

Was ist eine Cyberversicherung und was deckt sie?

Kontext | 07. Mai 2025

Cyberangriffe können Unternehmen und Privatpersonen ohne Vorwarnung treffen und grosse finanzielle Folgen nach sich ziehen. Präventionsmassnahmen helfen zwar, das Risiko stark zu minimieren, bieten jedoch keinen hundertprozentigen Schutz. Eine Cyberversicherung bietet finanzielle Absicherung und unterstützt bei der Vorbeugung, aber auch während und nach einem allfälligen Angriff.

Cyberversicherungen sind ein relativ neues Deckungskonzept und deshalb noch wenig bekannt. Vielen Unternehmerinnen und Unternehmern fehlt die Kenntnis über das Produkt und die vorhandenen Angebote. In der Schweiz verfügen dennoch bereits rund 10 Prozent der Unternehmen über eine Cyberdeckung. Neben präventiven Cybersicherheitsmassnahmen bieten Cyberversicherungen einen Rundumschutz gegen die finanziellen Folgen eines Angriffs aus dem Cyberspace, der jedes Unternehmen oder jede Privatperson zu jeder Zeit unerwartet treffen kann. Die in der Presse geschilderten Fälle sind dabei leider nur die Spitze des Eisbergs: Viele Einzelschicksale bleiben oft im Verborgenen und ergeben somit ein verzerrtes Bild in der Öffentlichkeit.

Cyberversicherungen spielen – neben der Deckung von finanziellen Schäden – auch bei der Prävention und Bewältigung von Cyberangriffen eine wichtige Rolle. In der heutigen digitalen Welt, in der Unternehmen zunehmend auf Technologien angewiesen sind, wird der Schutz vor Cyberangriffen und Datenverlust immer wichtiger. Daher versichern sich immer mehr Unternehmen gegen die Folgen eines Cyberangriffs. Denn ein erfolgreicher Cyberangriff kann erhebliche Kosten verursachen und sogar die Existenz von Unternehmen gefährden. Unternehmen aller Grössen und Branchen sind potenzielle Ziele von Cyberkriminellen.

Cyberversicherungen bieten Unternehmen und Privatpersonen eine zusätzliche Sicherheit, um sich gegen die finanziellen Folgen von Cyberfällen abzusichern. Was viele nicht wissen: Cyberversicherungen bieten aber auch Unterstützung vor, während und nach einem Angriff:

- **Vor einem Angriff** bieten viele Cyberversicherungen nützliche und zum Teil verbindliche Hinweise, wie sich Unternehmen gegen Cyberangriffe technisch und organisatorisch schützen können und sollen.
- **Während eines Angriffs** unterstützen einige Versicherungen Unternehmen bei der Bewältigung eines Vorfalls und versuchen damit den Schaden zu minimieren und das Weiterführen der Geschäftstätigkeiten sicherzustellen, die Reputation des Unternehmens zu schützen und den rechtlichen Verpflichtungen nachzukommen.
- **Nach dem Vorfall** unterstützen Cyberversicherungen Unternehmen in der Regel beim Aufbau einer resilienteren Cybersicherheitsinfrastruktur und von Notfallplänen.

Finanzielle Schäden werden bis zu den vereinbarten Beträgen von der Cyberversicherung gedeckt und umfassen meist folgende Bereiche:

- Wiederherstellung von Systemen und Daten aus vorhandenen Backups
- Gewinnausfall infolge des Betriebsunterbruchs: Im Falle eines Cyberangriffs kann das betroffene Unternehmen oft tagelang stillstehen. Dies führt zu erheblichen Einnahmeverlusten und kann das Unternehmen in ernsthafte finanzielle Schwierigkeiten bringen.

