Cyber-Versicherung

Warum Cyber-Versicherung?

Hackerangriffe und Datendiebstahl-Delikte steigen erschreckend stark an und treffen immer häufiger auch kleinere Unternehmen. Die finanziellen Folgen von Cyberkriminalität können sehr schnell existenzbedrohende Ausmaße für Unternehmen und Selbstständige annehmen.

Jeder, der geschäftlich mit vertraulichen Daten umgeht – seien es eigene oder die von Vertragspartnern – sollte sich und sein Business mit einer darauf zugeschnittenen Versicherung gegen Cyber-Risiken und Internetkriminalität absichern. Die Cyber-Versicherung bietet genau diese Sicherheit und deckt finanzielle Risiken ab, die durch Cyberattacken und Datenschutz-Verletzungen auf Sie zukommen könnten.

Beschreibung:

In der Cyber-Versicherung ist sowohl eine umfassende Versicherung möglicher Eigenschäden mitenthalten als auch eine Haftpflichtversicherung zur Absicherung bei Ansprüchen von dritter Seite (Fremdschaden) inklusive Verletzung von geistigem Eigentum/Persönlichkeitsrechten.

Eigenschadenversicherung – Abdeckung intern entstandener Schäden, Kosten und Aufwendungen durch:

- Wiederherstellung von Daten und Systemen nach Hackerangriff
- Betriebsstillstand nach Hackerangriff
- Verlust physischer Datenträger mit vertraulichen Daten wie Laptop, Smartphone, Festplatte
- Krisenmanagement und PR-Maßnahmen nach Hackerangriff

Cyber-Haftpflichtversicherung – bei Ansprüchen Dritter (Fremdschaden) Schadenersatzansprüche (Vermögensschäden) aufgrund:

- eines Verstoßes gegen gesetzliche sowie ggf. vertragliche Bestimmungen/Verpflichtungen zum Datenschutz
- eines Verstoßes gegen Geheimhaltungspflichten
- der Weitergabe eines Virus
- einer Persönlichkeitsrechtsverletzung nach Hacker-Angriff

Schadenbeispiele:

Datenklau im E-Commerce:
Ein mittelständisches Unternehmen ist im Onlinevertrieb Opfer von Datenklau geworden. Über mehrere Wochen konnten sich Hacker rechtswidrigen Zugang zu dem eigentlich streng gesicherten online-basierten Abrechnungssystem für Bezahlkarten verschaffen (Payment Processing Tool). Während dieser Zeit konnten die Hacker über rund 100.000 Kundendaten kopieren und unrechtmäßig nutzen. Das Schadenausmaß ist sowohl finanziell als auch reputationsmäßig immens:

- Forensische Dienstleistungen 15.000 €
- Rechtsberatung und Rechtsbeistand 35.000 €
- Gesetzliche Informationspflichten 25.000 €
- Media- und PR-Arbeiten 19.500 €
- Geltend gemachter Vermögensschaden der Payment Card Industry 495.000 €
- Versicherte Gesamtkosten 589.500 €

Manipulation eines Kartenlesers:
Unbekannte manipulierten die Kartenleser eines Restaurants. Dies ermöglichte den Hackern Daten von 700 Kunden abzugreifen. Dem Unternehmen entstand dadurch ein Millionenschaden.

Denial-of-Service-Attacke:
Ein Online-Shop wurde Opfer einer Denial-of-Service-Attacke. Der Online-Shop war 23 Stunden für Kunden nicht verfügbar. Daraus folgte:

- Plötzlicher Anstieg des eingehenden Datenflusses
- Allmähliche Überlastung führt zur Nichtverfügbarkeit der Website
- Als Gegenmaßnahme wurde der eingehende Datenfluss mit Hilfe des Internetanbieters analysiert und gefiltert, um böswillige Datenbewegungen von der normalen Geschäftsaktivität abzugrenzen
- Schrittweise Rückkehr zur normalen Geschäftstätigkeit

Kontakt
3 Banken Versicherungsmakler Gesellschaft m.b.H. – Innsbruck, Linz, Wien, Klagenfurt, Graz
Dr. Josef Riedl T +43 664 805563 597, josef.riedl@3bvm.at
Stefan Straif T +43 664 805563 591, stefan.straif@3bvm.at
Bernhard Prenn T +43 664 805563 598, bernhard.prenn@3bvm.at
Uwe Kalsberger T +43 664 805563 594, uwe.kalsberger@3bvm.at