Gothaer GewerbeProtect Cyber-Versicherung
Informationsbroschüre für Vertriebspartner*innen.

Gothaer

ZUKUNFT WIRD
AUS MUT GEMACHT.

AUF DEN GESCHÄFTSERFOLG KONZENTRIEREN.

Dies unterstützen wir mit modularen Versicherungs-Bausteinen. **Und** bieten so einen Rundum-Cyber-Schutz mit umfassenden Präventionsleistungen.

24-STUNDEN CYBER-SOFORTHILFE

Inhaltsverzeichnis

	Zeichnungskapazitäten	3
	Vertragsabschluss	4
	Highlights der Bedingungen	5
	Anhaltspunkte Versicherungssummenermittlung	14
	Prozess zu Präventionsleistungen	15
	Vertragsverlängerung	15
	Schadenprozess und Key Learnings	16
	Schadenbeispiele	18
	Dienstleistungsübersicht	21
	Fragen und Antworten	22
	Glossar	25

Zeichnungskapazitäten

Die Gothaer Allgemeine Versicherung AG zeichnet die Gewerbe Cyber-Risiken auf Basis der aktuellsten Versicherungsbedingungen zur GGP Cyber-Versicherung.

Die GGP Cyber-Versicherung gilt für Gewerbekunden bis zu einem Jahresumsatz von 10 Mio. Euro.

Cyber-Versicherung für Gewerbekunden und freie Berufe (bis 10 Mio. Euro Jahresumsatz)

Vertragsgrundlage	Versicherungssumme	Maximierung	Vertragslaufzeit
AVB zur GGP Cyber-Versicherung	bis 2.500.000 EUR	1-fach p. a.	bis max. 3 Jahre

Zeichnungsfähige Risiken

Die GGP Cyber-Versicherung zeichnet Cyber-Risiken von Firmen, die ihren Sitz ausschließlich in Deutschland haben. Auslandsrisiken sind nicht zeichenbar. Über 2.800 verschiedene Stichwörter beinhaltet die GGP Cyber-Versicherung und bietet somit für nahezu alle Branchen die passende Cyber-Versicherungslösung an. Weitere Informationen finden Sie im Stichwortverzeichnis für die Cyber-Versicherung.

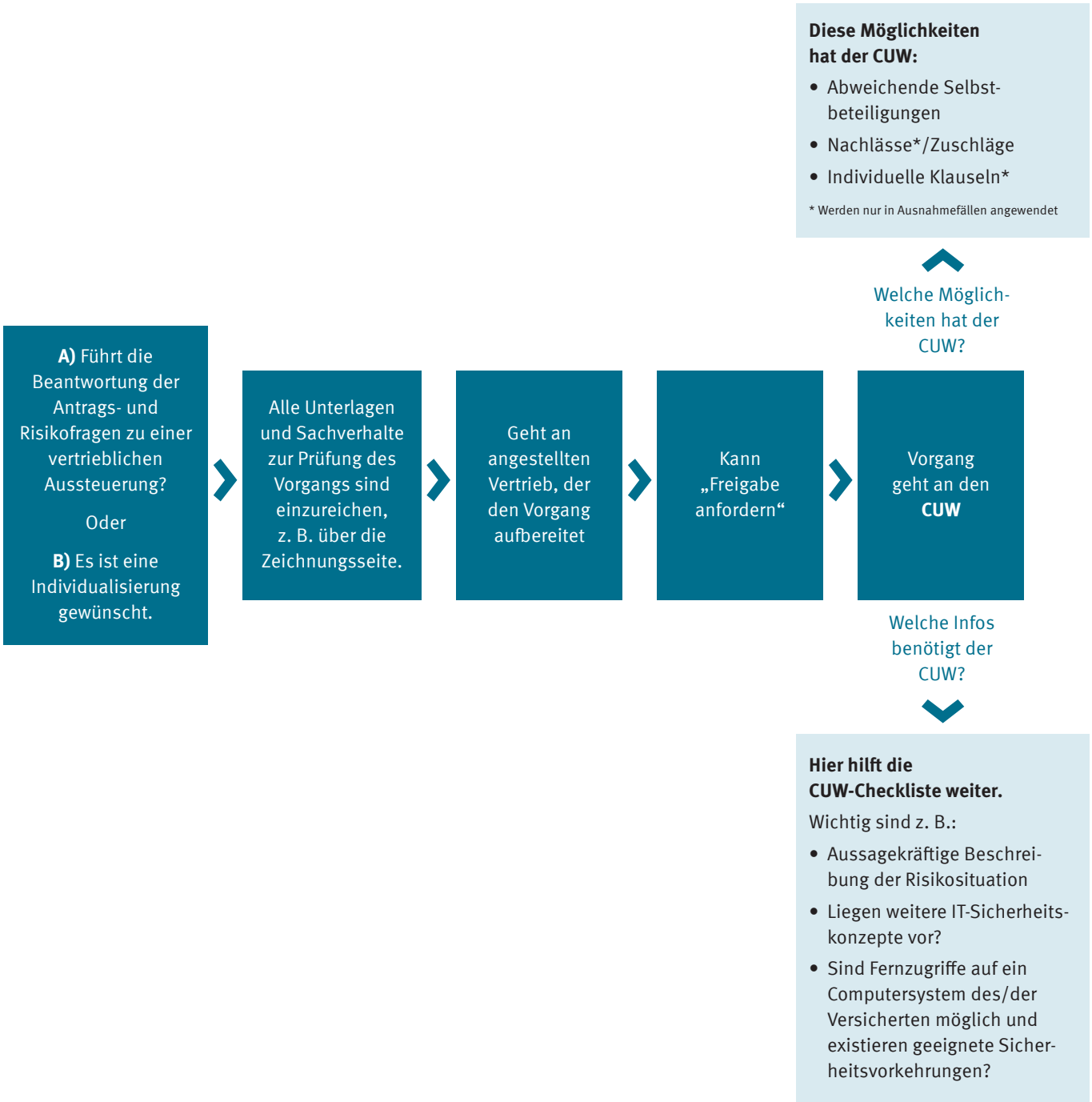
Jedoch werden die nachfolgenden Branchen im Cyber-Segment als **kritisch betrachtet:**

- Finanzinstitute (Banken, Kreditkartenunternehmen, Versicherungen, Krankenkassen)
- Größere Verkehrsbetriebe
- Größere Krankenhäuser
- Größere Versorgungsbetriebe (Strom, Wasser, Gas, Wärme, Telekommunikation)
- Cloud-Service-Provider
- Betreiber von Rechenzentren
- Online-Zahlungsplattformen
- Unternehmen der Rüstungsindustrie
- Bergbau-Unternehmen, Gewinnung von Rohstoffen (Öl, Gas, Kohle, Erze), Fracking
- Raffinerien, Kokereien
- Wettbüros, Lotterien, Online-Spielcasinos
- Anbieter von pornografischen Inhalten, Betrieb von Bordellen

Vertragsabschluss

Die Tarifierung kann über den TAA/TR am Point of Sale abgeschlossen werden. Auch in der GGP Cyber-Versicherung stehen die Prozesse der Dunkelverarbeitung und der elektronischen Unterschrift zur Verfügung.

Aussteuerung/Individualisierung



Highlights der Bedingungen

Die GGP Cyber-Versicherung bietet einen leistungsstarken Versicherungsschutz. Grundlage hierfür sind die ausgezeichneten Vertragsbestimmungen. Diese werden regelmäßig überprüft, um sicherzustellen, dass die Entwicklungen am Versicherungsmarkt frühzeitig erkannt und berücksichtigt werden können.

Folgende Voraussetzungen für den Versicherungsfall gelten:

Datenrechtsverletzung

... ist jede Verletzung von datenschutzrechtlichen Bestimmungen, anwendbaren Geheimhaltungspflichten und Vertraulichkeitserklärungen, Persönlichkeitsrechten eines Dritten infolge des Missbrauchs des Computersystems eines Versicherten oder einer Kreditkartenverarbeitungsvereinbarung mit einem Kreditinstitut durch einen Versicherten.

IT-Sicherheitsverletzung

... liegt vor, wenn ausgehend vom Computersystem eines Versicherten Programme auf dem Computersystem eines Dritten installiert werden, auf das Computersystem eines Dritten unbefugt zugegriffen wird oder ein (Distributed) Denial-of-Service-Angriff gegen Dienste auf dem Computersystem eines Dritten vorgenommen wird.

Hacker-Angriff

... liegt vor, wenn unbefugt Schadsoftware und/oder Schadhardware (z. B. Keylogger) auf dem Computersystem eines Versicherten installiert wird, bei einem sonstigen unbefugten Zugriff auf das Computersystem eines Versicherten durch Dritte oder bei einem (Distributed) Denial-of-Service-Angriff gegen Dienste auf dem Computersystem des Versicherten.

