CYBERVERSICHERUNG FÜR GEWERBE / ÄRZTE & HEILBERUFE

Entspannt bleiben, auch bei Cyberattacken.

GESCHÄFTSPARTNER-INFORMATION Juni 2022

fhs 057.04 – 07.2022

Alte Leipziger
ALH Gruppe

Inhalte

→ **Warum brauchen Unternehmen eine Cyberversicherung?**

Was unser Produkt auszeichnet:

→ Kostenloses Präventionspaket bei Alte Leipziger inklusive

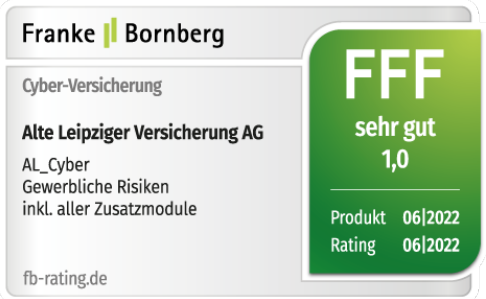
→ Soforthilfe im Notfall

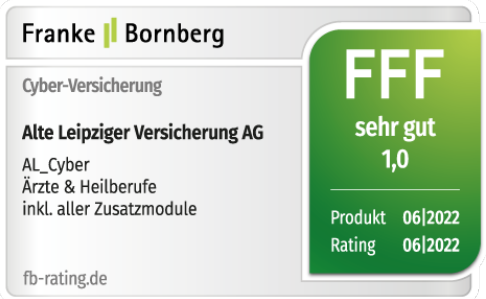
→ Modulbaukasten – individueller Versicherungsschutz

- → Modul Eigenschaden
- → Zusatzmodul Betriebsunterbrechung
- → Zusatzmodul CEO-Fraud
- → Modul Drittschaden
- → Zusatzmodul Datenschutz
- → Zusatzmodul E-Payment

Ausgezeichnete Produktqualität

Vertrauen Sie dem besten Cyberschutz am Markt!





Das renommierte Ratingunternehmen Franke & Bornberg vergibt für unsere Cyberversicherung die Note „Sehr gut“ (1,0).

AL_Cyber ist damit das am besten bewertete Produkt am deutschen Markt.

Wie sicher ist die IT Ihrer Kunden?

IT Sicherheit – Ihre Kunden sorgen vor, z. B. mit …

- Zugriffssicherung, z. B. durch individuelle und mit einem Passwort gesicherte Zugänge für alle Nutzer
- Sensible Daten werden nur verschlüsselt versendet
- Firewall, Antivirensoftware und regelmäßige Sicherheitsupdates
- Mindestens wöchentlichen Sicherungskopien

Wozu also eine Cyberversicherung?

- Wenn z. B. durch einen Hackerangriff Kundendaten entwendet und veröffentlicht wurden oder die Arbeitsfähigkeit beeinträchtigt wird, benötigt Ihr Kunde schnellstmöglich exzellente Hilfe und Unterstützung.
- Außerdem übernehmen wir im Schadenfall Kosten, auf denen Ihr Kunde sonst sitzen bleiben würde.

Darum benötigen Ihre Kunden eine Cyberversicherung

IT Sicherheit

1

Eigene Vorsorge

z. B. Passwortschutz, Firewall, Datensicherung etc.

2

Prävention

z. B. Schulungen für die Mitarbeitenden, um für Cyberrisiken zu sensibilisieren

3

Soforthilfe im Notfall

z. B. telefonische Notfall- und Krisenunterstützung, Erreichbarkeit 24/7

4

Rest-Risiko

Finanzielle Absicherung, wenn es zu Schäden gekommen ist

Darum ist die Cyberversicherung der Alte Leipziger die richtige Wahl:

- Kostenloses Präventionspaket inklusive
- Optional: zusätzliche Präventionsleistungen zu Sonderkonditionen buchbar
- Schäden eindämmen durch schnelle Hilfe

Welchen Schutz bietet eine Cyberversicherung?

Versichert werden **Vermögensschäden** aufgrund einer **Informationssicherheitsverletzung**.

Informationssicherheitsverletzung

Beeinträchtigung der

Verfügbarkeit | Integrität | Vertraulichkeit

Elektronische Daten

informationsverarbeitende Systeme

Informationssicherheitsverletzung – Was ist das?

Cyberversicherung: Hilfe bei **Vermögensschäden** aufgrund einer **Informationssicherheitsverletzung**

Hacker-Angriff beeinträchtigt die VERFÜGBARKEIT

Definition

- Die elektronischen Daten oder informationsverarbeitenden Systeme sind **temporär oder dauerhaft nicht zugänglich**.

Beispiel Heilwesen:

- Cyberkriminelle dringen durch eine Sicherheitsschwachstelle im Betriebssystem in das Netzwerk der Arztpraxis ein. Daraufhin **verschlüsseln** sie das Praxisverwaltungssystem.

Schadsoftware reduziert die INTEGRITÄT

Definition

- Die **Daten sind nicht vollständig oder wurden verändert** oder die korrekte Funktionsweise von Systemen ist nicht gewährleistet.

Beispiel Heilwesen:

- Ein Arzt öffnet den Dateianhang einer scheinbar vertrauenswürdigen E-Mail und lädt sich damit einen Virus in seine Systeme, der daraufhin **sämtliche elektronische Patientenakten löscht**.

Schädigung durch Mitarbeiter verletzt die VERTRAULICHKEIT

Definition

- Die Daten **werden Unberechtigten zugänglich gemacht.**

Beispiel Heilwesen:

- Eine unzufriedene Arzthelferin kopiert nach Feierabend heimlich Patientendaten samt Diagnosen und Behandlungsmethoden und **veröffentlicht diese im Internet**, um den Ruf ihres Chefs zu schädigen.

„Mir passiert das doch nicht!“ – Sicher?

Neue Arbeitswelt – neue Risiken. Was 2019 noch unvorstellbar war, ist jetzt gelebte Arbeitswelt. Viele Angestellte arbeiten nach wie vor zumindest zeitweise aus dem privaten Bereich – und nicht selten mit privaten Geräten. Das sorgt für neue „Geschäftsmodelle“ bei Cyberkriminellen.

Fakten

Über 90 % der befragten Unternehmen glauben nicht, dass sich durch die Corona-Pandemie neue Cyber-Bedrohungen ergeben hätten.

Aber: In der Hälfte der Unternehmen wird während der Pandemie mobil gearbeitet und jedes vierte Unternehmen berichtet von verstärkten Cyberangriffen
(Quelle: GDV-Branchenreport Cyberrisiken im Mittelstand 2021)

„Mir passiert das doch nicht!“ – Sicher?

