SOPHOS
Cybersecurity delivered.

Sophos Guide zu Cyber-Versicherungen

Wie gute Cybersecurity Versicherungsprämien und Risiken reduziert

Der Markt für Cyber-Versicherungen befindet sich im Wandel: Zum ersten Mal in seiner über 15-jährigen Geschichte verhärtet sich der Markt und die Bedingungen für Versicherungsnehmer erschweren sich zusehends. Viele Unternehmen haben zwar bereits einen Cyber-Versicherungsschutz. Häufig gestaltet sich die Verlängerung von Policen jedoch schwierig, da Kapazitäten sinken und Prämien in die Höhe schnellen.

Starke Cybersecurity unterstützt Unternehmen in mehrfacher Hinsicht in Sachen Cyber-Versicherung: vereinfachte Genehmigungsverfahren, niedrigere Prämien sowie eine geringere Wahrscheinlichkeit von Schadenfällen. Unser Guide verschafft Ihnen einen Überblick über die aktuelle Lage auf dem Cyber-Versicherungsmarkt und erklärt, wie sich Ihre Cybersecurity positiv auf Ihre Versicherung auswirken kann. Außerdem erfahren Sie mehr über die Technologien und Services von Sophos, mit denen Sie sowohl Ihre Prämien als auch Ihr Risiko senken können.

Sophos-Whitepaper. Juli 2021

Die Grundlagen

Welche Vorteile bietet Ihnen eine Cyber-Versicherung?

Cyber-Versicherungen – 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 eine Cyber-Versicherung Ihnen drei entscheidende Vorteile:

1. **Finanzieller Schutz**. Der Versicherer trägt aus Cybersecurity-Vorfällen entstehende Vermögensschäden
2. **Operative Unterstützung**. Bei Vorfällen leisten externe Experten (IT-Forensik-Analysten, Anwälte für Datenschutzrecht und PR-Experten) Ihrem Unternehmen Soforthilfe
3. **Krisenvorsorge**. Eine Cyber-Versicherung bestärkt das Vertrauen Ihrer Kunden, Partner, Zulieferer und Mitarbeiter in Ihr Unternehmen, da Sie auf Cybersecurity-Vorfälle vorbereitet und abgesichert sind

Laut der „Cyber Claims Study" von NetDiligence aus dem Jahr 2020 werden Versicherungsansprüche bei einer breiten Palette an Vorfällen, am häufigsten jedoch bei Ransomware-, Social-Engineering-, Hacker- und BEC(Business Email Compromise)-Angriffen geltend gemacht*.

Was leisten Cyber-Versicherungen?

Cyber-Versicherungen decken durch Cyberangriffe entstandene Kosten ab. Je nach Anbieter variieren die Inhalte einer Cyber-Versicherung. In der Regel umfasst der Leistungsumfang jedoch Folgendes:

- 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

Schutz bei Eigen- und Drittschäden

Viele Policen decken sowohl Eigen- als auch Drittschäden ab. **Eigenschäden** umfassen die aus der Reaktion auf den Angriff entstehenden 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 jedoch auf 50.000 Euro beschränkt.

* Quelle: NetDiligence Cyber Claims Study 2020. Daten für Organisationen mit einem Jahresumsatz von unter 2 Milliarden USD