Produkt

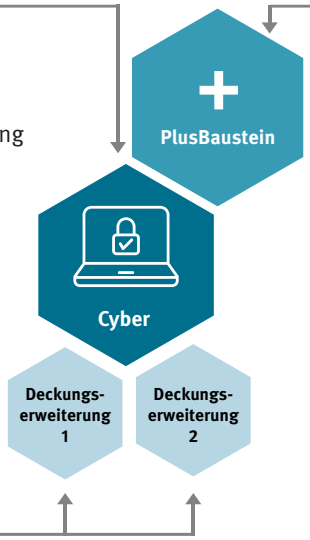
Der nachfolgende Überblick nennt die wichtigsten Highlights der Versicherungsbedingungen. Die **Grunddeckung der GGP Cyber-Versicherung** beinhaltet die wichtigsten Bausteine einer Cyber-Versicherung. Sie beinhaltet folgende Deckungen:

- Cyber-Haftpflicht
- Cyber-Vertragsstrafe PCI-DSS
- Cyber-Eigenschaden Assistance-Dienstleistung
- Cyber-Erweiterte Eigenschäden
- Cyber-Betriebsunterbrechung
- Cyber-Erpressung

Die GGP Cyber-Versicherung – Aufbau des Produktes und Deckungsinhalte

Grunddeckung: GGP Cyber
- Cyber-Haftpflicht
- Cyber-Vertragsstrafe PCI-DSS
- Cyber-Eigenschaden Assistance-Dienstleistung
- Cyber-Erweiterte Eigenschäden
- Cyber-Betriebsunterbrechung
- Cyber-Erpressung

Deckungserweiterungen (optional):
- Einschluss Vertragsstrafen wegen Verletzung von Datenschutzbestimmungen und Geheimhaltungspflichten
- Einschluss Cyber-Diebstahl/Cyber-Betrug



PlusBaustein (optional):
Erhöhung der generellen Sublimits um das 2,5-Fache für ausgewählte Bestandteile
- Unterschied besteht in den Höhen der zusätzlich vereinbarten Versicherungssummen und Entschädigungsgrenzen sowie in einzelnen Leistungskomponenten.

Ziel: leistungsstarke Grunddeckung und Individualisierungsmöglichkeiten des Versicherungsschutzes

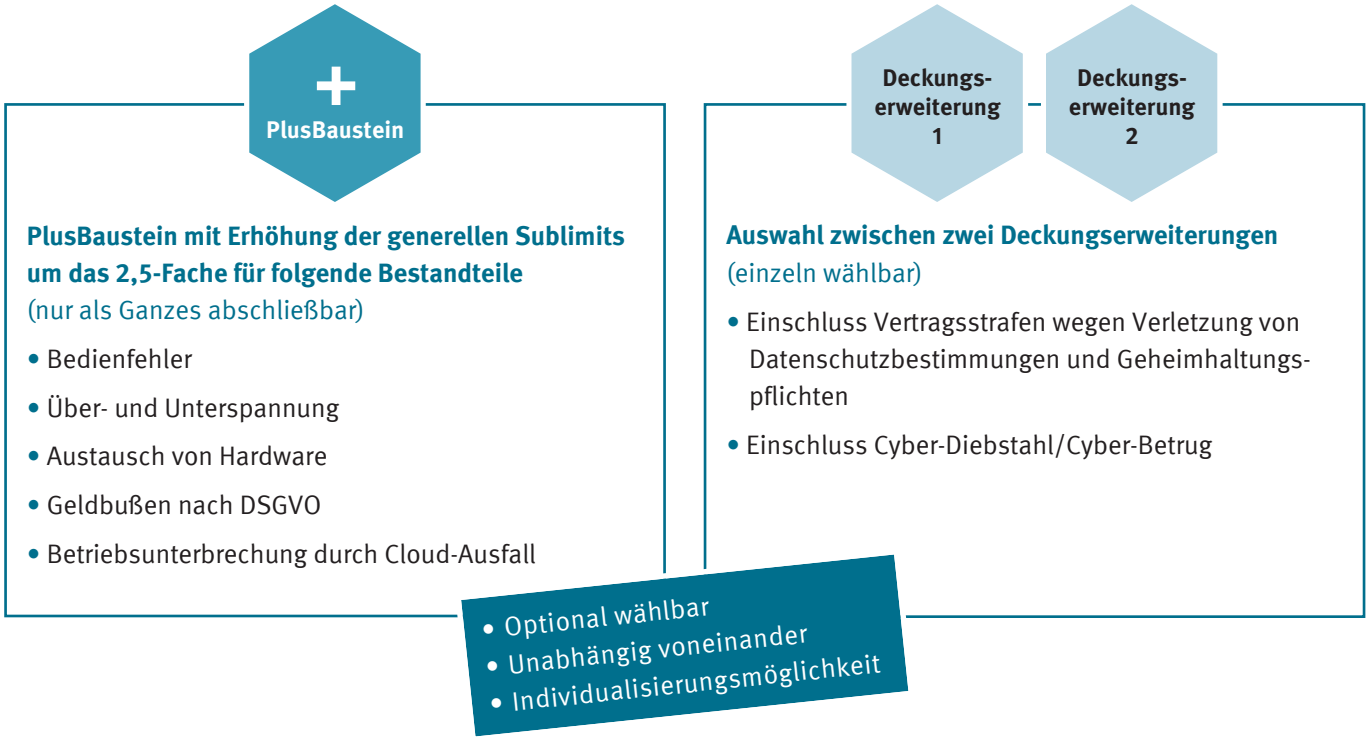
Highlights der Grunddeckung GGP Cyber-Versicherung

- **Leistungsstarker Versicherungsschutz** bei Datenrechts- und IT-Sicherheitsverletzungen sowie bei Hacker-Angriffen
  - Prüfung der Haftpflichtfrage und Abwehr unberechtigter Schadensersatzansprüche
  - Kostenübernahme bei behördlichen Verfahren wegen Datenrechtsverletzungen und bei freiwilliger Anzeige
  - Übernahme von Eigenschäden
  - BU und Wiederherstellung von Daten und Programmen durch Bedienfehler
  - Übernahme des Schadens und der Mehrkosten durch eine unmittelbare, unvorhersehbare BU oder eine vorsorgliche Systemabschaltung aufgrund eines Hacker-Angriffs
- **24-Stunden-Cyber-Soforthilfe ohne Selbstbeteiligung.** Unser Expert*innen-Team leitet Tag und Nacht umgehend Maßnahmen zur Schadensbegrenzung und Beweissicherung (Forensik) ein.
- Für ein halbes Jahr **kostenfreie Präventions- und Schulungsmaßnahmen,** um Mitarbeitende für Cybergefahren zu sensibilisieren (46 % aller Cybervorfälle werden durch unbeabsichtigtes Fehlverhalten eigener Mitarbeiter*innen verursacht.)

Kriterium	GGP Cyber-Versicherung
Zahlweisen	Monatliche, vierteljährliche, halbjährliche und jährliche Zahlweise
Tarif	Stetiger Tarif
Tarifkombination	Alle Kombinationen aus Versicherungssumme, Umsatz und Selbstbehalt wählbar
Wählbare Versicherungssummen	100.000 EUR, 250.000 EUR, 500.000 EUR, 1 Mio. EUR, 1,5 Mio. EUR, 2 Mio. EUR, 2,5 Mio. EUR
Wählbare Selbstbeteiligung	1.000 EUR, 2.500 EUR, 5.000 EUR

PlusBaustein und Deckungserweiterungen in der GGP Cyber-Versicherung

Es gibt drei optionale Erweiterungen zur GGP Cyber-Versicherung: den **PlusBaustein** und **zwei Deckungserweiterungen,** die unabhängig voneinander abgeschlossen werden können.



Prozess:

- Direkte Erfassung im Angebotssystem
- Hohe Transparenz, ob der Kunde in der GGP Cyber-Versicherung versicherbar ist
- Direkter Versicherungsschutz und umgehende Policierung
- Dunkelverarbeitungsfähig, kein Papierantrag mehr

Cyber-Schaden-Hotline:

- Separate Hotline-Nummer nur für Gothaer Kunden
- 24/7/365-Erreichbarkeit
- Inkl. IT-Support und Forensik, sofern erforderlich auch vor Ort
- Ohne Selbstbeteiligung

Versicherungsinhalte

Im Folgenden werden die wesentlichen Versicherungselemente im Überblick dargestellt.

Drittschäden (Haftpflichtversicherung)

- **Haftpflichtversicherung:**
  - Prüfung der Haftpflichtfrage
  - Abwehr unberechtigter Schadensersatzansprüche
  - Freistellung des Versicherten von berechtigten Schadensersatzansprüchen

- **Versicherungsschutz für behördliche Verfahren wegen Datenrechtsverletzungen:**
  Kosten, die dem Versicherten durch die Abwehr von gegen ihn wegen einer Datenrechtsverletzung eingeleiteten Straf-, Ordnungswidrigkeits- oder sonstigen behördlichen Verfahren entstehen. Umfasst auch die Kosten, die dem Versicherten durch die freiwillige Anzeige einer Datenrechtsverletzung gegenüber Datenschutzbehörden entstehen.