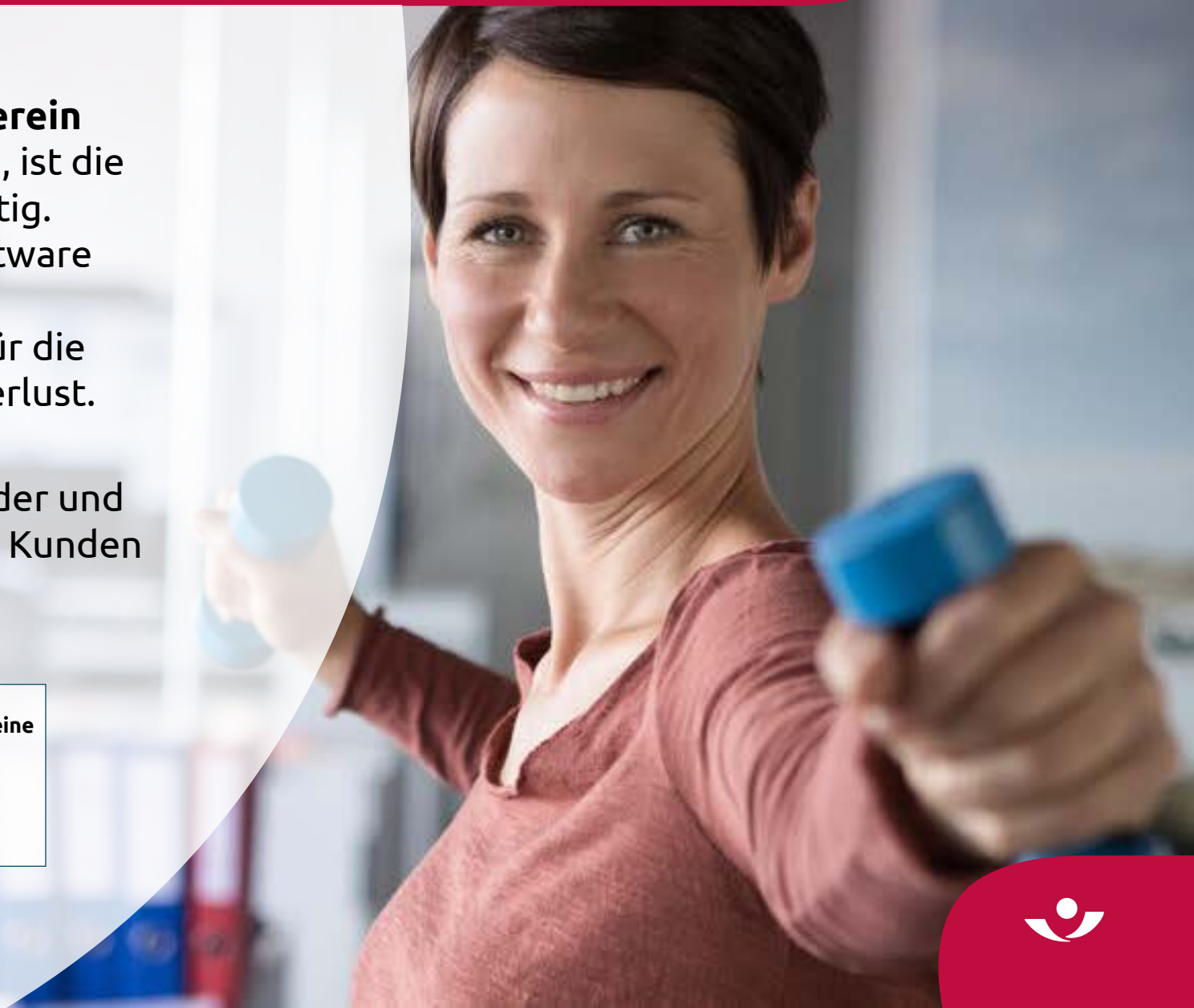
Für jedes Unternehmen, ob **Bürobetrieb, Verein** oder Unternehmen aus der **Freizeitbranche**, ist die ständige Verfügbarkeit der IT-Systeme wichtig. Ohne Zugriff auf Kundendaten, Betriebssoftware oder Website drohen neben einer Betriebsunterbrechung auch hohe Kosten für die Schadensbehebung bis hin zu Reputationsverlust.

Werden Kundendaten von Cyberkriminellen veröffentlicht, können Datenschutz-Bußgelder und geltend gemachte Haftpflichtansprüche der Kunden die Folge sein.

Fakten

Der Verfassungsschutz registriert alle 3 Minuten einen Cyberangriff auf eine Firma in Deutschland – KMU sind besonders oft betroffen.

Die Schadensumme durch kriminelle Cyberattacken im Jahr 2020 in Deutschland beträgt 223 Mrd. Euro. (Quelle: Bitkom)



„Mir passiert das doch nicht!“ – Sicher?

Gerade **Hotels** und **Gaststätten** sind sehr auf ihre IT angewiesen. Sind die Website oder das Buchungssystem lahmgelegt, bleiben Reservierungen aus und Abrechnungen sind nicht mehr möglich. Hohe Umsatzeinbußen bis zum kompletten Stillstand des Betriebes können die Folge sein.

Da Rechnungen oft mit Kreditkarten bezahlt werden, ist eine Vielzahl an Kreditkartendaten vorhanden. Werden diese gestohlen, drohen nicht nur hohe Datenschutz-Bußgelder, sondern auch Haftpflichtansprüche der Gäste und Vertragsstrafen durch den Kreditkartenanbieter.

Fakten

In einer Unternehmensbefragung gaben 88% der Firmen an, im Jahr 2020 Ziel von Cyberattacken gewesen zu sein. (Quelle: Bitkom)

„Mir passiert das doch nicht!“ – Sicher?

Auch für **Bau-** und **Handwerksbetriebe** sind IT-Systeme heutzutage ein wichtiger Bestandteil der täglichen Arbeit, sei es das Einsehen und Bearbeiten von Auftragsdaten und Bauplänen, das Verwalten von Kundendaten, das Erstellen von Rechnungen oder die Materialbestellung.

Bei **Industrie-** und **Herstellungsbetrieben** ist die Fertigung oft automatisiert und computergesteuert. Werden diese Systeme lahmgelegt, steht die komplette Produktion still und Aufträge können nicht erfüllt werden.

Fakten

Pro Tag werden durchschnittlich 394.000 neue Schadprogramm-Varianten registriert. (Quelle: BSI)

Etwa 3 von 4 kleinen und mittleren Unternehmen wären ohne funktionierende IT stark bis sehr stark eingeschränkt. (Quelle: GDV/Forsa)

„Mir passiert das doch nicht!“ – Sicher?

Gerade für **Handels- und Dienstleistungsbetriebe** ist die Verfügbarkeit der IT-Systeme überlebenswichtig. Ohne funktionierendes Warenwirtschaftssystem fehlt der Zugriff auf wichtige Auftragsdaten, die Lagerdatenbank oder die Kundendaten.

Werden die Website oder der Online-Shop lahmgelegt, z. B. mit einer DDoS-Attacke, können keine Bestellungen mehr angenommen werden und es drohen hohe Umsatzverluste.

