LEISTUNGSVERGLEICH CYBER-RISK

	HISCOX CyberClear Baubranche bis 25 Mio. € Umsatz	MARKEL Pro Cyber VEMA-Konzept inkl. alle Bausteine	VHV VERSICHERUNGEN CYBERPROTECT	VERSICHERUNGSKAMMER BAYERN CyberSchutz Plus	württembergische Cyber-Police
Prävention - Leistungen vor Eintritt des Versicherungsfalles					
Krisenplan (kostenfrei)	✓	✓	✓ (je nach Aufwand kostenpflichtig)	✓	+ in Abstimmung mit VR möglich
Cyber-Training für Mitarbeiter des VN (kostenfrei)	✓	✓	✓	✓	✓
Soforthilfe (bereits bei Verdacht eines Vers.-falles) ohne Anrechnung auf Versicherungssumme ohne Selbstbehalt	✓	✓	✓	✓ max. 48 Stunden	+ in Abstimmung mit VR möglich
Assistance / Netzwerk					
Krisenberater	✓ über HiSolutions	✓ über msg systems AG	✓	✓	✓ über KPMG Forensic
Single Point of contact für Versicherungsnehmer (Hotline des Krisenberaters)	24 Stunden / 7 Tage	24 Stunden / 7 Tage	24 Stunden / 7 Tage	24 Stunden / 7 Tage	24 Stunden / 7 Tage
Hotline des Versicherers	24 Stunden / 7 Tage	24 Stunden / 7 Tage	24 Stunden / 7 Tage	24 Stunden / 7 Tage	24 Stunden / 7 Tage
Internationales Netzwerk des Krisenberaters	✓	✓	✓	✗	✓
Riskaudit des Krisendienstleisters	+ in Abstimmung mit VR möglich	+ vor Schadenfall gegen Kostenbeteiligung	+ in Abstimmung mit VR möglich	+ vor Schadenfall gegen Kostenbeteiligung	+ in Abstimmung mit VR möglich
Deckungsauslöser					
Hacker - Angriffe (gezielte u. ungezielte)	✓	✓	✓	✓	✓

	HISCOX CyberClear Baubranche bis 25Mio. € Umsatz	MARKEL Pro Cyber VEMA-Konzept inkl. alle Bausteine	VHV VERSICHERUNGEN CYBERPROTECT	VERSICHERUNGSKAMMER BAYERN CyberSchutz Plus	württembergische Cyber-Police
DoS - Denial of Service (Unterbrechung IT-System)	✓	✓	✓	✓	✓
Infektion der Systeme mit Schadsoftware (Viren, Würmer, Trojaner usw.)	✓	✓	✓	✓	✓
Datenrechtsverletzung	✓	✓	✓	✓	✓
Bedienfehler	✓	✓	✓	✓ bei Ertragsausfall	✓
Rechtsverletzung durch Werbung Medien	✗	✓	✓	✓ sofern Datenschutzverletzung	✓
Versicherungsleistungen					
Geltungsbereich	weltweit	weltweit	weltweit	weltweit; Ausschluss USA; common law	weltweit; Ausschluss USA, Kanada
Mitversicherte Unternehmen	VN und seine Tochtergesellschaften im Inland u. Ländern des EWR und UK	VN und seine Tochtergesellschaften im Inland u. Ländern des EWR	Versicherungsnehmer und im Versicherungsschein genannten mitversicherten Unternehmen	VN und seine Tochtergesellschaften mit Sitz in Deutschland sofern benannt	VN und seine Tochtergesellschaften
Rückwärtsdeckung	✓ unbegrenzt	✓ unbegrenzt	✓ 5 Jahre	✓ nicht für bekannte Sachverhalte/Schäden	✓ unbegrenzt
Nachmeldefrist	✓ 5 Jahre n. Beendigung d. Vertrages	✓ 10 Jahre n. Beendigung d. Vertrages	✓ 5 Jahre n. Beendigung d. Vertrages	✓ 3 Jahre n. Beendigung d. Vertrages	✓ 5 Jahre n. Beendigung d. Vertrages
Vorrangiger Versicherungsschutz (keine Subsidiarität)	✓	✓	✓	✓	✓

