SOPHOS

Sophos Guide zu Cyberversicherungen

Wie Sie mit moderner Cybersecurity einen besseren Versicherungs-Status und niedrigere Prämien erzielen.

Der Markt für Cyberversicherungen bleibt in Bewegung. Da er auf die wachsende Anzahl der Schadenfälle und damit verbundene Kosten reagiert, ist mit unverändert schwierigen Bedingungen zu rechnen. Die meisten Unternehmen haben mittlerweile eine Cyberversicherung. Doch sie müssen jetzt ein immer höheres Maß an Cybersicherheit nachweisen. Auch die Policen werden komplexer – und die Prämien steigen.

Zwar gibt es ein großes Angebot an Cyberversicherungen, aber die Anbieter sind wählerisch und meiden in der Regel Antragsteller, die ein hohes Risiko darstellen. Unternehmen, die in eine moderne Cyberabwehr investieren, können ihr Cyberrisiko reduzieren und dadurch auch ihren Versicherungs-Status verbessern. Bessere Konditionen beim Versicherungsschutz, niedrigere Prämien und höhere Deckungssummen: Eine starke Cyberabwehr bietet viele Vorteile für Versicherungsnehmer.

Unser Guide verschafft Ihnen einen Überblick über die aktuelle Lage auf dem Cyberversicherungs-Markt und erklärt, wie sich Ihre Cybersecurity positiv auf Ihre Cyberversicherung auswirken kann. Außerdem erfahren Sie mehr über die Technologien und Services von Sophos, mit denen Sie Ihr Cyberrisiko minimieren und Ihren Versicherungs-Status optimieren können.

Sophos-Whitepaper. Dezember 2023

Die Grundlagen

Welche Vorteile bietet eine Cyberversicherung?

Cyberversicherungen – unter anderem auch als Datenschutz-, Cyber-Risk- oder Hacker-Versicherungen bekannt – schützen Sie vor den Auswirkungen von Cyberangriffen (jedoch nicht vor den Angriffen selbst). Im Allgemeinen bietet Ihnen eine Cyberversicherung vier entscheidende Vorteile:

1. **Finanzieller Schutz.** Der Versicherer trägt aus Cybersecurity-Vorfällen entstehende Vermögensschäden
2. **Sichere Geschäftsbeziehungen.** Immer mehr Unternehmen setzen mittlerweile eine Cyberversicherung bei potenziellen Geschäftspartnern voraus
3. **Operative Unterstützung.** Bei Vorfällen leisten externe Experten (IT-Forensik-Analysten, Anwälte für Datenschutzrecht und PR-Experten) Ihrem Unternehmen Soforthilfe
4. **Krisenvorsorge.** Eine Cyberversicherung bestärkt das Vertrauen Ihrer Kunden, Partner, Zulieferer und Mitarbeiter in Ihr Unternehmen, da Sie auf Cybersecurity-Vorfälle vorbereitet und abgesichert sind

Gründe für Versicherungsansprüche

Laut der „Cyber Claims Study" von NetDiligence aus dem Jahr 2023 werden Versicherungsansprüche bei einer breiten Palette an Vorfällen geltend gemacht, die häufigsten Gründe sind jedoch:

1. Ransomware
2. Business Email Compromise
3. Hacker
4. Diebstahl von Geld
5. Fehlverhalten von Mitarbeitern[1]

Was leisten Cyberversicherungen?

Cyberversicherungen decken durch Cyberangriffe entstandene Kosten ab.

Je nach Anbieter variieren die Inhalte einer Cyberversicherung. In der Regel umfasst der Leistungsumfang jedoch Folgendes:

- Kosten durch Betriebsausfälle
- Forensische Analyse zur Ermittlung der Angriffsquelle
- Lösegeldforderungen und Unterstützung durch Spezialisten bei der Verhandlung der Lösegeldsumme
- Kosten zur Wiedererlangung des Zugriffs auf IT-Systeme sowie zur Wiederherstellung von Daten aus Backups und anderen Quellen
- Rechtskosten
- Presse- und Öffentlichkeitsmaßnahmen
- Benachrichtigung von Kunden und/oder Behörden
- Credit-Monitoring-Services für Betroffene

Wichtiger Hinweis, wenn Sie nach einer passenden Police suchen: Nicht alle Anbieter übernehmen durch Betriebsausfälle entstandene finanzielle Schäden (z. B. Einkommensverluste oder zusätzliche Arbeitskosten aufgrund des Cyberangriffs).

Bei einem Cybersecurity-Vorfall tritt Ihr Versicherungspartner in Aktion und stellt Ihnen Experten zur Seite, die Ihnen bei der Behebung des Vorfalls helfen. Im Falle eines Ransomware-Angriffs ergreift der Versicherer meist folgende Maßnahmen:

- Zuteilung eines Experten, der Sie beim Umgang mit Lösegeldforderungen und -verhandlungen berät
- Ermittlung der kostengünstigsten Lösung zur Datenwiederherstellung (Lösegeldzahlung, Backups usw.)
- Beauftragung der zur Behebung des Vorfalls erforderlichen Dienstleister

1 NetDiligence Cyber Claims Study 2023 Report

Schutz bei Eigen- und Drittschäden

Viele Policen decken sowohl Eigen- als auch Drittschäden ab. Eigenschäden umfassen die aus der Reaktion auf den Angriff entstandenen direkten Kosten, z. B. Kosten für Rechtsberatung, Forensik, Kundenbenachrichtigungen, PR-Maßnahmen usw. Drittschäden beziehen sich in der Regel auf Kosten in Zusammenhang mit Gerichtsverfahren.