- **Ausgegliederte Datenverarbeitung:**
  Versicherungsschutz besteht auch für eine vom Versicherten durch Freistellungsverpflichtung übernommene gesetzliche Haftpflicht privatrechtlichen Inhalts wegen einer Datenrechtsverletzung oder einer sonstigen Pflichtverletzung (Tun und Unterlassen) des Versicherten gegenüber einem Dritten, die eine IT-Sicherheitsverletzung oder einen Hacker-Angriff zur Folge hat, wenn diese gegen ein Unternehmen geltend gemacht wird, das vom Versicherten mit der Verarbeitung von Daten Dritter beauftragt ist.

- **Einstweiliger Rechtsschutz, Unterlassungs- oder Widerrufsklagen:**
  Kosten eines Verfahrens wegen einer Datenrechtsverletzung oder einer sonstigen Pflichtverletzung (Tun oder Unterlassen) des Versicherten gegenüber einem Dritten, die eine IT-Sicherheitsverletzung oder einen Hacker-Angriff zur Folge hat, wenn im Verfahren der Erlass einer einstweiligen Verfügung gegen den Versicherten begehrt wird.

- **Medienhaftpflicht:**
  Versicherungsschutz besteht für Ansprüche Dritter wegen der Verletzung von Persönlichkeits- und Namensrechten, Urheber- und Markenrechten und daraus resultierenden Wettbewerbsrechten durch digitale Medieninhalte.

Eigenschaden Assistance-Dienstleistungen

- **Kosten für sicherheitstechnische Dienstleistungen:**
  Kosten für die Honorare, Auslagen und Aufwendungen eines qualifizierten Dienstleistungsunternehmens, das mit der Erstanalyse sowie mit der Definition und Einleitung von Gegenmaßnahmen zur Schadenminimierung sowie zur Bestätigung und Ermittlung der Ursache eines Versicherungsfalls (Forensik) beauftragt wurde. Eine im Versicherungsschein oder seinen Nachträgen vereinbarte Selbstbeteiligung fällt für die sicherheitstechnische Dienstleistung nicht an.

- **Kosten für Verbesserungsempfehlungen und Verbesserungsmaßnahmen:**
  Übernahme von Honoraren, Auslagen und Aufwendungen des Dienstleistungsunternehmens für Empfehlungen zur Verbesserung der Informationssicherheit der vom Versicherungsfall direkt betroffenen Teile des Computersystems des Versicherten.
  Kosten für angemessene und geeignete Maßnahmen, welche zur Schließung der für den Versicherungsfall ursächlichen und direkt betroffenen Sicherheitslücke dienen.

- **Kosten im Zusammenhang mit Benachrichtigungspflichten:**
  Kosten für notwendige und angemessene Kosten, die dadurch entstehen, dass der Versicherte aufgrund einer Datenrechtsverletzung gesetzliche oder behördliche Benachrichtigungspflichten erfüllen muss. Versicherungsschutz besteht auch für die notwendigen und angemessenen Kosten der Einrichtung und des Betriebs eines Callcenters und einer einzurichtenden Website zur Information und Abwicklung von Anfragen der von der Datenrechtsverletzung Betroffenen sowie Dritter.

- **Kosten für Kommunikations- und Public-Relations-Maßnahmen:**
  Kosten für notwendige und angemessene Kosten für Kommunikations- und Public-Relations-Maßnahmen des Versicherten, Kosten für Abwehr oder Minderung eines Reputationsschadens. Dies umfasst auch die Kosten für die Erstellung und das Versenden von Goodwill-Coupons, nicht jedoch die darin gewährten Vorteile selbst.

- **Kosten für Datenüberwachungsdienstleistungen:**
  Im Falle einer Datenrechtsverletzung für Kosten eines Monitoring-Services (Kreditüberwachungsdienstleistung), um für einen Zeitraum von bis zu 12 Monaten den Missbrauch personenbezogener, von der Datenrechtsverletzung betroffener Daten zu überprüfen.

- **Kosten der Wiederherstellung von Daten und Programmen:**
  Im Falle eines Hacker-Angriffs auf das Computersystem des Versicherten für Kosten:
  – zur Feststellung, ob Daten und Programme wiederhergestellt, erneut erfasst oder neu erhoben werden können
  – zur Entfernung von Schadsoftware
  – zur Wiederherstellung des früheren, betriebsbereiten Zustandes der Daten und Programme
  – für den Austausch von Hardwarekomponenten des Versicherten, wenn das Entfernen von Schadsoftware sowie das Wiederherstellen von Daten und Programmen nicht möglich oder wirtschaftlich nicht sinnvoll sind

- **Kosten für Krisenmanager:**
  Für die notwendigen und angemessenen Honorare, Gebühren und Auslagen des vom Versicherer beauftragten Krisenmanagers. Hierzu zählen insbesondere Reise-, Unterbringungs-, Übersetzungs- und Kommunikationskosten, auch infolge einer von einem Dritten angedrohten Handlung.

Betriebsunterbrechung

Versicherungsschutz besteht unter Berücksichtigung der im Versicherungsschein ausgewiesenen zeitlichen Selbstbeteiligung und der vereinbarten Haftzeit für den unmittelbar durch eine unvorhergesehene Betriebsunterbrechung verursachten Betriebsunterbrechungsschaden eines Versicherten, wenn diese Unterbrechung unmittelbar und ausschließlich durch einen Hacker-Angriff verursacht wird. Eine Betriebsunterbrechung liegt auch bei einer vorsorglichen Systemabschaltung vor, sofern diese durch einen Hacker-Angriff bedingt und durch einen vom Versicherer beauftragten, qualifizierten Dienstleister oder eine zuständige Behörde, sofern die Entscheidung der Behörde durch ein qualifiziertes Dienstleistungsunternehmen als sinnvoll bestätigt wird, veranlasst wurde.

Sofern die Betriebsunterbrechung die vereinbarte zeitliche Selbstbeteiligung überschreitet, besteht auch Versicherungsschutz für den Teil des Betriebsunterbrechungsschadens, der während der zeitlichen Selbstbeteiligung eingetreten ist.

Im Falle einer versicherten Betriebsunterbrechung erstattet der Versicherer dem Versicherten auch alle angemessenen und notwendigen Mehrkosten, die dieser nach Zustimmung des Versicherers für die provisorische Aufrechterhaltung oder zur Beschleunigung der Wiederherstellung des Betriebes aufwendet. Auch mitversichert ist die Betriebsunterbrechung bei der VN durch

einen Ausfall der Cloud-Services oder der Computersysteme eines namentlich benannten Dienstleisters. Bei dem Deckungsinhalt Betriebsunterbrechung durch Cloud-Ausfall ist das Sublimit zu berücksichtigen.

Vertragsstrafen

- **PCI-DSS:**
  Kosten für die Abwehr unberechtigter und die Freistellung von berechtigten Forderungen zur Zahlung von Vertragsstrafen, die durch einen E-Payment-Service-Provider wegen einer Verletzung des vereinbarten Payment-Card-Industry-Datensicherheitsstandards (PCI-DSS) gegen einen Versicherten geltend gemacht werden

Erweiterte Eigenschäden

- **Eigenschäden durch mitversicherte Personen:**
  - Bei Verletzung von Geheimhaltungspflichten bezüglich Daten
  - Bei Verletzung von Persönlichkeitsrechten infolge eines Missbrauchs des Computersystems
  - Bei Hacker-Angriff durch eine mitversicherte Person

- **Bedienfehler:**
  Betriebsunterbrechung und Datenwiederherstellung wegen Bedienfehlern am Computersystem der VN durch eine mitversicherte Person

- **Sachschäden am Computersystem:**
  Versicherungsschutz für Sachschäden am Computersystem des Versicherten aufgrund von Hacker-Angriffen

- **Unter- und Überspannung, elektromagnetische Störung:**
  Versicherungsschutz bei Unter- und Überspannungen sowie elektromagnetischen Störungen am Computersystem des Versicherten, für Kosten der Wiederherstellung von Daten und Programmen sowie für den Betriebsunterbrechungsschaden

- **Geldbußen:**
  Sofern kein gesetzliches Versicherungsverbot entgegensteht, besteht Versicherungsschutz für auf Basis der EU-Datenschutzgrundverordnung wegen einer Datenrechtsverletzung gegen ein versichertes Unternehmen rechtskräftig verhängte Geldbußen.

