



Cyber-Versicherung

# Das Plus für mehr Datensicherheit.

Wir bieten Schutz bei Cyber-Attacken.

**W&M** württembergische

Ihr Fels in der Brandung.

## Cyber-Kriminalität – die unsichtbare Bedrohung

Mitarbeiter im Homeoffice, Kundenkommunikation per Videotelefonie und digitale Absatzwege: Die rasanten Entwicklungen der Informations- und Kommunikationstechnik bieten so viele Chancen wie Risiken – branchenübergreifend, über alle Betriebsgrößen hinweg. Sicherheit vor Onlinebetrug und anderen IT-Risiken war nie wichtiger.

### Unsere Lösung: Die Cyber-Versicherung.

- Im Schadenfall schnelle und unbürokratische Hilfe über unser Cyber-Service-Telefon, 24 Stunden am Tag, 7 Tage die Woche
- 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 (Mitversicherung von Verzögerungsschäden)
- ✓ Zeitlich unbegrenzte Rückwärtsversicherung
- ✓ Versicherungsschutz der Daten auch in einer Cloud inkl. Ertragsausfallversicherung
- ✓ **Neu: Kostenloses multimediales Cyber Portal**

### Besonderer Mehrwert – mit unserem Cyber Portal

Der Versicherungsschutz beinhaltet die kostenlose Nutzung unseres multimedialen Cyber Portals. Diese Lernplattform sensibilisiert und schult Mitarbeiter zielgerichtet, nachhaltig und praxisorientiert zu wichtigen Cyberthemen:

- Digitale Kurse mit Lernvideos und interaktiven Prüfungen z.B. zu E-Mail-Sicherheit, sichere Passwörter und Onlinebanking
- Praxisnahe Werkzeuge wie z.B. realistische Phishing-Simulationen
- Moderne Benutzerverwaltung zur Bewertung des Sensibilisierungsgrades
- Motivationsinstrumente durch die Vergabe von Zertifikaten
- Demozugang zum Kennenlernen

# Cyber-Attacken gehören zu den höchsten Risikofaktoren.

Es kann jeden treffen!

## **Beispiel: Telefonanlage.**

Kriminelle Angreifer drangen in die Telefonanlage eines Mittelständlers mit 150 Beschäftigten ein. Sie fischten dort aber weder Daten ab, noch versuchten sie Firmengeheimnisse 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 Eindringlinge 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, 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 System einer Apotheke ein und spionierte über Monate die Daten von wahrscheinlich bis zu 400 Kunden aus. Für den Apotheker 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 eine komplett neue Kundendatenbank erstellen lassen.

## **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 Geiselhaut.**

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: Onlineshop.**

Ein Onlineshop wurde Opfer einer Cyber-Attacke. Als Folge war der Shop fast 48 Stunden nicht verfügbar. **Der Schaden belief sich auf fast 200.000 Euro.**

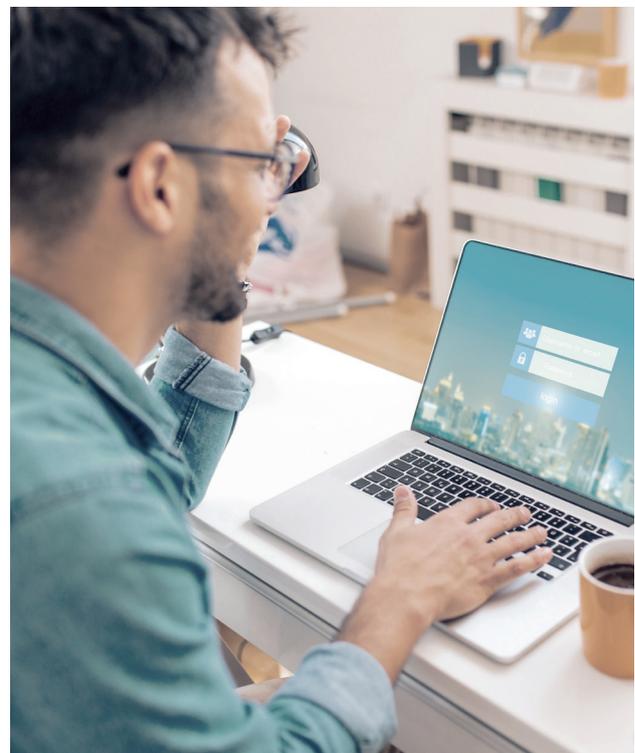
## **Beispiel: Produktions-/Industrieanlagen.**

Hacker hatten die vollautomatisierte Produktionsstraße eines deutschen Nahrungsmittelherstellers manipuliert und die Einstellungen zur Beigabe von Gewürzen verändert. Erhebliche Rechercheaufwände und Kosten durch den Ertragsausfall waren entstanden.

**Der Schaden belief sich auf 80.000 Euro.** Die Motive der unbekanntenen Angreifer liegen bis heute im Dunkeln.

## **Beispiel: Payment Provider.**

Ein Handelsunternehmen wickelt die Zahlungen des Onlineshops 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.**



# Top-Versicherungsleistungen: Cyber-Deckung bei der Württembergischen.

## Versicherungsumfang – **Versichert ist die Informationssicherheitsverletzung:**

---

### 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 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. Einer unbefugten Nutzung von IT Systemen

### 3. Einer Zerstörung und Beschädigung von elektronischen Daten durch einen Bedienfehler an IT-Systemen des Versicherungsnehmers

### 4. Verletzung datenschutzrechtlicher Bestimmungen

### 5. Verletzung der Datenvertraulichkeit von Daten Dritter

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

## Versicherungsleistungen – **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 Ordnungswidrigkeitsverfahren
- 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

#### 1. 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 (Lizenzwerb)

#### 2. 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 Informationssicherheitsverletzung
- Kostenübernahme auch wenn nach Prüfung kein ersatzpflichtiger Schaden vorliegt
- Verzicht auf Selbstbehalt

## 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 IT-Hardware

---

## Elektronischer Zahlungsverkehr

---

## Fehlerhafter Versand von Waren/Warenverluste

---

## Telefonmehrkosten (bspw. unberechtigte Nutzung von gebührenpflichtigen Hotlines)

---

## Kostenloses multimediales Cyber Portal

---

## Nicht versichert sind:

---

- Personen- oder Sachschäden (mit Ausnahme von versicherten Daten, Programmen, fehlerhaftem Versand von Waren und Austausch von IT-Hardware), kaufmännische Betriebsunterbrechung (Kundenabwanderung)
- Bußgelder (mit Ausnahme von Regressansprüchen Dritter infolge der Zahlung von Geldstrafen oder Bußgeldern)

## Versicherungssummen

---

- Kombinierte Haftstrecke für alle versicherten Deckungs-Bausteine
- Mögliche Versicherungssummen (einfache Maximierung): 125.000 €, 250.000 €, 500.000 €, 1 Mio. €, 2 Mio. €, 3 Mio. € und 5 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 (Schadensereignis), 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, Onlinehandel (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.