Fakten

Laut einer Unternehmensbefragung haben im Jahr 2020 die Cyberattacken „Infizierung mit Schadsoftware“ und „Distributed Denial of Service (DDoS)“ bei über der Hälfte der Befragten einen Schaden verursacht.
(Quelle: Bitkom-Studie 2021)

In diesen und weiteren Fällen sind Ihre Kunden mit unserem Cyberschutz abgesichert

- Der Klassiker: ein unachtsamer Klick im Internet und schon ist es passiert, die Daten werden verschlüsselt.
- Kriminelle erstellen täuschend echte Kopien von E-Mails (Phishing), um Zugangsdaten/Passwörter von Nutzern auszuspionieren.
- Ein unzufriedener Mitarbeiter will sich an der Firma rächen und schleust Schadsoftware ein.
- Ein Hacker bricht in die IT-Systeme ein und löscht, beschädigt, blockiert oder kopiert Daten.
- Die Website des Unternehmens wird gekapert.
- Eine DoS- oder DDoS-Attacke legt den Online-Shop lahm.
- Ein Computervirus/-wurm, Trojaner oder andere Schadsoftware beeinträchtigen die elektronischen Daten oder IT-Systeme.

Betriebsunterbrechungen oder Datenschutz-Lecks sind die Folge.

Kostenloses Präventionspaket inklusive!

Warum macht das Präventionspaket Sinn?

Ihre Kunden sorgen schon vor? Und sichern ihre Daten? Das ist prima! **Aber Hand aufs Herz:**

- Wie sicher sind wohl die Passwörter der Mitarbeitenden?
- Oder deren IT-Geräte, die gerade in Zeiten von Homeoffice vielerorts genutzt werden – Stichwort „Bring your own device“?
- Und wie oft haben Sie sich selbst schon dabei ertappt, eine E-Mail zu öffnen, bei der Sie nicht ganz sicher sind, von wem sie kommt?

Diese und weitere Themen werden im Rahmen des kostenlosen Präventionspakets behandelt. Mit Hilfe von eingängigen E-Learnings und Fragen zur Lernkontrolle werden Mitarbeitende für Themen der Cybersicherheit sensibilisiert.

Wie erhalten Kunden Zugriff auf das kostenlose Präventionspaket?

Diese Präventionsmaßnahmen können von Ihren Kundinnen und Kunden und den mitversicherten Personen und Unternehmen **jährlich** durchgeführt werden – unabhängig von der Mitarbeiter-Anzahl.

Das kostenlose Präventionspaket umfasst:

- Online Schulungen zu Themen der IT-/Datensicherheit in Form von E-Learnings mit eingebauten Fragen zur Lernkontrolle
- Phishing-Simulationen in Form fingierter E-Mails, auf die die Empfänger korrekt reagieren sollten

Die Registrierung auf der Onlineplattform erfolgt unter: https://alte-leipziger.cyberdirekt.de

Die personalisierten Zugangsdaten für den oder die IT-Verantwortliche/n erhalten Ihre Kunden mit den Antrags-/Vertragsunterlagen.

Hier erhalten Ihre Kundinnen und Kunden auch alle relevanten Informationen zur Nutzung der Präventionsleistungen.

Vorteile durch das Präventionspaket im Schadenfall

Haben **im Schadenfall mindestens 75 % der mitversicherten Personen** des versicherten Unternehmens und der mitversicherten Unternehmen jährlich die Schulungen zu IT-/Datensicherheit und Phishing absolviert?

Dann reduziert sich für diesen Schadenfall die festgelegte **Selbstbeteiligung um 50 %.** Diese Regelung gilt nicht für die zeitliche Selbstbeteiligung im Rahmen des Zusatzmoduls Betriebsunterbrechung.

Der Nachweis über die durchgeführten Präventionsmaßnahmen muss für das aktuelle Versicherungsjahr, in dem der Schadenfall eingetreten ist, erbracht werden. Sofern im aktuellen Versicherungsjahr die Präventionsmaßnahmen noch nicht im erforderlichen Umfang durchgeführt wurden, so genügt der Nachweis für das vorherige Versicherungsjahr.

Soforthilfe im Notfall!

Was ist eine (Cyber-)Notfallsituation?

Hinweis:

Cyber-Hotline rund um die Uhr (24/7) zur Meldung von eingetretenen, bevorstehenden oder vermuteten Schadenfällen:

06171 66-2206

Anhaltspunkte für eine Notfallsituation können z. B. sein:

- Die Antivirensoftware oder die Firewall melden eine Infektion der IT-Systeme.
- Die Antivirensoftware oder die Firewall weisen Auffälligkeiten in den Logdateien auf.

Cyberattacken sind Notfallsituationen, bei denen schnell gehandelt werden muss!

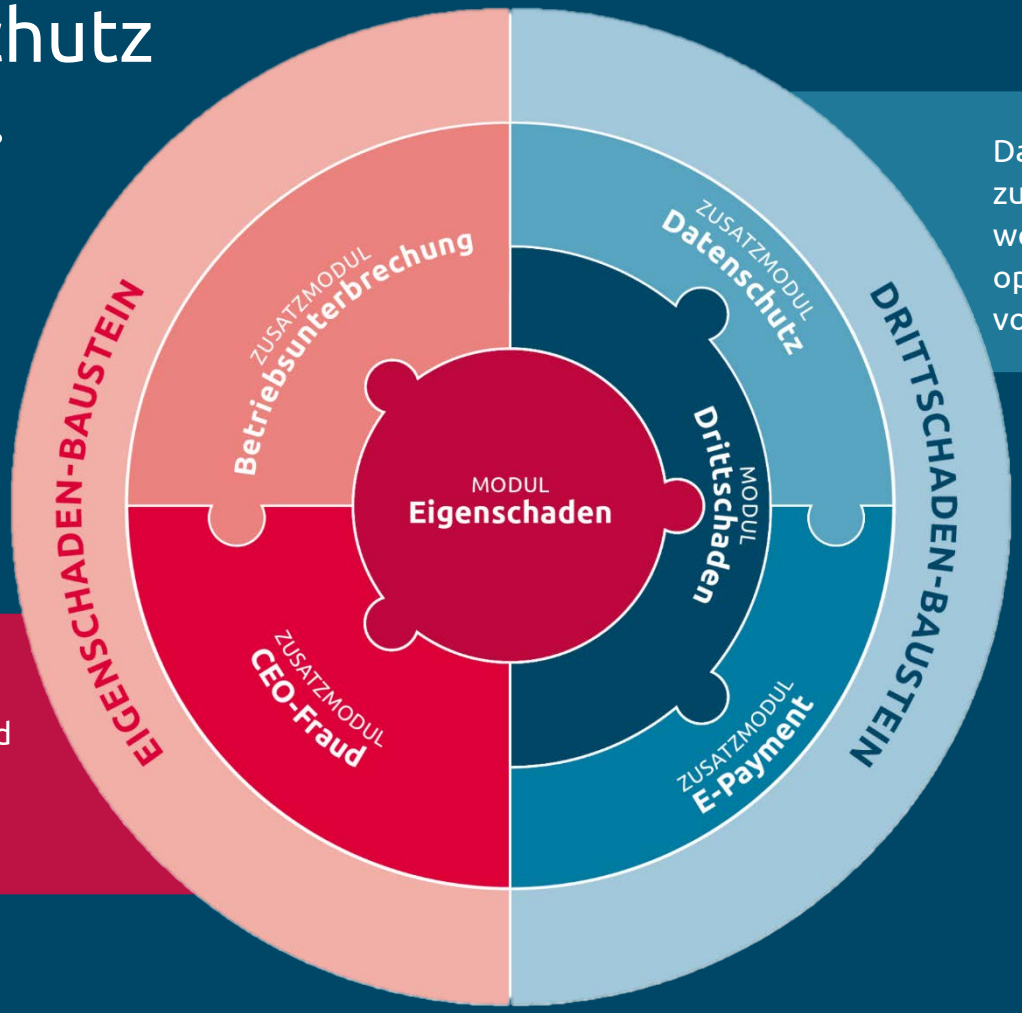
Ist der Versicherungsnehmer in einer **Notfall-situation**, übernimmt die Alte Leipziger die **Kosten eines Dienstleisters für die erste telefonische Notfall- und Krisenunterstützung** in Form von:

