Cyber-
Versicherung

Dittmeier
Versicherungsmakler

Cyber-Versicherung gegen Computer-Kriminalität

Cyber-Kriminalität kann überall stattfinden, wo Computer, Smartphones und andere IT-Geräte genutzt werden. Praktisch alle digitalisierten Prozesse im Verkehrsbetrieb können betroffen sein, besonders dann, wenn eigene Daten und solche von Vertragspartnern verarbeitet werden. 100%ige Sicherheit gibt es trotz Virenprogrammen und Firewall nicht – lagern Sie deswegen das Restrisiko auf eine Cyber-Versicherung aus! Die Cyber- bzw. IT-Versicherung schützt Ihren Betrieb vor den Kosten durch Schäden an Computersystemen bei technischen Defekten, kriminellen Angriffen von außen (egal ob gezielt oder ungezielt) oder Untreue der eigenen oder ehemaligen Mitarbeiter. Außerdem sind auch Verstöße gegen die die EU-DSGVO im Versicherungsschutz enthalten.

Die Cyber-Versicherung deckt die wichtigsten Gefahren

Beispiele für versicherte Gefahren:

- Hacker-Angriffe
- Schäden durch Schadeprogramme (z. B. Viren, Trojaner)
- Gezielte und ungezielte (zufällige) Angriffe
- Erpressung
- Datenrechtsverletzungen nach EU-DSGVO
- Bedienfehler der Mitarbeiter
- Betrug durch Pishing
- ... und vieles mehr

Jeder Verkehrsbetrieb ist gefährdet

Die Übersicht zeigt, in welchen Bereichen Sie Gefahren von Hackern, egal ob absichtlich oder zufällig, ausgesetzt sind.

E-Mail
Sie nutzen beruflich E-Mails

Surfen im Internet
Ihre Mitarbeiter nutzen das Internet

Öffentliches WLAN
Sie nutzen öffentliche WLAN-Netzwerke außerhalb des Büros

Eigene Webseite
Sie haben eine eigene Webseite

Hardware
Sie und Ihre Mitarbeiter nutzen Geräte wie USB-Stick, Funkmaus oder Laptop

Social Media
Facebook oder Twitter können in Ihrem Unternehmensnetzwerk aufgerufen werden

Datenbank
Ihre Kundendaten sind in einer zentralen Datenbank gespeichert

Telefon
Sie nutzen das Telefon zur Erteilung oder Annahme von Aufträgen

Umfang einer Cyber-Versicherung

Die Cyber-Versicherung deckt folgende Bereiche:

Eigenschäden	✓ Kosten der Datenwiederherstellung und System-Rekonstruktion ✓ Wirtschaftliche Schäden durch Betriebsunterbrechung
Drittschäden	✓ Schadenersatzforderungen von Kunden wegen Datenmissbrauch und/oder Lieferung ✓ Entschädigung berechtigter und Abwehr unberechtigter Forderungen
Serviceleistungen	✓ IT-Forensik-Experten zur Analyse, Beweissicherung und Schadenbegrenzung ✓ Anwälte für IT- und Datenschutzrecht zur Erfüllung der Informationspflichten ✓ PR-Spezialisten für Krisenkommunikation zur Eindämmung des Imageschadens

Die Angst vor Cyberattacken wächst

Es kann jeden jederzeit treffen. Deutschland ist ein großer Markt für Cyberkriminelle, welche gerne die kleinen, mittelständischen und nicht nur die großen Unternehmen aus Deutschland angreifen. Ziel ist es hierbei, an möglichst viel Geld heranzukommen – z. B. durch Erpressung oder Verschlüsselung der sensiblen Daten oder Ausspionierung der Kundendaten.

Jedes vierte mittelständische Unternehmen in Deutschland ist bereits Opfer eines Angriffs auf die eigene IT-Infrastruktur geworden – Tendenz steigend. Ob sogenannte Denial-of-Service-Attacken, die ganze IT-Infrastrukturen lahmlegen, Betrugsmaschen wie „Fake President" oder der Missbrauch sensibler Daten durch ausgeschiedene Arbeitnehmer – die IT-Landschaft ist ein Einfallstor für Kriminelle, die den unternehmerischen Erfolg bedrohen.

Weiteres Risiko durch die EU-DSGVO

Als Verkehrsbetrieb verwalten Sie viele Daten Ihrer Kunden und das bedeutet: Für alle Unternehmen, die personenbezogene Daten verarbeiten, gilt seit 2018 die EU-Datenschutz-Grundverordnung (EU-DSGVO). Im Falle von Verstößen gegen die EU-DSGVO drohen Firmen Bußgelder seitens der Datenschutzbehörden bis zu 20 Mio. Euro bzw. 4 % des gesamten Jahresumsatzes.