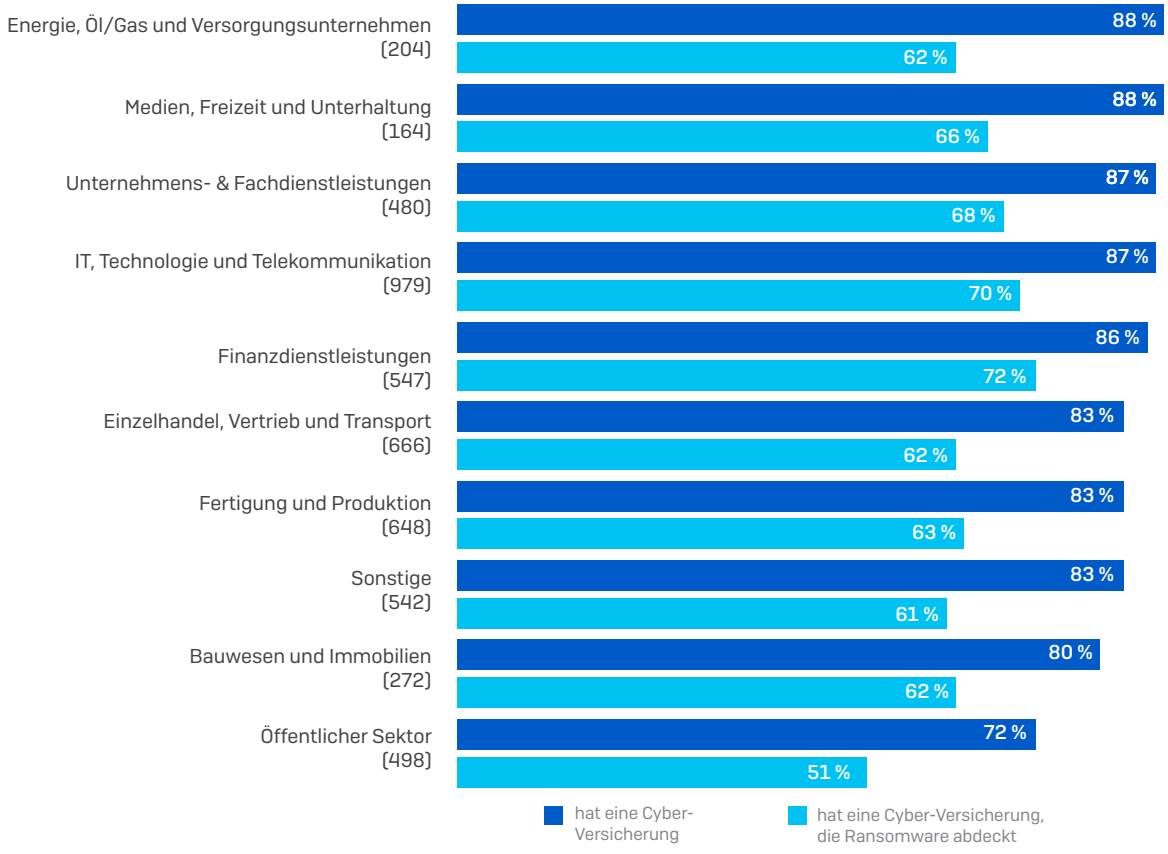
Cyber-Versicherungen in der Praxis

Wie verbreitet sind Cyber-Versicherungen?

Wie aus einer von Sophos in Auftrag gegebenen, unabhängigen Befragung von 5.000 IT-Entscheidern in mittelständischen Unternehmen hervorgeht, verfügen 84 % der Unternehmen bereits über Cyber-Versicherungsschutz*. Cyber-Versicherungen sind in allen Branchen weit verbreitet, allen voran in Versorgungsunternehmen (Energie, Öl und Gas) mit 88 % sowie in Unternehmen aus dem Bereich Medien, Freizeit und Unterhaltung. Diese hohe Zahl hat ihren Grund: Cybervorfälle können in dieser Branche besonders verheerende Konsequenzen nach sich ziehen, und da Versorgungsunternehmen häufig auch noch alte, anfällige Infrastrukturen nutzen, steht dieser Sektor häufig im Fokus von Angreifern.

Allerdings decken Cyber-Versicherungen bei lediglich 64 % der befragten Unternehmen Ransomware-Angriffe ab, sodass eines von fünf Unternehmen (20 %) trotz Versicherungsschutz ggf. die gesamten Kosten eines Ransomware-Vorfalls tragen muss*. Stellen Sie deshalb unbedingt sicher, dass Sie Ihre Versicherungspolice sowie den enthaltenen Schutz genau verstehen.

