Gothaer Cyber-Versicherung für Unternehmen
Informationsbroschüre für Vertriebspartner*innen.

Gothaer
ZUKUNFT WIRD AUS MUT GEMACHT.

24-STUNDEN-CYBER-SOFORTHILFE

CYBER-SCHUTZ DIE HÖCHSTE PRIORITÄT GEBEN.

Das unterstützen wir mit umfassenden Lösungen gegen die zahlreichen Gefahren der digitalen Welt. **Und** sorgen dafür, dass bei einem Cyber-Schaden der Betrieb schnellstmöglich weiterläuft.

Inhaltsverzeichnis

Kontakt

Kontaktdaten

Gothaer Allgemeine Versicherung AG
Komposit Industriekunden
Produktmanagement & Underwriting Cyber

Gothaer Allee 1
50969 Köln

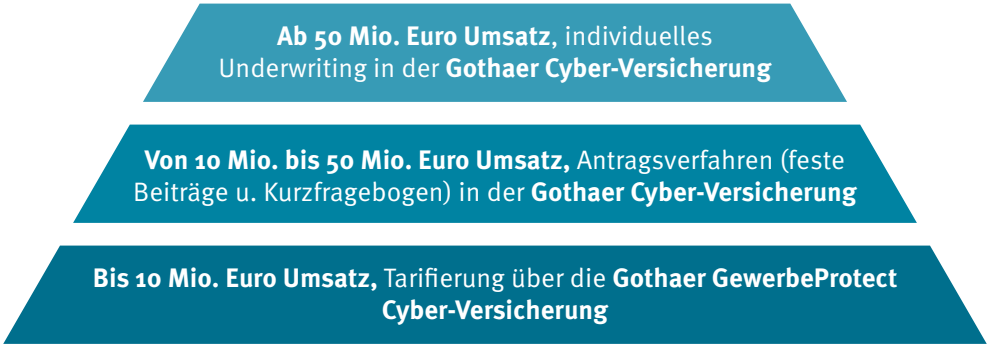
E-Mail: cyber@gothaer.de

Zeichnungskapazitäten

Die Gothaer Allgemeine Versicherung AG zeichnet Cyber-Risiken grundsätzlich auf Basis der jeweils aktuellsten Versicherungsbedingungen für Gewerbekunden bis 10 Mio. Euro Jahresumsatz über die Gothaer GewerbeProtect Cyber-Versicherung sowie für Unternehmen ab einem Jahresumsatz von 10 Mio. Euro über die Gothaer Cyber-Versicherung. In diesem Rahmen zeichnet die Gothaer Grunddeckungen und Exzedenten als Führungs- und Beteiligungsgeschäft.

Nähere Informationen zur Gothaer GewerbeProtect Cyber-Versicherung finden Sie in den separaten Informationen zu diesem Produkt.

Überblick Gothaer Cyber-Versicherungen für Unternehmen



Nachstehende Informationen gelten für Unternehmen ab einem Jahresumsatz von 10 Mio. Euro.

Cyber-Versicherung für Unternehmen ab 10 Mio. Euro Jahresumsatz

Vertragsgrundlage	Deckungssummen bis	Maximierung	Vertragslaufzeit
AVB zur Gothaer Cyber-Versicherung	10.000.000 EUR, im Einzelfall höhere Deckungssummen möglich	• 1-fach p. a.	• 1 Jahr

Zeichnungsfähige Risiken

Die Gothaer Versicherung zeichnet Cyber-Risiken von Firmen, die ihren Sitz in Deutschland oder in Österreich haben. Nahezu alle möglichen Branchen werden hierbei berücksichtigt.
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)

Hier ist eine Zeichnung nur nach eingehender Einzelfallprüfung möglich.

Bei den nachfolgenden Branchen verzichtet die Gothaer derzeit im Cyber-Segment auf die Bereitstellung von Versicherungsschutz:

- 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

Angebotseinholung / Vertragsabschluss

Die Gothaer bietet ein unkompliziertes Antragsverfahren mit festen Beiträgen und Kurzfragebogen für mittlere Unternehmen von 10 Mio. Euro Jahresumsatz bis 50 Mio. Euro Jahresumsatz. Darüber hinaus verfügt die Gothaer über professionelles Underwriting-Know-how zur individuellen Angebotserstellung. Die Prozessabläufe werden nachfolgend beschrieben.

