Risikoschutz

Das Plus für mehr Datensicherheit.
Unsere Cyber-Versicherung.

Unsere Cyber-Versicherung: die richtige Wahl für Unternehmen mit Informations- und Kommunikationstechnik.

Die Cyber-Versicherung schützt Unternehmen nicht nur vor den wirtschaftlichen Folgen von IT- und Cyberrisiken. Im Schadenfall stehen Ihnen über unsere Experten-Hotline IT-Spezialisten an Ihrer Seite und leisten Ihnen schnelle und unbürokratische Hilfe. Selbst wenn sich herausstellt, dass es sich um kein ersatzpflichtiges Ereignis handelt, ist dieser Service für Sie kostenfrei. Gemeinsam mit Ihnen leiten sie die notwendigen Maßnahmen ein.

Was ist versichert?

- Im Schadenfall schnelle und unbürokratische Hilfe über unser Cyber-Service-Telefon, 24 Stunden am Tag, 7 Tage die Woche (Forensiker)
- Übernahme der Kosten für Ursachenermittlung, Behebung der Schadenursache und Rekonstruktion von Daten und Systemen nach einem Hackerangriff
- Mitversicherung von Mehrkosten und Ertragsausfällen aufgrund Betriebsunterbrechung

Highlights unserer Cyber-Versicherung:

- ✓ Verzicht auf den Erfüllungsschadenausschluss
- ✓ Zeitlich unbegrenzte Rückwärtsversicherung
- ✓ „Fake President“ (Täter gibt sich als Geschäftsführer aus) nach einer Informationssicherheitsverletzung mitversichert

Optional: Schutz vor den finanziellen Folgen einer Cyber-Erpressung auf Anfrage abschließbar.

W&W württembergische

Ihr Fels in der Brandung.

Unsere Cyber-Versicherung. Beispiele aus der Praxis.

Beispiel: Telefonanlage.
Kriminelle Angreifer drangen in die Telefonanlage eines Mittelständlers mit 150 Beschäftigten ein. Sie fischten dort aber weder Daten ab, noch versuchten sie Firmengeheimnissen abzuhören – sondern sie telefonierten. Die Hacker riefen besonders teure Nummern an, möglicherweise eigens dafür geschaltete gebührenpflichtige Dienste. Der Gesamtschaden zeigte sich auf der Telefonrechnung: in kürzester Zeit hatten die Eindringlingen 60.000 Euro vertelefoniert.

Beispiel: Arztpraxis.
In einer Arztpraxis geriet über einen geöffneten E-Mail-Anhang eine aggressive Schadsoftware ins System. Um Patientendaten zu schützen wurde das gesamte System heruntergefahren. Der laufende Betrieb in der Praxis wurde per Hand weitergeführt und Patienten wurden nach Hause geschickt und Behandlungen mussten abgesagt werden. Zudem wurden Datensätze mit Patientendaten entwendet. Gesamtschaden ca. 20.000 Euro.

Beispiel: Datendiebstahl.
Ein von der Ukraine, Weißrussland und Afrika aus operierender Betrüger-Ring drang ins Kassensystem eines renommierten Restaurants ein und spionierte über Monate die Kreditkartendaten von wahrscheinlich bis zu 400 Gästen aus. Für den Wirt war der Schaden enorm: rund 115.000 Euro hat ihn die Cyber-Attacke gekostet, denn er musste einen hoch spezialisierten IT-Forensiker kommen lassen, der eine Woche lang nach dem Virus suchte. Außerdem musste er ein komplett neues Kassensystem anschaffen.

Beispiel: Website.
Die Webseite einer Gaststätte wurde von Hackern so verändert, dass statt eines mondänen Restaurant-Bildes die Innenansicht eines in die Jahre gekommenen Fast-Food-Restaurants gezeigt wurde. Die Löschung und Wiederherstellung der Website kostet 3.500 Euro. Der Reputationsverlust ist nicht abschätzbar.

Beispiel: Daten in Geiselhaft.
Ein Trojaner verschlüsselte den Zugang zum IT-System und die eigene Website eines Sanitär-Installateurs. Der Inhaber bekam das Angebot, die Verschlüsselung gegen Zahlung eines fünfstelligen Betrags wieder aufzuheben. Das Unternehmen schaltete einen Computerfachmann und die Polizei ein. Der Gesamtschaden betrug 42.000 Euro.

Beispiel: Online Shop.
Ein Online Shop wurde Opfer einer Cyber-Attacke. Als folge war der Shop fast 48 Stunden nicht verfügbar. Der Schaden belief sich auf fast 200.000 Euro.

