COGITANDA®
DATAPROTECT AG

CYBER VERSICHERUNG

Cyber – Was ist das?

Cyber – ein Begriff, der uns in den Medien seit einigen Jahren zunehmend intensiv begegnet. Doch was genau ist damit eigentlich gemeint? Das Wörterbuch Duden liefert zu „Cyber“ die folgende Definition: „die von Computern erzeugte virtuelle Scheinwelt“.

Bei COGITANDA® würden wir nicht von einer „Scheinwelt“ sprechen, da diese von Computern erzeugte Welt sehr real und inzwischen von höchster Bedeutung ist. Wir sehen hier eher eine digitale Parallelwelt, in die bisher analoge Geschäftsmodelle Schritt für Schritt übertragen werden.

Genau an diesem Punkt setzen wir bei COGITANDA® an. Wertschöpfungsketten – sogar ganze Geschäftsmodelle – laufen heute - teilweise schon durchgängig - digital ab. Kein Wunder also, dass sich auch die Kriminalität von analog in Richtung digital verlagert und das macht uns alle in nie dagewesener Form angreifbar. Cyber-Kriminelle attackieren dabei digitale Systeme von Unternehmen und privaten Haushalten mit dem Ziel, sensible Daten zu stehlen oder zu manipulieren.

COGITANDA – Wer wir sind.

Wir sind eine Unternehmensgruppe, die sich auf den Umgang mit Cyber-Risiken, deren Bewältigung sowie deren Versicherbarkeit fokussiert. Cyber-Versicherungen sind für uns eng verknüpft mit Risiko-Vorbeugung und professioneller Schadenbearbeitung. Ein sachgerechter und fairer Versicherungsschutz für die Versicherungsnehmer ist für unser Team immer das oberste Ziel.

Das COGITANDA® Team besteht aus Experten aller relevanten Fachrichtungen. Von Versicherungsmanagern und Fachexperten bis zu mit den neusten IT-Entwicklungen vertraute Spezialisten. Unsere Schaden-Mitarbeiter werden unterstützt durch externe Spezialisten, wie z.B. Forensiker oder Anwaltskanzleien. Wir betreuen kleine und mittelständische, aber auch industrielle Unternehmen in allen Cyber-Risiko-Themen. Von der Prävention bis zur Schadenbehebung sind wir für unsere Versicherungsnehmer da. Wir machen nur Cyber, dafür besser als andere.

Cyber Risiko Prävention

Das Verstehen von Cyber-Risiken und das Ergreifen geeigneter Maßnahmen ist die eine, das Versichern verbleibender Risiken die andere Seite einer Medaille. Die Eintrittswahrscheinlichkeit eines Cyber-Schadens lässt sich durch technische und organisatorische Maßnahmen positiv beeinflussen – ausschalten lässt sie sich nicht. Um die verbleibenden Risiken geht es primär bei der Cyber-Versicherung.

Unser Quotierungsprozess enthält nur acht, dafür aber relevante IT-Risikofragen, ein zentraler Bestandteil unserer Risikoprüfung. So stellen wir sicher, dass Versicherungsnehmer einen gewissen Grad an vorbeugenden Maßnahmen selbst initiieren und einen technischen „Grundschutz“ besitzen. Über diese für die Quotierung wichtigen Fragen hinaus, bietet COGITANDA® auf Wunsch jede Form von Cyber Risiko-Prävention an, von der Mitarbeiterschulung über Audits bis hin zu Hard- und Softwarelösungen zum Schutz vor Cyber-Angriffen. Alles aus einer Hand in Sachen Cyber-Risken, wenn gewünscht.

Die Frequenz gravierender Cyber-Vorfälle nimmt deutlich zu, damit auch die Bedeutung der Cyber-Versicherung. Cyber ist eine noch sehr junge Versicherungssparte, zu der es allgemein wenig Erfahrung und kaum Spezialisten gibt. Wir bei COGITANDA® beschäftigen uns seit Jahren mit Cyber und wir machen nichts Anderes – dafür besser als jeder andere.