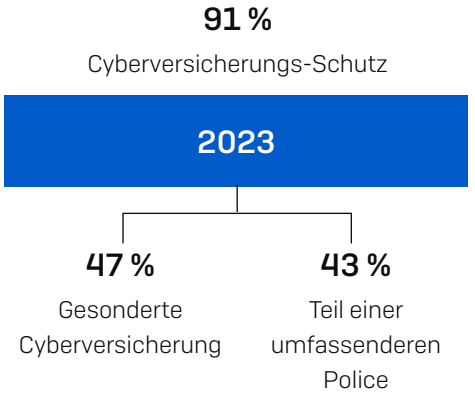
Mitunter sehen Versicherungen Entschädigungsgrenzen bzw. Sublimite für Erstschäden oder bestimmte Arten von Erstschäden vor. So kann sich die vereinbarte Versicherungssumme für Erstschäden beispielsweise auf 500.000 Euro belaufen, wobei sich die Deckung von PR-Kosten auf 50.000 Euro beschränkt.

Cyberversicherungen in der Praxis

Wie verbreitet sind Cyberversicherungen?

Cyberversicherungen sind mittlerweile die Norm: Wie aus einer von Sophos in Auftrag gegebenen, unabhängigen Befragung hervorgeht, hatten im Jahr 2023 bereits 91 %[2] eine Cyberversicherung – dies entspricht einem deutlichen Anstieg gegenüber 2020 mit 84 %[3], bewegt sich jedoch im Wesentlichen auf dem Niveau von 2022 (92 %). Von den Unternehmen, die im Jahr 2023 eine Cyberversicherung hatten, hatten 47 % eigenständige Cyberpolicen und 43 % einen Cyberversicherungs-Schutz im Rahmen von umfassenderen Policen.

Diese Zahlen allein liefern jedoch kein vollständiges Bild. Policen variieren im Umfang und decken teilweise Ransomware nicht ab – die Hauptursache für Cyberversicherungs-Ansprüche. Knapp jedes zehnte Unternehmen, das im Jahr 2022 eine Cyberversicherung hatte, war nicht gegen Ransomware versichert und musste bei einem Vorfall für alle Folgekosten aufkommen.



2 The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption, Sophos
3 The State of Ransomware 2021, Sophos

Cyberversicherungen im Branchenvergleich

Im Branchenvergleich wies der Bildungssektor (Grund- und weiterführende Schulen sowie Hochschulen) den höchsten Cyberversicherungs-Schutz auf (96 %). Dabei war Cyberschutz als Teil einer umfassenderen Police in diesem Sektor weiter verbreitet als gesonderte Cyberversicherungen.

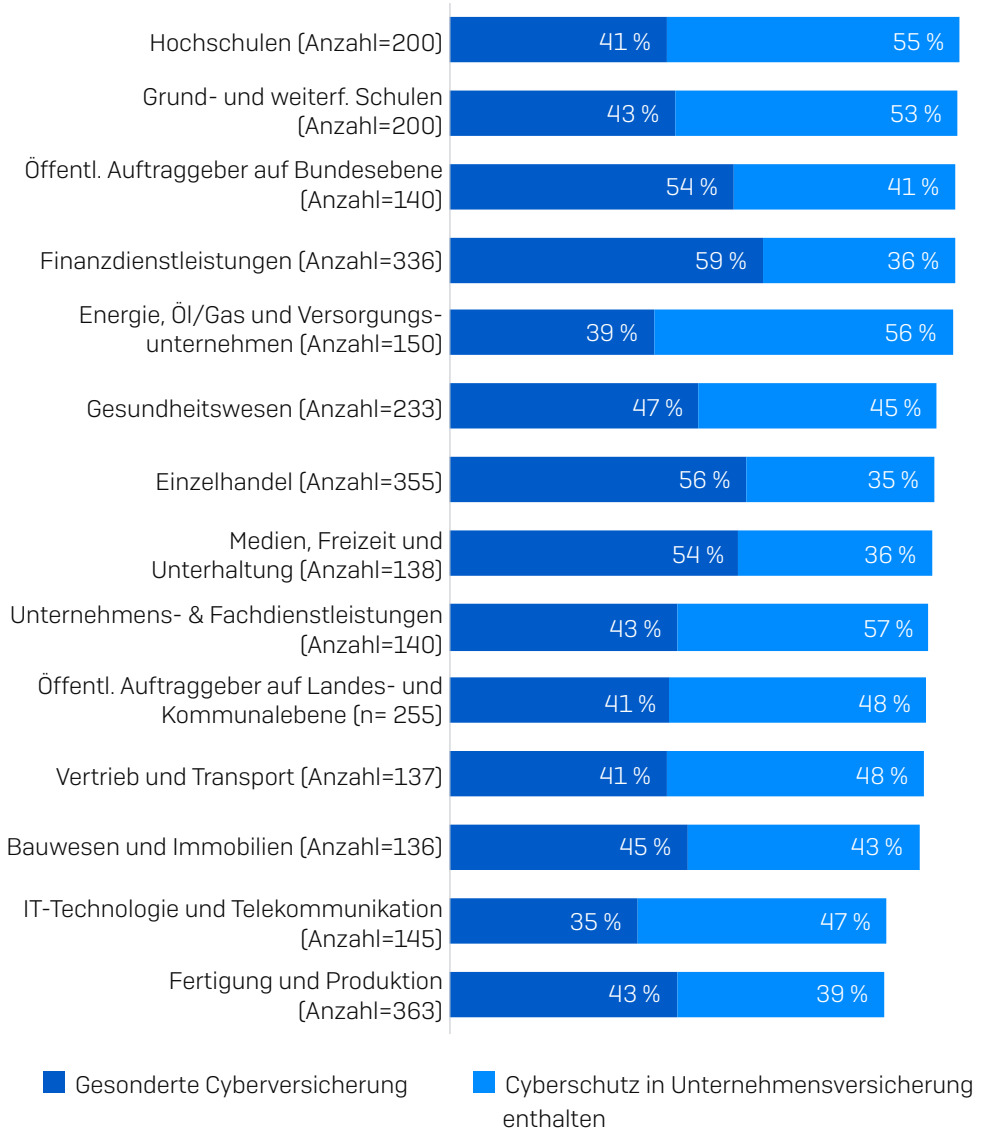
Diese hohe Versicherungsrate überrascht wohl kaum: In unserem Ransomware-Report 2023 meldete dieser Bereich das höchste Aufkommen an Ransomware-Angriffen (80 % der Hochschulen und 79 % der Grund- und weiterführenden Schulen gaben an, dass sie im vergangenen Jahr von Ransomware betroffen waren). Finanzdienstleister verfügten am ehesten über gesonderte Cyberversicherungen (59 %), dicht gefolgt vom Einzelhandel (56 %).