Beispiel: Payment Provider.
Ein Handelsunternehmen wickelt die Zahlungen des online Shops über einen zertifizierten Payment Provider ab. Bei diesem kam es zu einer Cyber-Attacke. Grundsätzlich haftet der Payment Provider, aber der Shop Betreiber hatte dennoch immense Aufwände und Kosten: Sicherheitsüberprüfungen, Information an die Kunden, Umsatzausfälle und Reputationsschäden.

Beispiel: Produktions-/Industrieanlagen.
Hacker hatten die vollautomatisierte Produktionsstraße eines deutschen Nahrungsmittelherstellers manipuliert und die Einstellungen zur Beigabe von Gewürzen verändert. Die betroffene Produktionscharge war unbrauchbar, erhebliche Rechercheaufwände und Kosten durch den Ertragsausfall entstanden. Der Schaden belief sich auf 130.000 Euro. Die Motive der unbekannten Angreifer liegen bis heute im Dunkeln.

Versicherungsumfang.

Versichert ist die Informationssicherheitsverletzung. Dazu gehören:

1. Verletzungen der Netzwerksicherheit durch

- eine Übermittlung von Schadsoftware (Malware, wie z. B. Viren, Trojaner etc.)
- einen Denial-of-Service-Angriff
- eine Verhinderung des autorisierten Zugangs Dritter zu Ihren Daten
- eine unberechtigte Aneignung von Authentifizierungsinformationen (Zugangscodes, Passwörter)
- Computersabotage (§303b StGB)
- eine unberechtigte Veränderung oder Löschung von gespeicherten Daten
- einen Diebstahl oder einen Verlust von IT-Systemen
- eine unberechtigte Veröffentlichung oder Weitergabe von Daten Dritter durch Mitarbeiter

2. Verletzung datenschutzrechtlicher Bestimmungen

3. Verletzung der Datenvertraulichkeit von Daten Dritter

4. Verletzung der Informationssicherheit durch die „Fake President-Methode“ (Betrug Mithilfe von Informationstechnologie)

Was ist konkret versichert?

Im Falle einer Informationssicherheitsverletzung kann eine Entschädigungsleistung aus folgenden Bausteinen erfolgen:

Haftpflicht

- Schadenersatzansprüche Dritter wegen eines Vermögensschadens
- Haftungsfreistellung bei Datenverarbeitung durch Dritte
- Rechtsverteidigungskosten bei strafrechtlichen Ermittlungs- und Ordnungswidrigkeitenverfahren
- Ansprüche der Payment Card Industry einschließlich Vertragsstrafen
- Haftung bei Weitergabe eines Computervirus an Dritte
- Ansprüche wegen unrechtmäßiger Kommunikation/Veröffentlichung von digitalen Medieninhalten
  - Verletzung von Patenten, Markenrechten, Urheberrechten
  - Plagiat, widerrechtliche Verwendung oder Diebstahl von Ideen oder Informationen oder missbräuchliche Verlinkung
  - Rufschädigung
  - Verletzung des Persönlichkeitsrechts einer Person
  - Veröffentlichung von Informationen aus der Privatsphäre
  - Kommerzielle Verwendung des Namens
  - Verletzung des Wettbewerbsrechts

Eigenschaden

Datenschaden

- Maschinelle Wiedereingabe von Daten aus Sicherungsdatenträgern
- Wiederbeschaffung/Wiedereingabe von Stamm- und Bewegungsdaten
- Wiederbeschaffung/Wiedereingabe von Betriebssystemen und Standardprogrammen
- Wiedereingabe von individuell hergestellten Programmerweiterungen
- Kosten durch Kopierschutzstecker oder Verschlüsselungsmaßnahmen (Lizenzerwerb)

Mehrkosten- und Ertragsausfall

- Mehrkosten und Ertragsausfall, die im Zeitraum der Betriebsunterbrechung entstehen

Kosten

Forensik-Kosten (Kosten für Ursachenermittlung)

- Feststellung ob eine Informationssicherheitsverletzung vorliegt
- Ermittlung der Ursache der Informationssicherheitsverletzung
- Ermittlung des Umfangs der Informationssicherheitsverletzung
- Empfehlung geeigneter Maßnahmen zur Reaktion und künftigen Abwehr auf diese Informationssicherheits-verletzung
- Kostenübernahme auch wenn nach Prüfung kein ersatzpflichtiger Schaden vorliegt
- Verzicht auf SB