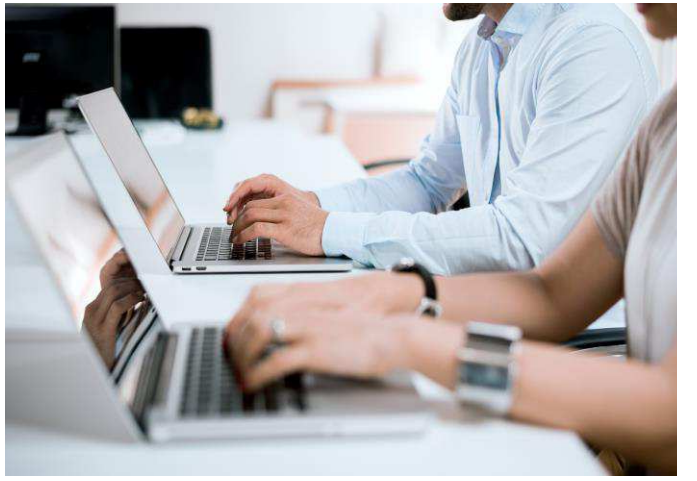
Cyber Versicherung

COGITANDA® bietet Cyber-Versicherung in einer sehr modularen Form an und unterscheidet in der höchsten Aggregationsstufe fünf Deckungsgruppen.

- Angriffe auf Reputation und Identität
- Angriffe auf Zahlungsmittel und Konten
- Angriffe auf Hard- und Software sowie Daten
- Betriebsunterbrechung
- Haftpflicht sowie Datenschutzvorfälle

Diese fünf Deckungsgruppen können im COGITANDA® Deckungskonfigurator passgenau individualisiert werden. Neben einer Vielzahl von wählbaren Policen-Limiten und Policen-Selbstbehalten können auch für einzelne Deckungselemente Limite und Selbstbehalte individuell festgelegt oder Deckungen zu- oder abgewählt werden. So gestalten Berater Cyber-Versicherungsschutz für Ihre Kunden bedarfsgerecht und modular und stellen sicher, dass Prämie nur für das bezahlt wird, was der jeweilige Versicherungsnehmer tatsächlich benötigt und haben möchte.

Zusätzlich gibt es Sonderdeckungen zur Abrundung des Versicherungsschutzes. Der Deckungskonfigurator „Cyber Pro+“ ist damit das erste „Produkt“ im Markt, das den individuellen Cyber-Versicherungsschutz von kleinen und mittleren Unternehmen, aber auch von kleineren Industrieunternehmen gleichermaßen passgenau abbilden kann.



Cyber Schaden Management

Beim Schaden sofort da, rund um die Uhr

Soforthilfe: Melden Sie uns Schäden telefonisch oder online. Unsere Experten sind für Sie da. Nutzen Sie hierzu unsere 24-Stunden Schaden-Service Hotline an 365 Tagen.

Schaden beheben: Wir beheben das konkrete Problem und decken auch wirtschaftliche Folgeschäden.

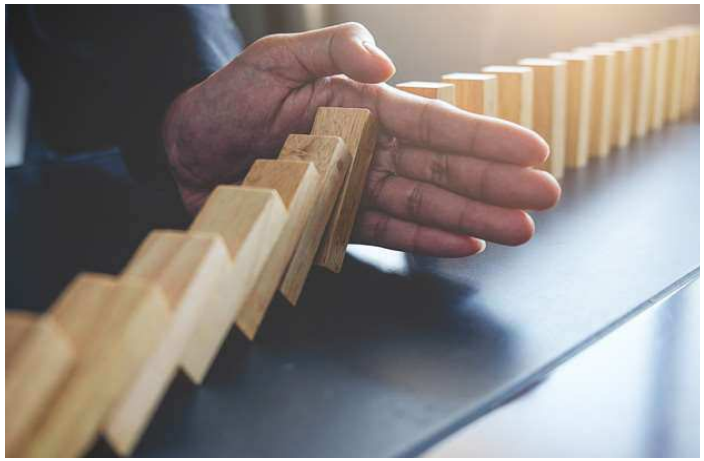
Prävention verbessern: Aus Schaden wird man klug. Jetzt heißt es für die Zukunft lernen und die Prävention verbessern. Währenddessen läuft das Unternehmen schon wieder rund.

