Deckungsübersicht

Versichert sind Schäden, die durch einen rechtswidrigen Eingriff eines Kriminellen, Online-Betrug oder durch Schadprogramme in die Computersysteme des Versicherungsnehmers und der im Haushalt lebenden Personen entstehen. Versichert ist die Unterstützung bei Cyber-Erpressung und Cyber-Mobbing und Schäden, die durch das Verschulden des Versicherungsnehmers und der im Haushalt lebenden Personen an Dritten entstehen.

	Variante Basis	Variante Plus
Eigen- und Drittschadenkomponente	✓	✓
Versicherungssumme	EUR 5.000,–	EUR 10.000,–
Bagatellgrenze	EUR 100,–	EUR 100,–
monatliche Bruttoprämie	EUR 4,99	EUR 7,99
1-Jahresvertrag (mit automatischer Verlängerung)	–	–
Risikofragen	nein	nein
Klauselnummer	3028K	3029K

Deckungsbausteine

	Variante Basis	Variante Plus
Diebstahl von Finanzmittel (Versicherungssumme EUR 3.000,–)	✓	✓
Datenwiederherstellung / Entfernung von Schadsoftware	✓	✓
Hardware Ersatz	✓	✓
Cyber Erpressung	✓	✓
Online Einkauf/Verkauf (Versicherungssumme EUR 3.000,–)	✓	✓
Haftung für Netzwerksicherheit	✓	✓
Haftung für Privatsphäre und Datenschutzverletzung	✓	✓
Identitätsdiebstahl	–	✓
Cybermobbing	–	✓
Social Media und Datenschutzverletzung	–	✓
Smart-Home Deckung	–	✓

Deckungsbausteine im Detail

Diebstahl von Finanzmittel

Personen werden Opfer einer Phising-Attacke oder einer E-Mail-Manipulation. Es wird durch einen nicht autorisierten Zugriff Dritter auf das Bankkonto, die Kreditkarte, etc., oder eines Gerätes für mobile Zahlung des Kunden zugegriffen. Kriminelle versuchen über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Nutzers zu gelangen (Kontoplünderung).

Datenwiederherstellung und Entfernung von Schadsoftware

Die IT-Geräte und/oder Softwareprogramme funktionieren wegen eines Cybervorfalles nicht mehr. Es entstand ein Datenverlust, eine Datenmanipulation oder eine Datenverschlüsselung auf den Computersystemen des Kunden. Kriminelle versuchen mit infizierten Anhängen, gefälschten E-Mails oder Webseiten Viren, Trojaner oder andere Schadsoftware in Umlauf zu bringen.

Hardware-Ersatz

Die Hardware funktioniert nach einem Cybervorfall nicht mehr ordnungsgemäß. Durch die Verbreitung von Schadprogrammen entsteht ein Datenverlust, eine irreparable Schädigung der Hardware.

Cybererpressung

Es erfolgt ein Angriff auf das Computersystem des Kunden. Beispielsweise wird eine Schadsoftware von einem Hacker installiert oder das IT-Gerät wird komplett verschlüsselt und lässt sich nicht mehr bedienen. Der Erpresser fordert Lösegeld um das IT-Gerät wieder frei zu geben. In den letzten Jahren haben sich Kriminelle bei Erpressungen meist auf Ransomware (Schadsoftware die Daten kidnappt) konzentriert. Oft erhält das Opfer eine E-Mail, in der der Entschlüsselungs-Key gegen eine Zahlung in der digitalen Währung Bitcoins angeboten wird.

Online-Einkauf und Online-Verkauf

Personen erleiden Vermögensschäden, die durch Transaktionen im Internet beim Kauf oder Verkauf durch mobile Zahlung oder Kreditkarten entstehen. Beispielsweise beim Kauf von Waren im Internet die es gar nicht gibt. Oder wenn Personen Waren verkaufen, die der Käufer nicht bezahlt.

Haftung für Netzwerksicherheit

Personen haften für Schäden an Dritten. Schadsoftware wird ausgehend vom Computersystem an den Dritten weiter gegeben. Beispielsweise in Form eines E-Mails oder eines USB-Sticks.

Haftung für Privatsphäre und Datenschutzverletzung

Personen begehen bei einem Cybervorfall Datenschutzverletzungen. Namen, Fotos, vertrauliche Aufzeichnungen und sonstige Daten gelangen nach dem Cybervorfall ins Internet.

Identitätsdiebstahl

Es werden personenbezogene Daten gestohlen. Die im Internet gestohlenen Daten werden von dem Dieb benutzt, um sich die virtuelle Identität anzueignen. Dies können beispielsweise der Name, Fotos, Aufzeichnungen etc. sein. Mit dem Identitätsdiebstahl kann beispielsweise im Namen der Kunden Online-Betrug begangen werden.

Cybermobbing

Personen werden mit Cybermobbing konfrontiert und/oder erleiden sonstige Reputationsschäden im Internet. Beispielsweise mit Versand von E-Mails oder SMS, Belästigung im Chat oder im Instand Massaging, auf Webseiten oder durch die Verbreitung von Videos.

Social-Media und Datenschutzverletzung

Medieninhalte und Medienaktivitäten Dritter werden vom Versicherungsnehmer auf sozialen Netzwerken verletzt. Beispielsweise wenn Kinder des Kunden andere Personen auf sozialen Netzwerken mobben oder Rufschädigung betreiben, oder wenn urheberrechtliche Dokumente (z. B. Bilder der Dritten), Texte, Videos etc. in sozialen Netzwerken verbreitet werden.