Cyber-Versicherungen im Branchenvergleich



Im öffentlichen Sektor sind Cyber-Versicherungen (72 %) und Versicherungsschutz vor Ransomware (52 %) am wenigsten verbreitet. Ein beunruhigendes Lagebild, da Cyberkriminelle öffentliche Einrichtungen häufig gezielt ins Visier nehmen und der öffentliche Sektor zu den Branchen zählt, die sich am wenigsten vor Ransomware schützen können. So geht aus dem Ransomware-Report 2021 von Sophos hervor, dass:

- Bildungseinrichtungen im vergangenen Jahr am häufigsten von Ransomware-Angriffen betroffen waren
- Behörden auf Landes- und Kommunalebene am wenigsten in der Lage waren, bei Ransomware-Angriffen eine Verschlüsselung der Daten zu verhindern

Im Branchenvergleich verfügen Finanzdienstleister über den höchsten Versicherungsschutz vor Ransomware-Attacken (72 %). Insgesamt wurden in diesem Bereich die meisten Cyber-Versicherungen abgeschlossen. Diese Branche ist ein sehr lukratives Ziel für Cyberkriminelle. So ist die Akzeptanz von Versicherungen bei Finanzdienstleistern besonders hoch.

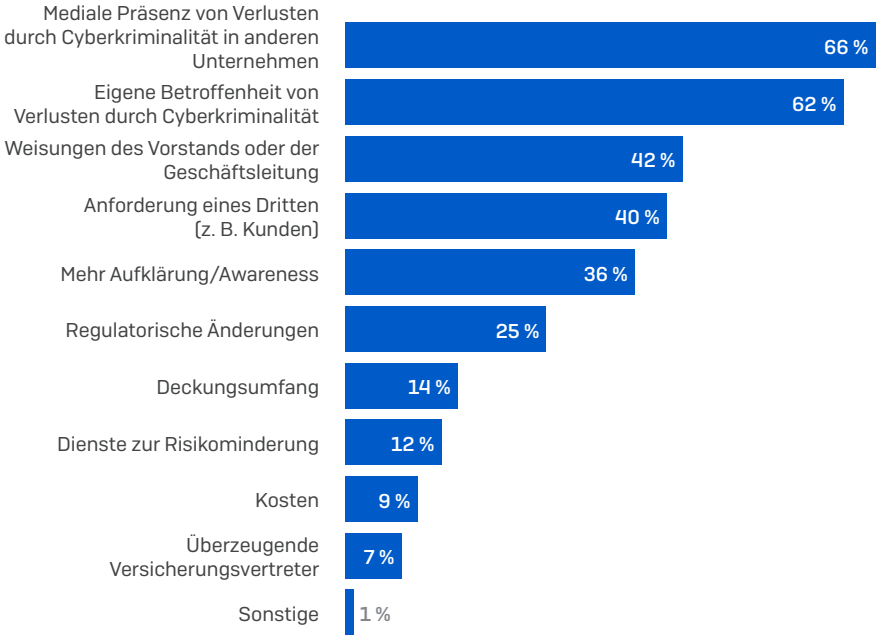
* Quelle: The State of Ransomware, 2020, Sophos

Cyberkriminalität erhöht die Nachfrage nach Versicherungen

Eine aktuelle, 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 Cyber-Versicherungen*. Es überrascht wohl kaum, dass die beiden häufigsten Beweggründe für Cyber-Versicherungen *die mediale Präsenz von Verlusten anderer Unternehmen* sowie *die eigene Betroffenheit von Cyberkriminalität* sind. Als dritter Faktor werden *Weisungen des Vorstands oder der Geschäftsleitung* angeführt. 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.

Was treibt Ihrer Meinung nach neue/vermehrte Abschlüsse von Cyber-Versicherungen an?

Bitte wählen Sie die drei Antworten aus, die am ehesten zutreffen:



Quelle: Cyber Insurance – The Market's View, Advisen – PartnerRe, September 2020.

Wie viel kosten Cyber-Versicherungen?

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.

* Quelle: Cyber Insurance – The Market's View, Advisen – PartnerRe, September 2020. Befragung von 260 Maklern und 190 Underwritern im Bereich Cyber-Versicherung in aller Welt

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.

