



Cyberversicherung

Moderne Unternehmensführung ohne digitale Prozesse ist heute nicht mehr möglich. Die Digitalisierung macht Unternehmen schneller und flexibler, aber auch anfälliger. Die globale Vernetzung, das Internet der Dinge (IoT) und die wachsende Anzahl digitaler Geschäftsmodelle sind in fast allen Branchen und Bereichen zu finden.

Cyber Risiken gehören seit Jahren zu den Top 3 Risikoproblemen für Unternehmen. Die Störung von Geschäftsprozessen und Unterbrechung von Produktionsabläufen können finanzielle Schäden bis hin zur Insolvenz nach sich ziehen. Aber auch der Diebstahl und die Veröffentlichung von Kundendaten können Vertrauen zerstören und durch staatliche Regulierungen, wie die Datenschutz-Grundverordnung (EU-DSGVO) empfindliche Bußgelder zur Folge haben.

Den Betrieb zusätzlich zur IT-Sicherheit auch mit einer Cyberversicherung zu schützen, wird immer mehr zum Standard sorgfältiger Unternehmensführung.

Generelle Produkteigenschaften

Haftpflicht

- Prüfung des Anspruches des Dritten
- Abwehr unberechtigter Ansprüche
- Befriedigung berechtigter Ansprüche

Eigenschaden

- Wiederherstellungskosten von Daten und Netzwerken
- Ertragsausfall durch Umsatzverluste
- Mehrkosten zur provisorischen Aufrechterhaltung/ beschleunigter Wiederherstellung des Betriebs
- IT-Bedienfehler
- Erpressungsgelder

Assistance-Leistungen

- Kosten für IT-Forensik, Rechtsberatung, PR-Berater
- Benachrichtigungskosten nach Datenschutzvorfall
- Weitere Kosten im Rahmen der EU-DSGVO

Risikogruppen

Sämtliche Unternehmen, ob groß oder klein, die:

- Daten speichern, verarbeiten oder IT in ihren Produktions- und Wertschöpfungsprozessen einsetzen und auf deren Nutzung angewiesen sind
- IT-Dienstleistungen an externen Unternehmen ausgelagert haben oder mit Cloud-Lösungen arbeiten
- Ihren Mitarbeitern die Nutzung des Homeoffice oder der eigenen Geräte (BYOD) ermöglichen
- Kreditkartenzahlungen verarbeiten oder vertragliche Vereinbarungen erfüllen müssen

Wichtige Vertragsbestandteile

- Präventionsleistungen (z. B. Mitarbeitertrainings)
- Assistance-Leistungen – Soforthilfen im Notfall (z. B. IT-Forensik durch Spezialisten zur Ursachenermittlung oder eine 24-Stunden-Hotline zur Benachrichtigung/ Beantwortung von Fragen von Geschädigten)
- Cyber-Haftpflicht – verschuldensunabhängig (z. B. bei Weitergabe von Schadsoftware oder bei Verstößen gegen den Datenschutz)
- Cyber-Betriebsunterbrechung (auch wenn die Systeme und Daten extern betrieben/gespeichert werden – z. B. über eine Cloud-Anbieter)
- Cyber- und Daten-Eigenschäden (z. B. bei Beschädigung, Zerstörung, Veränderung, Blockierung von Daten und IT-Systemen)
- Cyber-Vertrauensschäden (verursacht durch Mitarbeiter oder durch Dritte)
- Cyber-Erpressung (Krisenberatung und Erstattung von Erpressungsgeldern)

Gründe für eine Cyberversicherung

- Auch bei Bestehen optimaler technischer, organisatorischer und personeller Maßnahmen, besteht immer ein unkalkulierbares Restrisiko
- Firewalls und Virenprogramme werden nie einen 100 %-igen Schutz vor Angriffen bieten können
- Der größte Risikofaktor bleibt der Mensch (z. B. öffnen von kompromittierten Links, E-Mails und Dateien)
- Die Frequenz von Angriffen nimmt stark zu
- Aufwendungen für Schäden steigen
- Verschärfung der Gesetzeslage (EU-Datenschutz-Grundverordnung)
- Zunehmende Globalisierung und Abhängigkeit von Daten und IT-Systemen
- Steigende Nutzung von externen Dienstleistern und der damit einhergehende Kontrollverlust über Prozesse und Sicherheit (z. B. Cloud-Lösungen)
- Notwendigkeit einer professionellen Unterstützung im Krisenfall (IT-Forensik)