Cyberversicherungen nach Umsatz

Sicher auch nicht weiter überraschend ist, dass die Akzeptanz von Cyberversicherungen mit dem Umsatz steigt. 96 % der Unternehmen mit einem Jahresumsatz von mehr als 5 Mrd. US$ haben eine Cyberversicherung, verglichen mit 79 % der Unternehmen mit einem Umsatz von weniger als 50 Mio. US$.

Zudem sind in Unternehmen mit hohem Umsatz gesonderte Cyberversicherungen gängiger: 58 % der Unternehmen mit einem Jahresumsatz von mehr als 5 Mrd. US$ verfügen über eine gesonderte Cyberversicherung. Bei Unternehmen mit einem Jahresumsatz unter 10 Mio. US$ liegt der prozentuale Anteil dagegen lediglich bei 34 %. Insgesamt zeigt unsere Umfrage, dass die Akzeptanz von gesonderten Cyberversicherungen mit steigendem Umsatzvolumen stetig zunimmt[4].

Cyberversicherungen im Branchenvergleich, 2023



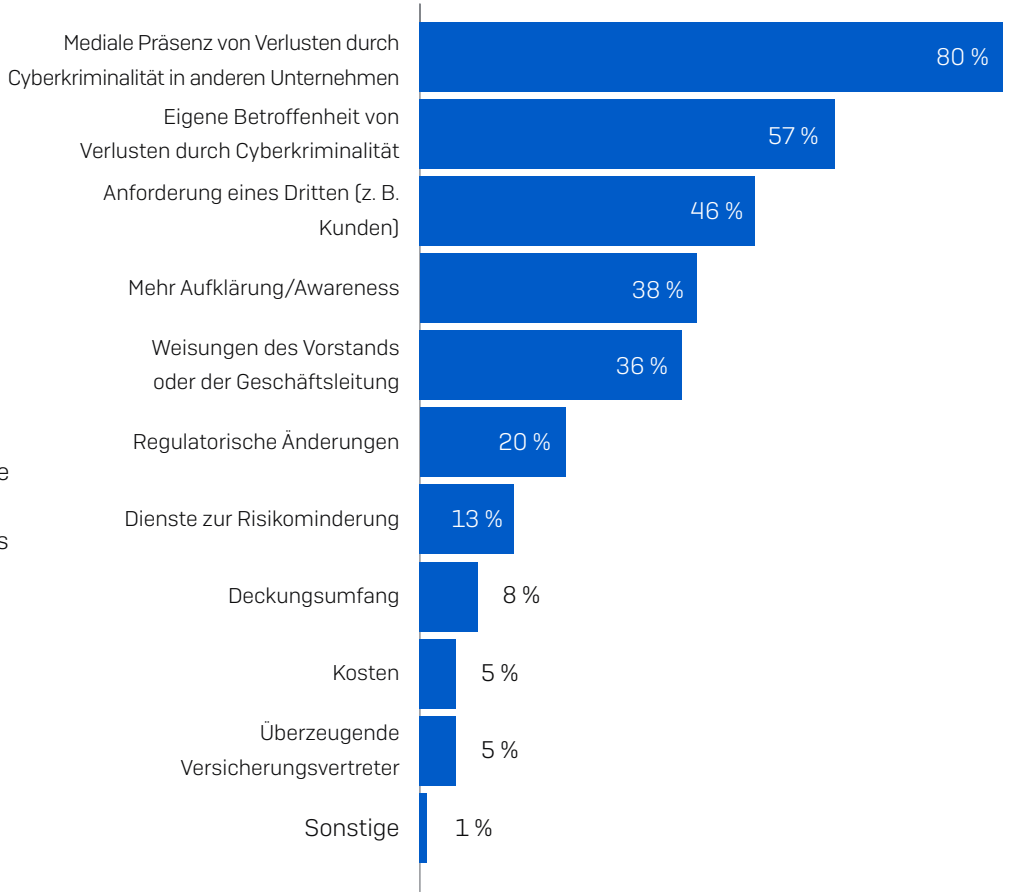
Hat Ihr Unternehmen eine Cyberversicherung? Ja, wir haben eine gesonderte Cyberversicherung. Ja, Cyberschutz ist als Teil einer umfassenderen Police enthalten (z. B. der Betriebshaftpflicht). Anzahl der erhaltenen Antworten jeweils in Klammer

