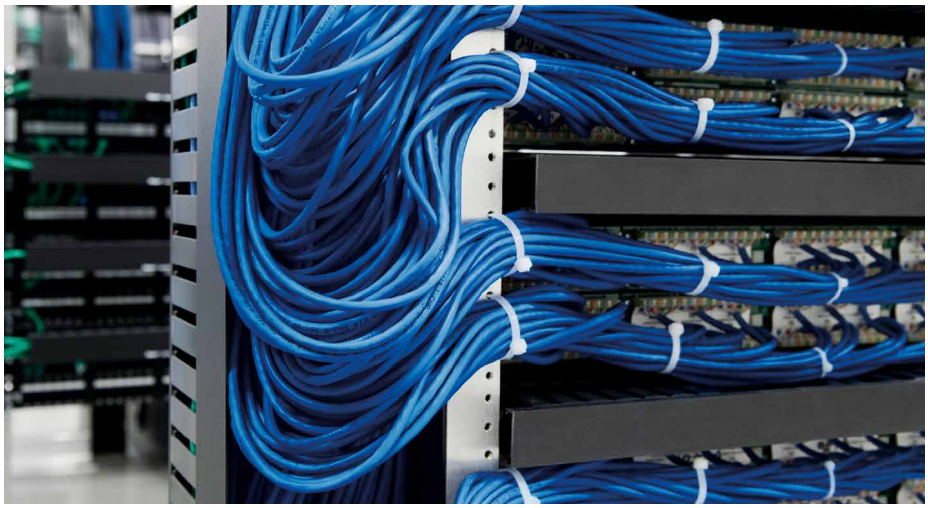
Zurich Cyber Security & Privacy Versicherung

Die Risiken durch Cyber-Angriffe können zum Verlust von sensiblen Daten sowie zum Unterbruch der Wertschöpfungskette von Unternehmen führen. Zurich bietet massgeschneiderte Lösungen an, um Unternehmen vor den Konsequenzen solcher Risiken zu schützen.



Ihre Vorteile auf einen Blick

- Versicherungslösung für mittlere, grosse und internationale Unternehmen
- Weltweite Absicherung gegen finanziellen Folgen durch Cyber-Risiken
- Zugang zu Expertinnen und Experten bei der Risikoanalyse (Pre-Breach) sowie im Schadensfall (Post-Breach)
- Breite Deckung für Drittschäden, Eigenschäden, Betriebsunterbruch und direkten finanziellen Schaden.

Wer profitiert von der Zurich Cyber Security & Privacy Lösung:

- Mittlere, grosse und internationale Unternehmen, die sich gegen die finanziellen Konsequenzen durch Cyber-Risiken absichern wollen.
- Die Zurich International-Programs-Lösungen bieten internationalen Unternehmen auch hier zuverlässigen weltweiten lokalen Service.
- Über unsere Captive-Lösungen bieten wir auch für Cyber-Risiken Lösungen im Bereiche Alternativer Risikotransfer an.

Was umfasst die Zurich Cyber Security & Privacy Lösung:

- Gemeinsam mit unseren Partnern bieten wir Ihnen auf Wunsch eine Risikoanalyse an und beteiligen uns bei Vertragsabschluss an den Kosten.
- Zurich unterstützt Sie durch eine breite Deckung für mögliche Schäden, z.B. aufgrund von Datenverlusten, Betriebsunterbruch oder direktem finanziellem Schaden durch Cyber-Risiken.
- Zurich begleitet Unternehmen umfassend bei Cyber-Vorfällen und unterstützt Sie dabei, die Folgen zu bewältigen. Unser 24/7 weltweites Krisenmanagement ist für Sie da. Wir vermitteln auf Wunsch Spezialistinnen und Spezialisten und übernehmen die Kosten, damit Ihre Systeme wieder funktionsfähig werden und Sie reibungslos weiterarbeiten können.