- **Sachschäden an Fertigungserzeugnissen:**
  Kosten für die Wiederbeschaffung der zur Fertigung der schadhaften Erzeugnisse verwendeten Roh-, Hilfs- und Betriebsstoffe und Kosten für die Entsorgung von unbrauchbaren Erzeugnissen aufgrund von Sachschäden an Fertigungserzeugnissen durch Veränderung oder Unterbrechung des Fertigungsprozesses durch einen Hacker-Angriff

- **Bring-your-own-device (BYOD):**
  Es besteht Versicherungsschutz auch dann, wenn der Versicherte im Rahmen von selbst definierten Richtlinien zur IT-Sicherheit den Einsatz von Bring-your-own-device zulässt. Das Computersystem des Versicherten umfasst insoweit dann auch die in diesem Rahmen eingesetzten informations- und telekommunikationstechnischen Geräte.

- **Rückwärtsversicherung:** 24 Monate

- **Nachmeldefrist:** 36 Monate

Cyber-Erpressung

Versicherungsschutz für Aufwendungen und Kosten infolge einer Cyber-Erpressung.

Optionale Deckungserweiterung

- **Verletzung von Datenschutzbestimmungen und Geheimhaltungspflichten:**
  Kosten für die Abwehr unberechtigter und die Freistellung von berechtigten Forderungen zur Zahlung von Vertragsstrafen aufgrund von Verletzungen von Geheimhaltungspflichten und anwendbaren datenschutzrechtlichen Bestimmungen, infolge einer Datenrechtsverletzung oder eines Hacker-Angriffs.

- **Cyber-Diebstahl:**
  - Bei Manipulation der Website oder der daran angeschlossenen Datenbanken und Programme
  - Bei Manipulation des Online-Bankings oder von Online-Zahlungssystemen versicherter Unternehmen
  - Bei Diebstahl oder Veränderung von Daten, welche zur Teilnahme am Zahlungsverkehr befähigen
  - Bei unberechtigter Nutzung der Telefonanlage

- **Cyber-Betrug:**
  Direkte Geldverluste durch die Täuschung einer mitversicherten Person als unmittelbare Folge eines Hacker-Angriffs auf das Computersystem des Versicherten

Für die oben aufgeführten Versicherungsinhalte wird kein Anspruch auf Vollständigkeit erhoben, sie dienen ausschließlich Informationszwecken.

Mindestsicherheitsanforderungen

Um Datenrechtsverletzungen, IT-Sicherheitsverletzungen und Hacker-Angriffe zu verhindern und die Wiederherstellung von Daten und Programmen zu ermöglichen, sind bestimmte Mindestanforderungen der technischen Einrichtungen, Systeme und Verfahren zur Informationssicherheit zu unterhalten.
Dies betrifft die Bereiche

- Datensicherung
- Netzwerksicherheit
- Patch-Management
- Datensicherheit und Benutzerkonten
- Notfallmanagement
- Mitarbeiterschulung
- Fernzugriffe

Anhaltspunkte zur Versicherungssummenermittlung

Die nachfolgenden Anhaltspunkte zur Versicherungssummenermittlung sollen lediglich für eine erste grobe Einschätzung des zu versichernden Cyber-Risikos Anwendung finden.

Der ermittelte Betrag stellt eine empfohlene Mindestabsicherung zur gewerblichen Cyber-Versicherung dar. Er wurde anhand rudimentärer Parameter und ohne Berücksichtigung der Gesamtsituation des Kunden ermittelt. Die nächstmögliche, über diesem Betrag liegende Versicherungssumme sollte dem Kunden als Mindestversicherungssumme vorgeschlagen werden.

Im persönlichen Kundengespräch sollte die individuelle Risikosituation des Kunden besprochen und von diesem dargestellt werden. Dies kann zu einem anderen Absicherungsbedarf führen.

Zur Abbildung der genauen Versicherungssumme ist der TAA/TR zu verwenden.

Anhaltspunkte zur Versicherungssummenermittlung:

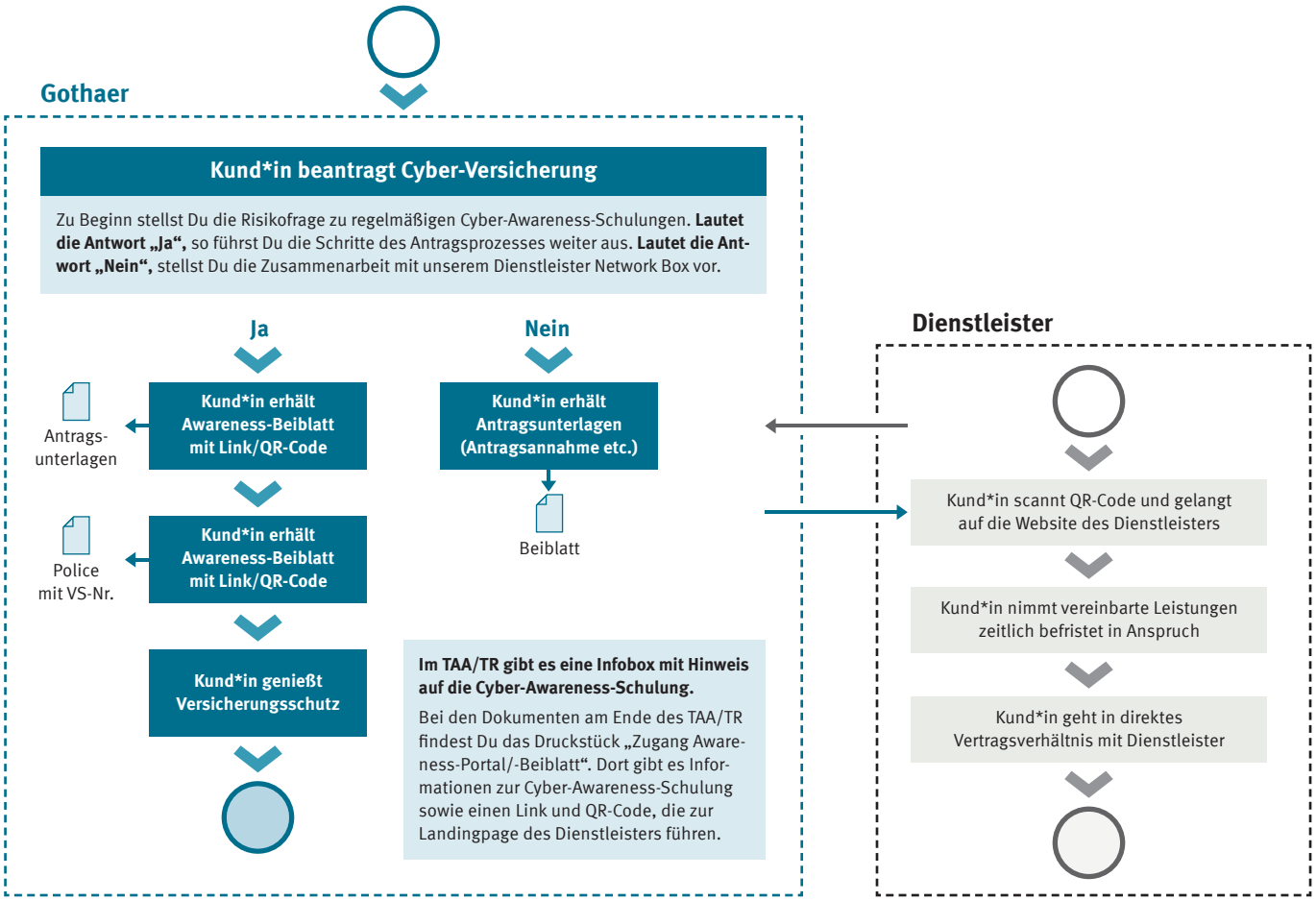
Betriebsunterbrechungsanteil:	15 % vom Jahresumsatz alternativ 33 % vom Jahresgewinn + 1,5 % vom Jahresumsatz	
Personenbezogene Datensätze:	50 EUR pro Datensatz	
Dienstleisterkostenanteil: (Beträge sind innerhalb einer Risikoklasse 1–4 festzulegen je nach Spannen der im TAA/TR ermittelten statistischen Daten, z. B. Anzahl Geräte)	Kleineres Risikopotential (Risikoklasse I) Mittleres Risikopotential (Risikoklasse II) Höheres Risikopotential (Risikoklasse III) Hohes Risikopotential (Risikoklasse IV)	50.000 EUR – 100.000 EUR 75.000 EUR – 175.000 EUR 125.000 EUR – 225.000 EUR 200.000 EUR – 250.000 EUR
Drittschadenanteil:	10 % vom Jahresumsatz	

Prozess zu Präventionsleistungen

In Zusammenarbeit mit unserem Kooperationspartner Network Box bieten wir für Gothaer Unternehmerkund*innen mit einer Cyber-Versicherung, exklusiv und für das erste halbe Jahr kostenfrei, die Cyber-Präventionsleistungen von Network Box an. Dazu gehören die Durchführung einer Phishing-Simulation samt Auswertung und die Schulung der Mitarbeitenden in Form von kurzen und professionellen eLearning-Einheiten.

