Cyberversicherung für Geschäftskunden

donau
VIENNA INSURANCE GROUP

Risiken erkennen

Mit dem Sicherheits-Check unseres Kooperationspartners Risk Experts Engineering GmbH werden Schwachstellen erkannt.

Maßnahmen ergreifen

Empfehlungen für mehr IT-Sicherheit

Unser Produkt

Sichert Unternehmen gegen die finanziellen Folgen eines digitalen Einbruchdiebstahls ab

Schadensmanagement

Unterstützt rasch und unkompliziert

Ja,

gegen Cyberrisiken bieten wir ganzheitliche Lösungen für Unternehmer.

So stell ich mir das vor

Der DONAU Cyber-Sicherheits-Check

Mit dem DONAU **Cyberversicherung Sicherheits-Check** erkennen Sie rasch und unkompliziert Sicherheitsschwachstellen und erhalten Empfehlungen, um Ihre IT-Sicherheit zu verbessern.

Die Internetkriminalität ist in den vergangenen Jahren rasant angestiegen und wird mit zunehmender Digitalisierung vermutlich noch weiter ansteigen.

Verschaffen Sie sich jetzt einen Überblick über den Sicherheitsstatus Ihres IT-Systems.

- Können Hacker auf einfachem Wege in Ihr IT-System eindringen?
- Sind die Daten Ihrer Webseitenbesucher ausreichend geschützt?
- Sind Sie offen für digitale Angriffe und wurden Sie bereits angegriffen?
- Ist Ihr Außenauftritt im Internet gefährdet?

Der Sicherheits-Check

Der Sicherheits-Check erfolgt mit einem speziell dafür entwickelten Programm unseres Kooperationspartners **Risk Experts Engineering GmbH.**

Der IT-Sicherheits-Check **analysiert Angriffsmöglichkeiten aus dem Internet auf bekanntgegebene Domains.** Der Scanner sucht nach vorhandenen Diensten und bewertet die Konfiguration dieser Dienste. Das Ergebnis wird mit den Scans anderer Praxen verglichen und enthält Empfehlungen, um die Sicherheit gemäß dem Stand der Technik zu erhöhen und Probleme bewusst zu machen.

Ja, sichern Sie Ihr Unternehmen gegen die Risiken der digitalen Welt ab.

Schützen Sie Ihr Unternehmen rechtzeitig vor einem digitalen Einbruch, damit Sie vor hohen finanziellen Schäden aufgrund von Internetkriminalität bewahrt bleiben.

Die Cyberversicherung der DONAU hilft zum Beispiel bei folgenden Szenarien

Schadsoftware

Mit einem USB-Stick wird eine Schadsoftware in das betriebliche Kommunikationsnetzwerk eingeschleust. Diese Schadsoftware legt nach und nach den Betrieb lahm. Kundendaten werden gelöscht, innerbetriebliche Seiten können nicht mehr geöffnet werden. Das Unternehmen wird dadurch handlungsunfähig: Rechnungen können nicht mehr ausgestellt werden, Kunden können nicht bedient werden, ein Imageschaden entsteht. Die DONAU Versicherung wird kontaktiert. Diese leitet die notwendigen Schritte ein und unterstützt wie folgt: Die IT-Experten benötigen 30 Stunden für die Datenwiederherstellung. Es fallen Kosten für das manuelle Eingeben von Daten an. Insgesamt steht das Unternehmen 45 Stunden still. Die IT-Spezialisten kümmern sich um die Neuinstallation, Rekonfigurationen und Reparaturen.

Die PR-Experten unterstützen mit einer Kampagne gegenüber der Öffentlichkeit. Der versicherte Schaden beträgt gesamt 60.000,– Euro.

Cyberangriff

Die Kunden eines Händlers erhalten etliche E-Mails ohne Inhalt und beschweren sich aufgrund dessen bei dem Unternehmen. Was ist passiert? Der Computer des Händlers ist von einem Virus befallen. Der IT-Experte löst das Problem. Kostenpunkt 200,– Euro. Kurze Zeit später meldet sich der Rechtsanwalt eines Geschäftskunden.

