LEISTUNGSVERGLEICH CYBER-RISK

	CyberEdge online 2019	CyberSchutz	AL_Cyber	ByteProtect Kompakt	Cyber-Police
Prävention - Leistungen vor Eintritt des Versicherungsfalles					
Krisenplan (kostenfrei)	✗	✓	✓	✓ Vorlage wird zur Verfügung gestellt	✓ Kurzanleitung (Erste Hilfe im Schadenfall)
Cyber-Training für Mitarbeiter des VN (kostenfrei)	✓ ab Jahresprämie 5.000 € (brutto)	✓	✓	✓ für 6 Monate über Online-Portal inkl. Schulungsnachweis nach DSGVO	✗ (aber externe Kooperation mit Perseus - 15% Rabatt auf Dienstleistungen)
Soforthilfe (bereits bei Verdacht eines Vers.-falles) ohne Anrechnung auf Versicherungssumme ohne Selbstbehalt	✓ (48 Stunden)	✓ (24 Stunden)	✓	✓ (Soforthilfe über T-Systems Hotline)	✓ (24 Stunden)
Assistance / Netzwerk					
Krisenberater	✓ über KPMG für IT-Forensik und CMS für Recht	✓	✓	✓ T-Systems und weitere Dienstleister	✓ über Perseus
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	⊕ in Abstimmung mit VR möglich	⊕ in Abstimmung mit VR möglich
Deckungsauslöser					

	AIG CyberEdge online 2019	Allianz CyberSchutz	ALH Gruppe AL_Cyber	AXA ByteProtect Kompakt	baloise Cyber-Police
Hacker - Angriffe (gezielte u. ungezielte)	✓	✓	✓	✓	✓
DoS - Denial of Service (Unterbrechung IT-System)	✓	✓	✓	✓	✓
Infektion der Systeme mit Schadsoftware (Viren, Würmer, Trojaner usw.)	✓	✓	✓	✓	✓
Datenrechtsverletzung	✓	✓	✓	✓	✓
Bedienfehler	✓	+	✓	✓	✓
Rechtsverletzung durch Werbung Medien	✗	✓	✓	✓	✓
Versicherungsleistungen					
Geltungsbereich	weltweit	weltweit	weltweit	weltweit	weltweit
Mitversicherte Unternehmen	VN und seine Tochtergesellschaften	VN und seine Tochtergesellschaften im Inland und EWR (neu hinzukommende Gesellschaften zunächst über Vorsorge mitvers.)	Versicherungsnehmer und im Versicherungsschein benannte mitversicherten Unternehmen in Deutschland	VN und seine Tochtergesellschaften im Inland u. Ländern des EWR	VN und seine Tochtergesellschaften im Inland u. EU-Länder
Rückwärtsdeckung	✓ unbegrenzt	✓ unbegrenzt	✓ unbegrenzt	✓ unbegrenzt	✓ unbegrenzt
Nachmeldefrist	✓ 3 Jahre n. Beendigung d. Vertrages	✓ 5 Jahre n. Beendigung d. Vertrages	✓ 60 Monate n. Beendigung d. Vertrages	✓ 3 Jahre n. Beendigung d. Vertrages	✓ 5 Jahre n. Beendigung d. Vertrages