	HISCOX CyberClear Baubranche bis 25Mio. € Umsatz	MARKEL Pro Cyber VEMA-Konzept inkl. alle Bausteine	VHV VERSICHERUNGEN CYBERPROTECT	VERSICHERUNGSKAMMER BAYERN CyberSchutz Plus	württembergische Cyber-Police
Max. Versicherungsleistung über Standardmodell (Antrag)	3.000.000 €	1.000.000 €	2,000,000 €	1.000.000 €	2.000.000 €
Haftpflichtansprüche Dritter inkl. Vermögensschäden	✓	✓	✓	✓ nur Vermögensschäden	✓
Max. Versicherungsleistung bei Individualanfrage	15.000.000 €	5.000.000 €	kein Limit	individuell je nach Einzelfall	5.000.000 €
Entschädigungsgrenzen / Sublimits / Selbstbehalte					
Assistanceleistungen	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	bis zu 50 % der Versicherungssumme
Erstattung von Forensikkosten	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	bis zu 50 % der Versicherungssumme
Schaden durch eigene Betriebsunterbrechung	Optional mit wählbarer Entschädigungsgrenze im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme
Mehrkosten durch Betriebsunterbrechung	im Rahmen der Entschädigungsgrenze	im Rahmen der Versicherungssumme	✓ im Rahmen des VS	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme
Vertragsstrafen an E-Payment Service Provider	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	⊕ im Rahmen der VS	max. 50.000 €	im Rahmen der Versicherungssumme
Cyber-Diebstahl	⊕ bis 250.000 € gegen Zuschlag (Zusatz-Baustein CYBER CRIME)	im Rahmen der Versicherungssumme	⊕ im Rahmen der VS	im Rahmen der Versicherungssumme, offene Regelung für alle Straftagen Dritter mit Bereicherungsabsicht	im Rahmen der Versicherungssumme
Schaden durch eigene Betriebsunterbrechung bei Ausfall fremder Dienstleister (Cloud-Ausfall)	⊕ 100.000 €; gegen Zuschlag	im Rahmen der Versicherungssumme	⊕ im Rahmen der VS	⊕	im Rahmen der Versicherungssumme
Vertragsstrafen bei Verletzung von Geheimhaltungsverpflichtungen	250.000 €	250.000 €	✗	✗	im Rahmen der Versicherungssumme

	HISCOX CyberClear Baubranche bis 25Mio. € Umsatz	MARKEL Pro Cyber VEMA-Konzept inkl. alle Bausteine	VHV VERSICHERUNGEN CYBERPROTECT	VERSICHERUNGSKAMMER BAYERN CyberSchutz Plus	württembergische Cyber-Police
Vertragsstrafen wegen Leistungsverzug	⊕ auf Anfrage	✗	✗	✗	✗
Bußgelder, Geldstrafen (Ausland)	250.000 €	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	✗	✗
Wiederherstellungskosten (Daten / IT-System)	im Rahmen der Versicherungssumme	✓	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme; Austausch von Hardware, wenn die Schadenursache nur dadurch beseitigt werden kann.
generelle Selbstbehalte	wahlweise 1.000 €, 2.500 €, 5.000 €, 10.000 €, 25.000 €	wahlweise 1.000 €, 2.500 € oder 5.000 € (höhere SB auf Anfrage möglich)	wahlweise 500 €, 1.000 €, 2.500 €, 5.000 €	Jahresumsatz bis 2.5 Mio €; 1.000 SB Jahresumsatz über 2.5 Mio €; 2.500€ SB Jahresumsatz über 10 Mio €; 5.000€ SB ab 15 Mio. € individuell bei Ertragsausfallschäden (CyberSchutz Plus); 12 Stunden	wahlweise 1.000 € oder 2.500 €
Verzicht auf nachfolgende Ausschlüsse					
Vorsatz	✓ außer bei Repräsentanten	✓ außer bei Repräsentanten	✓ außer bei Repräsentanten	✓ außer bei Repräsentanten	✓ außer bei Repräsentanten
Ausfall der privaten oder öffentlichen Infrastruktur	✗	✗	✓ private Infrastruktur über Zusatzbaustein BU bei technischen Problemen	✗	✗
rechtswidrige Datenerfassung	✗	✗	✗	✓	⊕ auf Anfrage versicherbar
Insolvenz	✓	✓	✓	✓	✓
Umgang mit nachfolgenden Sicherheitsvorschriften					