Folgende Deckungen werden abhängig vom Risiko angeboten:

Allgemein

- 24/7 Cyber Incident Management mit Zugang zu geprüften IT- und Servicedienstleistern
- Deckung des eigenen Computernetzwerks sowie von IT- und administrativen Dienstleistern
- Deckung von Computerkomponenten von industriellen Kontrollsystemen, Produktionsanlagen und Medizinalgeräten
- Vorsätzliche Handlungen von Mitarbeitenden eingeschlossen (ohne Crime-Deckung)
- Weltweite Deckung
- Einschluss von Grobfahrlässigkeit und Verzicht auf Kündigung im Schadensfall
- Internationale Programme (IPZ) und Captive-Lösungen

Kosten zur Datenwiederherstellung und Systemverbesserung:

- Aufgrund eines Cyber-Vorfalls
- Disaster Recovery, IT-forensische Analysen und Beseitigung von Schadsoftware
- Wiederherstellung oder Wiederbeschaffung von Daten und Informationen
- Wiederbeschaffung von beschädigter Hardware (Bricking)
- Identifikation von Schwachstellen und Massnahmen zur Sicherheitsverbesserung (Betterment)

Betriebsunterbruch und Mehrkosten:

- Aufgrund eines Cyber-Vorfalls oder eines Systemfehlers
- Aufgrund von freiwilligem Abschalten der Systeme, um weitere Schäden abzuwenden
- Aufgrund einer behördlichen Anordnung infolge einer Datenschutzverletzung
- Deckung von Nettogewinnausfall sowie Mehrkosten zur Aufrechterhaltung des Betriebs

Cyber Crime und Erpressung:

- Cyber-Erpressungszahlungen und Kosten für die Abwehr von Cyber-Erpressungen
- Cyber-Betrug durch gefälschte Zahlungsanweisungen durch Dritte (Social Engineering)
- Cyber-Diebstahl durch Manipulation der Computersysteme durch Dritte (E-Banking Hacking)

Haftpflicht und Ansprüche Dritter:

- Verlust, Diebstahl oder Veröffentlichung von Daten unabhängig von einem Cyber-Vorfall
- Verletzung von Datenschutzrecht inklusive DSG, GDPR oder anderen
- Verletzung von Namens-, Urheber- und Markenrechten
- Verfahrenskosten und Verteidigungskosten
- Regulatorischen Verfahren sowie Strafen und Bussen
- Vertragsstrafen bei einem Verstoss gegen PCI-DSS-Standards
- Zahlungen an Verbraucherschutz-Organisationen
- Einschluss von externen Dienstleistern und Lieferanten

Benachrichtigungskosten und Krisenmanagement:

- Aufgrund eines Cyber-Vorfalls
- IT-forensische Analysen zur Feststellung eines Cyber-Vorfalls
- Prüfung von Meldepflichten und Benachrichtigungspflichten
- Benachrichtigung von betroffenen Personen (inklusive freiwilliger Benachrichtigung)
- Callcenter, Kreditkarten- und Identity-Monitoring für betroffene Personen
- Rabattaktionen und Preisnachlässe für betroffene Personen
- Planung und Umsetzung von Public-Relations-Kampagnen

Reputationsschaden:

- Aufgrund negativer Berichterstattung über einen möglichen Cyber-Vorfall
- Deckung von Nettogewinnausfall durch Verlust von Kunden und Aufträgen

Gerne beraten wir Sie persönlich und individuell. Kontaktieren Sie einfach Ihre nächste Zurich-Agentur, rufen uns kostenlos an unter 0800 80 80 80 oder nehmen Sie direkt Kontakt auf mit Ihrem Makler/Broker. www.zurich.ch

ZH19692_DE_1902

Zürich Versicherungs-Gesellschaft AG
Hagenholzstrasse 60, 8050 Zürich
Telefon 0800 80 80 80, www.zurich.ch

ZURICH®