Im Anschluss kann das Network Box ReTeach Paket zu einem attraktiven Preis weitergeführt werden. So werden die vertraglichen Obliegenheiten der Gothaer Cyber-Versicherung bzgl. regelmäßiger Mitarbeiter-Präventionsschulungen erfüllt.

Awareness-Schulung – Prozessablauf



Vertragsverlängerung

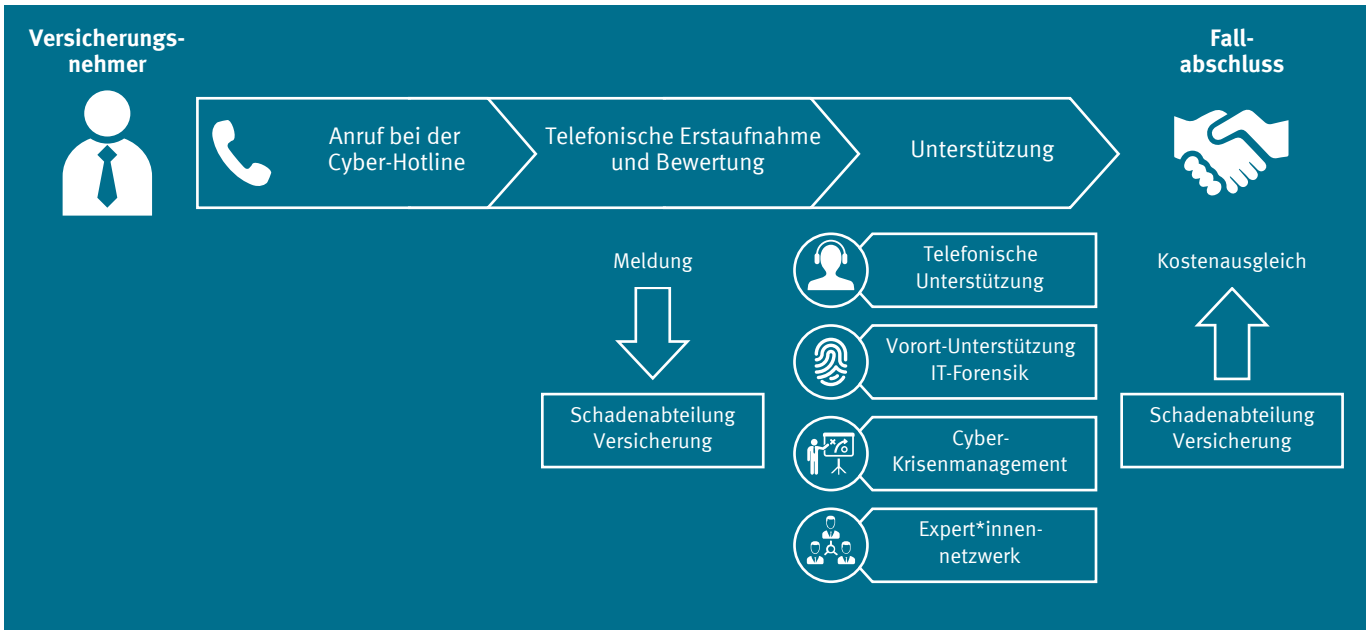
Grundsätzlich beträgt die Vertragslaufzeit max. 3 Jahre.

Unabhängig von der individuellen Laufzeit des Cyber-Vertrages gilt, dass sich dieser automatisch um ein Jahr verlängert – es sei denn, der Vertrag wird spätestens 3 Monate vor Vertragsende von einer der Vertragsparteien gekündigt.

Schadenprozess und Key Learnings

Idealer Schadenprozess

Im Folgenden finden Sie eine grafische Darstellung des idealen Schadenprozesses der Gothaer Cyber-Versicherung. Im Rahmen der individuellen Schadenbearbeitung und Unterstützung im Schadenfall durch das spezialisierte Dienstleisternetzwerk sind Abweichungen zum dargestellten Prozess möglich. Grundsätzlich findet jedoch der abgebildete Schadenprozess Anwendung.



Key Learnings

Im Rahmen der bisherigen Erfahrungen im Zusammenhang mit Schadenfällen zur Gothaer Cyber-Versicherung sind folgende wesentliche organisatorische und technische Punkte aufgefallen, welche nochmals besonders hervorzuheben und zu beachten sind.

Key Learnings organisatorisch

Häufig späte Einschaltung der Forensik

- Bei VERDACHT eines Cyber-Vorfalls sofortige Kontaktaufnahme mit der 24/7-Hotline!
- Klassische IT-Dienstleister sind keine Forensiker!

Häufiges Einfallstor E-Mail

- Awareness erhöhen. Nutzung des Dienstleisters Network Box!

Kurze Reaktionszeiten durch erprobtes Krisenmanagement

- Sofortiges Handeln und das Einschalten der richtigen Expert*innen hilft, den Schaden zu begrenzen
  ➜ Hotline!

Bedrohungslage und Business Impact analysieren

- Cyber-Versicherung grundsätzlich für jedes Unternehmen wichtig, das
  - wichtige Prozesse IT- oder webgestützt steuert,
  - hohe Bestände sensibler Daten verwaltet und/oder
  - über IT-Systeme Vermögenswerte verwaltet.

Key Learnings technisch

1 Obliegenheiten stellen für KMU häufig Hürden dar
Patch-Management, aktuelle und richtig konfigurierte Firewall und Antiviren-Software zwingend erforderlich

2 Kein Back-up, kein Mitleid
Back-up machen, testen und getrennt lagern!

3 Segmentierung des Netzwerks

4 Deaktivierung von Makros im Rahmen der Office-Anwendungen

5 Isolierung von Mails mit kritischen Anhängen

6 Individuelle Zugangskonten zum Computersystem und verpflichtende regelmäßige Passwortänderungen

Schadenbeispiele

Nachfolgend aufgeführte Schadenbeispiele können zu einer Anspruchsstellung unter einer Cyber-Versicherung führen.

Datenrechtsverletzung

Phishing-Angriff auf IT-Systemhaus:
Es erfolgt ein Angriff mittels Phishing auf die IT-Systeme eines Personalberatungsunternehmens. Ziel ist, die vorhandenen Personendaten permanent im Hintergrund abzugreifen. Der Angriff richtet keinen erkennbaren Schaden an der IT-Umgebung an, jedoch werden in großem Umfang Personendaten gestohlen. Diese Daten werden anschließend im Darknet zum Verkauf angeboten, woraufhin die betroffenen Kund*innen Schadensersatzansprüche gegenüber der Personalberatung anmelden.

Leistungen unter der GGP Cyber-Versicherung:
- Soforthilfe durch die 24/7/365-Cyber-Hotline
- Kosten für IT-Forensik
- Kosten für den Einsatz eines Krisenmanagers
- Kosten für PR-Maßnahmen
- Haftpflichtansprüche der betroffenen Kund*innen

Datenabgriff bei Lebensmittelproduzenten mit Kundenclub:
Es erfolgt ein Angriff über eine nicht geschlossene Sicherheitslücke auf die IT-Systeme eines Lebensmittelproduzenten mit Kundenclub. Die persönlichen Daten aller Mitglieder des Kundenclubs werden abgegriffen. Diese Kundendaten werden anschließend im Darknet zum Verkauf angeboten.

Leistungen unter der GGP Cyber-Versicherung:
- Soforthilfe durch die 24/7/365-Cyber-Hotline
- Kosten für IT-Forensik
- Benachrichtigungskosten und Einrichtung eines Callcenters
- Kosten für den Einsatz eines Krisenmanagers
- Kosten für PR-Maßnahmen
- Kosten für die Abwehr eines behördlichen Verfahrens

IT-Sicherheits-verletzung

DDoS-Attacke auf Schuhhandel:
Das Computersystem eines versicherten Unternehmens wird von einem Dritten zum Angriff auf ein Schuhgeschäft mit Online-Handel mittels einer Distributed-Denial-of-Service-Attacke benutzt. Dadurch kommt es bei dem Teil des Schuhhandels, der online erfolgt, zu einer mehrstündigen Betriebsunterbrechung, da die Internetseite nicht mehr erreichbar ist. Der Schuhhandel macht Schadensersatzansprüche gegenüber dem versicherten Unternehmen geltend.

Leistungen unter der GGP Cyber-Versicherung:
- Soforthilfe durch die 24/7/365-Cyber-Hotline
- Kosten für IT-Forensik
- Haftpflichtansprüche des betroffenen Schuhhandels

Hacker-Angriff

Computervirus in E-Mail:
Ein Mitarbeiter eines versicherten Unternehmens erhält von einem Dritten eine E-Mail mit einem Anhang, der einen Trojaner enthält. Der Mitarbeiter öffnet aus Neugierde oder Gewohnheit den Anhang. Daraufhin verschlüsselt der Trojaner unbemerkt mehrere Wochen lang die täglichen Back-ups. Erst dann „bricht er aus“ und verschlüsselt auch alle Clients, so dass der Betrieb unterbrochen wird. Für die Entschlüsselung wird ein Lösegeld gefordert. Wegen der Verschlüsselung der Back-ups gelingt die versuchte Datenwiederherstellung nicht. Das Lösegeld wird gezahlt.