- einer Experteneinschätzung zur geschilderten Lage,
- Empfehlungen für Sofortmaßnahmen zur Schadenbegrenzung,
- Empfehlungen für Sofortmaßnahmen zur Ursachenermittlung,
- einer ersten Bewertung der bisherigen Maßnahmen,
- ersten technischen Sofortmaßnahmen (sofern möglich/erforderlich).

Für die **Soforthilfe** fällt weder eine Selbstbeteiligung an noch werden diese Kosten auf die Deckungssumme angerechnet.

Dies gilt jedoch nur, sofern der VN die Notfallsituation über die dem Versicherungsschein beigelegte Telefonnummer für die Cyber-Soforthilfe meldet und somit der vom Versicherer beauftragte Dienstleister die telefonische Soforthilfe durchführt.

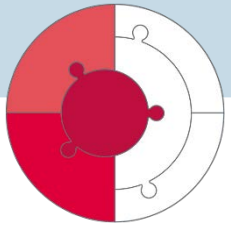
Der Modulbaukasten, der unseren Cyberschutz so individuell macht.



Das Modul **Drittschaden** kann zusätzlich zum Modul Eigenschaden abgeschlossen werden. **Datenschutz** und **E-Payment** sind optionale Zusatzmodule zur Absicherung von Drittschäden.

Das Modul **Eigenschaden** ist ein Pflichtmodul, **Betriebsunterbrechung** und **CEO-Fraud** sind optionale Zusatzmodule zur Absicherung von Eigenschäden.

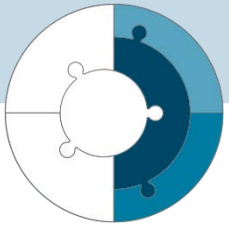
Modulbaukasten



Modul Eigenschaden

Zusatzmodul Betriebsunterbrechung

Zusatzmodul CEO-Fraud



Modul Drittschaden

Zusatzmodul Datenschutz

Zusatzmodul E-Payment

Entscheiden Sie mit Ihren Kunden: Welcher Schutz wird benötigt?

Modul Eigenschaden →

- Das Modul Eigenschaden stellt die Grunddeckung der Cyberversicherung dar und ist immer mitversichert.
- Versichert sind Schäden, die nach einer Informationssicherheitsverletzung beim VN selbst auftreten.

Zusatzmodul Betriebsunterbrechung (optional) →

- Kosten, die durch eine Betriebsunterbrechung aufgrund einer Informationssicherheits-verletzung entstehen, z. B. Entgangener Betriebsgewinn und fortlaufende Kosten.

Zusatzmodul CEO-Fraud (optional) →

- Erstattung durch CEO-Fraud entwendeter Geldbeträge
- CEO-Fraud, auch „Fake President Fraud“ genannt, beschreibt eine Betrugsmasche, bei der Firmen zur Überweisung von Geld manipuliert werden, weil sich ein unbefugter Dritter als Geschäftsführung ausgibt und eine Vertrauensperson zur Zahlung anweist.

Entscheiden Sie mit Ihren Kunden: Welcher Schutz wird benötigt?

Modul Drittschaden (optional) →

- Vergleichbar mit Haftpflichtschutz
- Es besteht Versicherungsschutz für den Fall, dass Ihr Kunde wegen einer Informations-sicherheitsverletzung von einem Dritten auf Schadensersatz in Anspruch genommen wird.

Zusatzmodul Datenschutz (optional) →

- Versicherungsschutz für Schadensersatz-ansprüche, die wegen einer Verletzung von datenschutzrechtlichen Vorschriften aufgrund einer Informationssicherheitsverletzung geltend gemacht werden.

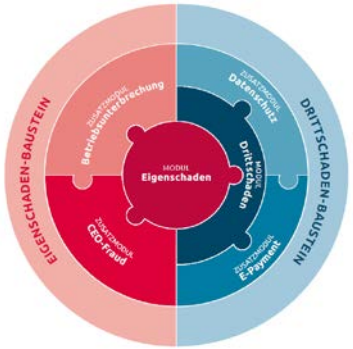
Zusatzmodul E-Payment (optional) →

- Versicherungsschutz für Forderungen zur Zahlung von Vertragsstrafen, die ein E-Payment Service Provider wegen einer Verletzung eines Payment Card Industry (PCI) Datensicherheitsstandards geltend macht.

Sie haben drei verschiedene Möglichkeiten, die Deckungssummen festzulegen:

Für den ganzen Vertrag

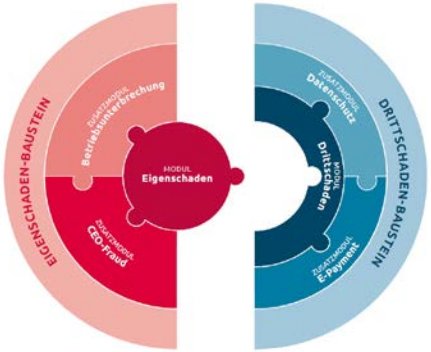
Es wird eine Deckungssumme und eine SB gewählt, die **pauschal für die ganze Cyberpolice** gilt.



- Schnell und einfach
- Geeignet für bspw. Cyber-Einsteiger unter den Vermittlern

Je Baustein

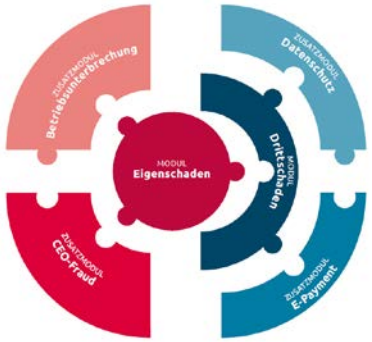
Es wird je eine Deckungssumme und eine SB für den **Eigenschaden-Baustein** und den **Drittschaden-Baustein** festgelegt.



- Eigen- und Drittschadenabsicherung separierbar
- Geeignet für Cyber-Kenner unter den Vermittlern

Je Modul

Es wird für **jedes einzelne Modul**, das ausgewählt wird, eine eigene Deckungssumme und eine eigene SB gewählt.



- Bedarfsgerecht
- Geeignet für Cyber-Profis unter den Vermittlern

Die einzelnen Module werden immer separat ausgewählt – unabhängig davon, auf welche Weise die Deckungssummen festgelegt werden.