	HISCOX CyberClear Baubranche bis 25Mio. € Umsatz	MARKEL Pro Cyber VEMA-Konzept inkl. alle Bausteine	VHV VERSICHERUNGEN CYBERPROTECT	VERSICHERUNGSKAMMER BAYERN CyberSchutz Plus	württembergische Cyber-Police
regelmäßige Datensicherung	mindestens einmal wöchentlich (siehe Antragsfragen und Obliegenheit)	bei Unternehmen bis 1 Mio. € Umsatz wöchentlich bei Unternehmen ab 1 Mio. € Umsatz täglich (siehe Antragsfragen)	mindestens einmal wöchentlich (siehe Obliegenheiten)	mindestens einmal wöchentlich (siehe Antragsfragen)	mindestens einmal wöchentlich (siehe Obliegenheiten)
Anti-Virenprogramme mit aktuellen Virendatenbanken	erforderlich, inklusive automatischer Aktualisierung (siehe Antragsfragen und Obliegenheit)	erforderlich, hiervon ausgenommen sind die Betriebssysteme von Apple, Unix und Linux (siehe Antragsfragen)	erforderlich, inklusive automatischer Aktualisierung (siehe Obliegenheiten)	erforderlich (siehe Obliegenheiten)	erforderlich, inklusive ständiger Aktualisierung (siehe Obliegenheiten)
Firewalls	erforderlich (siehe Antragsfragen und Obliegenheit)	erforderlich (siehe Antragsfragen)	erforderlich, inklusive ständiger Aktualisierung (siehe Obliegenheiten)	erforderlich (siehe Obliegenheiten)	erforderlich, inklusive ständiger Aktualisierung (siehe Obliegenheiten)
Patch-Management (automatisierter Prozess zum Aufspielen von Updates, Patches und Servicepacks zur Schließung von Sicherheitslücken)	erforderlich (siehe Antragsfragen und Obliegenheit)	nicht erforderlich	erforderlich, bei einfacher IT genügt auch eine regelmäßige manuelle Überprüfung (siehe Obliegenheiten)	erforderlich (siehe Obliegenheiten)	erforderlich (siehe Obliegenheiten)
Zugangskontrollen für Ihre IT-Systeme (z. B. Benutzerkennungen und Passwörter)	erforderlich, inklusive Rechtekonzept (siehe Antragsfragen)	nicht erforderlich	erforderlich, inklusive Rechtekonzept (siehe Obliegenheiten)	erforderlich, inklusive Rechtekonzept (siehe Obliegenheiten)	erforderlich, inklusive Rechtekonzept (siehe Antragsfragen)
Begrenzung der Leistungskürzung bei grob fahrlässiger Verletzung der Sicherheitsvorschriften	✗	✓ max. Kürzung um 20 % bei Schäden bis 250.000 €	✗	✗	✗
Versicherbare Branchen					
Dienstleister	✓ über Cyber Clear Standardmodell - Ausnahme Finanzdienstleister	✓ Ausnahme Banken, Versicherungen, Inkassodienstleister	✓ Ausnahme Vermögensverwaltung, Rating-Agentur, Inkassodienstleister	✓ IT-, Finanz- und Zahlungsdienstleister sind anfragepflichtig	✓ Ausnahme Banken, Geld-/Kreditinstitute, Dienstleister für Datenhaltung/ Datenbanken, Inkassodienstleister
öffentl. Unternehmen / Kommunen	+ auf Anfrage	+ auf Anfrage	✗	✗	✗
Produktionsunternehmen	✓ über Cyber Clear Modell Standard oder Hersteller	+ auf Anfrage	✓	✓	✓

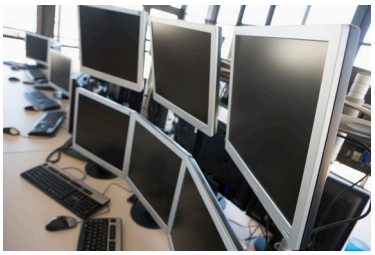
	HISCOX CyberClear Baubranche bis 25Mio. € Umsatz	MARKEL Pro Cyber VEMA-Konzept inkl. alle Bausteine	VHV VERSICHERUNGEN CYBERPROTECT	VERSICHERUNGSKAMMER BAYERN CyberSchutz Plus	württembergische Cyber-Police
Handel	✓ über Cyber Clear Modell Handel	✓	✓	✓	✓
Online-.Handel	✓ über Cyber Clear Modell Handel	✓ indiv. Anfrage (Markel Pro Onlineshops)	✓ Individuelles Underwriting bei mehr als 50% Onlineumsatz	✓	✓
Handwerk	✓ über Cyber Clear Standardmodell	✓	✓	✓	✓
Versicherungsmakler	✗	✓ Antrag Markel Pro Cyber für Vermittler	✓	✗	✓

