



- > Firmen und Freie Berufe
- > Cyberversicherung

Reale Sicherheit in der digitalen Welt.

Cyberattacken können den Lebensnerv Ihrer Berufstätigkeit treffen: Aufträge bleiben liegen, weil die IT nicht mehr läuft. Das Vertrauen von Geschäftspartnern ist erschüttert, weil personenbezogene Daten in die Hände Krimineller gelangt sind. Je länger die Arbeitsabläufe unterbrochen sind, desto stärker ist Ihr Geschäftserfolg gefährdet. Deshalb bietet die HDI Cyberversicherung einen weitreichenden Versicherungsschutz und eine professionelle Soforthilfe.

Ihre Fragen – unsere Antworten:

- 1 Was ist abgesichert?**
Die HDI Cyberversicherung schützt Sie vor den Risiken des digitalen Datenverkehrs, z. B. Informationssicherheitsverletzungen, dem Diebstahl personenbezogener Daten, der Verletzung von Betriebs- und Geschäftsgeheimnissen Dritter oder Internet-Attacken auf das betriebliche Netzwerk.
- 2 Warum eine Cyberversicherung?**
Der Versicherungsschutz beinhaltet nicht nur Haftpflichtansprüche Dritter infolge eines IT-Schadens. Auch sogenannte Eigenschäden sind abgesichert, wie z. B. die aufwendige Wiederherstellung verlorener Daten.
- 3 Warum die Cyberversicherung bei HDI?**
Sie werden durch uns und unseren IT-Sicherheitsdienstleister CYRISO (CYRISO Cyber Risk Solutions GmbH, ehemals SEC Consult) von Beginn an aktiv unterstützt – und das in den ersten 90 Minuten ohne Anrechnung auf den Selbstbehalt. Zudem begleiten wir Sie in rechtlichen Fragen bei Datenverstößen.

Ihre Vorteile

- > Cyberschaden-Hotline (24/7/365)
- > Cyber-Sicherheitstraining mit Perseus als obligatorischer Bestandteil
- > Hoch qualifizierter IT-Sicherheitsdienstleister CYRISO
- > Keine versteckten Obliegenheiten
- > Mitversicherung von IT-Systemen und Geräten der Mitarbeiter (Bring Your Own Device)
- > Forensik und Schadenfeststellung, sofern kein Versicherungsfall: 48 Stunden ohne Anrechnung des Selbstbehalts
- > Soforthilfe im Notfall
- > Rückwärtsdeckung für Schäden, die vor Vertragsbeginn eingetreten sind, aber nicht festgestellt wurden.
- > Optionale präventive IT Sicherheits-Checks durch spezialisierten Kooperationspartner
- > **Optionale Deckungserweiterungen** wie Internet-Diebstahl, Cyberspionage und Betriebsunterbrechung als Folge einer DOS-Attacke auf eine entgeltlich genutzte Cloud

Unser Tipp: Unsere Hotline ist rund um die Uhr für Sie da. Schon bei einem vermuteten Cyberangriff kann unser IT-Sicherheitsdienstleister sich auf Ihr System aufschalten oder binnen 24 Stunden vor Ort sein. So finden wir die digitale Schwachstelle schnell und erzielen die bestmögliche Lösung.

Sicherheit und Hilfe – wenn es kritisch wird.

Ein geschütztes Netzwerk sichert sensible Daten und Prozesse. Wenn der Schutz durch den Fehler eines Mitarbeiters oder einen Cyberangriff durchbrochen wird, bietet Ihnen die Cyberversicherung einen zeitgemäßen Schutz. Dies gilt auch für den Fall, dass IT-Systeme mit Schadsoftware infiziert wurden. Geräte Ihrer Mitarbeiter sind in den Versicherungsschutz eingebunden (Bring Your Own Device), soweit eine vertragliche Vereinbarung zwischen Arbeitgeber und Mitarbeiter besteht. Versteckte Obliegenheiten, wie z. B. die „Stand der Technik“-Klausel, gibt es hingegen nicht.

Was beinhaltet die Cyberversicherung?