Festlegung der Deckungssummen – Hilfestellungen

Diese Hinweise sollten immer berücksichtigt werden, unabhängig davon, wie die Deckungssummen festgelegt werden (je Modul, je Baustein oder für den ganzen Vertrag

Eigenschaden

Bei der Festlegung der Deckungssumme sollten – je nach Risikoeinschätzung – u. a. folgende Punkte berücksichtigt werden:

- Die Höhe der Kosten für die Wiederherstellung von Betriebssystemen, Datenbanken oder Verwaltungssystemen
- Die Kosten für einen IT-Dienstleister liegen durchschnittlich bei rund 300 € pro Stunde, sein Einsatz kann mehrere Tage dauern
- Die Höhe der Kosten für die Beauftragung eines Krisenmanagement- oder PR-Beraters

CEO-Fraud

Eine Orientierungshilfe für die Festlegung der Deckungssumme kann die Höhe etwaiger Zahlungsvollmachten für Mitarbeiter sein, bei denen die Zahlungsanweisungen nicht durch einen Vorgesetzten freigegeben werden müssen.

Betriebsunterbrechung

- Bei der Festlegung der Deckungssumme bzw. des Tagessatzes sollte insbesondere berücksichtigt werden:
- Vorjahresgewinn + jährliche fortlaufende Kosten (Der Tagessatz ist 1/365 dieser Summe und kann in 50 €-Schritten - max. 5.000 € - festgelegt werden. Dies gilt bei der Summenfestlegung je Modul)
- Wie viele Tage würde es dauern, bis die Betriebsfähigkeit nach einem Cyberschaden wieder voll hergestellt ist?
- Mögliche Kosten, die durch die Nutzung fremder IT (z. B. Leihe) zur Aufrechterhaltung der Arbeitsfähigkeit entstehen.

Weitere Hinweise zur Ermittlung der Deckungssumme und diverse Branchen-Beispiele finden Sie im Dokument fhs 093 im Vermittlerportal

Festlegung der Deckungssummen – Hilfestellungen

Diese Hinweise sollten immer berücksichtigt werden, unabhängig davon, wie die Deckungssummen festgelegt werden (je Modul, je Baustein oder für den ganzen Vertrag

Drittschaden

Bei der Festlegung der Deckungssumme sollten die Ausrichtung des Unternehmens sowie die Art und Anzahl der verarbeiteten oder gespeicherten Daten (z. B. Kundendaten) berücksichtigt werden. Sofern vertragliche Schadenersatzansprüche mitversichert werden sollen, sind diese ebenfalls zu berücksichtigen.

E-Payment

Neben der möglichen Vertragsstrafe gemäß Strafenkatalog des E-Payment-Serviceproviders sollten hier auch 10 € je gespeichertem Kreditkartendatensatz berücksichtigt werden.

Datenschutz

Neben dem möglichen zu leistenden Schadenersatz sollten auch die Kosten für die rechtsanwaltliche Beratung bei einem Datenschutzvorfall (ca. 250 € bis 400 € pro Stunde) und für die Benachrichtigung betroffener Kunden (ca. 2,50 € pro Kundendatensatz) berücksichtigt werden.

Weitere Hinweise zur Ermittlung der Deckungssumme und diverse Branchen-Beispiele finden Sie im Dokument fhs 093 im Vermittlerportal

Festlegung der Deckungssummen – Beispiele

Beispiel 1

	Modul ausgewählt ?	Ganzer Vertrag	Je Baustein	Je Modul
Eigenschaden-Baustein				
Modul Eigenschaden	✓	500.000 €	250.000 €	100.000 €
Zusatzmodul Betriebsunterbrechung	✓			72.000 € *
Zusatzmodul CEO-Fraud	—			-
Drittschaden-Baustein				
Modul Drittschaden	✓		100.000 €	50.000 €
Zusatzmodul Datenschutz	✓			50.000 €
Zusatzmodul E-Payment	—			-
		Gesamtdeckungssumme 500.000 € Jahresprämie **526 €**	Gesamtdeckungssumme 350.000 € Jahresprämie **438 €**	Gesamtdeckungssumme 272.000 € Jahresprämie **419 €**

Bei den aufgeführten Prämien handelt es sich um Beispiele für Brutto-Jahresprämien (gerundet). Berechnungsbasis: Hotel, Umsatz 1 Mio. €, SB 2.500 € (BU: 12 Std.)

* Tagessatz **400 €** x Haftzeit **180 Tage**

Die Selbstbeteiligungen werden entsprechend den Deckungssummen festgelegt.
Für das Zusatzmodul Betriebsunterbrechung muss die zeitliche Selbstbeteiligung immer – also auch bei den Varianten „Für den ganzen Vertrag“ und „Je Baustein“ – festgelegt werden.

Festlegung der Deckungssummen – Beispiele

Beispiel 1

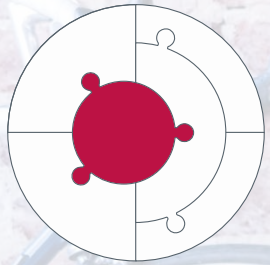
	Modul ausgewählt ?	Ganzer Vertrag	Je Baustein	Je Modul
Eigenschaden-Baustein				
Modul Eigenschaden	✓	1.000.000 €	750.000 €	500.000 €
Zusatzmodul Betriebsunterbrechung	✓			270.000 € *
Zusatzmodul CEO-Fraud	✓			50.000 €
Drittschaden-Baustein				
Modul Drittschaden	✓		500.000 €	100.000 €
Zusatzmodul Datenschutz	✓			250.000 €
Zusatzmodul E-Payment	✓			100.000 €
		Gesamtdeckungssumme 1.000.000 € Jahresprämie **1.128 €**	Gesamtdeckungssumme 1.250.000 € Jahresprämie **993 €**	Gesamtdeckungssumme 1.270.000 € Jahresprämie **1.086 €**

Bei den aufgeführten Prämien handelt es sich um Beispiele für Brutto-Jahresprämien (gerundet). Berechnungsbasis: Hotel, Umsatz 1 Mio. €, SB 2.500 € (BU: 12 Std.)

* Tagessatz **1.500 €** x Haftzeit **180 Tage**

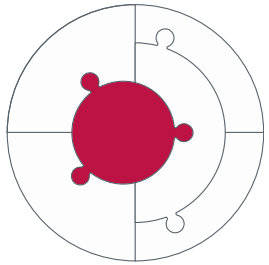
Die Selbstbeteiligungen werden entsprechend den Deckungssummen festgelegt.
Für das Zusatzmodul Betriebsunterbrechung muss die zeitliche Selbstbeteiligung immer – also auch bei den Varianten „Für den ganzen Vertrag“ und „Je Baustein“ – festgelegt werden.

Modul Eigenschaden



Das Modul Eigenschaden stellt die Grunddeckung der Cyberversicherung dar und ist immer mitversichert.