Legende: ✓ = versichert (im Rahmen der Bedingungen) ✗ = nicht versichert + = optional einschließbar

Dieses Druckstück dient nur der vorläufigen Information und ist eine unverbindliche Übersicht und Orientierungshilfe.
Weder die VEMA eG noch der genannte Versicherungsmakler übernehmen eine Gewähr für die Vollständigkeit, Richtigkeit und Aktualität der berücksichtigten Tarif-, Beitrags- und Leistungsdaten und allgemeinen Hinweisen.
Kosten, Umfang sowie Leistungen des Versicherungsschutzes ergeben sich aus den Allgemeinen Versicherungsbedingungen, den besonderen Bestimmungen der Tarife, der Versicherungspolice sowie weiteren schriftlichen Vereinbarungen.

Dieser Leistungsvergleich wurde am 15.07.2024 erstellt.

Cyber-Risk



© Monkey, ClipDealer, #727606

Erläuterungen zu den Leistungspunkten

Wir wollen, dass Sie verstehen, was Ihnen ein Tarif bieten kann. Denn viele Begriffe aus der Versicherungswelt können für einen Kunden verwirrend sein und zu Missverständnissen führen. Auf den nachstehenden Seiten beschreiben wir daher die einzelnen Leistungspunkte rund um die Cyberversicherung etwas anschaulicher. Wenn trotzdem noch Fragen offen sein sollten, zögern Sie bitte nicht, uns zu kontaktieren.

Wir sind als Ihr Ansprechpartner für alle Bereiche der Vorsorge sehr gerne für Sie da!

Krisenplan

In Zusammenarbeit mit dem Versicherer oder einem mit ihm kooperierenden externen IT-Dienstleister wird ein Krisenplan zur Verfügung gestellt, welcher den richtigen/genauen Ablauf bei einem Vorfall beschreibt.

Cyber-Training für Mitarbeiter des Versicherungsnehmers

Präventive Maßnahmen, die die Mitarbeiter für Szenarien vor, während oder nach einem Cyberangriff schulen.

Soforthilfe

Bereits bei Verdacht kann auf den Versicherer beziehungsweise den IT-Dienstleister zugegangen und eine Soforthilfe beansprucht werden. So kann ein möglicher Leistungsfall frühzeitig erkannt und die Folgen abgemildert werden.

Krisenberater

Er wird dem versicherten Unternehmen im Schadensfall zur Verfügung gestellt.

Single Point of Contact für Versicherungsnehmer (Hotline des Krisenberaters)

Eine zentrale Anlaufstelle für den Versicherungsnehmer, welche die Krisenbewältigung koordiniert.

Internationales Netzwerk des Krisenberaters

Krisenberater agieren nicht nur in Deutschland, sondern über die Landesgrenzen hinaus. Vor allem wichtig, wenn Teile des Unternehmens oder Tochterunternehmen im Ausland agieren.

Risk-Audit des Krisendienstleisters

Eine Art Risikoprüfung, die vom Versicherer respektive vom IT-Dienstleister in der Regel in Abstimmung und gegen Entgelt angeboten wird. Beim Risk-Audit wird das versicherte Unternehmen geprüft (Sicherheitsstandards etc.). Es werden Sicherheitslücken aufgedeckt und Verbesserungsvorschläge erstellt.

Hackerangriffe (gezielte und ungezielte)

Gezielte Hackerangriffe sind Angriffe, die es auf ein spezielles IT-System oder Netzwerk abgesehen haben. Hierbei haben die Angreifer große Ressourcen. Ungezielte Hackerangriffe sind beispielsweise x-fach verschickte Mails mit schädlichen Anhängen.

