

Was passiert – wenn Ihre IT stillsteht?

Tag für Tag sind Unternehmen jeder Größe und aller Branchen Cyberangriffen ausgesetzt: Mal werden Kundendaten gestohlen, mal Systeme lahmgelegt. Als Ihr Partner für den Erfolg tragen wir dazu bei, dass Sie für solche Attacken gewappnet sind. Und bieten Ihnen nicht nur finanziellen Schutz für hohe Vermögens- oder Sachschäden, die häufig aus Cyberattacken resultieren. Zusammen mit IT-Spezialisten leisten wir auch schnell und unbürokratisch Hilfe im Schadensfall, damit Ihr Unternehmen durch eine Betriebsunterbrechung nicht in eine existenzbedrohende Lage gerät.



CyberRisk Versicherung

- › „Echte Schadenbehebung“ über eine Direktverbindung des Versicherungsnehmers mit unserem Dienstleister online und vor Ort – **24 Stunden / 7 Tage die Woche**
- › **5-fache Versicherungssumme** bei zielgerichtetem Angriff (maximal 500.000 EUR)
- › Ersatz von Schäden durch **Betriebsunterbrechung** ohne Sublimit
- › Übernahme der Kosten der **Wiederherstellung von Daten und Programmen** ohne Sublimit
- › „Bring your own device“: Versicherung von Unternehmensdaten auf dienstlich genutzten Privatgeräten



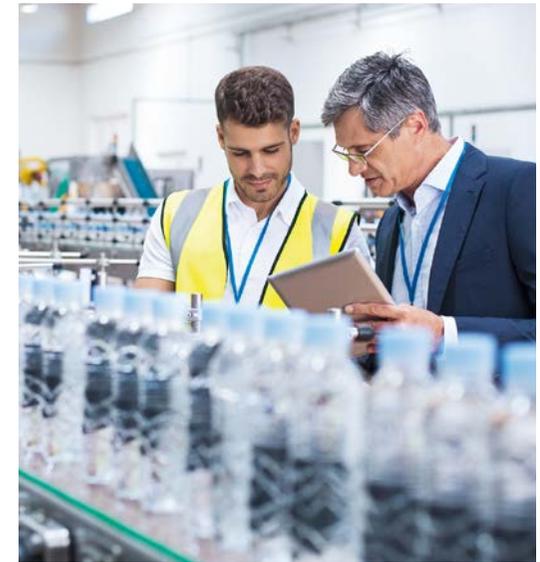
Versicherung gegen Wirtschaftskriminalität

- Die Vertrauensschadenversicherung schützt vor den Folgen krimineller Handlungen im Geschäftsverkehr eines Unternehmens. Im Rahmen des Grundbausteins **Wirtschaftskriminalität** sind u.a. auch über das Tatwerkzeug Internet
- › **Straftaten von Dritten**, z. B. durch
 - Vorspiegelung einer falschen Identität (Fake-President),
 - Nutzung einer fremden Identität (Fake-Identity) oder
 - Umleitung von Zahlungsströmen (Payment-Diversion),
 - oder
 - › **interne Straftaten** (Diebstahl, Untreue, Unterschlagung) versichert.



D&O-Versicherung

- › Absicherung der Geschäftsleitung, u. a. bei vorwerfbaren organisatorischen Mängeln, bei Lücken in der Überwachung des Geschäftsbetriebs oder der Auswahl ungeeigneter Mitarbeiter, z. B. durch
 - unzureichende Regelungen bei der Vergabe von Administrator- und Zugriffsrechten, beim Passwortschutz oder der Datensicherung
 - nicht vorhandene Vorkehrungen gegen menschliches Fehlverhalten (Übertragung falscher/geheimer Daten etc.), z. B. durch 4-Augen-Prinzip
 - fehlenden Schutz gegen technisches Versagen (Notstromversorgung, redundante Systeme, Versicherungen etc.)
- › Abwehrschutz bei Vorsatzvorwurf, z. B. auch bei Verstößen gegen Datenschutzvorschriften
- › Unbegrenzte Rückwärtsdeckung (für unbekannte Pflichtverstöße vor Vertragsbeginn)



Ihre Vorteile

- ✓ **Assistance-Dienstleistung**
- ✓ **Absicherung der Restrisiken**
 - Kosten
 - Betriebsunterbrechung
 - Drittschaden

Mindestvoraussetzungen (CyberRisk)

- › Funktionierende Datensicherung
- › Virenschanner und Firewall
- › Lizenzmanagement (zeitnahe Sicherheits-Updates)
- › Keine Admin-Rechte für Benutzer für die tägliche Arbeit