Smart-Home-Deckung

Die Smart Home Geräte funktionieren wegen eines Cybervorfalles nicht mehr, oder teilweise nicht mehr. Es entstand ein Datenverlust, eine Datenbeschädigung oder eine Datenverschlüsselung auf den Computersystemen des Kunden. Es erfolgte eine Verbreitung von Schadprogrammen (Virus, Trojaner, Spyware, etc.).

Was tun bei einem Cybervorfall?

Mit DONAU Sicher im Netz ist die erste Anlaufstelle im Schadensfall die

Hotline 050 330 333

Es wird ein Kontakt zu IT-Experten hergestellt

24 Stunden täglich, 365 Tage im Jahr

Unser IT-Dienstleister unterstützt in 2 Stufen

▪ Telefon

Manchmal genügt schon ein Anruf und unsere IT-Experten wissen Rat.

▪ Fernwartung

Der Spezialist der Hotline verbindet sich mit Ihrem System und löst auf diese Weise das Problem.

Welche Obliegenheiten müssen Sie beachten?

Wir leisten an unsere KundInnen wenn die KundInnen die Empfehlungen des Herstellers oder Lieferanten umgesetzt haben.

- **Beispiel:** Das WLAN des Router muss mit einer Verschlüsselung betrieben werden. Diese ist in der Regel bei den Werkseinstellungen standardmäßig eingestellt. Gegebenenfalls muss das Werkseinstellungspasswort durch ein neues, sicheres Passwort ersetzt werden (Installationsanleitung Hersteller beachten). Wenn diesem vorgegeben Vorgehen gefolgt wird, leisten wir im Versicherungsfall.

Wir leisten, wenn die Bereitstellung und Aktualisierung des Betriebssystems auf den IT- Geräten nach Installations-empfehlung des Herstellers erfolgt, und geeignete Technologien zur Erhöhung Sicherheit der Systeme, Geräte und Daten (z. B. Virenschutz, Firewalls, etc.) verwendet werden.

- **Beispiel:** Sicherheitsupdates, welche von den Software Entwicklern (z. B. Apple) ausgerollt werden, müssen zeitnah (maximal binnen 14 Tagen) installiert werden.

Wichtig

Wir empfehlen regelmäßige Sicherungen (Back Up) durchzuführen. Die Basis der Datenwiederherstellung ist die zuletzt durchgeführte Datensicherung

Was ist nicht versichert?

- Versicherungsfälle, die zu einem Schaden führen könnten, die vor Abschluss bekannt waren
- absichtliches, böswilliges, betrügerisches oder vorsätzliches Fehlverhalten der KundInnen
- jedes Handeln oder Unterlassen im Rahmen Ihrer beruflichen oder gewerbliche Tätigkeit
- Verlust oder Beschädigung der IT-Geräte, die Folgeschäden und der Nutzungsausfall dadurch
- Schäden durch Kriegsereignisse
- Investitions- oder Handelsverlust und die Unmöglichkeit, Wertpapiere zu veräußern
- Körperverletzungen, psychische Schäden, Trauma, Krankheit oder Tod; Versichert sind jedoch Angstzustände oder mentaler Stress (Baustein Identitätsdiebstahl und Cybermobbing).
- Diebstahl, Verletzung oder Missbrauch von geistigem Eigentum (Patente, Marken, Urheberrechte),Dieser Ausschluss gilt nicht für den Baustein Social-Media Haftung. Der Diebstahl, die Verletzung, oder der Missbrauch von Patenten bleiben jedoch immer ausgeschlossen.
- Ansprüche von Dritten, die von einem Versicherten gegen einen anderen Versicherten vorgebracht werden vertragliche Haftungen, die über die gesetzliche Haftung hinaus gehen
- Ausgaben für eine Verbesserung von IT- oder Smart-Home-Geräten, die über den Zustand vor dem Versicherungsfall hinausgehen
- Kryptowährungen (z. B. Bitcoin, Ethereum, Ripple, IOTA)
- Glücksspiele

Wie können die Kunden DONAU Sicher im Netz abschließen?

Webseite

Informationen zu DONAU Sicher im Netz sind auf unserer Webseite bei den Privatkunden zu finden.

https://www.donauversicherung.at/privatkunden/cyberversicherung

Wenn Sie für Ihre KundInnen DONAU Sicher im Netz beantragen, geben Sie bitte Ihre Vermittlernummer an. Ein entsprechendes Feld finden Sie bei der Beantragung über die Webseite.

Antrag

Wir stellen einen Antrag, der elektronisch befüllbar ist, zur Verfügung.

Der unterschriebene Antrag muss an die Vertragsverwaltung SHU zur Polizzierung übermittelt werden.

Ja,

mit uns kann man reden.

Bei Fragen wenden Sie sich gerne an Ihre regionale Führungskraft oder an die DONAU Cyber Hotline.

donau.cyber@donauversicherung.at

So stell ich mir das vor

Serviceline 050 330 330 | donau@donauversicherung.at

donau BROKER LINE

Aus Gründen der besseren Lesbarkeit wird auf die geschlechtsspezifische Differenzierung bei zusammengesetzten Wörtern und Produktnamen verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichstellung selbstverständlich für alle Geschlechter.

Hinweis: Zweck dieser Unterlage ist eine kurze und geraffte Information über unser Produkt. Es ist kein Angebot im rechtlichen Sinn. Der Inhalt wurde sorgfältig erarbeitet, doch kann die verkürzte Darstellung zu missverständlichen oder unvollständigen Eindrücken führen. Für verbindliche Informationen verweisen wir auf die vollständigen Antragsunterlagen, die Polizzen und die diesen zugrunde liegenden Versicherungsbedingungen.

Medieninhaber und Hersteller: DONAU Versicherung AG Vienna Insurance Group | Verlags- und Herstellungsort: Wien | Bildnachweis: shutterstock.com
J20-0122-DBL (20.09)