DoS – Denial of Service (Unterbrechung des IT-Systems)

Von Denial of Service – oder kurz DoS – spricht man, wenn etwas unzugänglich gemacht oder außer Betrieb gesetzt wird. Technisch passiert dabei folgendes: Bei DoS-Attacken wird ein Server gezielt mit so vielen Anfragen bombardiert, dass das System die Aufgaben nicht mehr bewältigen kann und im schlimmsten Fall zusammenbricht.

Infektion der Systeme mit Schadsoftware (Viren, Würmer, Trojaner etc.)

Durch das Öffnen von E-Mail-Anhängen oder den Download von infizierten Dateien werden IT-Systeme durch Viren, Würmer oder Trojaner infiziert.

Vorsatz Mitarbeiter (außer Repräsentanten)

Mitarbeiter lösen einen Cyberangriff vorsätzlich aus. Beispiel: Es werden Passwörter an Dritte weitergegeben. Dies gilt nicht für bedingungsseitig definierte Repräsentanten.

Beispielhafte Aufzählung von Repräsentanten:

- die Mitglieder des Vorstandes (bei Aktiengesellschaften),
- die Geschäftsführer (bei Gesellschaften mit beschränkter Haftung),
- die Komplementäre (bei Kommanditgesellschaften),
- die Gesellschafter (bei offenen Handelsgesellschaften),
- die Gesellschafter (bei Gesellschaften bürgerlichen Rechts),
- die Inhaber von Einzelfirmen,
- die nach den gesetzlichen Vorschriften berufenen obersten Vertretungsorgane (bei anderen Unternehmensformen, z. B. Genossenschaften, Verbänden, Vereinen, Körperschaften des öffentlichen Rechts, Kommunen),
- der dem Vorstehenden entsprechende Personenkreis (bei ausländischen Unternehmen) oder
- der Leiter der Rechtsabteilung, der IT-Abteilung oder des Risikomanagements.

Cyber-Risk

Datenrechtsverletzung

Eine Datenrechtsverletzung ist jeder Verstoß gegen gesetzliche Vorschriften oder vertragliche Vereinbarungen eines Versicherten, die den Schutz personenbezogener, persönlicher oder geschäftlicher Daten bezwecken und ein den gesetzlichen Bestimmungen entsprechendes Schutzniveau vorsehen. Im Zusammenhang mit Datenrechtsverletzungen bezeichnet der Begriff „Daten“ sowohl elektronische als auch physische Daten.

Eine Datenrechtsverletzung liegt insbesondere vor bei einem Verstoß gegen

- gesetzliche Datenschutzbestimmungen wie das Bundesdatenschutzgesetz, die Datenschutz-Grundverordnung oder vergleichbare ausländische Rechtsnormen zum Datenschutz;
- vertragliche Geheimhaltungspflichten;
- vertragliche „Payment Card Industry (PCI)“-Datensicherheitsstandards oder eine PCI-Datensicherheitsvereinbarung mit einem E-Payment-Service-Provider.

Bedienfehler

Ein Bedienfehler ist die unsachgemäße Bedienung oder Programmierung des IT-Systems eines Versicherten durch fahrlässiges oder grob fahrlässiges Handeln oder Unterlassen des Versicherten oder einer mitversicherten natürlichen Person, sofern die Bedienung oder Programmierung die Veränderung, Beschädigung, Zerstörung, Löschung, Verschlüsselung, Kopie oder das Abhandenkommen von Daten zur Folge hat.

Rechtsverletzung durch Werbung und Marketing

Eine Rechtsverletzung durch Werbung und Marketing liegt vor, wenn im Zusammenhang mit Veröffentlichungen zu Werbe- und Marketingzwecken für die Produkte oder die Dienstleistungen der Versicherten Rechte Dritter verletzt werden.

Rückwärtsdeckung

Dies bedeutet, dass Schäden unter den Deckungsumfang des Versicherungsvertrages fallen, wenn diese erst während der Dauer des Versicherungsvertrages festgestellt werden, obwohl das Schadenereignis vor dem Versicherungsbeginn lag.

Nachmeldefrist

Darunter versteht man den Zeitraum, in dem ein Schaden auf einen gekündigten Versicherungsvertrag zurückzuführen ist, wenn der Schadenszeitpunkt während des Versicherungszeitraums war.

Vorrangiger Versicherungsschutz (keine Subsidiarität)

Besteht Versicherungsschutz über die Cyberversicherung und einen anderen Versicherungsvertrag, dann kann der Versicherungsnehmer darauf bestehen, dass nach dem Vertrag der Cyberversicherung reguliert wird – keine Subsidiarität.

