

Wozu braucht man den CyberSchutz?

Kommunikations- und Informationstechnologien bilden das Rückgrat der modernen Unternehmenswelt. Dank der fortschreitenden Digitalisierung gelingt es, immer effizientere Lösungen für den Betriebsablauf zu entwickeln. Diese Entwicklung birgt jedoch auch neue Risiken. Denn aufgrund der Vernetzung sind Unternehmen anfällig wie nie zuvor für Cyberattacken, Datenschutz-Verstöße und Datenverlust.

▼ Beispiele

Zwei Beispiele zeigen, warum der CyberSchutz so wichtig ist:

Hackerangriff



Oliver M. leitet ein Outdoorgeschäft mit einem eigenen Onlineshop, der rund 100.000 Kunden zählt. Als sein Kreditkarten-Unternehmen ihn auf Ungereimtheiten hinweist und eine Prüfung des Vorfalls verlangt, merkt Oliver M., dass er das Opfer von Hackern geworden ist. Daraufhin kündigen die Behörden ein Datenschutz-Verfahren an. Oliver M. muss den Onlinevertrieb vorerst einstellen und einen externen Experten zur Beseitigung der IT-Schwachstellen beauftragen.

Schaden:	
80.000 EUR	Vertragsstrafe an das Kreditkarten-Unternehmen
385.000 EUR	Schaden durch die Betriebsunterbrechung
250.000 EUR	Kosten für die Information der Kunden über den Hackerangriff
20.000 EUR	Kosten während des behördlichen Datenschutz-Verfahrens
735.000 EUR	Gesamtschaden

Datenlöschung



Julia G. ist Geschäftsführerin eines Automobilzulieferers. Nach einer Auseinandersetzung mit einem Mitarbeiter aus der IT-Abteilung ist dieser so erbost, dass er das Unternehmen schädigen will. Er bleibt nach Dienstschluss heimlich im Betrieb und löscht die Festplatten, auf denen sensible Informationen einer aktuellen Produktion gespeichert waren. Am nächsten Tag steht nicht nur die eigene Produktion still, auch die Kunden des Unternehmens können nicht weiterarbeiten.

Schaden:	
45.000 EUR	für die Datenrettung
63.000 EUR	Schaden durch die eigene Betriebsunterbrechung
98.000 EUR	Betriebsunterbrechungsschaden bei den Kunden
30.000 EUR	Kosten für Ursachenklärung und den Anwalt
236.000 EUR	Gesamtschaden

Leistungen des CyberSchutz

Kostenübernahme bei Schäden im eigenen Unternehmen:

Wenn Ihnen Schäden entstehen durch Hackerangriffe auf Ihr Unternehmen oder weil die Behörde Ihren Betrieb aufgrund von Datenschutzverletzungen vorübergehend schließt, übernimmt die Allianz:

- die Kosten für die Wiederherstellung der Daten und der Funktionsfähigkeit des Computersystems,
- die Kosten und den entgangenen Gewinn durch eine daraus entstehende Betriebsunterbrechung,
- Informationskosten, wenn Sie Kunden über den Verlust von Daten informieren müssen,
- Kosten für die Behebung einer Sicherheitslücke, die für einen Cyberangriff ursächlich war.

Kostenübernahme bei Schäden, die Dritten entstanden sind:

Die Allianz prüft im Schadenfall zunächst, ob und in welcher Höhe Sie haftpflichtig gemacht werden können und wehrt unberechtigte Ansprüche ab. Besteht der Anspruch zu Recht, übernimmt die Allianz die Kosten bei:

- Verletzungen der Vertraulichkeit von Daten und Datenschutz, digital und physisch, wenn z. B. ausgedruckte Dokumente gestohlen werden,
- Netzwerksicherheitsverletzungen, wenn z. B. von Ihrem Computer aus Hackerangriffe auf Computer Ihrer Kunden gestartet wurden,
- Verstößen gegen das Marken-, Persönlichkeits- oder Wettbewerbsrecht in der digitalen Kommunikation,
- Vertragsstrafen von Kreditkarten-Unternehmen im E-Payment.

Zusätzliche Serviceleistungen:

Schadenermittlung: Im Versicherungsfall stehen Ihnen die Experten der Allianz für die Schaden- und Ursachenermittlung zur Verfügung. Zudem können Sie – nach Rücksprache – auf Kosten der Allianz einen externen Datenforensiker hinzuziehen, der Schadenursache und -höhe ermittelt und Sie zu Maßnahmen berät, die den Schaden mindern. Das gilt auch, wenn Sie einen konkreten Verdacht haben.