Die besonderen Stärken von COGITANDA

Cyber-Schutz
Maßgeschneiderter Versicherungsschutz und professionelle Schadenbearbeitung

Qualifiziert & Erfahren
Jahrzehntelanges Know-How in der Versicherungsindustrie

360° Security
Perfekt aufgestellt für die Bewältigung von Cyber-Risiken, Prävention, Versicherung und Schadenbehebung



Prävention bei Cyber ein Muss

Cyber-Kriminelle greifen digitale Systeme von Unternehmen und privaten Haushalten mit dem Ziel an, sensible Daten zu stehlen oder zu manipulieren. Der Verlust von kritischen Daten, Zahlungsmitteln, die Unbrauchbarkeit von IT-Systemen, Reputationsschäden, aber auch Inanspruchnahme auf Schadenersatz durch Dritte sind die Folgen. Völlig ausschließen kann man solche Risiken durch Präventionsmaßnahmen nicht, wohl aber ein gutes Stück reduzieren.

Risiken erkennen

Prävention beginnt mit der Erfassung und Bewertung von Risiken. Das sich so ergebende Risikobild vor Augen, gilt es technische und organisatorische Maßnahmen abzuleiten und zu implementieren.

Maßnahmen ergreifen

Es lassen sich im Wesentlichen zwei Kategorien von Schutz-Maßnahmen unterscheiden: technische (Schutz-Software, Daten-Verschlüsselung, Backups) und organisatorische Maßnahmen (Schulung von Mitarbeitern und Notfallkonzepte).

Prävention - Technische und organisatorische Maßnahmen

Im Grunde genommen … ist Cyber ganz einfach. Vor allem dann, wenn technische und organisatorische Maßnahmen klar definiert und Regeln eingehalten werden.

Schulung von Mitarbeitern und Führungskräften

Die digitale Welt dreht sich schnell und wir werden täglich mit veränderten technischen Bedingungen konfrontiert. Dieser Herausforderung proaktiv zu begegnen beginnt mit der kontinuierlichen Schulung von Mitarbeitern und Führungskräften, der Entwicklung und Tests von Notfallplänen bis hin zum Krisenplan (Fokus auf technische Abläufe).

Standortbestimmung (Audit)

IT-Experten führen Beratungsgespräche zur Infrastruktur der IT-Sicherheit durch. Mit einer solchen einmaligen Standortbestimmung lässt sich sehr schnell eine Schwachstellenanalyse (Risk-Audit) ermitteln. Schwerpunkte dieser Standard-Checks sind neben der externen und internen Schwachstellenanalyse die Analyse von Prozessen und Strukturen (ISO-Norm) unter Einhaltung der DSG-VO. Darauf gut aufsetzen lassen sich individuell vereinbarte Prüfmaßnahmen (z.B. Penetrationstest).

Optimierung und Stabilisierung (einmalig)

Aus den gewonnenen Daten ergeben sich Präventions-maßnahmen zur Schwachstellenbehebung, dem Aufbau und der Optimierung aktueller IT-Sicherheitsstrukturen (HW/SW), die Etablierung eines Business Continuity Managements und nicht zuletzt die Ableitung zur Unterstützung bei Zertifizierungen (ISO27001 etc.).

Refresh Audit und Optimierung (regelmäßig)

Zur Messung der Erfüllung definierter Sicherheitsziele und -vorgaben finden in regelmäßigen Abständen Audit und Schwachstellenchecks statt.

Servicierung und Monitoring (365/24)

Nur eine kontinuierliche Überprüfung der Systeme sowie Schulung der Mitarbeiter und Führungskräfte, Schwachstellenanalysen und deren Behebung schützt ein Unternehmen an 365 Tagen im Jahr vor den Risiken krimineller Cyber-Angriffe.

Das COGITANDA® Team steht Ihnen für Security-Fragen gerne unter praevention@cogitanda.com zur Verfügung.

Cyber-Versicherung abschließen

Die Frequenz gravierender Cyber-Vorfälle nimmt deutlich zu, damit auch die Bedeutung der Cyber-Versicherung. Cyber ist eine sehr junge Versicherungs-sparte, zu der es allgemein noch wenig Erfahrung und kaum Spezialisten gibt. Wir bei der COGITANDA® beschäftigen uns seit Jahren mit Cyber und wir machen nichts anderes – dafür besser als jeder andere. Deshalb lautet unsere Botschaft:

CYBER SIND WIR.®

Die besonderen Stärken von COGITANDA

Cyber-Schutz
Maßgeschneiderter Versicherungsschutz und professionelle Schadenbearbeitung

Qualifiziert & Erfahren
Jahrzehntelanges Know-How in der Versicherungsindustrie

360° Security
Perfekt aufgestellt für die Bewältigung von Cyber-Risiken, Prävention, Versicherung und Schadenbehebung

360° Schutz – Wir managen Cyber-Schäden

Bei Cyber ist eine schnelle und professionelle Schadenbehebung unerlässlich, um existenzbedrohende Folgen für den Versicherungsnehmer abzuwenden. Zur Sicherstellung, dass das Schadenmanagement ohne Reibungsverlust und eng verzahnt mit allen erforderlichen Spezialisten und Dienstleistern erfolgt, führen wir das Schadenmanagement in einer Tochtergesellschaft durch, die sich auf das Managen von Cyber-Schäden spezialisiert hat, die COGITANDA® Claims Services GmbH.