Durch die infizierte E-Mail sind am Computer des Geschäftskunden Schäden entstanden. Die elektronische Kundenkartei ist nicht mehr aufrufbar. Die Cyberversicherung des Händlers übernimmt die Kosten für die Wiederherstellung der Kundenkartei und Behebung der Schäden am Computer sowie die Anwaltskosten. Der versicherte Schaden inklusive Kosten des Anwalts beträgt 45.000,– Euro.

Umfassender Versicherungsschutz

Mit unserer Cyberversicherung verfügen Sie über einen umfangreichen Basisschutz, den Sie je nach Bedarf um weitere Bausteine ergänzen können.

Basisschutz

Deckt Schäden im Unternehmen (Eigenschaden) und Schäden bei Dritten (z. B. Lieferanten, Kunden). Auslöser können beispielsweise eingeschleuste Schadprogramme oder rechtswidrige Hackerangriffe sein. Folgende Schäden können dadurch entstehen:

- **Datenschutzverletzungen**
- **Zahlungssysteme fallen aus** (PCI-DSS)
- **Daten werden beschädigt oder gehen verloren**
- Schadensersatzforderungen wegen **Verletzung der Geheimhaltungspflicht**
- Ihre Programme richten durch **infizierte Software an fremden Servern oder Netzwerken** Schaden an
- Schäden aufgrund **unsachgemäßer Bedienung der Computersysteme** (z. B. Fehlprogrammierung durch einen Mitarbeiter, Installation von nicht freigegebenen Updates)

Erweiterbare Bausteine

- **Krisen- und PR-Management**
- **Leistung bei Betriebsunterbrechung von mehr als zwölf Stunden**
- **Support bei Erpressung**
- **Medienhaftpflicht** (Kostenübernahme der Prüfung und der Abwehr von Ansprüchen inklusive Anwalts- und Gerichtskosten)
- **Cyber-Betrug und Cyber-Diebstahl**
- **Outsourcing-Dienstleistungen***

Wählbare Versicherungssummen

- **EUR 75.000,–**
- **EUR 150.000,–**
- **EUR 300.000,–**
- **EUR 750.000,–**

Wählbarer Selbstbehalt

- **EUR 500,–**
- **EUR 1.000,–**
- **EUR 3.000,–**

* Outsourcing-Dienstleister sind IT-Dienstleister, die vom Versicherungsnehmer durch einen schriftlichen Vertrag beauftragt werden

Wir unterstützen Sie in drei Stufen

Mit der Cyberversicherung der DONAU können Sie sich im Schadensfall als erste Anlaufstelle an unsere Seviceline 050 330 330 wenden, wo ein Kontakt zu IT-Experten hergestellt wird. So erhalten Sie Sofort-Hilfe und das 24 Stunden täglich.

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.

Vor Ort

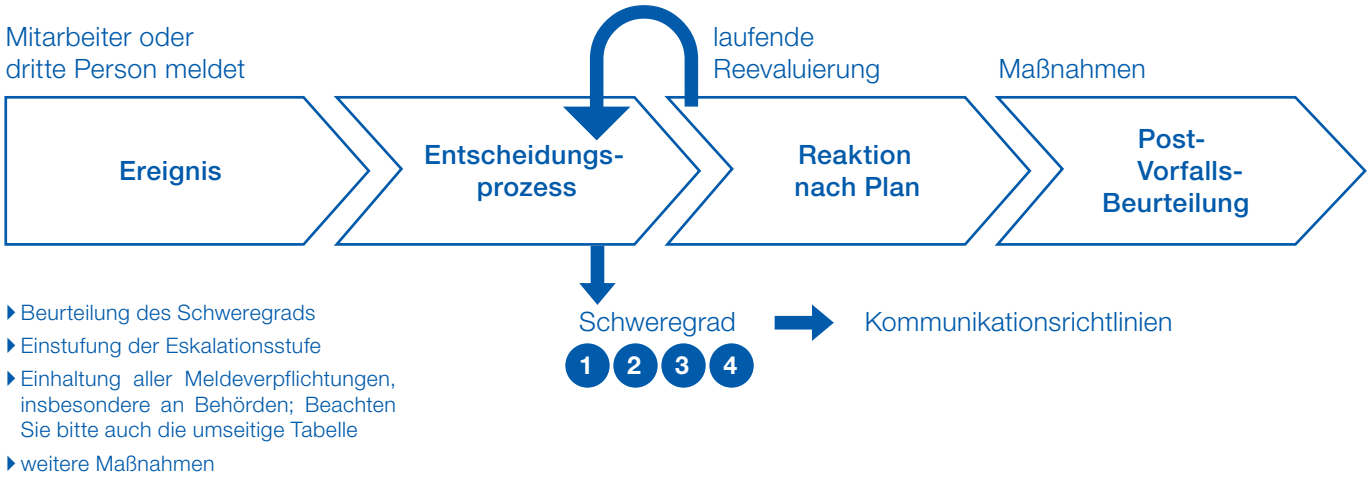
Der Experte kommt zu Ihnen und veranlasst alles Nötige im Haus.