4 The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption, Sophos

Cyberkriminalität erhöht die Nachfrage nach Cyberversicherungen

Eine von Advisen und PartnerRe durchgeführte Befragung von Maklern und Underwritern aus aller Welt wirft einen Blick auf die wichtigsten Treiber für neue bzw. vermehrte Abschlüsse von Cyberversicherungen. Die beiden häufigsten Beweggründe für Cyberversicherungen sind die mediale Präsenz von Verlusten anderer Unternehmen sowie die eigene Betroffenheit von Cyberkriminalität. An dritter Stelle steht jedoch die „Anforderung eines Dritten". Angesichts der Zunahme von Supply-Chain-Angriffen wird von Unternehmen immer häufiger verlangt, eine Cyberversicherung abzuschließen. Diese soll den Kunden absichern, wenn er infolge der Geschäftsbeziehung einen Cybervorfall erleidet.

Mehr als jeder Dritte (36 %[5]) nennt Weisungen des Vorstands oder der Geschäftsleitung als einen der Hauptgründe für den Abschluss einer Cyberversicherung. Letzteres erklärt sich dadurch, dass sich die Führungsebene der dramatischen Folgen bewusst ist, die Cybersecurity-Vorfälle im gesamten Unternehmen nach sich ziehen können. Der Schutz vor den Auswirkungen eines Cyberangriffs ist nicht mehr nur Sache der IT, sondern Aufgabe des gesamten Unternehmens.



Cyberversicherung: The Market's View – Advisen, PartnerRe

5 Cyberversicherung: The Market's View, PartnerRe und Advisen

Wie viel kosten Cyberversicherungen?

Genau wie bei anderen Versicherungen fließen verschiedene Faktoren in die Tarifgestaltung ein, wie etwa:

- **Demografische Daten:** Unternehmensgröße, Branche, Standort, Umsatz usw.
- **Risiko:** Art und Menge der gespeicherten/erfassten/verarbeiteten Daten
- **IT-Sicherheitsniveau des Unternehmens:** Cybersecurity-Lösungen, die das Unternehmen nutzt
- **Vorgeschichte:** Bei früheren Schadenfällen fallen Prämien höher aus
- **Versicherungsbedingungen:** Deckung/Haftungshöchstbetrag usw.

Achten Sie beim Abschluss Ihrer Versicherung unbedingt auch auf die Form der Selbstbeteiligung. Je nach Höhe und Art der Selbstbeteiligung kann die Höhe der Beiträge deutlich variieren. Vergleichen Sie deshalb die unterschiedlichen Tarife der Anbieter und prüfen Sie, welches Angebot am besten zu Ihren Bedürfnissen passt. Dagegen übernimmt der Versicherungsanbieter bei einer Integralfranchise den gesamten Schaden, sofern ein bestimmter Betrag überschritten wurde.

ABZUGSFRANCHISE

Deckungssumme: 100.000 EUR, Selbstbehalt: 10.000 EUR

Sie übernehmen 10.000 EUR, die Versicherung zahlt bis zu 90.000 EUR

Gesamtversicherungssumme 100.000 EUR

INTEGRALFRANCHISE

Deckungssumme: 100.000 EUR, Selbstbehalt: 10.000 EUR

Sie bezahlen bis zu 10.000 EUR. Wird dieser Betrag überschritten, zahlt der Versicherer bis zu 100.000 EUR

Gesamtversicherungssumme 100.000 EUR

Versicherungspakete

KMUs beziehen ihre Cyberversicherung nicht selten von einem einzigen Anbieter. Großunternehmen greifen hingegen häufig auf Versicherungspakete mehrerer Anbieter zurück, da ein Versicherer den erforderlichen Risikotransfer nicht abdecken kann. Dabei stellen Versicherungsmakler ihren Kunden individuelle Pakete von zwei, drei, vier oder mehr Anbietern zusammen. Der erste Versicherer deckt den primären Risikotransfer ab. Die anderen Anbieter tragen wiederum mögliche Risiken, wenn die primäre Deckung ausgeschöpft wurde.

Kooperationspartner

Cyberversicherer verfügen häufig über vorab zugelassene Anbieter, mit denen sie im Falle eines Vorfalls zusammenarbeiten. Wenn das vom Vorfall betroffene Unternehmen keine bestehenden Geschäftsbeziehungen zu Anbietern pflegt, wird der Cyberversicherer die Zusammenarbeit mit einem seiner Kooperationspartner vorschlagen oder sogar verlangen.