Modul Eigenschaden – versichert sind …



IT-Forensik/Schadenfeststellungskosten

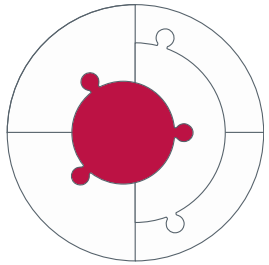
- Kosten für die Ursachenermittlung und Feststellung des versicherten Schadens
- Kosten des Versicherungsnehmers für externe Sachverständige und Mehrkosten durch den unterstützenden Einsatz von Mitarbeitern des VN

Datenwiederherstellung (gilt auch für Software und Programme) sowie Entfernung der Schadsoftware

Abwehr einer Cyber-Bedrohung/-Erpressung

- Kosten für Abwendung der Bedrohungslage durch einen von der Alte Leipziger zu benennenden und zu beauftragenden IT-Dienstleister
- Kosten für Krisenberatung und -management

Modul Eigenschaden – versichert sind …



EC-/Kreditkarten-Monitoring Service zur Überwachung und Prüfung von Bank-/ Kreditkartendaten

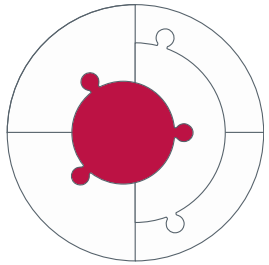
Cyberdiebstahl

- Verluste durch falsch ausgeführte, umgeleitete oder manipulierte Überweisungen
- Abhandenkommen von Geldern auf Konten inkl. Guthaben bei Online-Bezahlsystemen (z. B. PayPal, Apple-Pay, EC-Karten) infolge einer Informationssicherheitsverletzung
- Erhöhte Nutzungsentgelte, z. B. Telefonmehrkosten

Sicherheitsverbesserungen nach einem Angriff

- Honorare von beauftragten Sicherheitsberatern einschließlich der Kosten für angemessene Sicherheitsverbesserungen, wenn diese Maßnahmen geeignet sind, einen zukünftigen Angriff zu verhindern

Modul Eigenschaden – versichert sind …



Kosten für Krisenkommunikation und PR-Maßnahmen zur Wiederherstellung der öffentlichen Reputation, z. B. durch Krisenmanager

Aufwendungen vor Eintritt des Versicherungsfalls zur Vermeidung eines unmittelbar bevorstehenden Schadens

Schadenminderungskosten

- Aufwendungen des Versicherungsnehmers zur Minderung einer versicherten Betriebsunterbrechung oder zur Minderung eines sonstigen Schadens – unabhängig davon, ob der Versicherungsnehmer damit erfolgreich war oder nicht

Sachschäden an IT-Systemen

Eigenschaden – Beispiel, so schnell ist es passiert:

Ein Mitarbeiter öffnet den Anhang einer **E-Mail und aktiviert einen Trojaner.** Damit gelingt es einem Hacker, sich Zugang zu vertraulichen Kundendaten zu verschaffen und löscht diese stellenweise.

In diesem Fall übernehmen wir neben den Kosten für IT-Forensik und Schadenfeststellung auch die Kosten für die Entfernung der Schadsoftware und die Wiederherstellung der Daten.

Cybererpressung – Warum kein Lösegeld gezahlt werden sollte

Cybererpressung – Warum kein Lösegeld gezahlt werden sollte

Erfahrungen zeigen: **Wer einmal Lösegeld gezahlt hat, steht schnell auf einer „Kundenliste“ im Darknet**, wird als „zahlungswillig“ und „erpressbar“ gekennzeichnet und ist anschließend weiteren Zahlungsforderungen und häufiger neuen Angriffen ausgeliefert.

Außerdem bedeutet eine Lösegeldzahlung noch lange nicht, dass die verschlüsselten Daten auch tatsächlich wieder entschlüsselt werden, denn einen entsprechenden Entschlüsselungs-Code gibt es meist gar nicht. Und die Schadsoftware wird mit einer Zahlung auch nicht entfernt.

Bei einer Cyber-Erpressung im Zusammenhang mit einem Datendiebstahl und der Androhung einer Veröffentlichung der Daten bringt eine Lösegeldzahlung ohnehin nichts, da diese Daten auch weiterhin gestohlen bleiben.

Deshalb raten auch das BKA und die Polizei ausdrücklich davon ab, dieses „Geschäftsmodell“ von Kriminellen zu unterstützen.

Fakten

Laut einer Studie wurden 80 Prozent der Unternehmen, die eine Lösegeldforderung gezahlt haben, ein zweites Mal angegriffen – oft von denselben Angreifern.
(Quelle: Studie Cybereason 2022)

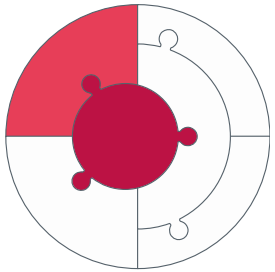
Cybererpressung – Was wird tatsächlich benötigt?

Mit unserem Partner für Cybersecurity bieten wir genau diese Unterstützung, sodass der entstandene Schaden nicht die Existenz Ihrer Kunden bedroht, aber gleichzeitig auch deren **Autonomie gestärkt wird**.

Nicht die Zahlung eines Lösegeldes!

Sondern professionelle und schnelle Unterstützung: Die Schadsoftware muss entfernt, alle betroffenen Systeme müssen bereinigt und die Originaldaten müssen wiederhergestellt werden.

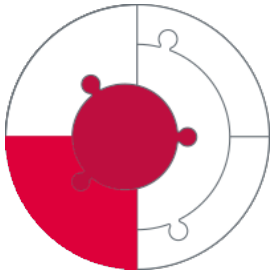
Zusatzmodul Betriebsunterbrechung – versichert sind…



- Gesamter Zeitraum der **Betriebsunterbrechung** ist abgesichert
- Unabhängig davon, ob ein versicherter Cyberschaden im eigenen Betrieb oder bei einem entgeltlich beanspruchten Cloud-Anbieter zu einer Betriebsunterbrechung beim VN führt
- **Entgangener Betriebsgewinn und fortlaufende Kosten** werden erstattet
- Mitversichert sind auch Mehrkosten, die für die **Fortführung des Betriebes** aufgewendet werden müssen, z. B. Nutzung fremder IT-Systeme

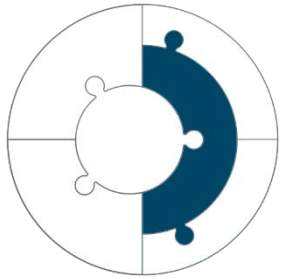
2/3 der Unternehmen haben Tage gebraucht, bis die IT-Systeme wiederhergestellt und die Schadsoftware beseitigt war.

Zusatzmodul CEO-Fraud – versichert sind …



- **Erstattung missbräuchlich entwendeter Geldbeträge**, die durch eine Vertrauensperson ausgezahlt wurden, weil
  - ein unbefugter Dritter sich als Geschäftsführung ausgegeben und die Vertrauensperson zu dieser Zahlung angewiesen hat oder
  - der Zahlungsverkehr aufgrund einer Mitteilung des Vertragspartners über eine neue Kontoverbindung abgewickelt werden soll, die Mitteilung tatsächlich jedoch durch einen unberechtigten Dritten erfolgte, der sich lediglich als Vertragspartner ausgegeben hat.