Leistungen unter der GGP Cyber-Versicherung:
- Soforthilfe durch die 24/7/365-Cyber-Hotline
- Kosten für IT-Forensik
- Kosten für die Wiederherstellung der Daten
- Kosten der Betriebsunterbrechung
- Lösegeld

Computervirus im Kassensystem einer Baumarktkette:
Ein Hacker hat das Kassensystem einer Baumarktkette mit einem Virus infiziert, welcher einen Prozess initiiert, der automatisch die Kreditkartendaten aus Zahlungsvorgängen an den Hacker sendet. Die Kreditkartendaten vieler Kund*innen werden vom Hacker im Darknet zum Kauf angeboten, woraufhin sich die Betroffenen mit Schadensersatzansprüchen melden. Zudem verlangen verschiedene Kreditkartenanbieter wegen Verstößen gegen PCI-Standards Vertragsstrafen.

Leistungen unter der GGP Cyber-Versicherung:
- Soforthilfe durch die 24/7/365-Cyber-Hotline
- Kosten für IT-Forensik
- Kosten für den Einsatz eines Krisenmanagers

- Haftpflichtansprüche der betroffenen Kund*innen
- PCI-DSS-Vertragsstrafen
- Benachrichtigungskosten und Einrichtung eines Callcenters
- Kosten für die Abwehr eines behördlichen Verfahrens

Hacker-Angriff auf Telefonanlage:
Die Telefonanlage eines versicherten Unternehmens wird von einem Hacker manipuliert. Hierdurch werden, über Tage unentdeckt, Telefonate umgeleitet und zusätzliche Telefonkosten in erheblicher Größenordnung verursacht.

Leistungen unter der GGP Cyber-Versicherung:
- Soforthilfe durch die 24/7/365-Cyber-Hotline
- Kosten für IT-Forensik
- Kosten durch Cyber-Diebstahl

Bedienfehler

Löschung von Steuerungsdaten durch Mitarbeiter:
Das versicherte Unternehmen ist eine Schreinerei, welche für einen großen Möbelhändler diverse Modelle vollautomatisiert produziert. Ein Mitarbeiter des versicherten Unternehmens löscht aus Versehen die Steuerungsdaten der diversen Sägeautomaten. In der Folge kommt es zu einer mehrtägigen Betriebsunterbrechung. Die Steuerungsdaten müssen aus Back-ups neu eingespielt und teilweise neu programmiert werden.

Leistungen unter der GGP Cyber-Versicherung:
- Soforthilfe durch die 24/7/365-Cyber-Hotline
- Kosten für die Wiederherstellung von Daten und Programmen
- Kosten der Betriebsunterbrechung

Dienstleistungsübersicht

Die Gothaer arbeitet im Rahmen der Cyber-Versicherung mit zentralen, spezialisierten Dienstleistungsunternehmen zusammen. Im Bedarfsfall besteht Zugriff auf verschiedene weitere Dienstleistungsunternehmen für Rechts- oder PR-Beratung sowie für das Krisenmanagement.

Bei Zustandekommen der Deckung bietet die Gothaer Allgemeine Versicherung AG eine Cyber-Hotline mit einer 24/7/365-Bereitschaft.

Dienstleistungen	Dienstleister
Risikoermittlung, Risikodialog, Schwachstellenanalyse, Ermittlung/Beratung Präventionsmaßnahmen	**Infraforce GmbH** (Kooperation mit TÜV)
24/7/365-Hotline, Forensik, Schadenermittlung, sicherheitstechnische Dienstleistungen, Wiederherstellung	**Allysca Assistance GmbH** (inkl. Zugriff auf IT-Forensik-Netzwerk)
Präventionsmaßnahmen, Sensibilisierung von MA in Datenschutz und Cybersicherheit	**Network Box Deutschland GmbH**
Ergänzung der Risikoanalyse	**PPI AG Informationstechnologie**
Krisenberatung, Public-Relations-Beratung	**Instinctif Deutschland GmbH**
Datenüberwachungsdienstleistungen	**Schufa Holding AG**
IT-/Cyber-Rechtsberatung, BDSG/DSGVO-Beratung, Benachrichtigungen	**DLA Piper LLP**

Fragen und Antworten

Nachfolgende Fragen entstehen häufig im Zusammenhang mit einer Cyber-Versicherung. Selbstverständlich sind viele weitere individuelle Themenkomplexe denkbar.

Wer ist Versicherungsnehmer?
Wer ist Versicherter?

Versicherungsnehmer ist das im Versicherungsschein genannte Unternehmen.

Versicherter ist der Versicherungsnehmer, seine Tochterunternehmen sowie die mitversicherten Personen. Gemeinsam mit den Tochterunternehmen bildet der Versicherungsnehmer die versicherten Unternehmen.

Welche Betriebsstätten sind vom Versicherungsschutz umfasst?

Es sind alle zum Versicherten gehörenden Betriebsstätten (z. B. Filial-, Neben- und Hilfsbetriebe, Zweigniederlassungen, Lager, Verkaufsstätten, Montagestätten und dergleichen) vom Versicherungsschutz umfasst.

Sind Tochterunternehmen mitversichert?

Ja, Tochterunternehmen gelten als mitversichert, sofern der Versicherungsnehmer direkt oder indirekt beherrschenden Einfluss ausüben kann.

Welche Personen sind vom Versicherungsschutz umfasst?

Mitversicherte Personen sind im Rahmen der Ausübung ihrer beruflichen/dienstlichen Verrichtung:

- Alle gesetzlichen Vertreter sowie solche Personen, die zur Leitung oder Beaufsichtigung eines versicherten Unternehmens angestellt sind
- Alle übrigen angestellten Betriebsangehörigen
- Alle sonstigen in den Betrieb eines versicherten Unternehmens eingegliederten und dessen Weisungsrecht unterliegenden Personen
- Alle aus den Diensten eines versicherten Unternehmens ausgeschiedenen vorgenannten Personen

Welches sind die deckungsauslösenden Tatbestände der Cyber-Versicherung?

Die Cyber-Versicherung bietet Versicherungsschutz im Falle von Datenrechtsverletzungen, IT-Sicherheitsverletzungen oder Hacker-Angriffen.

Wer zahlt den Versicherungsbeitrag?

Der Beitrag wird vom Versicherungsnehmer entrichtet.

Ist in der GGP Cyber-Versicherung eine „Innovationsklausel“ enthalten?

In der GGP Cyber-Versicherung ist keine Innovationsklausel berücksichtigt. Eine Umstellung auf neu erschienene Bedingungswerke ist jedoch möglich.

Besteht Versicherungsschutz für direkte Geldverluste?

Es besteht Versicherungsschutz für unmittelbare Vermögensschäden durch

- Manipulation der Website oder der daran angeschlossenen Datenbanken und Programme eines versicherten Unternehmens (z. B. des Angebotstools, des Web-Shops oder der Kundendatenbank)
- Manipulation des Online-Bankings oder von Online-Zahlungssystemen versicherter Unternehmen
- Diebstahl oder Veränderung von Daten (z. B. Phishing oder Pharming), welche die versicherten Unternehmen zur Teilnahme am Zahlungsverkehr befähigen
- Unberechtigte Nutzung der Telefonanlage versicherter Unternehmen

Sind Fake-President-Fälle (CEO-Fraud oder Business Email Compromise) versichert?

Im Rahmen eines Fake-President-Falles übernimmt die Gothaer Allgemeine Versicherung AG die Kosten für Honorare, Auslagen und Aufwendungen eines qualifizierten Dienstleistungsunternehmens zur Ermittlung der Ursache (Forensik), sofern einer der deckungsauslösenden Tatbestände vorliegt. Aus solch einem Vorfall resultierende direkte Geldabflüsse sind jedoch vom Versicherungsschutz nicht umfasst.

Kann das versicherte Unternehmen im Schadenfall auch eigene IT-Dienstleister beauftragen?

Die Schadenmeldung soll über die von der Gothaer bereitgestellte Cyber-Hotline erfolgen.

Was ist unter der regelmäßigen Sensibilisierung oder Schulung der Mitarbeitenden hinsichtlich IT- und Cyber-Sicherheit zu verstehen?

Überwiegend sehr unterschiedliche Unternehmensstrukturen und -größen machen eine pauschale Aussage über die Häufigkeit der durchzuführenden Sensibilisierungsmaßnahmen nur sehr schwer möglich. Aus diesem Grund ist es für die Cyber-Fachleute wichtig, dass in den zu versichernden Unternehmen geregelte Prozesse zur Durchführung entsprechender Maßnahmen etabliert sind (unabhängig davon, ob die Maßnahmen beispielsweise wöchentlich, monatlich oder quartalsweise durchgeführt werden). Entscheidend ist, dass eine regelmäßige jährliche Sensibilisierung und Schulung der Mitarbeitenden stattfindet.

