



Checkliste: Risikobewertung Cyber-Risk

Diese Checkliste liefert Anhaltspunkte dafür, wie groß die Cyber-Risiken für Ihr Unternehmen aus Sicht einer Versicherung ausfallen. Versicherungsgesellschaften legen anhand solcher Kriterien die Versicherungskosten fest. Genaue Zahlen werden Sie in diesem kleinen Papier nicht finden, dafür ist dann doch eine individuelle Bewertung erforderlich. Aber eine Tendenz sollte deutlich werden.

Für konkrete Auskünfte oder weitere Informationen können Sie uns einfach anrufen (030 863 926 990) oder eine [E-Mail](#) schreiben.

Einen Antrag auf Cyber-Versicherung können Sie auch direkt auf unserer Website stellen: www.acant-makler.de.

Potenziell risikoerhöhende Faktoren:

1. Online-Umsätze und Online-Zahlssysteme

- Ihr Unternehmen erwirtschaftet zehn Prozent des Umsatzes oder mehr im Internet.
- Ihr Unternehmen verarbeitet mehr als 25.000 Datensätze an Kreditkartendaten und/oder EC-Kartendaten im Jahr.
- Ihr Unternehmen ermöglicht Kreditkartenzahlung, ohne dass die PCI-Standards eingehalten werden oder musste in den letzten fünf Jahren bereits einmal Bußgelder wegen Verstöße gegen die PCI-Standards bezahlen.

2. Regionale Faktoren

- Ihr Unternehmen erwirtschaftet einen signifikanten Anteil der Umsätze in den USA / Kanada oder erbringt regelmäßig Leistungen an Kunden in dieser Region.
- Ihr Unternehmen hat Standorte außerhalb der EU.

Frank Schwandt - acant.service GmbH

030 863 926 990
0176 10318791
fs@acant-makler.de
www.acant-makler.de



acant
service GmbH
Versicherungsmakler

3. Frühere Vorfälle

- Ihr Unternehmen wurde in den letzten fünf Jahren Opfer einer Cyberattacke, einer Havarie oder eines Datenschutzverstößes, und im Zusammenhang damit ...
 - wurde ein Ermittlungs- oder Auskunftverfahren gegen Sie eröffnet.
 - wurden Schadensersatzansprüche gegen Sie gestellt.
 - hat Ihr Unternehmen finanzielle Verluste erlitten.
- In den letzten fünf Jahren wurde Ihr Unternehmen Opfer einer Cyber-Erpressung.
- In den letzten fünf Jahren musste Ihr Unternehmen Bußgelder aufgrund von Datenschutz-Verstößen oder mangelhafter PCI-Compliance (vgl. oben) zahlen.
- In den letzten fünf Jahren musste Ihr Unternehmen Bußgelder oder Entschädigungen aufgrund von Rechteverletzungen in der digitalen Kommunikation bezahlen (z. B. Spam-E-Mails oder Urheberrechtsverletzungen).

Potenziell risikomindernde Faktoren:

1. Technische Maßnahmen:

- Ihre IT-Abteilung hat eine Security Policy ausgearbeitet und implementiert, deren Einhaltung überwacht wird.
- Es erfolgt eine regelmäßige Datensicherung nach festgelegtem Plan. Die Backups werden getrennt von den Quelldaten gespeichert.
- Die technischen Maßnahmen zur Sicherung von Daten und Rechnernetz wie Virens Scanner, Firewall, Passwortschutz etc. sind implementiert, auf dem Stand der Technik und werden regelmäßig aktualisiert.
- Die verwendete Software wird regelmäßig durch die Patches und Programmaktualisierungen der Hersteller aktuell gehalten.

Frank Schwandt - acant.service GmbH

030 863 926 990
0176 10318791
fs@acant-makler.de
www.acant-makler.de



acant
service GmbH
Versicherungsmakler

2. Organisatorische Maßnahmen

- Es gibt klare und verbindliche Regeln für das Access Management / Rights Management.
- Es gibt klare und verbindliche Regeln zum Einsatz von Verschlüsselung, Passwortschutz und zur Trennung von privater und betrieblicher Nutzung der IT-Ressourcen.
- Es gibt klare und verbindliche Regeln zum Umgang mit personenbezogenen Daten – sowohl von externen Personen wie von Unternehmensangehörigen.
- Es existiert ein ausgearbeiteter IT-Notfallplan, mit dem die Mitarbeiter vertraut sind.
- Serverräume und andere relevante Technik sind durch Zugangskontrollen und andere Schutzmaßnahmen auch physisch vor Manipulation geschützt.