Cyber-Sicherheitsrat Deutschland e.V.

Werkzeugkasten Cybersicherheit

Cyberversicherungen

Definition, Einsatzgebiete & Diskussion

Wir sind wehrhaft

Cybersicherheit erscheint uns oft als unbezwingbare Aufgabe: ein **asymmetrisches Setting**, das Angreifern einen taktischen Vorteil gegenüber Sicherheitsexperten verschafft, wachsende Möglichkeiten und die **Professionalisierung von Cyberkriminellen**, **unklare Zuständigkeiten** und regulatorische Anforderungen bei IT-Sicherheitsinstitutionen und vieles mehr.

Das kann deprimieren.

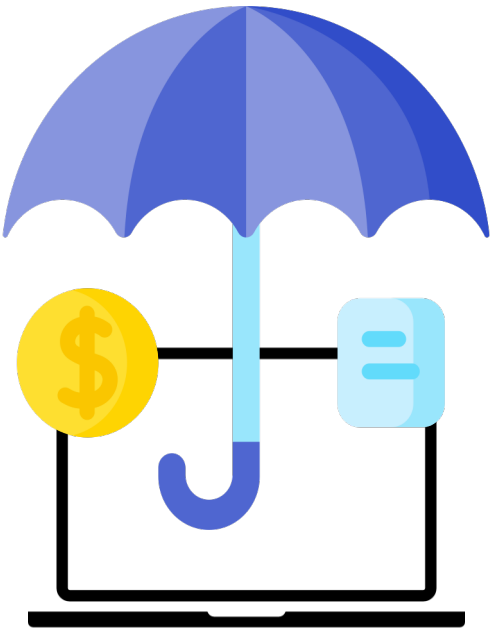
Was wir dabei oft vergessen sind die vielen Menschen, Ressourcen und Werkzeuge auf der anderen Seite, die tagtäglich daran arbeiten, Wirtschaft und Gesellschaft sicherer zu machen. In der Vergangenheit wurden **wirkungsvolle und starke Methoden** entwickelt, die nur an den richtigen Stellen genutzt werden müssen, um Angreifern einen Schritt voraus zu sein.
Es gibt für alles eine Lösung, man muss sie nur finden – vor allem im Bereich Cybersicherheit. Diese Publikationsreihe stellt übersichtsartig die wichtigsten **Methoden im Kampf gegen Cyberattacken** mit ihren Einsatzgebieten sowie Vor- und Nachteilen vor, damit zukünftig die richtigen Werkzeuge an den passenden Stellen parat stehen.

Ich wünsche Ihnen eine anregende Lektüre und interessante Einblicke in den Werkzeugkasten Cybersicherheit.

Hans-Wilhelm Dünn
Präsident
Cyber-Sicherheitsrat Deutschland e.V.

Cyberversicherung – Was ist das?

Cyberversicherungen sind in der Regel **Haftpflicht- oder Risikoversicherungen**, die Unternehmen und Organisationen gegen Cyberkriminalität und Datendiebstahl und die damit verbundenen finanziellen Gefahren absichern. Da es sich um ein relativ neues Versicherungsfeld handelt, hat sich noch keine einheitliche Bezeichnung durchgesetzt (vgl. Hacker-Versicherung, Cyberschutz, Datenschutz-Versicherung usw.). Je nach Schwerpunkt bieten sie ein **unterschiedliches Schutzniveau**.



Wie sind die Versicherungen gestaltet?

Der Markt für Cyberversicherungen **wächst rasant**. Die Beiträge waren im Jahr 2021 um 49 Prozent gestiegen, gleichzeitig verzeichnete die Branche jedoch einen **massiven Verlust** durch eine Schaden-Kostenquote von 124 Prozent. Das heißt, dass pro eingenommenem Euro gleichzeitig 1,24 Euro für Verwaltungskosten sowie die Bewältigung von Schadensfällen aufgewendet werden mussten.

Cyberversicherungen sind auf die verschiedenen Bedürfnisse von Unternehmen und Organisationen abgestimmt und bieten je nach Police einen unterschiedlichen Umfang. Grundsätzlich wird unterschieden in zwei Arten:

First-Party-Versicherungen decken Verluste und Kosten ab, die **direkt** durch den Cyberangriff verursacht wurden. Dazu gehören Kosten für **Rechtsbeistand** und **Krisenmanagement**, die **Wiederherstellung** von Daten und IT-Systemen sowie den Ausgleich von Einnahmeverlusten durch **Betriebsunterbrechungen**. Weitere Leistungen wie eine Untersuchung des Vorfalls und Unterstützung durch IT-Spezialisten können ebenfalls zum Portfolio gehören. Oftmals gibt es 24-Stunden-Hotlines, um im Fall eines Cyberangriffs z. B. durch die Bereitstellung von IT-Forensikern schnell reagieren und den Schadensumfang möglichst gering halten zu können.