Allerdings sind die meisten Versicherungsunternehmen auch offen für die Zusammenarbeit mit anderen seriösen Anbietern, insbesondere wenn bereits eine Geschäftsbeziehung und/oder Verträge bestehen. Dies wird als „Off-Panel-Genehmigung" bezeichnet. Natürlich bietet die Zusammenarbeit mit einem Anbieter, der das von dem Vorfall betroffene Unternehmen bereits kennt und mit seiner IT- und Geschäftsstruktur vertraut ist, viele finanzielle und betriebliche Vorteile.

Wenn Sie einen anderen Anbieter als den Kooperationspartner der Versicherung nutzen möchten, müssen Sie dies beim Versicherer frühzeitig beantragen. So kann die Cyberversicherungs-Abteilung Ihres bevorzugten Anbieters mit dem Versicherer Kontakt aufnehmen und die entsprechenden Genehmigungen einholen.

Erforderliche Leistungen

Bei der Auswahl einer Cyberversicherung gilt es auch, die richtige Deckungssumme zu ermitteln. Im Falle eines Cyberangriffs müssen Sie in der Lage sein, Ihre IT-Systeme wiederherzustellen und die Geschäftskontinuität zu gewährleisten. Gleichzeitig dürfen Versicherungsprämien Ihr Budget jedoch nicht sprengen.

Der finanzielle Aufwand zur Wiederherstellung nach einem Cyberangriff ist immens. Unternehmen zahlten im Jahr 2023 durchschnittlich 1,82 Mio. US$, um die Auswirkungen eines Ransomware-Angriffs zu beheben[6] – 2020 waren es 0,76 Mio. US$. Zwischenzeitlich war die Summe auf 1,85 Mio. US$ geschnellt. Der erfreuliche Rückgang zwischen 2021 und 2022 spiegelt vermutlich wider, dass mit der zunehmenden Verbreitung von Ransomware auch der Reputationsschaden durch einen Angriff geringer geworden ist. Gleichzeitig sind die Versicherungsanbieter besser in der Lage, den Betroffenen schnell und effektiv unter die Arme zu greifen und somit die Kosten zur Bedrohungsbeseitigung zu senken.

6 The State of Ransomware 2023, Sophos

Der Markt für Cyberversicherungen

Die Situation auf dem Versicherungsmarkt hat sich verschärft

Über Jahre hinweg herrschte auf dem Cyberversicherungs-Markt ein Überangebot. Versicherungsprämien waren dementsprechend vergleichsweise niedrig. Eigenständige Cyberversicherungen gibt es nun schon seit mehr als 15 Jahren. Im Jahr 2021 war jedoch erstmals eine Verhärtung des Marktes zu beobachten, da Auszahlungen schneller anstiegen als die Einnahmen der Versicherer durch Prämien. Die Schadenquote der Branche ist seit 2018 stetig gestiegen und belief sich im Jahr 2020 auf 72,8 %.[7] (Die Schadenquote beschreibt das Verhältnis der Beitragseinnahmen zu den Ausgaben für Schadenfälle. Wenn ein Versicherungsunternehmen etwa 80 Euro für Schadenfälle pro 160 Euro eingenommener Prämien zahlt, beträgt die Schadenquote 50 %.)

Diese Verhärtung des Marktes ist auf mehrere Faktoren zurückzuführen:

- Cyberangriffe nehmen zu und werden immer komplexer –
  - 57 % der IT-Manager verzeichneten mehr Cyberangriffe[8]
  - 59 % beobachteten komplexere Cyberangriffe[9]
- Die Kosten zur Bereinigung nach einem Cyberangriff sind gestiegen – wie bereits erwähnt, beliefen sich die durchschnittlichen Kosten für die Bereinigung eines Ransomware-Angriffs im Jahr 2023 auf stolze 1,82 Mio. US$

Durch diese Marktverhärtung ist es viel schwieriger geworden, einen entsprechenden Versicherungsschutz zu erhalten. Unsere Befragung von 5.600 IT-Experten, die Anfang 2022 durchgeführt wurde, bestätigte diese Entwicklung: 94 % der Unternehmen, die eine Cyberversicherung abgeschlossen haben, gaben an, dass sich die Versicherungskonditionen im letzten Jahr verändert hätten:

- 54 % gaben an, dass sie ein höheres Maß an Cybersicherheit nachweisen müssten, um eine Versicherung abschließen zu können
- 47 % meinten, dass die Policen komplexer seien
- 40 % gaben an, dass weniger Versicherer eine Cyberversicherung anböten
- 37 % schilderten, dass der Bearbeitungsprozess länger dauere
- 34 % sagten, der Versicherungsschutz sei teurer geworden[10]

„Unsere Cyberversicherung wurde teurer und der damit verbundene Aufwand immer größer."

Reiseagentur für Geschäftsreisen

Insbesondere öffentliche Einrichtungen traf die Verhärtung des Marktes, da diese aufgrund schwächerer Abwehrmechanismen häufig ein leichtes Ziel für Cyberkriminelle sind. Folglich war die Anbieterauswahl für öffentliche Einrichtungen, die ihren Versicherungsschutz verlängern wollten, begrenzt. Auch die Vertragsauflagen waren strenger. Bisweilen hatten sich Tarife sogar innerhalb eines Jahres verdoppelt.

„Bisher boten uns Versicherungsunternehmen eine Deckungssumme von 10 Mio. US$ an. Jetzt beträgt sie nur noch 5 Mio. US$."

Jack Kudale, CEO, Cowbell Cyber Inc.