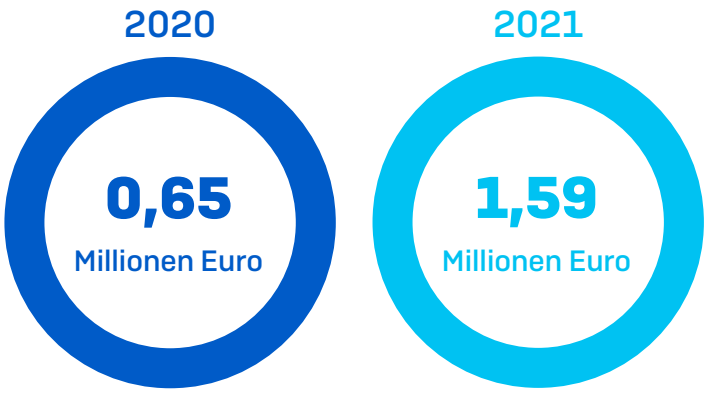
KMUs beziehen ihre Cyber-Versicherung nicht selten von einem einzigen Anbieter. Großunternehmen greifen hingegen häufig auf Versicherungspakete mehrerer Anbieter zurück, da ein Versicherer den erforderlichen Risikotransfer nicht abdecken kann. Dabei stellen Versicherungsmakler ihren Kunden individuelle 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.

Erforderliche Leistungen

Bei der Auswahl einer Cyber-Versicherung 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 und steigt immer weiter an. Im vergangenen Jahr beliefen sich die durchschnittlichen Bereinigungskosten bei einem Ransomware-Angriff auf 1,59 Millionen Euro und waren somit mehr als doppelt so hoch wie im Vorjahr (650.000 Euro)*.

Bereinigungskosten bei Ransomware haben sich im letzten Jahr verdoppelt



Dieser Anstieg ist vor allem auf die zunehmende Komplexität von Cyberangriffen zurückzuführen. Cyberkriminelle setzen verstärkt auf eine Kombination aus Automatisierung und manuellem Hacking. Die Folge sind zunehmend verheerende Angriffe sowie eine mühselige Wiederherstellung betroffener Systeme und Daten. Hinzu kommt, dass Unternehmen nicht nur die Kosten zur Wiederherstellung der IT-Systeme vor dem Angriff tragen, sondern sämtliche Systeme mit modernstem Schutz ausstatten müssen.

* Quelle: The State of Ransomware 2021, Sophos

Der Cyber-Versicherungsmarkt

Die Situation auf dem Cyber-Versicherungsmarkt verschärft sich

Bisher herrschte auf dem Cyber-Versicherungsmarkt ein Überangebot. Versicherungsprämien waren dementsprechend vergleichsweise günstig. Nach etwa 15 Jahren verhärtet sich jetzt der Markt jedoch zunehmend, da Auszahlungen schneller ansteigen als die Einnahmen der Versicherer durch Prämien. Die Schadenquote der Branche nahm drei Jahre in Folge zu und belief sich 2020 auf 72,8 %.* [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 entwickeln sich kontinuierlich weiter. Daher lässt sich das tatsächliche Angriffsrisiko eines Kunden nur schwer abschätzen
- Die Kosten zur Bereinigung nach einem Cyberangriff steigen
- Aufgrund der Corona-Pandemie sowie der zunehmenden Nutzung der Cloud hat sich die Vernetzung des Unternehmensumfelds beschleunigt, was wiederum die Angriffsanfälligkeit erhöht hat

Eine Konsequenz der Marktverhärtung sind höhere Prämien: Im vergangenen Jahr stiegen die Kosten für Standalone-Policen deutlich. Zudem ist es für viele Unternehmen aufgrund strengerer Risikoprüfungen und insgesamt rückläufiger Gesamtkapazitäten allgemein schwieriger, überhaupt eine Versicherung abschließen zu können.

„Unsere Cyber-Versicherung wurde teurer und der damit verbundene Aufwand immer größer."

Reiseagentur für Geschäftsreisen

Insbesondere öffentliche Einrichtungen trifft die Verhärtung des Marktes, da diese aufgrund schwächerer Abwehrmechanismen häufig ein leichtes Ziel für Cyberkriminelle sind. Folglich ist die Anbieterauswahl für öffentliche Einrichtungen, die ihren Versicherungsschutz verlängern möchten, begrenzt. Auch die Vertragsauflagen sind strenger. Bisweilen verdoppelten sich Tarife sogar innerhalb eines Jahres.

