

Hiscox CyberClear

Rundum-Schutz und außergewöhnliche Assistance-Leistungen bei Hacker-Angriffen und IT-Ausfällen

Bereits seit 2011 bietet Hiscox eine umfassende Cyber-Versicherung für Geschäftskunden und war damit der erste Versicherer mit einer solchen Deckung auf dem deutschsprachigen Markt. Hiscox schützt kleine und mittelständische Unternehmen – vorbeugend, mitten in der Krise, bei der Schadenregulierung und einer nachgelagerten Sicherheitsanalyse.

AUSGEWÄHLTE PRODUKT-HIGHLIGHTS DER CYBER-VERSICHERUNG

- **Allround-Deckung:** Hiscox CyberClear beinhaltet eine **Cyber-Eigenschadendeckung**, eine **Cyber-Haftpflichtversicherung** sowie Schutz bei einer **Cyber-Betriebsunterbrechung**. Die Zusatzbausteine Cyber-Betrug und Cyber-Betriebsunterbrechung bei Cloud-Ausfall sowie bei technischen Problemen können den Schutz vervollständigen.
- **Außergewöhnliche Assistance-Leistungen:** Hiscox kooperiert exklusiv mit dem IT-Sicherheitsexperten HiSolutions AG sowie der msg service AG, Krisen-PR-Spezialisten und spezialisierten Datenschutzanwälten. Sie unterstützen präventiv und agieren im Ernstfall wie ausgelagerte Cyber-Krisenabteilungen. Kostenfreie* Cyber-Schulungen und ein Cyber-Krisenplan sind integrale Bestandteile der vielseitigen Hiscox Leistungen vor, während und nach einem Schadenfall, die garantierter Teil des Bedingungswerks sind.
- **Transparentes Bedingungswerk im Sinne des Kunden:** Gemäß unserer Versicherungs-Philosophie zeichnet sich Hiscox CyberClear durch ein klares und einfaches Bedingungswerk aus, das keine versteckten Klauseln enthält und auf marktübliche Obliegenheiten vor Eintritt des Versicherungsfalles verzichtet – so gibt es keine „Stand der Technik“- oder „Erprobungs“-Klausel.
- **Weite Definition bezüglich Cybervorfall-Auslösern:** Durch die nicht abgeschlossene Aufzählung von Cybervorfall-Auslösern (Triggern) sind auch neuartige Cyber-Risiken mitversichert.
- **Übernahme von Cyber-Eigenschäden und Kosten:** Hiscox erstattet Kunden u. a. Eigenschäden wie Kosten für Krisenmanagement, IT-Forensik, begleitende PR-Maßnahmen, die Wiederherstellung der Daten und des IT-Systems (inkl. Wiederherstellungskosten für IT-Hardware), die Kosten für gesetzliche Informationspflichten sowie die Aufwendungen für Datenschutzanwälte, Strafrechtsschutz und eine nachgelagerte Sicherheitsanalyse. Alle Eigenschadenpositionen werden im Bedingungswerk separat erläutert.
- **Erweiterung der Cyber-Betriebsunterbrechung:** Diese wurde unter anderem ausgedehnt auf Wechselwirkungsschäden bei anderen Versicherten, freiwillige Abschaltung bei der Reparatur oder um weitere Schäden an Daten oder dem IT-System zu vermeiden sowie auf Unterbrechungen aufgrund einer Anordnung durch Datenschutzbehörden. Ertragsausfälle und Mehrkosten werden übernommen, wenn es nach versicherten Ereignissen zum Stillstand des Betriebs kommt.
- **Schutz physischer und elektronischer Daten:** Ob Laptop, Smartphone oder Papierakte – Hiscox leistet, wenn Daten abhandengekommen, nicht mehr verfügbar sind oder missbraucht wurden. Der Versicherungsschutz umfasst personenbezogene, persönliche und auch geschäftliche Daten.
- **Reduzierter Selbstbehalt bei absolviertem Cyber-Training:** Der Selbstbehalt kann im Schadenfall um 25% reduziert werden, wenn mindestens 80% der Mitarbeitenden in den vergangenen 12 Monaten das im Rahmen von Hiscox CyberClear angebotene Online-Training absolviert haben.
- **Umfassendes Deckungskonzept:** Hiscox CyberClear enthält bereits in der Grunddeckung alle elementaren Deckungsbausteine und leistet vorrangig vor anderen Versicherungsverträgen. Zudem gilt im Versicherungsfall eine Beweiserleichterung für den Versicherungsnehmer.

*Das kostenfreie Paket enthält 100 Lizenzen.



**HISCOX
BUSINESS
ACADEMY**

EXKLUSIVE LEISTUNGEN AB DEM ERSTEN TAG

Kostenfreier Zugriff auf E-Learning zu Top-Themen wie Datenschutz & Cyber-Sicherheit, auf rechtssichere Vorlagen, Checklisten und vieles mehr.

Außerdem: Versicherungssiegel zum Download – das Trust-Element für die Akquise!