In der zweiten Jahreshälfte 2023 zeichnete sich teilweise ein weicherer Markt ab. Zwar haben sich die Kapazitäten durch den Markteintritt neuer Akteure erhöht, doch gehen Versicherungsgeber zunehmend selektiv vor. So erhalten Unternehmen, die ein geringes Risiko darstellen, bessere Konditionen beim Versicherungsschutz, während Unternehmen mit höherem Risiko Schwierigkeiten haben, eine Cyberversicherung abzuschließen.

Cyberversicherungen zahlen

Die gute Nachricht für alle, die eine Cyberversicherung besitzen: Grundsätzlich zahlen die Cyberversicherungs-Anbieter, sollten Sie Opfer eines Cyberangriffs werden. Dem Ransomware-Report 2022 von Sophos zufolge übernahmen Versicherungsgesellschaften bei 98 % der entsprechend versicherten Unternehmen die aus dem Angriff resultierenden Kosten. In fast drei Viertel der Vorfälle (73 %) trugen Versicherer die Bereinigungskosten zur Wiederherstellung kompromittierter Systeme. Bei 36 % der Vorfälle zahlte die Versicherung das Lösegeld und bei 33 % wurden sonstige Kosten, etwa für Betriebsausfälle oder entgangene Gewinne, übernommen.

7 S&P Global, 1. Juni 2021
8 The State of Ransomware 2022, Sophos
9 The State of Ransomware 2023, Sophos
10 Cyber Insurance 2022: Reality from the InfoSec Frontline, Sophos

Unternehmen stärken ihre Abwehr für bessere Versicherungsbedingungen

Die Verhärtung des Marktes hat fast alle Unternehmen (97 %) mit Cyberversicherungen veranlasst, ihre Cyberabwehr zu optimieren, um ihren Versicherungs-Status zu verbessern.

- 64 % haben neue Technologien/Dienstleistungen eingeführt
- 56 % bieten mehr Aus- und Weiterbildungsmaßnahmen für ihre Mitarbeiter an
- 52 % haben ihre Prozesse/Verhaltensweisen geändert[11]

Aber welche Änderungen sollten Sie vornehmen?

Wie können Sie Ihren Cyberversicherungs-Status verbessern?

11 Cyber Insurance 2022: Reality from the InfoSec Frontline, Sophos

Mit modernen Cybersecurity-Lösungen können Sie Ihren Cyberversicherungs-Status optimieren

Es besteht ein direkter Zusammenhang zwischen Cybersecurity und Cyberversicherungen. So bestätigten 95 % der Unternehmen, die 2023 eine Versicherung abgeschlossen hatten, dass die Qualität ihrer Abwehrmaßnahmen direkten Einfluss auf ihren Versicherungs-Status hatte[12]. Durch die Investition in starke Abwehrmechanismen erhalten Sie bessere Konditionen bei Cyberversicherungen:

1. Bessere Konditionen beim Versicherungsschutz

60 % der Unternehmen, die über eine Cyberversicherung verfügen, gaben an, dass ihre Abwehrmechanismen eine wichtige Rolle beim Abschluss einer Cyberversicherung spielten[13]. Anbieter konzentrieren sich zunehmend auf die Kontrolle – und Reduzierung – von Risiken. Mit modernen Cybersecurity-Lösungen können Sie Ihr Cyberrisiko senken und erhalten im Gegenzug bessere Konditionen beim Versicherungsabschluss. Die spezifischen Anforderungen können je nach Versicherer variieren. In den meisten Fällen werden jedoch die folgenden Schutzmechanismen vorausgesetzt:

Mehrstufige Authentifizierung (MFA)

Eine grundlegende Anforderung ist die mehrstufige Authentifizierung (MFA). Damit möchten Versicherer sichergehen, dass gängige Sicherheitslücken geschlossen werden, bevor sie Risiken übernehmen.

„Wir können unsere Cyberversicherung nur verlängern, wenn wir MFA für den Remote-Zugriff aktivieren."

IT-Support- und Service-Anbieter

„Mir wurde gesagt, dass unsere Cyberversicherung gekündigt wird, wenn wir MFA nicht innerhalb eines Jahres einführen."

Gesundheitsdienstleister

12 The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption, Sophos
13 The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption, Sophos

Endpoint Detection and Response (EDR) oder Extended Detection and Response (XDR)

Modernster Endpoint-Schutz, der Bedrohungen automatisch blockiert, ist die wesentliche Grundlage für eine starke Cyberabwehr. Cyberkriminelle entwickeln ihre Techniken ständig weiter, zweckentfremden legitime IT-Tools, bedienen sich gestohlener Anmeldeinformationen und nutzen ungepatchte Schwachstellen aus. Endpoint-Schutz allein reicht hier nicht mehr aus. Um modernste Ransomware und Sicherheitsverletzungen (und damit auch Schadenfälle) abzuwehren, ist es wichtig, proaktiv nach verdächtigen Aktivitäten zu suchen, diese zu analysieren und darauf zu reagieren, bevor Cyberkriminelle ihren Angriff ausführen können.