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

Jack Kudale, CEO, Cowbell Cyber Inc.

Gute Cybersecurity wirkt sich positiv auf Cyber-Versicherungen aus

Es besteht ein direkter Zusammenhang zwischen Cybersecurity und Cyber-Versicherungen. Eine starke Cyberabwehr unterstützt Unternehmen in mehrfacher Hinsicht:

1. Gute Cybersecurity erleichtert den Abschluss von Cyber-Versicherungen

Um eine Cyber-Versicherung abschließen zu können, müssen Unternehmen häufig nachweisen, dass sie moderne Schutztechnologien nutzen. Hierzu zählen meist Managed Detection and Response (MDR) Services, Endpoint oder Extended Detection and Response (EDR/XDR) sowie Next-Gen-Endpoint-Schutz.

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

Globaler Anbieter von IT-Technologie und -Lösungen

Auch Multi-Faktor-Authentifizierung (MFA) wird häufig vorausgesetzt. Damit möchten Versicherer gängige Sicherheitslücken schließen, bevor sie Risiken übernehmen.

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

IT-Support- und Service-Anbieter

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

Gesundheitsdienstleister

2. Gute Cybersecurity kann Prämien reduzieren

So wie eine Alarmanlage die Beiträge für Ihre Hausratsversicherung senken kann, hilft moderne IT-Sicherheit bei der Reduzierung der Kosten Ihrer Cyber-Versicherung. 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

3. Gute Cybersecurity verringert die Wahrscheinlichkeit von Schadenfällen und somit höheren Beiträgen in der Zukunft

Wie bei anderen Versicherungsformen müssen Sie nach einem Schadenfall mit höheren Beiträgen in den folgenden Jahren rechnen. Wenn Sie das Risiko eines Cyberangriffs minimieren, sinkt auch die Wahrscheinlichkeit, dass Sie Ihre Versicherung in Anspruch nehmen müssen – und Ihre Beiträge in die Höhe schnellen.

4. Gute Cybersecurity reduziert das Risiko, dass die Versicherung nicht 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.

„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

Indem Sie Sicherheitslücken schließen, stellen Sie sicher, dass Ihr Versicherungspartner im Ernstfall für Schäden aufkommt.

5. Gute Cybersecurity minimiert Schäden und Kosten durch Vorfälle

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.

Wie Sophos helfen kann

Anforderungen von Versicherern erfüllen und Beiträge minimieren

Modernster Schutz vor Bedrohungen

Sophos bietet modernsten Schutz vor Bedrohungen, den Versicherer zunehmend voraussetzen und mit dem Sie Ihre Beiträge minimieren. Dazu profitieren Sie von der Threat-Intelligence- und Cybersecurity-Expertise unserer SophosLabs, Sophos AI und Sophos SecOps.

- Mit **Sophos Managed Threat Response (MTR)** sind Sie optimal geschützt: Sie erhalten 24/7 Managed Detection and Response mit Threat Hunting durch ein Expertenteam, als Fully-Managed-Service. Unsere Experten haben bereits bei Tausenden Kunden weltweit Angriffe erfolgreich erkannt und beseitigt.
- Mit **Sophos Extended Detection and Response (XDR)** können Sie in Ihrer gesamten Umgebung nach Bedrohungen suchen und Angriffe stoppen, bevor Schaden entsteht.
- **Sophos Intercept X** bietet weltweit führenden Schutz vor Ransomware für Endpoints und Server. Mehrschichtiger Schutz wehrt Angreifer an zahlreichen Punkten der Angriffskette ab:
  - CryptoGuard stoppt Ransomware und setzt verschlüsselte Dateien wieder in ihren Ursprungszustand zurück
  - Exploit Prevention blockiert die Techniken, die Hacker für Angriffe verwenden
  - Deep-Learning-KI erkennt gängige und sogar bisher völlig unbekannte Bedrohungen
- Die **Sophos Firewall** schützt Ihr Netzwerk vor komplexen Angriffen und sichert Ihre Daten vor Hackern und Ransomware.

Multi-Faktor-Authentifizierung (MFA)

Mit Sophos-Lösungen erfüllen Sie MFA-Auflagen und profitieren dabei von zusätzlichem Schutz.