In unserem gruppeninternen Schadencenter werden Versicherungsnehmer rund um die Uhr direkt von uns betreut. Wir managen die Behebung des Schadens und veranlassen und überwachen alle erforderlichen Schritte zur Schadenbehebung.

Beim Schaden sofort da, rund um die Uhr

Soforthilfe: Melden Sie uns Schäden telefonisch oder online. Unsere Experten sind für Sie da. Nutzen Sie hierzu unsere 24-Stunden Schaden-Service Hotline an 365 Tagen.

Schaden beheben: Wir beheben das konkrete Problem und decken auch wirtschaftliche Folgeschäden.

Prävention verbessern: Aus Schaden wird man klug. Jetzt heißt es für die Zukunft lernen und die Prävention verbessern. Währenddessen läuft das Unternehmen schon wieder rund.

Bei Cyber-Schäden muß jeder Handgriff sitzen

Cyber ist spätestens auf der Schadenseite die vielschichtigste und anspruchsvollste Versicherungssparte überhaupt. Eine Vielzahl von Spezialisten gilt es in der nötigen Qualität und Quantität zur Verfügung zu haben und im Schadenfall präzise und schnell einzusetzen. Nachfolgend ein paar Beispiele für solche Spezialisten.

Callcenter - 24/7: Rund um die Uhr Notruf-Callcenter, 365 Tage im Jahr. Wer hier klassische Call-Center-Mitarbeiter erwartet, irrt. Es geht nicht nur darum, rund um die Uhr erreichbar zu sein. Es werden Spezialisten gebraucht, die einen Fall richtig einschätzen, Soforthilfe leisten und umgehend die richtigen Schritte einleiten können, auch morgens um 03:00 Uhr.

Forensik: Forensiker analysieren die Form, Täterschaft und Auswirkungen eines Angriffs auf eine IT-Infrastruktur, es geht um Analyse, Aufklärung und Sofortmaßnahmen. Auch technische Fehlersuche sowie die Durchführung von Schulungen und Schwachstellen-Analysen sind das Feld von Forensikern.

IT-Spezialisten: Alles, was IT-technisch an Tätigkeiten zur Schadensbehebung ansteht. Bereinigung oder Austausch von Hardware, Neuinstallation von Software, Daten-wiederherstellung, etc.

Datenschutzexperten: Datenschutzvorfälle analysieren, Maßnahmen festlegen und durchführen bzw. überwachen.

Hardware- und Software-Lieferanten: Hardware und Software sind regelmäßig betroffen von Cyber-Angriffen, nicht immer lässt sich der Schaden reparieren, sondern ein Austausch ist erforderlich.

Anwälte/Rechtsbeistand: Vor allem in Haftpflicht-Fällen sind geeignete Anwälte unverzichtbar, aber auch bei Datenschutzvorfällen und Reputationsschäden.

Krisenberater: Stillstehende IT-Systeme, kompromittierte Konten, gestohlene Identitäten, das ist Krise pur für die Betroffenen. Trotz alledem jetzt nicht den Kopf zu verlieren, sondern diese Krise mit kühlem Blut zu managen helfen, das ist Aufgabe von Krisenberatern.

Kommunikations-Spezialisten: Insbesondere im Falle von gestohlenen Identitäten und/ oder Fällen von Rufschädigung ist eine professionelle Kommunikation das einzig wirksame Mittel. Das gehört in die Hände eines Kommunikations-Spezialisten.

Die besonderen Stärken von COGITANDA

Cyber-Schutz
Maßgeschneiderter Versicherungsschutz und professionelle Schadenbearbeitung

Qualifiziert & Erfahren
Jahrzehntelanges Know-How in der Versicherungsindustrie

360° Security
Perfekt aufgestellt für die Bewältigung von Cyber-Risiken, Prävention, Versicherung und Schadenbehebung