Leitfaden im Cyber-Schadensfall

Bitte stellen Sie sicher, dass dieser Leitfaden für die Reaktion auf Vorfälle immer verfügbar und auch in analoger Form an leicht zugänglicher Stelle in der Praxis hinterlegt ist. Dasselbe gilt für die Polizze.

Aktualisieren Sie diesen Leitfaden zu Ihrer eigenen Sicherheit regelmäßig.

Dieser Leitfaden ist ein essenzielles Tool zur optimalen und raschen Bewältigung eines eingetretenen IT-Notfalls. Er hilft, bereits vorab Verantwortlichkeiten, Prozesse und Maßnahmen zu definieren, um diese im Ernstfall parat zu haben. Überdies unterstützt er Entscheidungsträger dahingehend, die Vorfälle nach Schweregrad einzustufen und die dafür vorgesehenen Eskalationsprozesse zu initiieren.



Erklärungen & Hinweise zur Verwendung dieses Leitfadens

- Zweck dieses Leitfadens ist die Zurverfügungstellung einer kurzen und gerafften Handlungsempfehlung, welche im Notfall herangezogen werden kann. Der Inhalt wurde zwar sorgfältig erarbeitet, doch können die Anforderungen je nach Praxis unterschiedlich sein, weswegen diese Empfehlungen keinen IT-Notfallplan ersetzen. Für verbindliche Informationen verweisen wir auf die vollständigen Antragsunterlagen, die Polizzen und die zugrundeliegenden Versicherungsbedingungen.

Wenden Sie sich im Schadensfall bzw. zur Schadensmeldung sowie in Zweifelsfällen bitte immer an die **DONAU 24/7-Serviceline unter 050 330 330**

In jedem Fall gilt es Ruhe zu bewahren.

Was ist NICHT zu tun

- Zur Kontaktaufnahme betroffene/gehackte Endgeräte verwenden.
- Eigenmächtige Reparaturen und Wiederherstellungsversuche unternehmen – **IT-Systeme abschalten!**

Was ist zu tun

- Nehmen Sie jeden Vorfall ernst. **Keine Scheu vor der Kontaktaufnahme, wir stehen auf Ihrer Seite.**
- Eine Führungskraft bzw. verantwortliche Person sollte sich bei der Serviceline melden.
- Nur die **Serviceline 050 330 330** zur Schadensmeldung verwenden.
  - Die Serviceline verbindet Sie automatisch mit dem IT-Dienstleister.
  - Es erfolgt eine Aufnahme und Beurteilung des Schadens.
  - Entsprechende Maßnahmen werden vereinbart.
- **IT-Systeme unbedingt eingeschaltet lassen!**

Fragen im Krisenfall

Bei Vorliegen von einem „JA“ sind die Maßnahmen nach **Schweregrad 2/3/4** einzuleiten (siehe unten).