	AIG CyberEdge online 2019	Allianz CyberSchutz	ALH Gruppe AL_Cyber	AXA ByteProtect Kompakt	baloise Cyber-Police
Vorrangiger Versicherungsschutz (keine Subsidiarität)	✓	✓	✓	✓ jedoch Subsidiär zu Haftpflicht	✓
Max. Versicherungsleistung über Standardmodell (Antrag)	3.000.000 €	500.000 €	5.900.000 € je Schaden, 11.800.000 € je Versicherungsjahr	1.000.000 €	1.000.000 €
Haftpflichtansprüche Dritter inkl. Vermögensschäden	✓	✓	✓	✓	✓
Max. Versicherungsleistung bei Individualanfrage	10 Mio. €, Individualanfragen laufen über CyberEdge 2019	5.000.000 €	kein Limit	5.000.000 €	5.000.000 €
Entschädigungsgrenzen / Sublimits / Selbstbehalte					
Assistanceleistungen	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	Sublimit individual vereinbar, max. bis zur Versicherungssumme
Erstattung von Forensikkosten	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	Sublimit individual vereinbar, max. bis zur Versicherungssumme
Schaden durch eigene Betriebsunterbrechung	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	Sublimit individual vereinbar, max. bis zur Versicherungssumme
Mehrkosten durch Betriebsunterbrechung	im Rahmen der Versicherungssumme	soweit es sich um Schadenminderungskosten handelt	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	Sublimit individual vereinbar, max. bis zur Versicherungssumme
Vertragsstrafen an E-Payment Service Provider	20% der Versicherungssumme, max. 500.000 €	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	bis 5 % der VSU	Sublimit individual vereinbar, max. bis zur Versicherungssumme
Cyber-Diebstahl	⊕ 20 % der VSU, max. 500.000 €	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	bis 10 % der VSU	Sublimit individual vereinbar, max. bis zur Versicherungssumme
Schaden durch eigene Betriebsunterbrechung bei Ausfall fremder Dienstleister (Cloud-Ausfall)	⊕ 20 % der VSU, max. 500.000 €	⊕ bis zur Versicherungssumme	im Rahmen der Versicherungssumme	bis 10% der VSU	⊕ bis 100.000 € (im individuellen Underwriting bis 250.000 € möglich)
Vertragsstrafen bei Verletzung von Geheimhaltungsverpflichtungen	✗	✗	✗	✗	Sublimit individual vereinbar, max. bis zur Versicherungssumme

	AIG CyberEdge online 2019	Allianz CyberSchutz	ALH Gruppe AL_Cyber	AXA ByteProtect Kompakt	baloise Cyber-Police
Vertragsstrafen wegen Leistungsverzug	✗	✗	✗	✗	Sublimit individual vereinbar, max. bis zur Versicherungssumme
Bußgelder, Geldstrafen (Ausland)	+ 20 % der VS, max. 500.000 €	Bussgeld soweit rechtlich zulässig	im Rahmen der Versicherungssumme (DSGVO-Bußgelder)	✗	Sublimit individual vereinbar, max. bis zur Versicherungssumme
Wiederherstellungskosten (Daten / IT-System)	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	im Rahmen der Versicherungssumme	Sublimit individual vereinbar, max. bis zur Versicherungssumme
generelle Selbstbehalte	wahlweise 5.000 € oder 10.000 €	wahlweise 1.000 €, 2.500 €	wahlweise 0, 250, 500, 1.000, 2.500, 5.000 € (Betriebsunterbrechnung: 0, 8, 12, 24, 48 Stunden)	wahlweise 1.000 €, 2.500 € oder 5.000 €	wahlweise 500 €, 1.000 € oder 2.500 € wahlweise 6 h, 12 h oder 24 h
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	✗	✗	✗	✓ bezogen auf Telekommunikation	✗
rechtswidrige Datenerfassung	✗	✗	✓	✓	✓
Insolvenz	✓	✓	✓	✗	✓
Umgang mit nachfolgenden Sicherheitsvorschriften					
regelmäßige Datensicherung	erforderlich (siehe Antragsfragen)	erforderlich, kein genaues Intervall (siehe Antragsfragen)	mindestens einmal wöchentlich (siehe Obliegenheiten)	mindestens einmal wöchentlich (siehe Obliegenheiten)	mindestens einmal wöchentlich, inklusive physischer Trennung (siehe Obliegenheiten)
Anti-Virenprogramme mit aktuellen Virendatenbanken	erforderlich (siehe Antragsfragen)	erforderlich (siehe Antragsfragen)	erforderlich, inklusive automatischer Aktualisierung (siehe Obliegenheiten)	erforderlich, inklusive automatischer Aktualisierung (siehe Obliegenheiten)	erforderlich, inklusive automatischer Aktualisierung (siehe Obliegenheiten)
Firewalls	erforderlich (siehe Antragsfragen)	erforderlich, inklusive Überprüfung und Aktualisierung bei Bedarf (siehe Antragsfragen)	erforderlich, inklusive ständiger Aktualisierung (siehe Obliegenheiten)	erforderlich (siehe Obliegenheiten)	erforderlich, inklusive ständiger Aktualisierung (siehe Obliegenheiten)

