HISCOX
WISSEN VERSICHERT.

CYBER-VERSICHERUNG BY HISCOX 2022

VERÄNDERUNGEN IM BEDINGUNGSWERK (HISCOX CYBERCLEAR 06/2022)

Die dynamische Risikoentwicklung im Zusammenhang mit Cyber-Gefahren (z.B. vermehrte Häufigkeit und wachsender Umfang von Kumul-Schäden; Notwendigkeit der Abgrenzung zu nicht-versicherbaren systemischen Risiken) erfordert eine fortlaufende Bewertung und Anpassung der Cyber-Versicherungsbedinungen. Wir verfolgen dabei das Ziel, zukunftsfähige und faire Cyber-Lösungen anbieten zu können.

Die wesentlichen Änderungen der neuen Bedingungen Hiscox CyberClear 06/2022 haben wir nachfolgend für Sie zusammengestellt. Eine vollständige Übersicht sämtlicher Änderungen im Detail finden Sie unter makler.hiscox.de/cyber-informationen.

Erhöhte Flexibilität und Bedarfsorientierung in der Deckung
Eine stärkere Modularität der einzelnen Deckungskomponenten ermöglicht eine noch individuellere Zusammenstellung des Versicherungsschutzes:

- Cyber-Diebstahl als optionaler Baustein
- Cyber-Betriebsunterbrechung als optionaler Baustein

Anpassungen der Cyber-Betriebsunterbrechung
Stärkere Orientierung am tatsächlichen Bedarf der Versicherungsnehmer:

- Flexible Gestaltung der Cyber-Betriebsunterbrechung ermöglicht zielgenaue Anpassung auf individuelle Bedürfnisse: Je nachdem, wo der Kunde seine IT-Systeme und Daten hat - in der Cloud oder On-Premises (vor Ort). Der Abschluss dieser beiden Bausteine ist unabhängig voneinander möglich.
- Beginn der Haftzeit mit Eintritt der Cyber-Betriebsunterbrechung, nicht mehr bei Anzeige beim Dienstleiter (jedoch weiterhin Obliegenheit zur unverzüglichen Anzeige des Schadens).
- Zeitlicher Selbstbehalt statt Wartezeit in der Betriebsunterbrechung: Die bisher vorhandene Wartezeit wird standardmäßig auf einen zeitlichen Selbstbehalt umgestellt. Erst nach Ablauf des zeitlichen Selbstbehalts beginnt der Versicherungsschutz.
- Betriebsunterbrechung nach technischen Problemen ist nicht mehr im Basis-Versicherungsumfang enthalten sondern kann optional gegen Zuschlag eingeschlossen werden. Antragskunden bis 10 Mio. Euro Umsatz, die diesen Baustein bisher standardmäßig mit-versichert hatten, erhalten ihr Neuordnungsangebot ohne diese Erweiterung und können dies ebenfalls auf Anfrage einschließen.

Abgrenzung nicht-cyberbedingter „Media-Haftpflicht"-Versicherungsfälle
Voraussetzung für die Mitversicherung von Schäden im Rahmen einer Rechtsverletzung durch Werbung oder Marketing ist das Vorliegen eines definierten Cyber-Triggers (Netzwerksicherheitsverletzung, Bedien- oder Programmierfehler, Datenrechtsverletzung, Cyber-Erpressung). Cyber-unabhängige Schäden bleiben über entsprechende Vermögensschaden-Haftpflichtlösungen versicherbar.

Konkretisierung Ausschluss Gewaltsame Auseinandersetzungen und Cyber-Operationen
Wie bisher bleiben gewaltsame Auseinandersetzungen und Cyber-Operationen vom Versicherungsschutz ausgeschlossen.
Es erfolgt darüber hinaus nunmehr eine Konkretisierung hinsichtlich der Definition einer Cyber-Operation.

Ergänzung und Modifikation von Ausschlüssen
Abgrenzung von nicht-versicherbaren systemischen Risiken sowie weitere Klarstellungen, u.a.:

- Konkretisierung des Ausschlusses „Technischer Infrastruktur" u.a. durch Ergänzung um Gas- und Wasserstoffversorgung und Computer- und Datennetze sowie Satelliten als externe Netzstrukturen
- Ergänzung des Ausschlusses rechtswidrige Erfassung von Daten um die rechtswidrige Nutzung von Daten
- Aufnahme eines Ausschlusses für Naturkatastrophen
- Aufnahme eines Ausschlusses für Sach- und Personenschäden
- Aufnahme eines Ausschlusses für Kernenergie und Radioaktivität

HISCOX
WISSEN VERSICHERT.

Einschränkung der automatischen Mitversicherung neuer Tochtergesellschaften
Aufnahme einer Klarstellung für die automatische Mitversicherung bei Verschmelzung. Zudem gilt automatische Mitversicherung neuer Tochtergesellschaften nur bei im Verhältnis zur Muttergesellschaft analogem IT-Sicherheitsniveau, gleicher Branche und keinen Fernzugriffsmöglichkeiten auf IT-Systeme von Kunden (Managed Service Provider - MSP).

Aufnahme von Obliegenheiten vor Eintritt des Versicherungsfalles
Die Mindestanforderungen an das IT-Sicherheitsniveau wurden nunmehr als Obliegenheiten vor Eintritt des Versicherungsfalles in die Bedingungen integriert:

- Durchführung einer vollständigen Datensicherung in mindestens wöchentlichem Turnus und Aufbewahrung der Datensicherung für mindestens 30 Tage. Für die Erstellung dieser Datensicherung ist eine Offline-Datensicherung mit dauerhafter physischer Trennung von den zu sichernden IT-Systemen oder eine unveränderbare Online-Datensicherung, auf die Administratoren nur mit einer Zwei-Faktor-Authentifizierung oder aus einer separaten Domain zugreifen können, zu nutzen.
- Einspielen von Sicherheitsupdates (Patch-Management) innerhalb von 30 Tagen nach Veröffentlichung des Updates durch den Hersteller.
- Betrieb von Altsystemen (Betriebssysteme, für die keine Sicherheitsupdates mehr bereitgestellt werden) ausschließlich in einer isolierten Netzwerkumgebung ohne direkten Internetzugang und mit durchgehender Kontrolle des Datenverkehrs.

Die technischen Obliegenheiten entsprechen den Mindestanforderungen an die IT-Sicherheit, welche für jeden Kunden als Standard definiert werden. Daher muss jeder Kunde bei Neueindeckung bereits das Vorhandensein der oben stehenden Voraussetzungen bestätigen.

Weiterführende Informationen finden Sie über den QR-Code oder unter: **makler.hiscox.de/cyber-informationen**

Hiscox
Arnulfstraße 31, 80636 München

Für Makler
T +49 89 54 58 01 100
E hiscox.info@hiscox.de
W **makler.hiscox.de**

Für Endkunden
T +49 89 54 58 01 700
E myhiscox@hiscoxdirekt.de
W **hiscox.de**