- Eine Cyberversicherung kann dazu dienen, den Geschäftsverlust abzusichern, der durch einen Cyberangriff verursacht wird. Dazu gehören auch entstandene Mehrkosten, um den Geschäftsbetrieb aufrechtzuerhalten.
- Begleichung von Haftpflichtansprüchen von geschädigten Dritten: Eine Cyberversicherung ist nicht nur für die Deckung direkter Schäden von Bedeutung. Sie ist auch entscheidend, um Haftungsansprüche Dritter, die als Folge eines Cyberangriffs entstehen können, zu verhindern. Insbesondere Datenpannen können zu erheblichen Haftungsansprüchen gegen das betroffene Unternehmen führen. Eine Cyberversicherung kann in solchen Fällen die Kosten für Rechtsstreitigkeiten, Schadenersatzforderungen oder Bussgelder abdecken.
- Mehrkosten zur Weiterführung der Datenverarbeitung
- Kosten für eine rechtliche Verteidigung
- Kosten für die Krisenkommunikation
- forensische Kosten zur Ursachenanalyse
- Unterstützung bei Erpressungsversuchen

Was oft nicht oder nicht immer gedeckt ist:

- der Wert der Daten, die für immer und unwiderruflich verloren sind
- Bussen und Konventionalstrafen
- Lösegelder bei Erpressungen. In diesem Zusammenhang ist es wichtig, rasch und überlegt zu reagieren. Das Bundesamt für Cybersicherheit (BACS) rät generell von der Zahlung eines Lösegelds ab. Darüber hinaus empfiehlt Ihnen das BACS dringend, sich nicht an die Täterschaft zu wenden, sondern die weiteren Schritte mit der Polizei zu diskutieren und zu koordinieren. Melden Sie den Vorfall unbedingt auch Ihrem Cyberversicherer, damit weitere Schäden abgewendet werden können.

Die meisten Versicherer, die Ihre Büroräumlichkeiten, Mobilien oder Produktionsstätten gegen Feuer oder Haftpflichtansprüche von geschädigten Dritten versichern, bieten entweder eigenständige Cyberversicherungspolicen an oder Zusatzleistungen auf den oben genannten Leistungen.

In der Regel erwarten die Versicherer, dass Ihr Unternehmen grundlegende Cybersicherheitsmassnahmen anwendet und den Entwicklungen in diesem Bereich Rechnung trägt. Hilfreich sind ausserdem Zertifikate oder Labels, die Ihre Bemühungen und Massnahmen bescheinigen und auch einen raschen Zugang zu Cyberversicherungslösungen ermöglichen. Solche Labels sind zum Beispiel «Cyber-Safe» und «Cyber Seal».

Da Cyberversicherungsprodukte noch sehr unterschiedlich ausgestaltet sind, lohnt es sich, eine Zweitmeinung einzuholen. Es besteht auch die Möglichkeit, mit einer Maklerin oder einem Makler zusammenzuarbeiten, die oder der Sie bei der Wahl eines geeigneten Versicherungsanbieters unterstützen kann. Setzen Sie sich direkt mit Ihrer Versicherung in Verbindung, holen Sie Offerten über Ihre Maklerin oder Ihren Makler ein oder nehmen Sie an einem der zahlreichen Orientierungsanlässe teil.

Die folgenden Mitglieder des SVV (in alphabetischer Reihenfolge) bieten solche Erstversicherungsprodukte für Schweizer Kundinnen und Kunden an:

- AIG
- Allianz Suisse
- AXA
- Axis
- Baloise

- Berkley
- Chubb
- Generali
- Great Lakes
- HDI
- Helvetia
- Liberty
- Mobiliar
- SCOR
- Swiss Re Corporate Solution
- Vaudoise
- Zurich

Cyberisiken

Lesen Sie mehr zum Thema

Add to PDF generator

«Keine Ausreden - machen!»: Eine Kampagne für mehr Cybersicherheit

Die Sensibilisierungskampagne «Keine Ausreden - machen!» führt Privatpersonen und KMU die Wichtigkeit einer starken Cybersicherheit vor Augen.

Kontext 24.04.2025

[Weiterlesen](#)

Add to PDF generator

Die digitale Alarmzentrale: ein Leitfaden zu MDR-Diensten

MDR-Dienste haben sich als wirksames Mittel zur Erhöhung der Cybersicherheit erwiesen. Der SVV-Leitfaden soll KMU dabei unterstützen, eine geeignete MDR-Lösung für ihre Bedürfnisse zu finden.

Publikation 22.04.2025

[Weiterlesen](#)

Add to PDF generator

KMU: In sechs Schritten zu mehr Cybersicherheit

Mit dem Leitfaden von Swiss Cyber Defence DNA können sich KMU einfach und effizient gegen Cyberkriminalität schützen.

Listicle 17.04.2025

[Weiterlesen](#)