Auswirkung	Möglich?
Liegt ein Datenleck vor?	☐ ja ☐ nein
Gibt es eine Lösegeldforderung im Zusammenhang mit einem IT-Vorfall?	☐ ja ☐ nein
Liegt ein Vertrauensbruch durch einen Arbeitnehmer vor?	☐ ja ☐ nein
Liegt ein Gesetzesverstoß (DSGVO etc.) vor?	☐ ja ☐ nein
Sind Server oder für den Gesamtbetrieb wesentliche Netzwerkkomponenten (z. B. Firewall, zentrale Router etc.) betroffen?	☐ ja ☐ nein
Könnten Kunden/Lieferanten geschädigt sein?	☐ ja ☐ nein
Kann der Vorfall öffentlichkeitswirksam werden?	☐ ja ☐ nein
Werden in Ihrem Netzwerk personenbezogene Daten und/oder Gesundheitsdaten gespeichert?	☐ ja ☐ nein

IT-Notfall Schweregrade | Verantwortlichenmatrix und Kommunikationsrichtlinien

Ergänzen Sie die Tabelle um weitere Akteure. Die zugehörigen Kontaktdaten müssen separat gespeichert werden.

	1 Sicherheitsereignis ▸ Normalbetrieb möglich; ▸ Schaden möglich		2 Sicherheitsvorfall ▸ möglicher finanzieller Verlust ▸ möglicher Reputationsverlust		3 schwerer Sicherheitsvorfall ▸ möglicher Datenschutz-Vorfall ▸ hoher finanzieller Schaden ▸ Reputationsverlust		4 Sicherheitsnotfall ▸ massiver Reputationsverlust ▸ Datenschutz-Sanktionen ▸ Schadensersatzforderung ▸ Kerngeschäft betroffen	
	involviert	informiert	involviert	informiert	involviert	informiert	involviert	informiert
Management		x		x	x		x	
DONAU Versicherung	x		x		x		x	
Rechtsberater/ggfs. Datenschutzbehörde		o		x	x		x	
Public Relations Öffentlichkeitsarbeit, die dazu dient, das Vertrauen wieder aufzubauen		o		x	x		x	
IT-Verantwortlicher		x	x		x		x	
Datenschutzbeauftragter		x		x	x		x	

x verpflichtend o optional

Die DONAU-Vorteile auf einen Blick

- mit dem **Sicherheits-Check** erkennen Sie Schwachstellen im IT-System*
- **24 Stunden Support**, 7 Tage in der Woche - per Telefon, Fernwartung oder direkt vor Ort
- **Spezialisten stehen zur Verfügung**
  IT-Fachleute, Anwälte, Krisenmanager, Marketing- und PR-Agenturen
- **mit unseren Versicherungsleistungen decken Sie die wichtigsten Fälle ab**
  Datenverlust, Datenschutzverletzungen und auch Schäden Dritter
- **nur eine Anlaufstelle**
  entsprechende Experten werden eingesetzt, Maßnahmen koordiniert und abgestimmt
- **Eigen- und Fremdschäden**
  Egal, wo der Schaden im Informations- und Kommunikationssystem entsteht, ob in Ihrem Unternehmen oder bei Dritten, Sie sind finanziell abgesichert.**
- **Kosten für die IT-Experten werden bis 48 Stunden nach Auftreten des Schadensfalls übernommen**, auch wenn sich danach herausstellt, dass es sich nicht um einen Schadensfall im Rahmen der Cyberversicherung handelt.

* Der Sicherheitscheck erkennt einige Schwachstellen im System und kann daher das Risiko eines Cyber-Angriffs minimieren, aber nicht zur Gänze ausschließen.

** Bis zur Höhe der Versicherungssumme

So stell ich mir das vor

050 330 330 donau@donauversicherung.at donauversicherung.at/kontakt donauversicherung.at DONAUVersicherungAG

Personenbezogene Bezeichnungen in diesem Dokument beziehen sich auf alle Geschlechter in gleicher Weise. 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 | DB6-1AiO (22.07)

Die DONAU ist stolzer Förderer des Nationalparks Hohe Tauern.

donau VIENNA INSURANCE GROUP