Modul Drittschaden – versichert sind …



Dieses optionale Modul bietet Versicherungsschutz für den Fall, dass Ihr Kunde wegen einer **Informationssicherheitsverletzung** von einem Dritten auf Schadensersatz in Anspruch genommen wird.

Beispiel Drittschaden:

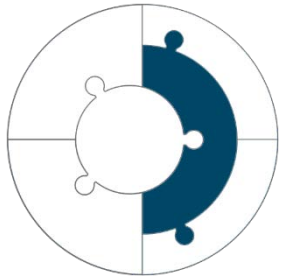
Ein Unternehmen stellt eine Datei für Kunden zum Download bereit, die unbeabsichtigt mit einem Computervirus infiziert ist. Daraufhin stellen geschädigte Kunden Schadensersatzansprüche.

Modul Drittschaden – Beispiel Schadsoftware heruntergeladen

Die Angestellte eines Architekturbüros erhält eine **E-Mail von einem unbekannten Absender**. Bedenkenlos öffnet sie die Mail, da im Büro täglich viel E-Mail-Verkehr mit unbekannten Absendern herrscht. Der Absender verweist als Beleg für die Korrespondenz auf ein **Word-Dokument im Anhang**, welches die Angestellte daraufhin öffnet.

Am nächsten Tag beschwert sich ein Geschäftspartner des Architekturbüros darüber, dass die Angestellte ihm eine **mit einem Virus infizierte Datei zugeschickt habe, die seinen Rechner infiziert habe.**

Modul Drittschaden – versichert sind …



- **Gegenstand der Haftpflicht**

  Ansprüche aufgrund gesetzlicher Haftpflichtbestimmungen privatrechtlichen Inhalts

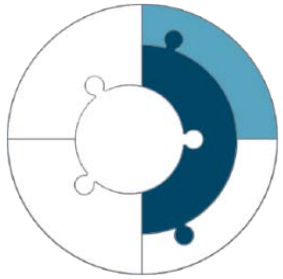
- **Rechtswidrige elektronische Kommunikation**

  Ihr Kunde hat elektronische Medieninhalte veröffentlicht, die zu Persönlichkeitsrechts-, Namensrechts-, Urheberrechts oder Markenrechtsverletzungen (und daraus resultierenden Verstößen gegen das Wettbewerbsrecht) führen.

Innerhalb dieses Moduls zuwählbar:

- **Versicherungsschutz bei vertraglichen Schadensersatzansprüchen**
  (= Ansprüche wegen vergeblicher Aufwendungen im Vertrauen auf ordnungsgemäße Vertragserfüllung sowie Mehraufwendungen wegen Verzögerung der Leistung)

Zusatzmodul Datenschutz



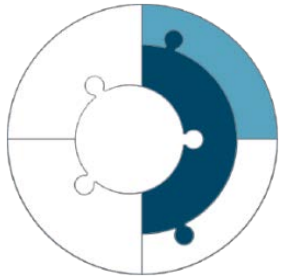
Nach der aktuellen Rechtslage im Bereich Datenschutz sind Unternehmen, die Ziel einer Cyberattacke waren, bei denen also bspw.

- Daten von Kunden gestohlen oder
- von Unbefugten eingesehen wurden,

verpflichtet, die Aufsichtsbehörde innerhalb von 72 Stunden umfassend zu informieren.

Unabhängig von den Informationspflichten kann das attackierte Unternehmen auch schadenersatzpflichtig gegenüber Dritten, z. B. Kunden, werden.

Zusatzmodul Datenschutz - versichert sind …



Kosten …

- für **Schadenersatzansprüche Dritter**, die gegen den Versicherungsnehmer aufgrund einer Datenschutzrechtsverletzung geltend gemacht werden,
- für die **Rechtsberatung zu Informationspflichten**,
- für die **Benachrichtigung betroffener Dateninhaber** (z. B. Kunden),
- für die **Beauftragung eines externen Callcenters** oder die **Einrichtung einer speziellen Website zur Beantwortung von Rückfragen**.

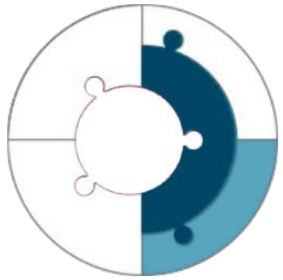
Zusatzmodul Datenschutz – Beispiel Hackerangriff

Unbekannte Täter hacken sich in die Systeme einer großen Arztpraxis und stehlen sensible Patientendaten.

In diesem Fall übernehmen wir nicht nur

- Die **Kosten für die Schadenersatzansprüche der betroffenen Dateninhaber**, sondern auch
- die **Kosten für die IT-Forensik zur Identifikation der betroffenen Patienten**,
- das **Anwaltshonorar für die Beratung über die Informationspflichten** sowie
- die **Kosten für die Information der betroffenen Dateninhaber über den Diebstahl der Daten .**

Zusatzmodul E-Payment – versichert sind …



- Versicherungsschutz für **Forderungen zur Zahlung von Vertragsstrafen**, die ein E-Payment-Serviceprovider wegen einer Verletzung eines „Payment Card Industry (PCI)“-Datensicherheitsstandards geltend macht.

Einfach online abschließen.

Die Antragstellung geht ganz einfach über unseren Online-Rechner E@SY WEB Sach. Es gibt wenige Risikofragen und die Obliegenheiten haben wir mit leicht verständlichen Erläuterungen ergänzt.

Hier AL_CYBER einfach online abschließen:

www.al-rechner.de/cyber

Wie wird die Prämie ermittelt?

Maßgeblich für die Prämie sind neben den Risikomerkmalen – wie z. B. die ausgeführte **Tätigkeit**, der **Umsatz**, die **Anzahl und Art der verarbeiteten Daten** und **die IT-Durchdringung des Unternehmens** – auch der gewählte Deckungsumfang, also Module, Deckungssummen und Selbstbeteiligungen.

Daher lässt sich an dieser Stelle keine Faustformel ableiten. Um Ihnen die Festlegung des Deckungsumfangs zu erleichtern, finden Sie im Online-Rechner zu jedem Modul Infotexte.

Besonderheit bei der Zielgruppe Ärzte/Heilberufe:

Diese wird nach Personen berechnet, dadurch erhalten Sie schnell bzw. mittels sehr weniger Informationen eine Prämie.

Obliegenheiten: Transparent formuliert

Bei Vertragsabschluss ist zu bestätigen, dass die erforderlichen Voraussetzungen in Bezug auf die IT- Sicherheit vorhanden sind.