Mit EDR- und XDR-Programmen können Sicherheitsspezialisten potenzielle Kompromittierungen erkennen und analysieren und komplexe Cyberangriffe so bereits beseitigen, bevor Schaden entsteht. Wie der Name vermuten lässt, nutzt EDR ausschließlich Datenpunkte von Endpoint-Protection-Technologien. XDR hingegen bezieht seine Datenquellen von Endpoint-Lösungen und aus der weiteren IT-Security-Umgebung (einschließlich Firewall-, E-Mail-, Cloud- und mobilen Sicherheitslösungen). XDR bietet somit maximale Transparenz und beschleunigt die Erkennung und Reaktion. Die meisten Cyberversicherer setzen EDR voraus. Ohne EDR können Unternehmen in der Regel nur schwer eine Cyberversicherung abschließen.

Managed Detection and Response (MDR)

MDR ist ein 24/7 Fully-Managed Service, der durch ein Team von Sicherheitsexperten bereitgestellt wird. Diese sind auf das Erkennen und Bekämpfen von Cyberangriffen spezialisiert, gegen die reine Technologie-Lösungen machtlos sind. Der Service bietet optimalen Schutz vor Cyberbedrohungen und minimiert das Risiko und die Wahrscheinlichkeit, die Versicherung in Anspruch nehmen zu müssen. Auch wenn Managed Detection and Response (MDR) von Versicherern nicht zwingend vorausgesetzt wird, gelten Unternehmen, die MDR Services nutzen, häufig als Premium-Kunden, da sie das geringste Risiko darstellen.

„Unsere Rechtsabteilung besteht auf einer Ransomware-Versicherung. Mit Sophos MDR ist dies möglich."

Globaler Anbieter von IT-Technologie und -Lösungen

Incident-Response-Plan

Vorbereitung ist die beste Strategie, um zu verhindern, dass sich ein Cyberangriff zu einem weitreichenden Sicherheitsvorfall entwickelt. Nach einer Sicherheitsverletzung stellen Unternehmen oft fest, dass ihnen ein Incident-Response-Plan viele Kosten, Probleme und Betriebsunterbrechungen erspart hätte. Ein detaillierter Plan, mit dem Sie die Folgen eines Vorfalls abmildern, reduziert Ihr Cyberrisiko und macht Sie für Versicherungsanbieter attraktiver.

2. Versicherungsprämien senken

62 % der Unternehmen mit einer Cyberversicherung bestätigten, dass die Qualität ihrer Abwehrmaßnahmen direkten Einfluss auf ihren Versicherungs-Status hatte[14]. So wie eine Alarmanlage die Beiträge für Ihre Hausratversicherung reduzieren kann, hilft moderne Cybersicherheit, die Kosten für Ihre Cyberversicherung zu senken. Die genaue Berechnungsgrundlage wird von Versicherern zwar wie ein Geheimnis gehütet, Kunden zufolge wirkt sich die Qualität ihrer IT-Sicherheit jedoch positiv auf ihre Prämien aus.

„Da EDR nicht auf allen unseren Appliances installiert war, haben sich unsere Versicherungskosten verdoppelt."

Web-Hosting-Unternehmen

„Bei Measured können Kunden, die Sophos MDR oder Sophos-Endpoint-Produkte nutzen, ihre Cyber-Versicherungsprämien um bis zu 25 % senken."

Measured Insurance

3. Schadenfälle minimieren

Wie bei anderen Versicherungen haben Sie ggf. Schwierigkeiten, Ihre Police zu verlängern, nachdem Sie einen Versicherungsanspruch geltend gemacht haben. Unternehmen, die ihre Versicherung in Anspruch genommen haben, verzeichnen in den Folgejahren außerdem einen erheblichen Anstieg ihrer Prämien. Wenn Sie das Risiko eines Cyberangriffs mit einer starken Cyberabwehr minimieren, sinkt auch die Wahrscheinlichkeit, dass Sie Ihre Versicherung in Anspruch nehmen müssen – und Ihre Beiträge in die Höhe schnellen.

4. Sicherstellen, dass die Versicherung zahlt

Wenn Sie Sicherheitsvorgaben nicht systematisch durchsetzen, erhalten Sie im Schadenfall unter Umständen keine finanzielle Unterstützung. Geht Ihr Versicherer davon aus, dass Sie Angreifern aufgrund unzureichender IT-Security „Tür und Tor geöffnet haben", sind Sie unter Umständen nicht anspruchsberechtigt. Indem Sie Sicherheitslücken schließen, stellen Sie sicher, dass Ihr Versicherungspartner im Ernstfall für Schäden aufkommt.

„Wir leisten keine Zahlungen für jedwede Ansprüche, Verluste, Datenpannen oder Bedrohungen, die von der Nutzung veralteter bzw. nicht unterstützter Software oder Systeme herrühren."

Hiscox Cyberclear™, Police-Vertragstext, Juni 2021

5. Schäden und Kosten durch Vorfälle minimieren

Eine schnelle und angemessene Reaktion auf Cyberangriffe kann die daraus resultierenden finanziellen und sonstigen Schäden erheblich reduzieren. Mit einer Incident-Response-Strategie für Malware und Zugang zu Incident-Response-Experten mildern Sie mögliche Folgen eines Angriffs ab.

14 The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption, Sophos

So kann Sophos helfen

Verbessern Sie Ihre Cyberabwehr

Mit Sophos erfüllen Sie viele Kontrollmechanismen, die Versicherer zunehmend voraussetzen und mit denen Sie Ihre Beiträge minimieren. Profitieren Sie von der Threat-Intelligence- und Cybersecurity-Expertise unserer Sophos X-Ops.