Welche Mitarbeitenden sollen hinsichtlich Security-Awareness geschult werden?

In erster Linie gilt es, die Personen im Unternehmen zu sensibilisieren, welche täglich das Computersystem der versicherten Unternehmen zur Ausübung ihrer beruflichen Tätigkeit nutzen.

Wie hat ein ausreichend komplexes Passwort auszusehen?

Grundsätzlich ist es wichtig, dass keine Standardeinstellungen verwendet werden und die Werkseinstellungen der Passwörter abgeändert wurden (z. B. nicht oooo oder 1234 verwenden). Idealerweise beinhaltet ein ausreichend komplexes Passwort eine Kombination aus Klein- und Großbuchstaben, Zahlen und Sonderzeichen.

Was ist bei der Erstellung und Aufbewahrung von Back-ups zu beachten?

Bei der Erstellung von Back-ups ist darauf zu achten, dass vollständige Datensicherungen durchgeführt werden, welche den gesamten Datenbestand berücksichtigen. Sehr sinnvoll ist es zudem, diese Datensicherungen täglich, mindestens jedoch wöchentlich durchzuführen und auf Systemen zu speichern, welche außerhalb des Datensicherungsprozesses physisch vom Unternehmensnetzwerk getrennt sind. So wird verhindert, dass etwaige sich im Netzwerk befindende Viren oder Trojaner auch die Back-ups verschlüsseln können.

Was versteht man unter den Begriffen „E-Commerce-Unternehmen“ und „Online-Marktplätze“ im Kontext des Deckungsantrags?

Im Rahmen des Deckungsantrags steht für die Gothaer im Vordergrund, ob die zu versichernden Unternehmen ihren Umsatz ausschließlich über E-Commerce oder Online-Marktplätze erwirtschaften. Werden nur geringe Anteile des Jahresumsatzes als Online-Geschäfte generiert, wird dies noch nicht unter E-Commerce im Sinne des Deckungsantrags verstanden.

Was ist hinsichtlich der Überschneidungen mit anderen Versicherungsprodukten zu beachten?

Dem Cyber-Team der Gothaer ist bewusst, dass es Überschneidungen zu anderen Versicherungsprodukten wie beispielsweise Haftpflicht-, Vertrauensschaden-, Betriebsunterbrechungs- oder technischen Versicherungsprodukten gibt. Da sich der Cyber-Versicherungsmarkt in einem ständigen Wandel befindet, hat sich die Gothaer dafür entschieden, dass ihre Cyber-Versicherungsprodukte im Schadenfall immer den Vorrang vor anderen Versicherungsprodukten erhalten.

Glossar

Antivirenprogramm

Ein Antivirenprogramm muss als Echtzeitscanner aufgesetzt sein und über eine automatische Aktualisierung (Live-Update) der vom Hersteller zur Verfügung gestellten aktuellen Virensignaturen verfügen. Das Antivirenprogramm muss dabei auf allen Endgeräten sowie auf allen Serversystemen eingesetzt werden.

Back-up

Back-up bezeichnet das Kopieren von Dateien und deren Archivierung auf separaten Systemen, um die Wiederherstellung der Originaldaten nach Zerstörung, Beschädigung oder Verlust zu ermöglichen. Bei der Erstellung von Back-ups ist darauf zu achten, dass vollständige Datensicherungen durchgeführt werden, welche den gesamten Datenbestand berücksichtigen. Ein Back-up hat dabei mindestens täglich zu erfolgen. Die Datensicherung muss zudem auf Systemen gespeichert werden, welche außerhalb des Datensicherungsprozesses physisch vom Unternehmensnetzwerk getrennt sind und auf die ohne administrative Rechte nicht zugegriffen werden kann. Dies gilt auch für cloudbasierte Back-up-Lösungen.

Bring-your-own-device (BYOD)

BYOD bedeutet, dass private Endgeräte wie Mobiltelefone, Tablets, Notebooks etc. in das versicherte Unternehmen mitgebracht und dort dienstlich eingesetzt werden dürfen. Problematisch ist BYOD, da unter anderem personenbezogene bzw. vertrauliche Daten auf privaten Geräten gespeichert werden und diese in der Regel nicht über die gleichen Schutzmaßnahmen verfügen wie Unternehmensgeräte.

Chief Information Security Officer (CISO)

CISO bezeichnet die/den Verantwortliche*n für die Informationssicherheit des Unternehmens. Hauptaufgaben sind unter anderem die Sicherstellung des Datenschutzes sowie das Aufstellen von Richtlinien und Zielen für die IT-Sicherheit.

Client

Als Clients werden die einzelnen Arbeitsplatzrechner der Nutzer*innen in einem Unternehmensnetzwerk bezeichnet. Diese ermöglichen den Zugriff auf Server, welche den Nutzern Ressourcen in Form von Anwendungen, Speicherkapazitäten oder Rechenleistungen zur Verfügung stellen.

Cloud-Computing

Cloud-Computing beschreibt die bedarfsorientierte Bereitstellung von IT-Ressourcen wie Server oder Software-Anwendungen zur Datenverarbeitung durch externe Anbieter über das Internet.

Computervirus

Als Computervirus wird ein Schadprogramm bezeichnet, welches sich zum Teil unkontrolliert im Computersystem ausbreitet. Wesentliches Merkmal eines Computervirus ist die Fähigkeit, sich selbstständig über weitere Computersysteme zu vervielfältigen und zu verbreiten. Hierfür verbirgt sich der Computervirus in Dateien, die z. B. über USB-Sticks oder E-Mail-Anhänge weiterverbreitet werden können.

Consumer-Redress-Fund

Unternehmen können infolge einer Datenrechtsverletzung dazu verpflichtet werden, Geldmittel in einem Konsumentenschutzfonds zu hinterlegen. Diese Gelder sollen sicherstellen, dass ausreichend Kapital zur Befriedigung der betroffenen Endverbraucher*innen zur Verfügung steht, wenn diese ihre Ansprüche gegenüber dem Unternehmen geltend machen.

Darknet

Das Darknet ist ein Verbund einer Vielzahl von privaten Computern, welche direkt ohne zentrale zwischengeschaltete Server miteinander verbunden sind (sogenanntes Rechnernetz). Je nach gewähltem Inhalt existieren mehrere dieser Rechnernetze, in welchen eine verschlüsselte Datenübertragung zwischen den Teilnehmer*innen erfolgt. Der Zugang zum Darknet, welches sowohl für legale als auch für illegale Zwecke genutzt werden kann, wird über ein sogenanntes TOR-Programm („The Onion Router“) ermöglicht, welches zugleich über verschiedene Verfahren und Services eine anonyme Kommunikation zwischen Sender*innen und Empfänger*innen sicherstellt.

Denial-of-Service-Attacke (DoS-Attacke)

Eine Denial-of-Service-Attacke hat die Nichtverfügbarkeit eines Computersystems oder eines Webservers aufgrund von unzähligen Anfragen eines Angreifers an den Server, welcher diese Anfragen nicht mehr bewältigen kann, zur Folge.

Eine spezielle Form ist die Distributed-Denial-of-Service (DDoS)-Attacke. Hierbei handelt es sich um den gleichzeitigen und konzentrierten Angriff mittels Zusammenschluss einer Vielzahl einzelner Computer auf Computersysteme oder Webserver, welche die Vielzahl der Anfragen nicht mehr beantworten können.

Einheitliche Schnittstellenkontrolle

Unter einer Schnittstellenkontrolle wird die einheitliche Überwachung und Absicherung der Schnittstellen im Netzwerk verstanden. Ziele sind sowohl die Sicherstellung des Datenschutzes als auch die Abwehr von Angriffen über externe Speichermedien. Einige zu berücksichtigende Punkte sind unter anderem

- Die Kontrolle und Begrenzung hinsichtlich des Einsatzes von Speichermedien (z. B. Speicherkarten, USB-Sticks, DVDs)
- Die Blockierung von unzulässigen Endgeräten und Softwareanwendungen im Netzwerk
- Die automatische Verschlüsselung von Festplatten und mobilen Speichermedien
- Die Etablierung von Vorschriften bezüglich der Dateitypen, die Mitarbeitende auf ein bestimmtes Medium übertragen dürfen

EU-Datenschutz-Grundverordnung (EU-DSGVO)

Die am 25.05.2018 in Kraft getretene EU-DSGVO hat zum Ziel, die Datenschutzrechte in der EU zu harmonisieren und zu stärken, und ist anwendbar bei der Verarbeitung von personenbezogenen Daten im Inland. Als „Grundverordnung“

enthält sie eine Vielzahl von Öffnungsklauseln, die Spielraum für nationales Recht der Mitgliedstaaten schaffen. Im Zuge dessen wurde auch das Bundesdatenschutzgesetz (BDSG-neu) an die neue Verordnung durch Umsetzung der Öffnungsklauseln angepasst.