Krisenkommunikation, Mediation, Reputationssicherung

- Angemessene und notwendige Kosten für PR- oder Krisenmanagement-Maßnahmen
- Kosten für angemessene Marketingmaßnahmen und Öffentlichkeitsarbeit
- Abwendung einer Rufschädigung und Wiederherstellung der positiven öffentlichen Wahrnehmung durch Beauftragung eines Mediators oder Krisenkommunikationsunternehmens

Informations-/Benachrichtigungskosten Kreditkartenmonitoring

- Kosten für die Benachrichtigung der Betroffenen und der verantwortlichen Datenschutzbehörde
- Kosten für Kreditkartenmonitoring zur Prüfung und Benachrichtigung der Betroffenen

Kosten für den Austausch von Hardware

Elektronischer Zahlungsverkehr

Fehlerhafter Versand von Waren/Warenverluste

Telefonmehrkosten (bspw. unberechtigte Nutzung von gebührenpflichtigen Hotlines)

Nicht versichert sind:

- Personen- oder Sachschäden (mit Ausnahme von versicherten Daten, Programmen, fehlerhaftem Versand von Waren und Austausch von Hardware), kaufmännische Betriebsunterbrechung (Kundenabwanderung)
- Bußgelder

Versicherungssummen

- Kombinierte Haftstrecke für alle versicherten Deckungs-Bausteine
- Mögliche Versicherungssummen (einfache Maximierung): 125.000 €, 250.000 €, 500.000 €, 1 Mio. €, 2 Mio. €

Sublimits (Entschädigungsgrenzen)

- 50% der Versicherungssumme für Kostenpositionen

Laufzeit

- Einjährige Verträge
- Versicherungsjahr entspricht dem Geschäftsjahr
- Versicherungsschutz besteht auch für Versicherungsfälle, die während der Wirksamkeit des Vertrags eintreten (Schadenereignis), deren Ursache aber bereits vor Vertragsbeginn gesetzt und dem Versicherungsnehmer nicht bekannt war.

Betriebsarten, Selbstbehalte und Voraussetzungen.

Betriebsarten

mit einfacher Prüfung

Alle Betriebsarten, sofern nicht als Risiko mit detaillierter Prüfung oder Ausschlussrisiko definiert und Umsatz bis 5 Mio. €

mit detaillierter Prüfung

Risiken ab einem Gesamtumsatz von 5 Mio. € und Risiken, die aufgrund ihrer Betriebsart einer besonderen Prüfung bedürfen; z. B. Druckerei, Verlag, Werbeagentur, Fotolabor, Film- und Tonstudio, Journalist, Architekt, Ingenieur, Rechts-, Wirtschafts- und Steuerberater, Reisebüro, IT-Dienstleister sofern nicht Softwareentwicklung, Online-Handel (auch teilweise), Versandhandel

Nicht versichert werden

z. B. Krankenhaus, Blutuntersuchungslabor, Softwareentwicklung, Webhoster, Provider, Bank, öffentliche Verwaltung

Selbstbehalt

- Generell 1.000 € für Unternehmen bis zu einem Jahresumsatz von 20 Mio. €/2.500 € für Unternehmen ab einem Jahresumsatz von 20 Mio. €
- Für Ertragsausfall und Mehrkosten zeitlicher Selbstbehalt 12 Stunden
- Der Selbstbehalt wird bei einem Schadenereignis nur einmal in Abzug gebracht. Es zieht der jeweils höhere Selbstbehalt.
- Bei der Nutzung der Experten-Hotline der Württembergischen wird kein Selbstbehalt angerechnet.

Voraussetzungen für den Versicherungsschutz

- Mindestens wöchentliche Datensicherung
  - Getrennte Aufbewahrung
  - Möglichkeit der Rücksicherung
- Übliche, ständig aktualisierte Schutzmaßnahmen und regelmäßige Überprüfung der Rücksicherung gegen die bestimmungswidrige Veränderung/Löschung gespeicherter Daten durch Firewalls, Antivirenprogramme, Zugriffsrechte und unverzügliche Installationen von Updates und Patches
- Prüfung digitaler (Medien-)inhalte vor deren Veröffentlichung
- Bei vom Hersteller nicht mehr gepflegten (supporteten) Systemen, geeignete Sicherungsmaßnahmen treffen, z.B. keine Netzanbindung bei betroffenen Geräten
- Sofern ein IT-Dienstleister eingesetzt wird, werden die genannten Maßnahmen mit dem Dienstleister vertraglich vereinbart.