	AIG CyberEdge online 2019	Allianz CyberSchutz	ALH Gruppe AL_Cyber	AXA ByteProtect Kompakt	baloise Cyber-Police
Patch-Management (automatisierter Prozess zum Aufspielen von Updates, Patches und Servicepacks zur Schließung von Sicherheitslücken)	erforderlich (siehe Antragsfragen)	erforderlich (siehe Antragsfragen)	erforderlich (siehe Obliegenheiten)	erforderlich (siehe Obliegenheiten)	erforderlich (siehe Obliegenheiten)
Zugangskontrollen für Ihre IT-Systeme (z. B. Benutzerkennungen und Passwörter)	erforderlich (siehe Antragsfragen)	erforderlich (siehe Antragsfragen)	erforderlich (siehe Obliegenheiten)	erforderlich (siehe Obliegenheiten)	erforderlich, inklusive Rechtekonzept (siehe Obliegenheiten)
Begrenzung der Leistungskürzung bei grob fahrlässiger Verletzung der Sicherheitsvorschriften	✗	✗	✗	✗ max. Kürzung um 20 % bei Schäden bis 100.000 € bei Verletzung von gesetzlichen oder behördlichen Maßnahmen zur Minderung und Verhütung eines Schadens	✓ max. Kürzung um 20 % bei Schäden bis 250.000 €.
Versicherbare Branchen					
Dienstleister	✓ Ausnahmen beachten	✓ jedoch für Finanzdienstleister anderes Produkt	✓ Ausnahme Finanz-/Inkasso-/IT-Dienstleister	✓ Ausnahme Banken, Versicherungen, Zahlungsdienstleister, IT-Dienstleister	✓
öffentl. Unternehmen / Kommunen	✓	+ auf Anfrage	✗	✓	✗
Produktionsunternehmen	✓	✓	✓	✓	✓
Handel	✓	✓	✓	✓	✓
Online-.Handel	✓ über Antragsmodell nur wenn der Onlinehandel max. 50 % des Umsatzes beträgt; darüberhinaus individuelle Anfrage möglich.	✓	✓ Individuelles Underwriting bei mehr als 70 % Onlineumsatz	✓	✓

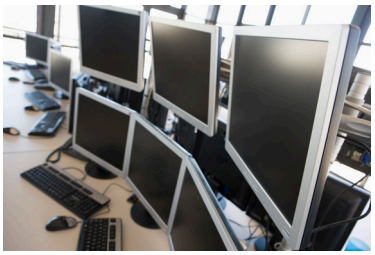
	AIG CyberEdge online 2019	Allianz CyberSchutz	ALH Gruppe AL_Cyber	AXA ByteProtect Kompakt	baloise Cyber-Police
Handwerk	✓	✓	✓	✓	✓
Versicherungsmakler	✓ soweit diese nicht auch Finanzdienstleistungen (Kredite, Konten, Geldanlage, etc.) vermitteln oder dazu beraten	✓	✓ keine Drittschadendeckung möglich	✓	✓

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

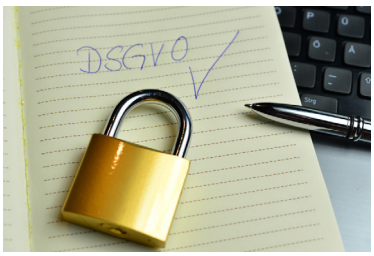
- die Wiederherstellung der ursprünglichen Funktionsfähigkeit des IT-Systems,
- die Wiederherstellung oder Reparatur von Daten,
- der Aufbau provisorischer Zwischenlösungen, um den Betrieb eines Versicherten aufrechtzuerhalten oder zeitnah wieder aufzunehmen sowie
- die Isolation und Säuberung der IT-Hardware,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