Gerade deshalb ist es wichtig, sich um die IT-Sicherheit im Unternehmen zu kümmern und sich vor den finanziellen Folgen eines Schadens zu schützen. Wenn z. B. Kundendaten von Ihrem Server gestohlen werden, müssen Sie alle möglicherweise betroffenen Kunden sofort und umfänglich darüber informieren. Geschieht dies nur zögerlich oder verspätet, haften Sie gegenüber jeder Person, der wegen eines Verstoßes gegen diese Verordnung ein Schaden entstanden ist.

Schadenbeispiele einer Cyber-Versicherung:

E-Mail
- Spionage
- Kontozugriff
- Erpressung

Surfen im Internet
- Spionage
- Kreditkarten-missbrauch

Öffentliches WLAN
- Spionage
- Erpressung

Eigene Webseite
- Infizierung
- Erpressung

Hardware
- Spionage
- Erpressung

Social Media
- Spionage
- Erpressung

Datenbank
- Spionage
- Erpressung
- Bedienungsfehler

Telefon
- Spionage
- Kontozugriff
- Erpressung

Fragebogen für ein Angebot

Der Abschluss einer Cyber-Versicherung und die Annahme durch den Versicherer erfordert eine Risikoprüfung, denn ein gewisser Eigenschutz ist unerlässlich. Bitte beantworten Sie daher folgende Fragen so gut wie möglich.

	Ja	Nein
Wie hoch war Ihr Vorjahresumsatz? _____ €		
Beläuft sich der Anteil Ihres Online-Umsatzes auf maximal 25% des Gesamtumsatzes (Online-Umsatz gilt als solcher, wenn er über die eigene Firmenwebsite erzielt wird)?	☐	☐
Der jährliche Umsatz in den USA und Kanada beträgt max. 25%, aber höchstens 500.000 € (nur direkter Umsatz, keine Tochterunternehmen)?	☐	☐
Werden von Ihnen Unternehmensrichtlinien in Bezug auf Datensicherheit, Datenschutz und Umgang mit Firmeneigentum durchgesetzt, die von allen Personen befolgt werden müssen, die Zugriff auf Ihr Netzwerk oder auf Ihnen anvertraute sensible Daten haben?	☐	☐
Wird in all Ihren ITK-(Informations- und Kommunikations-)Systemen Folgendes regelmäßig aktualisiert/aufgespielt/vorgenommen? · Aktualisierung von Anti-Viren-Programmen? · Aktualisierung der Firewalls? · Aufspielung von Patches (Korrekturauslieferungen für Software, zur Schließung von Sicherheitslücken)? · Erneuerung der Contentfilter (z.B. zur Sperrung von illegalen Websites in Ihrem Unternehmensnetzwerk)? · Datensicherung (Back-Up) Ihrer Netzwerkdaten und Konfigurationsdateien (mindestens 1x wöchentlich)?	☐	☐
In den letzten 5 Jahren kam es zu keiner Inanspruchnahme durch einen Dritten bzw. zu keinem Schaden (z. B. finanzielle Verluste, Betriebsunterbrechungsschaden) oder zu keiner Straf-/Bußgeldzahlung z. B. aufgrund eines/einer · Verletzung/Verstoßes gegen die Netzwerksicherheit entstandenen elektronischen Diebstahls · Netzwerk- oder Dateischadens · Rechtsstreits in Bezug auf Inhaltsverletzungen · Verletzung der Privatsphäre · Identitätsdiebstahl/Urheberrechtsverletzung · Denial of Service (DoS) - oder Distributed Denial of Service (DDoS)-Attacke · Computerviruskontamination/Virenbefalls · Diebstahls von Informationen · Beschädigung von Netzwerken Dritter · Umstandes, dass Dritte nicht auf Ihr Netzwerk zugreifen konnten oder aufgrund vergleichbarer Vorfälle	☐	☐
Sie bearbeiten, speichern oder übermitteln im Jahr nicht mehr als 20.000 Kreditkartendaten?	☐	☐
Sie bestätigen hiermit, dass Sie die Standards gemäß PCI DSS einhalten?	☐	☐

Absender Firma: _____

Ansprechpartner: _____

Telefon: _____ E-Mail: _____

_____

Datum/ggf. Unterschrift

Ihr Ansprechpartner für weitere Informationen:

Thomas Adamik, Telefon +49 (0)931 98 00 70-83,
E-Mail: thomas.adamik@dittmeier.de

Dittmeier Versicherungsmakler GmbH

Kaiserstraße 23-25 · 97070 Würzburg
Telefon +49 (0)931 98 00 70-0
Telefax +49 (0)931 98 00 70-583
E-Mail info@dittmeier.de
Internet www.dittmeier.de

AV-A-2161-1.0-15.07.19