhand der Kosten auch klar, dass die Bewältigung und das Management eines solchen Vorfalls in der Regel externe Expertise erfordern.

Welche Leistungen werden benötigt?

Damit der bisher beschriebene Schutz durch die Cyber-Risk-Versicherung erlangt werden kann, ist bei der Versicherungspolice auf die Deckung der folgenden Punkte zu achten.

Zur Absicherung von Eigenschäden, müssen folgende Punkte versichert sein:

- Kosten IT-Forensik
- Kosten Rechtsberatung und Rechtsbeistand

- Informations- und Benachrichtigungskosten (Dateninhaber, Meldeverfahren, Call-Center)
- Kosten Kreditüberwachungsdienstleistungen (Opferschutz bei gestohlenen Kreditkartendaten)
- Kosten Krisenmanagement und Beratung
- Kosten PR-Beratung und Maßnahmen
- Betriebsunterbrechungsschäden
- Vertragsstrafen wie PaymentCard-Industrie
- Erstattung von Lösegeld bei Erpressung
- Wiederherstellungskosten (IT-Reparatur wie Webserver, Netzwerk, Programme, Daten)
- Kosten Sicherheitsanalysen wie Audits und Penetrationstests sowie Kosten für Sicherheitsverbesserungen
- Schadenminderungs- / Mehrkosten wie erhöhte Personalkosten oder Aushilfshardware.

Zusätzlich müssen folgende Vermögensschäden von Dritten abgesichert sein:

- Datenschutzrechtliche Schäden
- Schadenersatzforderungen von Geschädigten und berechtigten Dritten

Weiterhin gilt es den jeweiligen Umfang richtig zu bestimmen. So muss der Versicherungsschutz weltweit gelten, da Cyber-Angriffe keine „Grenzen“ kennen. Auch sollten Sublimite (Begrenzungen der Versicherungsleistung) gar nicht oder nur gezielt wie bei Vertragsstrafen der PaymentCard-Industrie existieren und angemessen sein. Ebenso sollte die Dauer einer Betriebsunterbrechung für mindestens 6 Monate abgesichert sein. Zusätzlich ist zu klären welche Rechtsverletzungen mitversichert sind. Ideal ist hier eine Exklusion bestimmter Bereiche wie Patente und Wettbewerb und damit eine automatische Inklusion aller weiteren Bereiche wie Datenschutzrecht, Persönlichkeitsrecht, Lizenzrecht, usw.

Zur vollständigen Darlegung der Leistungen müssen auch die Abgrenzungen bekannt sein, wann eine Cyber-Risk-Versicherung nicht leistet:

- Personen- und Sachschäden fallen unter Haftpflichtversicherungen und werden hier nicht abgedeckt
- Strafzahlungen aus gerichtlichen Verhandlungen werden ebenso nicht erstattet
- Leistungen, die durch andere Versicherungen erstattet werden, werden nicht doppelt erstattet

Bestimmung der Deckungssummen

Die Bestimmung der notwendigen Deckungssummen gestaltet sich für Unternehmen recht schwierig, da meist nicht abzusehen ist welche Summen im Schadensfall entstehen. Das obige Schadensbeispiel bei einem Zugriff auf Kundendaten endet mit einer Gesamtsumme über einer halben Million Euro, die sich aus unterschiedlichen Teilkosten zusammensetzt. Schadensunerfahrene Personen fehlt hier meist die notwendige Kenntnis, um die richtige Dimensionierung vorzunehmen.

Daher sehen Versicherungen verschiedene Faktoren vor, um die Deckungssumme passend zu ermitteln. Zunächst wird zwischen Eigenschäden und Drittschäden unterteilt. Bei Drittschäden fließen eine allgemeine Risikobewertung des Unternehmens (Geschäftstätigkeit) und branchenspezifische Werte statistisch erfasster Schadensfälle ein. Ein wesentlicher Faktor ist mit welchen Vermögenswerten das Unternehmen hantiert und welche potentiellen Schäden abgedeckt werden sollen. Eventuell ist auch eine Mehrfachhaftung (Leistung weiterer Deckungssummen nach dem ersten Schadenfall im Jahr) gewünscht.
Aus diesen Faktoren ermittelt sich dann die Deckungssumme für Drittschäden.