Maximale Versicherungsleistung über Standardmodell (Antrag)

Gibt die Höhe der Entschädigungsleistung über das Standardmodell in Euro an.

Haftpflichtansprüche Dritter inklusive Vermögensschäden

Nach einem Cyber-Angriff können z. B. sensible Kundendaten entwendet und verbreitet werden, wodurch Dritte geschädigt werden. Beispiele: Ein Patentrechtsanwalt wird gehackt und sensible Kundendaten machen die Runde oder bei einem Finanzdienstleister werden sensible Kontodaten/Bankdaten entwendet.

Erstattung von Forensik-Kosten

Gibt die Höhe der Leistung für Forensik-Kosten in Euro an. Forensik-Kosten sind Kosten eines Versicherten für externe IT-Forensik-Analysen zur Ermittlung der Ursache eines versicherten Ereignisses, die Identifizierung der Betroffenen sowie die Kosten für die Erstellung eines abschließenden Berichts zur forensischen Analyse.

Schaden durch eigene Betriebsunterbrechung

Höhe der Leistung für Schäden durch eigene Betriebsunterbrechung in Euro infolge eines Cyberangriffs. Eine versicherte Cyber-Betriebsunterbrechung liegt vor, wenn die Produktion eines Versicherten oder die Erbringung von Dienstleistungen durch einen Versicherten vollständig oder teilweise unterbrochen ist und wenn diese Unterbrechung unmittelbar und ausschließlich durch ein versichertes Ereignis entstanden ist.

Mehrkosten durch Betriebsunterbrechung

Höhe der Leistung für Mehrkosten durch Betriebsunterbrechung in Euro infolge eines Cyberangriffs. Mehrkosten sind insbesondere Kosten für die Benutzung anderer Anlagen, die Anwendung anderer Arbeits- oder Fertigungsverfahren, die Inanspruchnahme von Lohndienstleistungen oder Lohnfertigungsleistungen, den Bezug von Halb- oder Fertigfabrikaten, einmalige Umprogrammierungskosten sowie Kosten, die durch die Ermittlung und Feststellung einer versicherten Cyber-Betriebsunterbrechung entstehen, soweit der Versicherte sie den Umständen nach für geboten halten durfte.

Cyber-Risk

Vertragsstrafen an E-Payment-Service-Provider

Der Versicherer erstattet Vertragsstrafen, die ein Versicherter einem E-Payment-Service-Provider wegen der Verletzung eines PCI-Datensicherheitsstandards oder einer PCI-Datensicherheitsvereinbarung zahlen muss.

Cyber-Diebstahl

Der Versicherer ersetzt Vermögensschäden, die einem Versicherten dadurch entstehen, dass unmittelbar infolge einer Netzwerksicherheitsverletzung Gelder (auch Kryptowährungen), Waren oder Wertpapiere abhandenkommen oder erhöhte Nutzungsentgelte anfallen.

Schäden durch eigene Betriebsunterbrechung bei Ausfall fremder Dienstleister (Cloud-Ausfall)

Schäden, die entstehen, wenn ein Clouddienst einen Cyberangriff erleidet, nicht mehr erreichbar ist und das versicherte Unternehmen aufgrund dessen den Betrieb unterbrechen muss.

Vertragsstrafen bei Verletzung von Geheimhaltungsverpflichtungen

Der Versicherer erstattet Vertragsstrafen, die ein Versicherter wegen der Verletzung von Geheimhaltungspflichten und Datenschutzvereinbarungen zahlen muss.

Vertragsstrafen wegen Leistungsverzug

Der Versicherer erstattet Vertragsstrafen, die ein Versicherter wegen verzögerter Leistungserbringung zahlen muss. Beispiel: Vertragsstrafe bei einem Zulieferer, der nicht pünktlich liefern kann.

Bußgelder, Geldstrafen (Ausland)

Der Versicherer ersetzt – soweit dies in der ausländischen Rechtsordnung, nach der das Bußgeld verhängt wird, rechtlich zulässig sein sollte – Bußgelder, die eine Datenschutzbehörde oder ein Gericht wegen einer Datenrechtsverletzung gegen einen Versicherten verhängt.