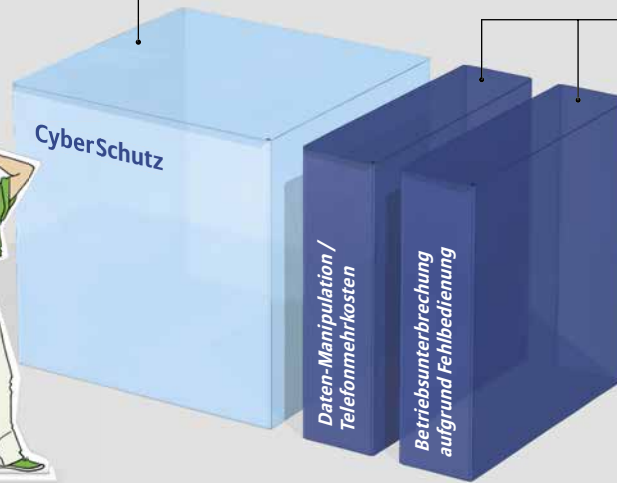
Krisenkommunikation: Die Allianz übernimmt nach vorheriger Abstimmung die Kosten eines Krisenkommunikationsberaters, um Reputationsschäden zu verhindern oder zu mindern. Wir empfehlen Ihnen auf Wunsch gerne einen geeigneten Dienstleister.



Die Allianz erstellt mit Ihnen gemeinsam ein Risikoprofil, um Ihr Unternehmen optimal abzusichern. Für identifizierte Sicherheitslücken werden Ihnen auf Wunsch Servicepartner vermittelt, die Ihnen helfen, die Sicherheitslücken zu schließen.

▼ Prinzip und Leistungen

- Kostenübernahme bei Schäden im eigenen Unternehmen
- Kostenübernahme bei Schäden, die Dritten entstanden sind
- zusätzliche Serviceleistungen



Mit den zuwählbaren Bausteinen „Daten-Manipulation / Telefonmehrkosten“ und „Betriebsunterbrechung aufgrund Fehlbedienung“ können Sie Ihren Schutz noch genauer an Ihren individuellen Bedarf anpassen.

Zusatzbaustein

Daten-Manipulation / Telefonmehrkosten:

Überweisen Sie infolge einer durch einen Cyberangriff herbeigeführten Daten-Manipulation (z.B. Veränderung von Kontodaten) von Ihren Konten irrtümlich und ohne Rechtsgrund Geld, ersetzt Ihnen die Allianz den hieraus entstandenen Schaden. Auch wenn Hacker Ihr Telefonsystem unberechtigt nutzen, übernimmt die Allianz die entsprechenden Mehrkosten.

Betriebsunterbrechung aufgrund Fehlbedienung:

Wenn eine nachlässige Fehlbedienung der Steuerungssoftware das IT-System einer Produktionsstraße schädigt und einen Produktionsstillstand auslöst, übernimmt die Allianz die Kosten der Betriebsunterbrechung.

Wie schließen Sie den CyberSchutz ab?

Mithilfe eines speziell entwickelten Fragebogens ermitteln wir Ihr Risikoprofil. Er gibt Ihnen gleichzeitig einen Einblick, worauf es beim Schutz gegen Cyber Risiken ankommt und hilft Ihnen einzuschätzen, wie gut Sie gegen IT-Risiken gewappnet sind. Diese Risikoanalyse ermöglicht Ihnen, Sicherheitslücken zu erkennen und gezielte Maßnahmen zu ergreifen, um diese zu schließen. Auf Wunsch vermitteln wir Ihnen dazu gerne einen spezialisierten Servicepartner.

§

Das sollten Sie wissen:

Besonders geeignet für: mittelständische Unternehmen, insbesondere Online-Handelsbetriebe, Hotels und produzierende Betriebe mit vernetzter Maschinensteuerung, z. B. durch SCADA.

Nicht geeignet für: Finanzdienstleister, z. B. Banken, können den CyberSchutz aufgrund ihrer speziellen Risikosituation nicht in Anspruch nehmen. Für diese Unternehmen und Unternehmen mit einem Umsatz über 150 Millionen EUR bieten wir gesonderte Lösungen an.

Zielgerichtete und nicht zielgerichtete Angriffe: Versichert sind Sie sowohl als Opfer eines Angriffs, der sich gezielt gegen Ihr Unternehmen oder eine Gruppe von Unternehmen richtet, zu der Ihr Unternehmen zählt, als auch bei massenhaft verbreiteten Angriffen, z. B. durch Phishing-E-Mails oder einen zufällig eingefangenen Virus im Internet. In beiden Fällen übernimmt die Allianz Haftpflichtansprüche und die Kosten der eigenen Betriebsunterbrechung.

Geistiges Eigentum: Der CyberSchutz übernimmt keine Kosten für die Verletzung des eigenen geistigen Eigentums, wie z. B. Patente oder Designs und Modelle.

Vorsatz: Wenn ein Mitarbeiter Ihrem Unternehmen vorsätzlich schadet, indem er beispielsweise Daten löscht oder veröffentlicht, übernimmt die Allianz die dadurch im Unternehmen entstehenden Kosten. Es werden hingegen keine Schäden übernommen, die von Repräsentanten, z. B. Geschäftsführern, Inhabern oder Vorständen, vorsätzlich herbeigeführt wurden.

Versicherungsbedingungen: Diese Information kann Ihnen nur einen Überblick über die Leistungen und Ausschlüsse geben. Für Ihren Versicherungsschutz maßgeblich sind die aktuellen Versicherungsbedingungen bei Vertragsabschluss und der Versicherungsschein.

CyberSchutz Schadenhotline: +49 75 31. 911 91 75
(rund um die Uhr erreichbar)