Hierzu zählen:

- Individuelle und mit einem Passwort gesicherte Zugänge für alle Nutzer der IT
- Schutz der IT mit einer Firewall gegen unberechtigten Zugriff
- Verschlüsselter Versand sensibler Daten
- Schutz vor Schadsoftware (z. B. Antivirenprogramm)
- Regelmäßige Sicherheitsupdates
- Mindestens wöchentliche Datensicherung (Sicherungsdatenträger physisch getrennt von den Originaldaten aufbewahren)
- Notfallplan (ab 5 Mio. € Umsatz)
- Einhaltung aller gesetzlichen, behördlichen sowie vertraglich vereinbarten Sicherheitsvorschriften

Hierbei handelt es sich um Kurzbeschreibungen. Den rechtsverbindlichen Wortlaut, nähere Erläuterungen und Empfehlungen zu den Obliegenheiten enthält das Dokument C 02.
Dieses und alle weiteren Druckstücke finden Sie im Vermittlerportal und im Online-Rechner.

TIPP:
IT-Sicherheit neutral prüfen lassen & optimieren.

Prüfung & Bestätigung
der IT-Sicherheit für Firmen mit bis zu 100 Mitarbeitenden

Unser Dienstleister infraforce – eine auf Cybersecurity spezialisierte Tochtergesellschaft des TÜV Hessen – bietet ein Servicepaket an, bei dem die IT-Sicherheit Ihrer Kunden überprüft und auf Wunsch auch mit einem Siegel bestätigt wird.

Prüfzertifikat: Versicherungskonforme IT-Sicherheit

Nach einer Selbstauskunft folgt ein Experten-Interview und – soweit notwendig – konkrete Handlungsempfehlungen, um die IT-Sicherheit zu erhöhen.

Mit dieser Bestätigung können Sie und Ihre Kunden dann sicher sein, dass die Obliegenheiten für den Abschluss einer Cyberversicherung bei der Alte Leipziger erfüllt sind.

Weitere Dienstleistungen zur Optimierung der IT-Sicherheit

Folgende Dienstleistungen bietet infraforce darüber hinaus zu Sonderkonditionen* an:

- Schwachstellenscan
- Endpoint Security Check
- Firewall Security Check
  - Optional inkl. W-Lan Security Check
- Firewall-Security Check
- CREM – Cyber Risk Exposure Map
- EUDAKON-Check

* Für Unternehmen mit bis zu 100 Mitarbeitenden

Schwachstellenscan

Beim **Schwachstellenscan** wird eine virtuelle Maschine im Unternehmensnetzwerk installiert, die von innen heraus die Systeme testet, indem sie versucht, über unterschiedlichste Protokolle mit ihnen zu kommunizieren und die Antworten auswertet. Dieser Scan verlangsamt die Systeme des Kunden nicht wesentlich.

Auf diese Weise werden verschiedene Schwachstellen aufgedeckt, z. B.:

- veralteter Software oder Betriebssystemen mit fehlenden Patches
- unsichere Verbindungen
- bis hin zu unscheinbaren Geräten, wie Routern oder Druckern, die noch immer das Standardpasswort verwenden

Endpoint Protection Security Check

Beim **Endpoint Protection Security Check** untersucht infraforce gemeinsam mit den Kunden den Antivirenschutz des Unternehmens und erarbeitet bei Bedarf eine Aufstellung an Verbesserungspotential.

- Beantwortet also die Frage „Wie gut/streng ist der Antivirenschutz des Unternehmens eingestellt?“
  - Z. B.: „Sperre von USB-Sticks“ oder „Sperre von Downloads“
- Was hat der Kunde im Antivirenschutz konfiguriert? Wo ist noch Luft nach oben? Wie könnte der Kunde die Einstellungen optimieren?
- Inklusive Empfehlungen zu Einstellungen und ggf. weiteren Produkten, um den Antivirenschutz zu verbessern

Firewall Security Check

Beim **Firewall Check** wird die **Konfiguration der Firewall** untersucht und auf Sicherheitslücken überprüft:

- In einem Erstgespräch analysiert infraforce gemeinsam mit den Kunden die technischen Einstellungen und organisatorischen Prozesse rund um die Firewall.
- Im Nachgang überprüft infraforce die bestehende Konfiguration, das Regelwerk und die Portsicherheit.
- Dabei wird auch geprüft, welche technischen Möglichkeiten das eingesetzte Produkt bietet.
- Im Anschluss an die Prüfung erhalten die Kunden einen Bericht mit Handlungsempfehlungen. Optional kann infraforce auch bei deren Umsetzung unterstützen.

Optional: inkl. W-Lan Security Check

- Überprüfung der Verschlüsselungstechnik und Durchführung eines Authentificationchecks
- Routerhardware und die zugehörige Firmware wird auf die Aktualität kontrolliert und die sicherheitskonforme Trennung der Gastnetze gescheckt.
- Im Anschluss an die Prüfung erhalten die Kunden einen Bericht mit Handlungsempfehlungen.

CREM – Cyber Risk Exposure Map

Die **Cyber Risk Exposure Map** ermittelt einen **Risikofaktor in Bezug auf aktuelle Cyber-Bedrohungen**:

- Zunächst werden die Cyberbedrohungen thematisch kategorisiert und in Gruppen geordnet.
- 15 Risiken werden in 6 Risiko-Gruppen zusammengefasst
  - Malware-Attacks,
  - Message-based Attacks,
  - Web-based Attacks,
  - Physical Attacks,
  - Compliance Threats und
  - Special Threats
- Sowohl Einzelrisiken als auch deren Gewichtung werden entsprechend der in den letzten drei Monaten vermehrt aufgetretenen Risiken aktualisiert und neu gewichtet und somit Einzelrisiken innerhalb der Ermittlung angepasst.
- Ergebnis ist ein Kurzbericht inkl. einer Dashboard-Übersicht

EUDAKON-Check

Beim **EUDAKON-Check** wird der Datenschutzes bei Ihren Kunden überprüft und mit den Anforderungen der EU-DSGVO abgeglichen.

Im Anschluss an die Dienstleistung erhalten Ihre Kunden einen GAP-Analyse-Bericht mit entsprechenden Handlungsempfehlungen, die sich nicht nur auf die allgemeine Rechtslage beziehen, sondern die branchenspezifischen Anforderungen des Unternehmens berücksichtigen.

Sorgen Sie dafür, dass Ihre Kunden entspannt bleiben können – auch bei Cyberattacken.

Die Risiken aus dem Netz sind vielfältig und nicht für alle Firmen gleichermaßen relevant. Gerne unterstützen wir Sie in der Beratung. Nehmen Sie Kontakt mit uns auf.

www.gewerbe-neu-entdecken.de/cyber

Franke Bornberg
Cyber-Versicherung
Alte Leipziger Versicherung AG
AL_Cyber
Gewerbliche Risiken
inkl. aller Zusatzmodule
fb-rating.de
FFF sehr gut 1,0
Produkt 06|2022
Rating 06|2022

Franke Bornberg
Cyber-Versicherung
Alte Leipziger Versicherung AG
AL_Cyber
Ärzte & Heilberufe
inkl. aller Zusatzmodule
fb-rating.de
FFF sehr gut 1,0
Produkt 06|2022
Rating 06|2022

Alte Leipziger
Versicherung AG
Alte Leipziger-Platz 1
61440 Oberursel
sach@alte-leipziger.de
www.vermittlerportal.de
vermittlerblog.alh.de

fhs 057.04 – 07.2022