Wiederherstellungskosten (Daten/IT-System)

Gibt die Höhe der Leistung für die Wiederherstellungskosten (Daten/IT-System) in Euro an.
Hierunter fallen

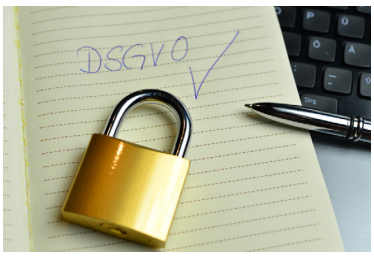
- die Wiederherstellung der ursprünglichen Funktionsfähigkeit des IT-Systems,
- die Wiederherstellung oder Reparatur von Daten,
- der Aufbau provisorischer Zwischenlösungen, um den Betrieb eines Versicherten aufrechtzuerhalten oder zeitnah wieder aufzunehmen sowie
- die Isolation und Säuberung der IT-Hardware, insbesondere die Entfernung von Schadprogrammen.

Ausfall der privaten oder öffentlichen Infrastruktur

Hierunter fallen Schäden aufgrund einer Störung oder eines Ausfalls der öffentlichen oder privaten technischen Infrastruktur.
Zur öffentlichen und privaten Infrastruktur gehören

- Strom- und Wasserversorgung,
- Netzstrukturen, die der überregionalen Informationsvermittlung dienen (insbesondere Telefon-, Internet- oder Funknetze sowie Leistungen von Internet- und Telekommunikationsanbietern respektive -providern),
- Domain Name Systems (DNS) sowie
- alle weiteren vergleichbaren privaten Einrichtungen oder Einrichtungen der Gebietskörperschaften.

Kein Versicherer verzichtet auf den Ausschluss für öffentliche Infrastruktur, da die Tragweite der Schäden gegebenenfalls unmessbar ist. Beispiel: Ein Stromnetzversorger der Stadt München wird gehackt. Alle Nutzer dieses Anbieters haben keinen Strom. Würde der Versicherer den öffentlichen Bereich nicht ausschließen, würden die Millionen Nutzer auch mit dazugehören.



Rechtswidrige Datenerfassung

Rechtswidrige Datenerfassung liegt vor, wenn ein Versicherter mit Kenntnis oder infolge grob fahrlässiger Unkenntnis eines Repräsentanten personenbezogene Daten im Sinne der Datenschutz-Grundverordnung (DSGVO) oder entsprechender ausländischer Rechtsnormen rechtswidrig erfasst.

Regelmäßige Datensicherung

Hier verlangt der Versicherer als Antragsfrage oder bestimmt in den Obliegenheiten, dass Daten regelmäßig gesichert werden müssen, z. B. mindestens monatlich, wöchentlich oder täglich.

Antivirenprogramme mit aktuellen Virendatenbanken

Antivirenprogramme, Virenscanner oder Virenschutzprogramme sind Softwares, die Schadprogramme wie z. B. Computerviren, Computerwürmer oder Trojaner aufspüren, blockieren und gegebenenfalls beseitigen sollen.

Cyber-Risk

Firewalls

Eine Firewall ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt, in der Regel an allen Netzübergängen zum Internet.

Patch-Management (automatisierter Prozess zum Aufspielen von Updates, Patches und Servicepacks zur Schließung von Sicherheitslücken)

Alle Systeme sollten immer auf dem aktuellsten Stand sein, sodass mögliche Sicherheitslücken geschlossen werden.

© kebox, ClipDealer, #109329

Zugangskontrollen für Ihre IT-Systeme (z. B. Benutzerkennungen und Passwörter)

Passwörter für Systeme, Computer, Netzwerke und manchmal auch ein abgestuftes Rechtekonzept mit administrativen Kennungen ausschließlich für IT-Verantwortliche.

Die Punkte „Antivirenprogramme mit aktuellen Virendatenbanken“, „Firewalls“, „Patch-Management (automatisierter Prozess zum Aufspielen von Updates, Patches und Servicepacks zur Schließung von Sicherheitslücken)“ und „Zugangskontrollen für Ihre IT-Systeme (z. B. Benutzerkennungen und Passwörter)“ sind, ebenso wie der Punkt „Regelmäßige Datensicherung“, entweder in den Obliegenheiten oder den Antragsfragen zu finden.

Rev. 102021