SCHADENSZENARIOEN

Offenlegung sensibler Kundendaten

Bei unserem Versicherungsnehmer, einem Bekleidungsunternehmen mit angebundenem Online-Shop, wurden die erfassten Kundendaten unzureichend verschlüsselt. Die sensiblen Daten gelangen daraufhin ins Web und sind somit offen einsehbar.

Hiscox beauftragt Datenschutzanwälte, die den Sachverhalt prüfen und diesen an die zuständige Datenschutzbehörde melden. Darüber hinaus zieht Hiscox ein Callcenter hinzu, welches in Absprache mit den beauftragten Datenschutzanwälten alle betroffenen Kunden über den Verlust der Daten informiert. Außerdem werden die Kunden aufgefordert, ihre Zugangsdaten zu erneuern. Die Aufwendungen für die Rechtsberatung sowie die Leistungen des Callcenters belaufen sich insgesamt auf 85.000 Euro.

Ransomware-Attacke mit Lösegeldforderung

Ein Unternehmen in der Logistikbranche wird Opfer eines Verschlüsselungs-Trojaners mit anschließender Lösegeldforderung. Der Versicherungsnehmer meldet sich unmittelbar bei Hiscox, als der Cyber-Angriff bemerkt wird und die Täter mit den Forderungen zur Datenfreigabe auf ihn zukommen.

Um die Art der Attacke sowie den Schaden am IT-System zu bestimmen, schickt Hiscox Experten des Krisendienstleisters zum Kunden vor Ort. Zusätzlich wird dem Kunden ein Spezialist zur Seite gestellt, der die Betriebsunterbrechungskosten ermitteln soll. Um eine lange und unternehmensschädigende Betriebsunterbrechung zu vermeiden, wird zügig ein mobiles Rechenzentrum aufgebaut, welches als Hilffsystem bis zur Wiederherstellung der IT-Systeme des Versicherungsnehmers fungiert. Hiscox erstattet die Kosten für die Betriebsunterbrechung von ca. 50.000 Euro und die Kosten für die Daten- und Systemwiederherstellung von ca. 470.000 Euro, der versicherte Gesamtschaden beläuft sich auf insgesamt auf rund 520.000 Euro.

Gezielter Hacker-Angriff von Extern

Bei einer mittelständischen Firma für Dienstleistungen im Online-Bereich wird nach einem Cyber-Angriff die komplette IT still gelegt: Mitarbeiter können ihre Arbeitsplätze nicht nutzen und die eingespielte Schadsoftware vernichtet nach und nach alle Daten – inklusive der erstellten Backups.

Hiscox beauftragt umgehend IT-Forensiker, die herausfinden, dass es sich um eine gezielte Schädigung des Versicherungsnehmers handelt – die Angreifer hatten sich über Monate hinweg immer tiefergehenden Zugriff zum IT-System verschafft und die kompletten Admin-Rechte erschlichen. Die neben der IT-Forensik verursachten Aufwendungen für Krisenmanagement, Wiederherstellungsarbeiten, Betriebsunterbrechung sowie die Abwehr von Schadenersatzansprüchen Dritter addieren sich auf einen Gesamtschaden von ca. 2 Mio. Euro.

Selbstverständlich können Sie sich an Ihren persönlichen
Versicherungsvermittler wenden oder uns direkt kontaktieren:

Hiscox

Arnulfstraße 31, 80636 München

Für Makler

T +49 89 54 58 01 100

E hiscox.info@hiscox.de

W makler.hiscox.de/cyber

Für Endkunden

T +49 89 54 58 01 700

E myhiscox@hiscoxdirekt.de

W hiscox.de/cyber

ASSISTANCE-LEISTUNGEN

Neben den Leistungen der Hiscox Business Academy garantieren wir unseren Kunden folgende weitere Services:

Präventiver Cyber-Krisenplan und Cyber-Training

Jedes versicherte Unternehmen erhält präventiv einen Cyber-Krisenplan. Zudem werden bis zu 100 Mitarbeitern kostenlose Online-Cyber-Trainings zur Sensibilisierung angeboten, um die Wahrscheinlichkeit eines Cyber-Schadens schon im Vorfeld zu reduzieren.

Bei aktiver Nutzung der Trainings durch die Mitarbeiter kann die Selbstbeteiligung im Schadenfall um 25% reduziert werden.

Soforthilfe durch IT-Sicherheitsexperten der HiSolutions AG und der msg service AG

IT-Sicherheitsexperten stehen Hiscox Kunden jederzeit, auch bereits im Verdachtsfall, für eine kostenfreie telefonische Unterstützung zur Verfügung.

Bei Bedarf helfen die Spezialisten auch beim Kunden vor Ort und fungieren wie eine ausgelagerte IT-Krisenabteilung und unterstützen ggfs. den lokalen Dienstleister.

Exklusive Krisenberatung durch das Hiscox Netzwerk

Im Krisenfall erhalten Kunden exklusive Betreuung durch das Hiscox Netzwerk aus qualifizierten IT-Experten, Datenschutzanwälten und PR-Spezialisten. So wird der Vorfall frühestmöglich eingedämmt.