Antragsverfahren (Unternehmen bis maximal 50 Mio. Euro Umsatz – alle Antragsfragen positiv beantwortet)

Benötigte Unterlagen:
Deckungsantrag zur Gothaer Cyber-Versicherung für Unternehmen mit einem Umsatz von EUR 10 Mio. bis EUR 50 Mio.

Weiterer Ablauf:
1) Einreichung des vollständig ausgefüllten sowie rechtsgültig unterzeichneten Deckungsantrages
2) Ergibt die Prüfung des Antrages keine Rückfragen, erstellt die Gothaer unaufgefordert den Versicherungsschein zur Cyber-Versicherung in dem von dem Versicherungsnehmer gewünschten Umfang.

Individuelles Underwriting (Unternehmen ab 50 Mio. Euro Umsatz)

Benötigte Unterlagen:
Fragebogen für Unternehmen zur Gothaer Cyber-Versicherung

Weiterer Ablauf:
1) Prüfung der eingegangenen Unterlagen durch einen Cyber-Underwriter
2) Erstellung eines individuellen Vorschlages zur Gothaer Cyber-Versicherung. Sofern das Risiko es erfordert, wird der zusätzliche Informationsbedarf benannt (Telefoninterview oder Risikodialog).

Kurzbeschreibung Telefoninterview:
Im Rahmen eines Telefoninterviews, welches von einem unserer Dienstleister durchgeführt wird und i. d. R. maximal 45 Minuten dauert, werden offen gebliebene Fragestellungen auf Grundlage der bis dahin vorliegenden Risikoinformationen (z. B. Risikofragebogen) geklärt. Hierfür stellt die Gothaer einen eingerichteten virtuellen Telefonkonferenzraum zur Verfügung. Als stiller Beobachter nimmt i. d. R. der zuständige Underwriter an dem Interview teil. Im Anschluss daran erhält die Fachabteilung eine Auswertung des Interviews und erstellt unter Berücksichtigung der daraus gewonnenen Erkenntnisse und soweit möglich, ein verbindliches Angebot für eine Cyber-Versicherung.

Kurzbeschreibung Risikodialog:
Bei einem Risikodialog besuchen Spezialisten unserer Dienstleister sowie der zuständige Underwriter persönlich das zu versichernde Unternehmen. Neben der Klärung offener Fragestellungen erfolgt zumeist eine Besichtigung der Serverräume oder der IT-Technik. Alternativ kann der Risikodialog auch virtuell z. B. via Teams-Meeting durchgeführt werden. Zusätzlich ist es möglich noch einen Schwachstellenscan am Computersystem des zu versichernden Unternehmens durchzuführen. Im Anschluss daran erhält die Fachabteilung eine Auswertung des Risikodialogs sowie des Schwachstellenscans und erstellt unter Berücksichtigung der daraus gewonnenen Erkenntnisse und soweit möglich, ein verbindliches Angebot für eine Cyber-Versicherung.

Highlights der Bedingungen

Die Gothaer Cyber-Versicherung basiert auf hervorragenden Vertragsbestimmungen und bietet somit ausgezeichneten Versicherungsschutz. Um diese Qualität jederzeit sicherzustellen, verfolgen die Cyber-Experten der Gothaer permanent die Entwicklungen am Versicherungsmarkt.

Gegenstand der Versicherung: Voraussetzung für den Versicherungsfall

Datenrechtsverletzung	IT-Sicherheitsverletzung	Hacker-Angriff
… 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.	… 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.	… 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.

Gothaer Cyber-Versicherung für Unternehmen ab 10 Mio. Euro Umsatz bis 50 Mio. Euro Umsatz

Der nachfolgende Überblick nennt die wichtigsten Highlights der Versicherungsbedingungen:

Produkt:

- Versicherungssumme, Selbstbehalte und Sublimits je nach Umsatz auswählbar
- Weltweiter Versicherungsschutz

