Cyber-Versicherung

Im Zuge der notwendigen Digitalisierung von Unternehmen, werden immer mehr Geschäftsbereiche von außen angreifbar. Cyberattacken, auch auf Mitarbeiter im Homeoffice, nehmen jedes Jahr erheblich zu und führen zu erheblichen Risiken.

Was zählt alles zu Cyber-Risiken?

Der Umfang von Cyber-Risiken ist extrem umfangreich und wächst mit neuen Technologien mit. Einige der häufigsten Cyber-Attacken sind:

- Phishing, wo der Empfänger eine E-Mail erhält und die dazu verleiten soll, Zugriff auf vertrauliche Daten, wie beispielsweise Zugangsdaten, zu erhalten.
- Social Engineering, wo der Empfänger so manipuliert wird, dass dieser beispielsweise vertrauliche Produktinformationen heraus gibt oder eine Finanztransaktion freigibt.
- Die Installation von Malware, die ohne Wissen des Nutzers im Hintergrund vertrauliche Informationen abgreift oder Systeme beschädigt.
- Angriffe auf Web-Applikationen, um beispielsweise Kundendaten oder andere sensible Daten zu gewinnen.

Hinweis
Die Cyber-Versicherung prüft im Schadenfall, ob und in welcher Höhe der Kunde schadenersatzpflichtig gemacht werden kann und wehrt unberechtigte Ansprüche ab.

Um welche Leistungen kann ich den Versicherungsschutz individuell erweitern?

- Sofort-Analyse durch einen erfahrenen IT-Experten
- Sofort-Maßnahmen zur Schadensbegrenzung durch ein IT-Team
- ofern möglich Wiederherstellung der Daten und Systeme
- Krisen- und PR-Beratung, um gegenüber Kunden den Vorfall professionell einzuordnen
- Kompensation der Umsatzverluste der durch die Cyber-Attacke verursachten Betriebsunterbrechung
- Übernahme von Schadensersatzansprüchen bei der Verletzung von Persönlichkeitsrechten

Wann habe ich keinen Versicherungsschutz?

Die Cyber-Versicherung kommt beispielsweise nicht für Schäden auf, die von Mitarbeitenden, z. B. Geschäftsführern, Inhabern oder Vorständen, vorsätzlich herbeigeführt wurden.

Info
Diese Aufzählung beinhaltet wesentliche Leistungsausschlüsse und ist nicht abschließend. Sofern einzelne Leistungspunkte für Sie wichtig sind, prüfen wir gerne Sondertarife.

Schadenbeispiele - welche Kosten werden erstattet?

- Ein in einer E-Mail versteckter Trojaner sperrt den Zugriff auf das Intranet und es wird eine Lösegeld-forderung gestellt.

- Nach einer Cyberattacke sind alle Rechner der Mitarbeiter infiltriert und müssen komplett neu aufgesetzt werden, um die Arbeit wieder aufnehmen zu können.

- Es besteht der Verdacht eines Hackerangriffs. Es wird vom Cyber-Versicherer ein Forensik-Dienstleister vermittelt, um eine Bedrohungsanalyse, die Untersuchungen auf Manipulationen im Filesystem, die Analyse der Netzwerkverbindungen und eine Risikoabschätzung vorzunehmen.