Goodwill-Coupon

Goodwill-Coupons werden Kund*innen aus Kulanz für entstandene Unannehmlichkeiten zur Verfügung gestellt. Sie beinhalten meist Rabatte bzw. Gutscheine für Dienstleistungen oder Produkte des herausgebenden Unternehmens. Es wird hiermit die Intention verfolgt, Reputationsverluste bei den Kund*innen zu minimieren.

Industrial Control System (ICS)

Der Oberbegriff Industrial Control System (ICS) umfasst verschiedene Arten von Steuerungssystemen in der industriellen Fertigungs- und Prozessautomatisierung. Wesentliche Merkmale sind die Überwachung und Steuerung von physischen Prozessen innerhalb industrieller Anlagen (siehe hierzu auch „SCADA“).

Intrusion-Detection-System (IDS)

Intrusion-Detection-Systeme sind Netzwerkanalyseprogramme, welche auf das Unternehmensnetzwerk gerichtete Angriffe selbstständig erkennen, ohne diese abzuwehren, sondern lediglich den Administrator darüber informieren. Zudem bieten Intrusion-Detection-Systeme den Vorteil, dass sie Angriffe auch dann noch erkennen, wenn die Firewall bereits überwunden wurde.

Intrusion-Prevention-System (IPS)

Intrusion-Prevention-Systeme sind in der Lage, Angriffe auf das Netzwerk zu erkennen und automatisch Gegenmaßnahmen zum Schutz des Netzwerks einzuleiten. Dafür arbeitet das IPS meist direkt mit der Firewall zusammen bzw. ist unmittelbar dahintergeschaltet und analysiert den Datenverkehr in Echtzeit.

IT/OT

IT (Information Technology) umfasst das gesamte Spektrum an Technologien zur Datenverarbeitung, wie Software, Hardware, Kommunikationstechnologien und damit verbundene Services. OT (Operational Technology) ist Hardware und Software, die eine Änderung durch die direkte Überwachung und/oder Kontrolle von physikalischen Geräten (z. B. in der Produktion), Prozessen und Ereignissen im Unternehmen erkennen oder bewirken.

Malware

Malware ist ein Oberbegriff für jegliche Art von Schadsoftware (beispielsweise Computerviren, Trojaner oder Ransomware), die es den Benutzer*innen ermöglicht, unerwünschte oder schädigende Funktionen auszuführen.

Patch

Ein Patch ist eine Softwarekomponente, welche die Korrektur von fehlerhaften Funktionen eines installierten Programms ermöglicht. Ziel ist es lediglich, die fehlerhaften Komponenten auszutauschen. Grundsätzlich lassen sich drei Typen von Patches unterscheiden: Bugfix, Hotfix und Update.

Patch-Management

Als Patch-Management ist eine zentrale Lösung anzusehen, die netzwerkweit und herstellerübergreifend in der Lage ist, die jeweils aktuellen Patches, Updates oder Servicepacks einzuspielen, und einen aktuellen Stand der Software, die in der Organisation oder in dem Unternehmen eingesetzt wird, abrufen lässt, unabhängig davon, ob die Software auf einem Server oder Client läuft.

Payment-Card-Industry-Data-Security-Standard (PCI-DSS)

Der PCI-DSS ist ein weltweit gültiger Sicherheitsstandard von Kreditkartenorganisationen für den Umgang mit Zahlungsdaten und enthält verbindliche Regeln zum Schutz der Kreditkartendaten vor Missbrauch und Diebstahl. Dieser Sicherheitsstandard gilt für alle Unternehmen, die solche Daten verarbeiten oder Kreditkarten akzeptieren.

Penetrationstest

Ein Penetrationstest ist eine Form der Schwachstellenanalyse und dient dem Auffinden von Sicherheitslücken im Unternehmensnetzwerk. Im Fokus steht die Ermittlung von Schnittstellen nach außen, über welche potentielle Angreifer in das Unternehmensnetzwerk eindringen könnten.

Pharming

Pharming ist eine Betrugsmethode, welche auf der Grundidee des Phishings beruht. Bei diesem Verfahren werden Anwender*innen durch eine Systemmanipulation gezielt auf betrügerische Websites umgeleitet. Ziel ist es, an persönliche Informationen wie z. B. Bankdaten zu gelangen.

Phishing

Phishing beschreibt den Versuch, mittels gefälschter E-Mails und/oder Websites Zugangsdaten (Benutzernamen und Passwörter) für bestimmte Dienste oder Websites zu erlangen. In den meisten Fällen handelt es sich um Zugangsdaten für das Online-Banking oder für Online-Shops, welche von den Angreifern im Anschluss missbräuchlich genutzt werden.

Ransomware

Ransomware ist eine Art von Malware, welche oftmals über Phishing-Mails auf das Computersystem von Anwender*innen gelangt. Ziel ist die Verschlüsselung der auf der Festplatte befindlichen Daten oder die Blockierung der Anmeldung am Computersystem. Die Blockierung bzw. Sperrung wird erst gegen Zahlung eines Lösegeldes wieder aufgehoben.

Restore-Test

Im Rahmen eines Restore-Tests wird die vollständige Wiederherstellung des Computersystems aus zuvor erstellten Back-ups getestet. Dieser Test soll Auskunft darüber geben, ob im Falle eines Datenverlustes oder Systemausfalls eine einwandfreie Wiederherstellung des Systems möglich ist.

Security-Audit

Security-Audits dienen der Ermittlung von Schwachstellen im IT-System von Unternehmen. Diese Form der Sicherheitsanalyse umfasst unter anderem einen Schwachstellenscan oder Penetrationstest sowie die Analyse der Zugänge zum Computersystem. Des Weiteren werden im Unternehmen aufgestellte Richtlinien zum Thema IT-Sicherheit und Datenschutz analysiert.

Security Information and Event Management (SIEM)	SIEM-Systeme identifizieren sicherheitsrelevante Ereignisse meist auf Grundlage von Benutzerverhalten und systemrelevanten Sicherheitsmeldungen im Unternehmensnetzwerk (Sammlung von Protokollen, die vom gewohnten Schema abweichende Trends und Muster anzeigen), bewerten diese Meldungen und informieren anschließend den Administrator, welcher diese Meldungen monitoren und ggfs. erforderliche Gegenmaßnahmen einleiten kann. SIEM-Systeme übernehmen somit die Sicherheitsüberwachung im Netzwerk, indem eine ganzheitliche Sicht auf die Sicherheit der IT gelegt wird.
Social Engineering	Im Rahmen von Social Engineering versuchen Angreifer, den Anwender durch Vortäuschung einer persönlichen Beziehung zur Installation von Schadsoftware oder zur Informationsherausgabe zu bewegen.
Software as a Service (SaaS)	Software as a Service stellt einen Teilbereich des Cloud-Computings dar, über den Anwender*innen Zugriff auf bestimmte Programme erhalten. Die Software sowie die zugehörige IT-Infrastruktur werden hierbei nicht mehr bei den Anwender*innen selbst betrieben und installiert, sondern über das Internet als Cloud-Anwendung von einem externen Dienstleister gegen Zahlung eines Nutzungsentgeltes zur Verfügung gestellt.
Supervisory Control and Data Acquisition (SCADA)	Bei Supervisory Control and Data Acquisition handelt es sich um Systeme zur Überwachung und Steuerung von überwiegend automatisiert ablaufenden technischen Prozessen. Diese Systeme werden zum Großteil im Bereich der kritischen Infrastrukturen (beispielsweise Energieerzeugung, Wasserversorgung etc.) eingesetzt (siehe auch „ICS“).
Trojaner	Ein Trojaner ist ein Programm, welches einen bösartigen oder schädlichen Programmcode beinhaltet und nach Installation im Hintergrund verdeckt unerwünschte Funktionen ausführt.
Virtual Private Network (VPN)	Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes (oft des Internets) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In VPNs können unter Zuhilfenahme kryptographischer Verfahren die Integrität und Vertraulichkeit von Daten geschützt und die Kommunikationspartner*innen sicher authentisiert werden, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.
Wurm	Ein Computerwurm ist eine Art von Malware. Dieses sich selbst vervielfältigende Schadprogramm mit eigenständiger Programmroutine hat die Eigenschaft, sich ohne fremde Hilfe weiterzuverbreiten, ohne dabei Dateien oder Bootsektoren zu infizieren.

Gothaer GewerbeProtect Cyber-Versicherung

Informationsbroschüre für Vertriebspartner*innen.

Gothaer

ZUKUNFT WIRD
AUS MUT GEMACHT.

Gothaer Allgemeine Versicherung AG
Gothaer Allee 1
50969 Köln

Telefon 0221 308-00
Telefax 0221 308-103
www.gothaer.de

118264 – 07.2023