Eigenschäden

Versichert sind Ihre eigenen Kosten, die durch einen Cyberschaden entstehen, z. B.:

- Rückwärtsdeckung für alle nicht festgestellten Informationssicherheitsverletzungen vor Vertragsbeginn
- Forensik und Schadenfeststellung
- Übernahme der Kosten für maximal 48 Stunden, sofern kein Versicherungsfall vorliegt (Selbstbehalt wird nicht angerechnet)
- Benachrichtigung von betroffenen Dritten und Datenschutzbehörden sowie verbundene Dienstleistungen
- Krisenkommunikation
- Kosten für Datenüberwachungsdienstleistungen
- Schwachstellenanalyse und Empfehlung von Systemverbesserungen
- Systemverbesserungen nach Verletzung der Netzwerksicherheit zur Schließung der Sicherheitslücke
- Abwehr einer Cyber-Erpressung inkl. Kosten für z. B. Belohnungsgelder
- Vertrauensschäden durch Dritte
- Entfernung von Schadsoftware und Wiederherstellung gelöschter und geschädigter Daten
- Kosten zur Wiederherstellung betriebsnotwendiger Hardware
- Erstattung eines Unterbrechungsschadens (nicht erwirtschafteter Betriebsgewinn und fortlaufende Kosten)
- Schadenminderungskosten zur Minderung des Betriebsunterbrechungsschadens
- Betriebsunterbrechung durch Datenverlust als Folge einer Informationssicherheitsverletzung oder eines Bedienfehlers
- Störung der IT-Systeme durch Infrastrukturausfälle von Systemen, die sich ausschließlich innerhalb der Kontrolle des Versicherten befinden

Optionale Erweiterungen für einen umfassenden Schutz

- > Leistungs-Update Garantie
- > Internet-Diebstahl
- > Cyber-Spionage
- > Betriebsunterbrechung als Folge einer DOS-Attacke auf eine entgeltlich genutzte Cloud

Drittschäden

Wir übernehmen die Schadenersatzansprüche von Dritten, die aus einem Hackerangriff, Datenverlust oder einer Datenrechtsverletzung resultieren können. Darüber hinaus bieten wir:

- Prüfung der Haftpflichtfrage
- unbegrenzte Rückwärtsdeckung
- Nachmeldefrist von fünf Jahren für Schäden während der Vertragslaufzeit
- Ansprüche wegen Urheber- und Namensrechtsverletzungen bei unberechtigter Veröffentlichung elektronischer Medieninhalte
- Forderungen zur Zahlung von Vertragsstrafen durch E-Payment-Service-Provider
- Verteidigung in Datenschutzverfahren
- Vertragsstrafen wegen Datenvertraulichkeitsverletzungen
- Immaterielle- und Personenschäden aufgrund von Persönlichkeitsverletzungen
- Vertragliche Freistellungsverpflichtungen gegenüber Auftragsdatenverarbeitern
- Vertragliche Schadenersatzansprüche

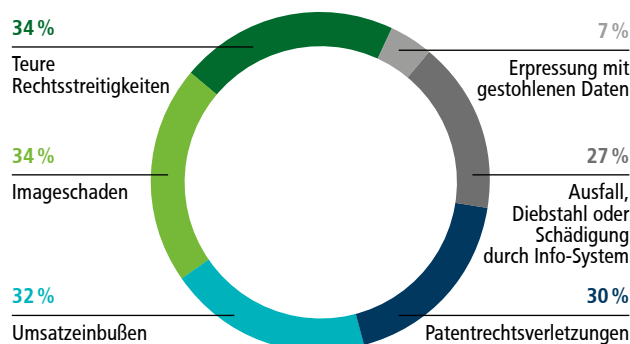
Umfassendes Cyber-Security-Konzept

46 % aller Cyberschäden werden durch die eigenen Mitarbeiter verursacht. Deshalb bieten wir mit unserem Kooperationspartner Perseus für Mitarbeitern von Firmen/Freie Berufe Kunden ein umfangreiches Präventionstraining an, um sie fit für die Themen Cybersicherheit und Datenschutz zu machen. Leicht verständlich. Und für alle Kunden der Cyber-Stand-alone-Versicherung kostenlos.

Dieses beinhaltet unter anderem:

- Digitale Schulungsformate
- Fingierte Phishingmails
- Werkzeugkasten für Cybersicherheit
- Digitale Tools für Cybersicherheit im Arbeitsalltag
- Laufende Information zu aktuellen Neuigkeiten
- Regelmäßige praktische Tipps

Die bedeutendsten Cyberrisiken aus Firmensicht



Quelle: YouGov, Schwerpunktthema aus dem Gewerbekundenmonitor Assekuranz 2017