Alle Branchen außer

- Finanzinstitute (Banken, Kreditkartenunternehmen, Versicherungen, Finanzdienstleister)
- Krankenkassen
- Online Zahlungsplattformen, E-Commerce Unternehmen, Online-Marktplätze
- Soziale Netzwerke, Dating-Plattformen
- Internet-, Cloud-Service-Provider, Telekommunikationsdienstleister, Rechenzentren
- IT-Dienstleister/Softwareentwicklung
- Ver- und Entsorgungsunternehmen, Verkehrsbetriebe, Stadtwerke, Kommunen, Behörden
- Krankenhäuser, Heime
- Politische Parteien, Verbände, Gewerkschaften
- Auskunfteien, Adress- und Datenhändler
- Medienunternehmen/Film
- Unternehmen der Rüstungsindustrie
- Unternehmen der Luft- und Raumfahrt, Flughäfen
- Bergbau-Unternehmen, Gewinnung von Rohstoffen (Öl, Gas, Kohle, Erze), Fracking
- Raffinerien, Kokereien
- Wettbüros, Lotterien, Online-Spielcasinos
- Anbieter von pornografischen Inhalten, Betrieb von Bordellen

versicherbar.

- Kombinierter Cyber-Schutz bei Drittschäden und Eigenschäden
- Erweiterte Leistungen wie Betriebsunterbrechung durch Cloud-Ausfall, Cyber-Diebstahl, Bedienfehler, Sachschäden am Computersystem, Über- und Unterspannung/elektromagnetische Störung, Geldbußen nach EU-DSGVO und Medienhaftpflicht
- Folgende Deckungsinhalte stehen mit einem Sublimit zur Verfügung:
  – Kosten für Verbesserungsempfehlungen und Verbesserungsmaßnahmen
  – Kosten für Datenüberwachungsdienstleistungen
  – Austausch von Hardware
  – Betriebsunterbrechung durch Cloud-Ausfall

– PCI-DSS Vertragsstrafen
– Vertragsstrafen wegen Verletzung von Datenschutzbestimmungen (sofern vereinbart)
– Vertragsstrafen wegen Nichterfüllung von Liefer- oder Abnahmeverpflichtungen (ab EUR 10 Mio. Umsatz und sofern vereinbart)
– Cyber-Diebstahl und Cyber-Betrug (sofern vereinbart)
– Bedienfehler
– Sachschäden am Computersystem
– Unter- und Überspannung, elektromagnetische Störung
– Geldbußen nach EU-DSGVO
– Sachschäden an Fertigungserzeugnissen
– Cyber-Erpressung
– Alle übrigen Deckungsinhalte stehen in Höhe der ausgewählten Versicherungssumme zur Verfügung.

Prozess:

- Kurzfragebogen mit wenigen einfachen Fragen
- Relevante Beiträge sind direkt ablesbar
- Direkter Versicherungsschutz und umgehende Policierung

Cyber-Schaden-Hotline:

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

Gothaer Cyber-Versicherung für Unternehmen ab EUR 50 Mio. Umsatz

Der nachfolgende Überblick nennt die wichtigsten Highlights dieser Versicherungsbedingungen:

Produkt:

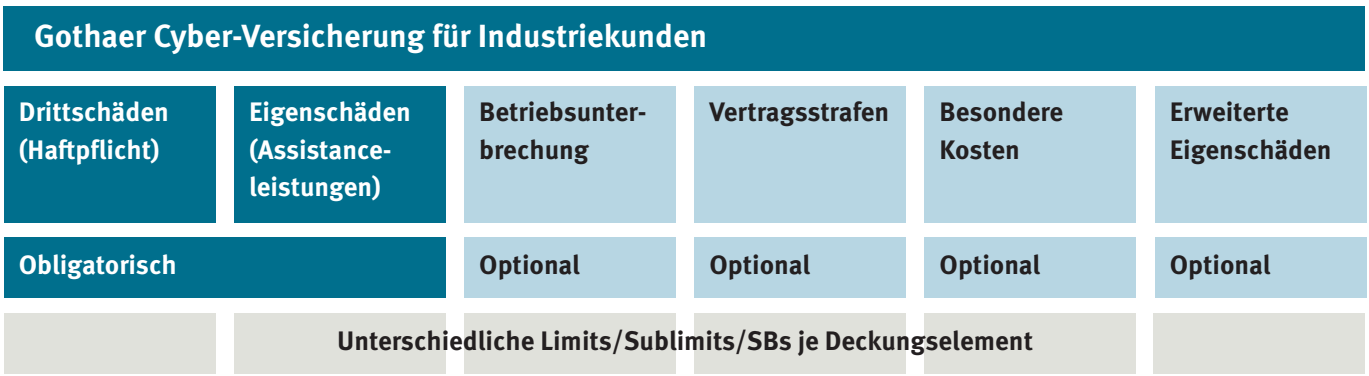
- Modulares Deckungskonzept – Bausteine optional wählbar
- Versicherungssumme, Selbstbehalte und Sublimits variabel
- Weltweiter Versicherungsschutz
- Kombinierter Cyber-Schutz bei Drittschäden und Eigenschäden
- Erweiterte Leistungen wie Betriebsunterbrechung durch Cloud-Ausfall, Cyber-Diebstahl, Bedienfehler, Sachschäden am Computersystem, Über- und Unterspannung/elektromagnetische Störung, Geldbußen nach EU-DSGVO, Sachschäden an Fertigungserzeugnissen und Medienhaftpflicht