Die Deckungssumme für Eigenschäden richtet sich in der Regel nach den realen Vermögenswerten im Unternehmen wie IT-Infrastruktur mitsamt Lizenzen.

Was ist bei einem Abschluss einer Cyber-Risk-Insurance zu beachten?

Möchte ein Unternehmen eine Cyber-Risk-Versicherung abschließen, sollte zunächst sichergestellt werden, dass der Umfang der benötigten Leistungen ermittelt wurde und bekannt ist. Es ist von wesentlicher Bedeutung, dass das Unternehmen weiß warum und wofür es diese Versicherung wünscht.

Mit diesem Wissen sollte ein Versicherungsmakler kontaktiert werden, um Angebote einzuholen. Die Nutzung eines Maklers hat den Vorteil, dass dieser Aufgrund der Versicherungsmaklerhaftung für eine durch unzureichende Beratung entstandene Unterversicherung haftet.

Mit dem Makler gilt es gemeinsam zu prüfen ob es aufgrund bestehender Versicherungen doppelte Deckungen geben kann und auf welche Versicherungen man zukünftig die Deckung streuen möchte.

Anschließung ist der Leistungsumfang der angebotenen Cyber-Risk-Versicherungen zu prüfen. Die zu beinhaltenden Komponenten sind in dem Abschnitt „Welche Leistungen werden benötigt?“ aufgeführt.

Zudem sind versteckte Ausschluss-Klauseln zu beachten wie beispielsweise:

- Anzeigepflicht jeder Gefahrenerhöhung
- Deckungsvoraussetzung IT-Sicherheitsbeauftragter (CISO) / Notfallplan
- Festschreibung Stand der Technik

Abschließend sind wie zuvor dargelegt die Deckungssummen zu verifizieren. Informationen über die Schadenshandhabung des Risikoträgers auf Basis von Kundenbewertungen können zusätzlich einen Indiz liefern, ob die Schadensregulierung in der Regel so gehandhabt wird, wie dies von dem interessierten Unternehmen gewünscht ist.

Experten-Empfehlung

Als Experte auf dem Gebiet Cyber-Risk-Insurance empfiehlt Christoph Brücher, Geschäftsführer der alleato assekuranzmakler GmbH, interessierten Unternehmen die Zusammenarbeit mit erfahrenen Maklern:

„Um für diesen neuen Bereich einen erfahrenen Versicherungsmakler als Partner zu identifizieren empfiehlt sich ein Blick auf die Internetseite vom Verband Deutscher Versicherungsmakler e.V. (http://www.vdvm.de/). Hier können nur Qualitätsmakler Mitglied werden.

Jeder Makler hat einen Branchen- und/oder Spartenschwerpunkt. Diesen kann man i.d.R. in einem Erstgespräch in Erfahrung bringen.“

Der Spartenschwerpunkt der alleato ist die Cyber-Risk-Versicherung, dabei nutzt sie einen innovativen Ansatz aus der Kombination von IT-Lösungen und dem Versicherungsschutz. Zur Risikoanalyse werden führende IT-Lösungen eingesetzt, die zur optimalen und bedarfsgerechten Angebotserstellung führen.

Weiterhin nennt der Cyber-Risk-Insurance Experte Brücher weitere Eckdaten des Versicherungsschutzes, die für Interessenten von Bedeutung sind:

So liegt der Versicherungsbeitrag in der Regel bei 2.000€ bis 10.000€ pro Million Euro Deckungssumme.
Je nach Deckungsgröße ist eine Mindestprämie von 490€ bis 5.000€ einzuplanen. Dabei sehen die Risikoträger einen Selbstbehalt von mindestens 1.000€ je Schadensfall vor.