Die zweite Art sind **Third-Party-Versicherungen**, die Verluste und Kosten abdecken, die durch **Ansprüche von Dritten aus entstandenen Sicherheitsvorfällen** resultieren. Dazu gehören Klagen und **Schadensersatzforderungen** von Kunden, Lieferanten oder anderen Parteien, die von dem Cyberangriff betroffen sind, sowie **Bußgelder** durch Verstöße gegen regulatorische Standards. Daneben gibt es weitere Produkte, die auf einzelne Problembereiche zugeschnitten sind, beispielsweise **Ausfallversicherungen** für Cloud-Dienste.

Cyber-Sicherheitsrat Deutschland e.V.

Welche Chancen gibt es?

Durch den Abschluss einer Cyberversicherung können Unternehmen eine **finanzielle Absicherung** gegen mögliche Verluste und Schäden aus Cybersicherheitsvorfällen erhalten. Sie können im Fall der Fälle **schnelle Unterstützung und Ressourcen** erhalten, um den verursachten Schaden möglichst gering zu halten.

Einige Cyberversicherungen umfassen darüber hinaus auch **Schulungen** für Mitarbeitende und eine **Beratung** von Verantwortlichen zur Verbesserung der IT-Sicherheit, um zukünftige Schadensfälle zu vermeiden. Unternehmen, die eine Cyberversicherung haben, können gegenüber Kunden und Partner kommunizieren, dass sie angemessen auf mögliche Cyberangriffe vorbereitet sind und damit einen **Wettbewerbsvorteil** erzielen.

Welche Risiken gibt es?

Cyberversicherungen können **sehr teuer** und insbesondere für kleine Unternehmen möglicherweise nicht erschwinglich sein. Zudem können **Einschränkungen und Ausschlüsse von Haftungsrisiken** in den Versicherungsbedingungen die Inanspruchnahme von Versicherungsleistungen erschweren. Hierzu gehört z.B. die unverzügliche Meldung eines Hackerangriffs innerhalb eines definierten Zeitkorridors zur Wahrung des Versicherungsschutzes.

Da es sich um ein relativ neues Feld der Schadensabsicherung handelt, das auch technologisch vielen Neuerungen unterworfen ist, kann die **Komplexität** der Regelungen enorm sein. Unternehmen müssen sicherstellen, dass sie den genauen Schutzumfang und seine Grenzen verstehen. Darüber hinaus ist eine Cyberversicherung **keine Garantie gegen Cyberangriffe** und kann nicht alle denkbaren Risiken decken.

In einigen Branchen ist es für Versicherungsinteressenten schwer, überhaupt eine Cyberpolice abzuschließen, da das Schadenspotential unabsehbar hoch ist, beispielsweise im Gesundheitswesen oder der Lebensmittelindustrie. Zudem werden Verträge oft nur **unter Vorbehalt** angeboten oder wenn Betroffene bestimmte Mindeststandards im Bereich IT-Sicherheit gewährleisten.

Praxisbeispiele zeigen zudem, dass einige kriminelle Hacker in Ransomwareangriffen ihre Opfer dazu aufrufen, die Versicherungsbedingungen der eigenen Cyberversicherung offenzulegen, um ihre **Lösegeldforderung daran anzupassen**. In der Regel stellt dies einen Verstoß gegen die Versicherungsbedingungen dar. Das Phänomen zeigt, dass Cyberversicherungen zwar eine Absicherung für Lösegelderpressungen sein können, kriminelle Hacker jedoch ebenfalls ihr Geschäftsmodell danach ausrichten. Auch deswegen wird aktuell darüber diskutiert, ob **Lösegeldzahlungen** bei Ransomware grundsätzlich verboten werden sollten. Einige Versicherer haben dies bereits in ihren Angeboten ausgeschlossen.

Cyber-Sicherheitsrat Deutschland e.V.

Wem nutzen Cyberversicherungen?

Cyberversicherungen können in einer **Vielzahl von Anwendungsfeldern** eingesetzt werden. Unternehmen aller Größen und Branchen, öffentliche Institutionen und Start-ups können von einer Cyberversicherung profitieren.
Da sich Cyberpolicen auch mit den **Deckungsleistungen anderer Versicherungen** überschneiden können (bspw. Betriebs- oder Vermögensschadenhaftpflicht) sollte vor Abschluss geprüft werden, ob eventuell schon ein **Versicherungsschutz** besteht.

Fazit

Insgesamt bieten Cyberversicherungen Unternehmen und Organisationen einen wichtigen **Schutz gegen die finanziellen Folgen von Cyberangriffen**. Sie können finanzielle Absicherung und eine schnelle **Unterstützung im Schadensfall** bieten.
Interessenten sollten den Umfang der Versicherung im Einzelnen prüfen. Zudem handelt es sich bei dem Werkzeug hauptsächlich um ein **reaktives Element**, das durch Präventionsmaßnahmen ergänzt werden muss, sodass im besten Fall kein Schadensereignis eintritt.