Sophos Endpoint Detection and Response (EDR)

Sophos EDR kombiniert die robuste, präventive Cybersecurity von Sophos Endpoint mit leistungsstarken Erkennungs- und Reaktionsfunktionen. So können Sicherheitsanalysten und IT-Administratoren nach verdächtigen Aktivitäten auf Endpoints und Servern suchen, diese analysieren und darauf reagieren. Erkennungen werden mit KI-basierten Analysen priorisiert, damit Sie sehen, wo Sie Ihre wertvolle Zeit und Ressourcen am besten einsetzen sollten. Benutzer können per Remote-Zugriff auf Geräten Analysen vornehmen, Software (de)installieren, aktive Prozesse beenden, Skripts oder Programme ausführen, Konfigurationsdateien bearbeiten und vieles mehr.

Sophos Extended Detection and Response (XDR)

Je mehr Einblicke IT-Teams haben, desto schneller können sie reagieren. Sophos XDR nutzt Telemetriedaten von vorhandenen Sicherheitstools anderer Hersteller und Sophos-Lösungen, sodass Sie nach verdächtigen Aktivitäten in der gesamten Umgebung suchen, diese analysieren und darauf reagieren können.

- **Erkennung:** KI-basierte Erkennungen bieten umfassende Transparenz über verdächtige Aktivitäten für alle wichtigen Angriffsflächen. Außerdem können Sie Bedrohungen mit unserer einfachen Suche ohne SQL schnell aufspüren.
- **Analyse:** Mit automatisch erstellten Fällen und priorisierten Erkennungen können Sie sich schnell auf das Wesentliche konzentrieren. Zudem liefert unsere von Sicherheitsexperten entwickelte Benutzeroberfläche Ihnen die Informationen und Tools, die Sie für Ihre Analysen benötigen.
- **Reaktion:** Dank leistungsstarker Fallmanagement-Tools und umfassender Reaktionsmaßnahmen können Sie effizient mit anderen Teammitgliedern zusammenarbeiten und Angriffe schnell beseitigen.

Sophos Managed Detection and Response (MDR)

Sophos MDR ist der MDR-Service, dem weltweit die meisten Kunden vertrauen. Dank 24/7 Bedrohungserkennung, -analyse und -reaktion durch ein Expertenteam als Fully-Managed Service sind Sie mit Sophos MDR optimal geschützt. Sophos MDR bereinigt Vorfälle in durchschnittlich nur 38 Minuten. Unser Team minimiert erheblich das Risiko eines schwerwiegenden Cybervorfalls und optimiert Ihren Versicherungs-Status.

Schadenfälle minimieren

Sophos bietet weltweit führenden Schutz vor Ransomware, Hacker-Angriffen und anderen komplexen Bedrohungen. Mit unseren Lösungen minimieren Sie das Risiko eines Cybersecurity-Vorfalls. Gleichzeitig sinkt dabei auch die Wahrscheinlichkeit, dass Sie Ihre Versicherung in Anspruch nehmen müssen und Ihre Beiträge in die Höhe schnellen.

„Wir können nicht alle Bedrohungen und Angreifer selbst stoppen, deshalb verlassen wir uns auf Sophos."

Vancouver Canucks

Auszeichnungen von Analysten und Kunden

Unsere Lösungen sind vielfach ausgezeichnet durch Kunden, Analysten und unabhängige Testinstitute:

Sophos Managed Detection and Response (MDR)

- Von Gartner® Peer Insights als „Customers' Choice™" für Managed Detection and Response (MDR) 2023 ausgezeichnet (durchschnittliche Bewertung von 4,8/5)
- „Overall Leader" für Managed Detection and Response (MDR) in den G2 Grid® Herbstreports, 2023
- Nummer 1 bei der MITRE Engenuity ATT&CK Evaluation für Managed Services, 2022

Sophos Extended Detection and Response (XDR)

- „Overall Leader" für XDR in den G2 Grid® Herbstreports, 2023
- Nummer 1 bei den MITRE Engenuity ATT&CK Evaluations 2023 (Turla)
- Am besten bewerteter Anbieter und einziger Leader im Omdia Universe für Comprehensive Extended Detection and Response (XDR)

Sophos Endpoint Detection and Response (EDR)

- 2022 zum 13. Mal in Folge als ein Leader im Gartner® Magic Quadrant™ for Endpoint Protection Plattforms positioniert
- Von Gartner® Peer Insights zum zweiten Mal in Folge als „Customers' Choice™" für Endpoint Protection Platforms 2023 ausgezeichnet (durchschnittliche Bewertung von 4,8/5)
- „Overall Leader" für Endpoint Protection Suites und EDR in den G2 Grid® Herbstreports, 2023. Nummer 1 bei der MITRE Engenuity ATT&CK Evaluation (Turla), 2023
- AAA-Bewertungen und eine 100%ige Gesamtschutzbewertung in den Kategorien „Enterprise" und „SMB" im Endpoint Security Report von SE Labs, Q3 2023.

Weitere Informationen zu Sophos-Lösungen erhalten Sie hier

Sophos bietet branchenführende Cybersecurity-Lösungen für Unternehmen jeder Größe und schützt Kunden in Echtzeit vor komplexen Bedrohungen wie Malware, Ransomware und Phishing. Bewährte Next-Gen-Funktionen mit der Power von Machine Learning und künstlicher Intelligenz sichern Unternehmensdaten effektiv.

2023-12-06 (WP-NP)

SOPHOS