Interne Versicherungsstatistiken belegen, dass die seit Jahren in den USA etablierte Cyber-Risk-Versicherung nun auch in Deutschland Akzeptanz findet. So wächst das Interesse an der Versicherung exponentiell, entsprechend haben auch die gemeldeten Schadensfälle zugenommen.

Quellen

[1] e-crime Studie KPMG
https://www.kpmg.com/DE/de/Documents/e-crime-studie-2015.pdf

[2] Cyber Risk & Cybercrime Versicherung
https://www.versicherungscheck24.de/cyber-risk-versicherung/#weshalb-ist-eine-cyber-risk-oder-cybercrime-versicherung-sinnvoll

[3] alleato
http://www.alleato.eu

[4] Hiscox
https://www.hiscox.de/geschaeftskunden/cyber-versicherung/]

[5] KuV24
https://www.kuv24-datenrisiken.de/KuV24+Cyber+-+FAQs/index.html?pageid=1884

Über Werth IT

Die Werth IT GmbH kennt die Forderungen von Unternehmen an die IT-Sicherheit von SAP Systemen und nimmt den besonderen IT-Security-Bedarf sehr ernst. Aus diesem Grunde hat das Experten-Team mit hohem Bewusstsein für Qualität einen SAP-Security Scanner entwickelt, der vollständig das Prüfspektrum für SAP-Systeme abdeckt.

Mit dem intuitiv bedienbaren SAP-Security Scanner setzt die Werth IT GmbH bewusst auf die leichte Handhabung und aussagekräftige Ergebnislisten, die heute bereits namhaften Unternehmen helfen, die vorhandenen SAP-Sicherheitslücken auch bei wachsender Komplexität und gleichzeitigem Fachkräftemangel effizient zu schließen.

Als Vorreiter in der IT-Security von SAP Systemen ist es das Ziel der Werth IT GmbH, dass digitale Unternehmensdaten genau dort bleiben sollen, wo sie hingehören – nämlich im Unternehmen. Um das gemeinsam sicher zu erreichen, setzt sich der IT-Dienstleister voller Leidenschaft immer für faire Partnerschaften und wertschätzende Kundennähe ein.

http://www.werth-it.de

Über alleato assekuranzmakler GmbH

Als unabhängiger Versicherungsmakler haben wir das Ziel, das Vermögen und die Gesundheit unserer Mandanten zu schützen und diese als verlässlicher Ansprechpartner in allen Fragen rund um das Thema Versicherungen ganzheitlich zu begleiten. Ob Unternehmen, Freiberufler oder Privatperson - wir bieten Lösungen, die optimal auf die individuellen Bedürfnisse zugeschnitten sind. Durch laufende Marktbeobachtung sind wir in der Lage, unseren Mandanten aus den zahlreichen Versicherungsprodukten das passende Angebot anzubieten. Hierfür steht Ihnen ein Team aus erfahrenen und kompetenten Versicherungsexperten zur Verfügung.

Unsere Leistungen im Überblick

- Unabhängige Risiko- und Bedarfsanalyse
- Entwicklung von innovativen Deckungskonzepten
- Auswahl verschiedener Angebote
- Abschluss bei den Gesellschaften
- Service-Dienstleistungen wie Schadensregulierung
- Laufende Optimierung Ihrer Verträge
- Spezielle Branchenlösungen

Qualität ist uns wichtig!

Als Zeichen unseres hohen qualitativen Anspruchs haben wir uns dem Verband Deutscher Versicherungsmakler e.V. (VDVM) angeschlossen und verpflichten uns damit auf die Einhaltung verbindlicher Verhaltensregeln und Geschäftsprinzipien. Diese Leitlinien gehen weit über die gesetzlichen Anforderungen hinaus und garantieren Ihnen höchste Seriosität und Kompetenz. So können wir sicherstellen, dass immer der Kunde im Mittelpunkt unserer Tätigkeit steht.