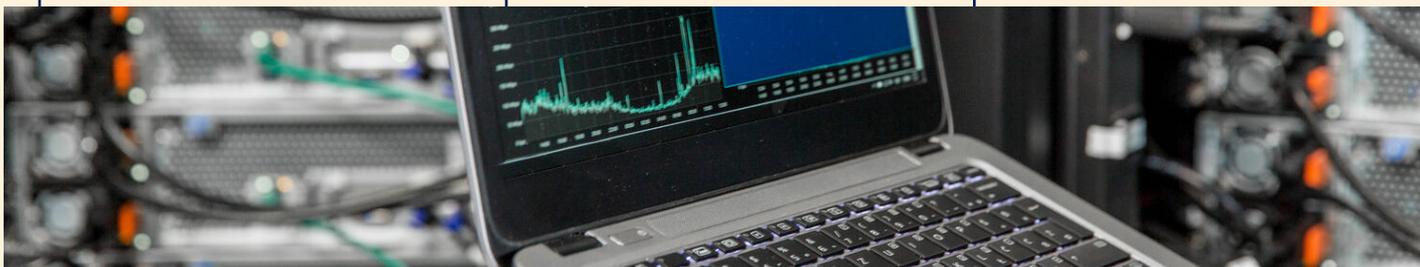
Die Frage ist nicht ob, sondern wann Sie eine Cyber-Attacke trifft.

Ein Hackerangriff auf die Systeme Ihres Unternehmens kann weitreichende Folgen nach sich ziehen. Neben den Kosten der Datenwiederherstellung und Software-Reinstallation drohen Ihrem Unternehmen Gewinnausfälle durch Betriebsunterbrechung. Aufwände für die Benachrichtigung gemäß Bundesdatenschutzgesetz sowie die Rechtsverfolgung können weitere Folgekosten der Cyber-Attacke darstellen. Wir kommen für den finanziellen Schaden auf und ersetzen Ihrem Unternehmen sämtliche mit dem Hackerangriff verbundenen Kosten.



Schadenbeispiel: Virus befällt IT

- 1 Eine vermeintliche Kunden-E-Mail schleuste einen Virus in die Systeme eines Unternehmens ein.
- 3 Folgen des Systemzusammenbruchs: Bestellungen, Auftragsvergabe, Rechnungserstellung und Kommunikation waren nicht mehr möglich.
- 5 Die Abarbeitung der Kundenanfragen und Fertigstellung der Aufträge erforderten den Einsatz aller Mitarbeiter am folgenden Wochenende.



- 2 Der Virus führte zur Zerstörung der Daten auf dem Server. Das Netzwerk des Unternehmens wurde heruntergefahren. Die IT war nicht mehr verfügbar.
- 4 Von R+V vermittelte IT-Spezialisten stellten das Netzwerk und die Daten innerhalb von drei Tagen wieder her.
- 6 **R+V kam im Rahmen der CyberRisk Versicherung für alle Kosten auf.**

Schadenbeispiel: Fehlkonfiguration Website

Durch eine versehentlich fehlerhafte Konfiguration der Website konnten zehn Zimmer eines Hotels vier Wochen lang doppelt gebucht werden.

Als ein Gast einchecken wollte, wurde die Überbuchung bemerkt. Eine Prüfung der Systeme ergab, dass aufgrund der Doppelbuchungen im Folgemonat sechs Gäste pro Nacht in einem anderen Hotel untergebracht werden mussten.

Die entstandenen Mehrkosten wurden dem Hotel im Rahmen der CyberRisk Versicherung erstattet.

Systematische und umfassende Beratung

Als Unternehmer tragen Sie nicht nur für Ihren Betrieb Verantwortung, sondern auch für Ihre Mitarbeiter, Ihre Kunden und für sich selbst. Deshalb beraten wir Sie gerne ganzheitlich und gehen dabei systematisch vor: Zunächst ermitteln wir, welchen konkreten Risiken Sie in den verschiedenen Handlungsfeldern ausgesetzt sind, und beziehen dabei auch Branchenspezifika mit ein. In einer ganzheitlichen Risikoanalyse stellen wir Ihre aktuellen Risiken heraus und zeigen Ihnen auf, welche Lösungen wir zu Ihrer Risikoabsicherung anbieten können.



Damit Sie im Schadensfall handlungsfähig bleiben!



IT-Sicherheit – Chefsache mit vielen Aspekten

- ✓ Gesamtverantwortung
- ✓ Persönliche Haftung
- ✓ Strafrecht
- ✓ Störung des Betriebsfriedens
- ✓ Daten und Programme
- ✓ Haftung des Unternehmens
- ✓ Handlungsfähigkeit
- ✓ Cyberkriminalität
- ✓ Wirtschaftskriminalität



Lassen Sie sich ganzheitlich und bedarfsgerecht beraten. Jetzt Termin vereinbaren!