- **Sophos Central**, unsere cloudbasierte Management-Plattform für die Next-Gen-Security-Produkte von Sophos, erzwingt MFA und sichert so den Zugriff auf alle Ihre Schutzlösungen.*
- **Sophos ZTNA** ermöglicht den Zugriff auf Ihre Anwendungen mit MFA von jedem Standort.**
- Die **Sophos Firewall** unterstützt MFA für das Admin- und Benutzerportal sowie Remote Access VPN. Sophos-Firewall-Benutzer können zudem für noch mehr Sicherheit über Sophos Central auf die Verwaltungsoberfläche der Firewall zugreifen.
- **Sophos Cloud Optix** überwacht AWS-/Azure-/GCP-Konten auf Root- und IAM-Benutzerzugriff ohne MFA, damit Sie Compliance sicherstellen können.

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.

Sophos Intercept X Advanced with XDR ist die Nr. 1 bei Endpoint Protection:

- Zum zwölften Mal in Folge Leader im Gartner Magic Quadrant for Endpoint Protection Platforms
- Bestes Produkt Small Business Endpoint – SE Labs
- 1. Platz beim Malware-Schutz – AV Comparatives
- Nr. 1 beim Exploit-Schutz – MRG Effitas

Sicherstellen, dass die Versicherung zahlt

Mit **Sophos XDR** lassen sich Sicherheitsprobleme (z. B. veraltete Software), aufgrund derer Versicherer ggf. nicht zahlen, schnell und einfach ermitteln. Mit diesen Informationen können Sie Probleme beheben und sicherstellen, dass Ihr Versicherungspartner im Ernstfall für Schäden aufkommt.

SOPHOS-XDR-ABFRAGE ZUR PRÜFUNG, OB SOFTWARE AKTUELL ODER VERALTET IST

```
-- VARIABLE $$Version$$   String

--VARIABLE  $$Name$$    String

SELECT name, version, publisher,

CASE

  WHEN version = '$$Version$$' THEN 'Software is up-to-date'

  WHEN version != '$$Version$$' THEN 'Software is outdated'

  ELSE 'Application Not Installed'

END AS Status FROM programs WHERE name = '$$Name$$';
```

Auswirkungen eines Vorfalls eindämmen

Wenn der Worst Case eintritt und Sie Opfer eines Cyberangriffs werden, holen unsere **Sophos-Rapid-Response**-Experten Sie schnell aus der Gefahrenzone und minimieren die Auswirkungen und Kosten des Vorfalls.

Rapid Response steht sowohl Sophos-Kunden als auch Nichtkunden zur Verfügung. Unser Team hat bereits Hunderte Unternehmen beim Umgang mit Cyberangriffen unterstützt. Zudem arbeiten unsere Experten eng mit Versicherern zusammen und unterstützen etwa forensische Analysen. Wenn Kunden bereits Sophos-Lösungen nutzen, kann unser Rapid-Response-Team noch schneller und effizienter Hilfe leisten.

* MFA wird für alle neuen Konten erzwungen. MFA wird für alle vorhandenen Konten empfohlen und ab 1. September 2021 erzwungen.

** Derzeit im Early-Access-Programm. Voraussichtlich im Oktober 2021 allgemein verfügbar

Fazit

Die Situation auf dem Cyber-Versicherungsmarkt verschärft sich zunehmend, was wiederum strengere Auflagen von Versicherern und höhere Prämien zur Folge hat. Gute Cybersecurity unterstützt Sie dabei, die Kosten Ihrer Cyber-Versicherung und die Wahrscheinlichkeit von Schadenfällen zu reduzieren. Zudem stellen Sie so sicher, dass Ihr Versicherungspartner im Ernstfall für Schäden aufkommt.

Sophos bietet modernste Cybersecurity-Lösungen, mit denen Sie Ihren Cyber-Versicherungsschutz optimieren können. Sie möchten Ihre spezifischen Anforderungen besprechen? Wir beraten und unterstützen Sie gerne. Kontaktieren Sie unser Team unter sales@sophos.de.

Lernen Sie hier unsere Cybersecurity-Lösungen kennen.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

22-04-29 DE (PC)

SOPHOS