Prozess:

Individuelle Risikoprüfung durch den Underwriter.

Cyber-Schaden-Hotline:

- Separate Hotline-Nummer nur für Gothaer Kunden
- 24/7/365-Erreichbarkeit
- Inklusive 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
  - Geldmittel, zu deren Hinterlegung der Versicherte verpflichtet ist, z. B. in einen Consumer-Redress-Fund zur Entschädigung von Ansprüchen von Verbrauchern
- **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 sind 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.
- **Rechtsschutz:**
  Kostenersatz für die außergerichtliche und gerichtliche Abwehr der von einem Dritten geltend gemachten Ansprüche (insbesondere Anwalts-, Sachverständigen-, Zeugen- und Gerichtskosten, soweit den Umständen nach geboten).
- **Einstweiliger Rechtsschutz, Unterlassungs- oder Widerrufsklagen:**
  Kosten eines Verfahrens wegen einer Datenrechtsverletzung oder einer sonstigen Pflichtverletzung (Tun oder Unterlassen) des Versicherten gegen-

über einem Dritten, die eine IT-Sicherheitsverletzung oder einen Hacker-Angriff zur Folge hat, in dem 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.

Eigenschäden/Assistance-Dienstleistungen

- **Kosten für sicherheitstechnische Dienstleistungen:**
  Kosten für die Honorare, Auslagen und Aufwendungen eines qualifizierten Dienstleistungsunternehmens, das zur Erstanalyse, zur 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 die zur Abwehr oder Minderung eines Reputationsschadens entstehen. Hiervon umfasst sind 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 ist
- **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.

Besondere/optionale Deckungserweiterungen

- **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.

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.
- **Nichterfüllung von Liefer- oder Abnahmeverpflichtungen** (nur bei Industriekunden)**:**
  Kosten für die Abwehr unberechtigter und die Freistellung von berechtigten Forderungen zur Zahlung von Vertragsstrafen, die der Versicherte wegen nicht erfüllten eigenen Liefer- oder Abnahmeverpflichtungen aufgrund einer Betriebsunterbrechung in Folge eines Hacker-Angriffs zu leisten hat.
- **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, in Folge einer Datenrechtsverletzung oder eines Hacker-Angriffs.
- **Erweiterte Eigenschäden:**
  Eigenschäden durch mitversicherte Personen:
  - bei Verletzung von Geheimhaltungspflichten bezüglich Daten
  - bei Verletzung von Persönlichkeitsrechten infolge Missbrauch des Computersystems
  - bei Hacker-Angriff durch eine mitversicherte Person

  Cyber-Diebstahl:
  - bei Manipulation der Website oder daran angeschlossener 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 der Versicherten.

  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.

- **Erpressung:**
  Versicherungsschutz für Aufwendungen und Kosten infolge einer Cyber-Erpressung.
- **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

Für die oben aufgeführten Versicherungsinhalte wird kein Anspruch auf Vollständigkeit erhoben, sie dienen ausschließlich Informationszwecken. Als rechtsverbindlich gelten allein die im Einzelfall schriftlich vereinbarten Bedingungen nebst Versicherungsschein.

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
– Patchmanagement
– Datensicherheit und Benutzerkonten
– Notfallmanagement
– Mitarbeiterschulung
– Fernzugriffe

Vertragsverlängerung

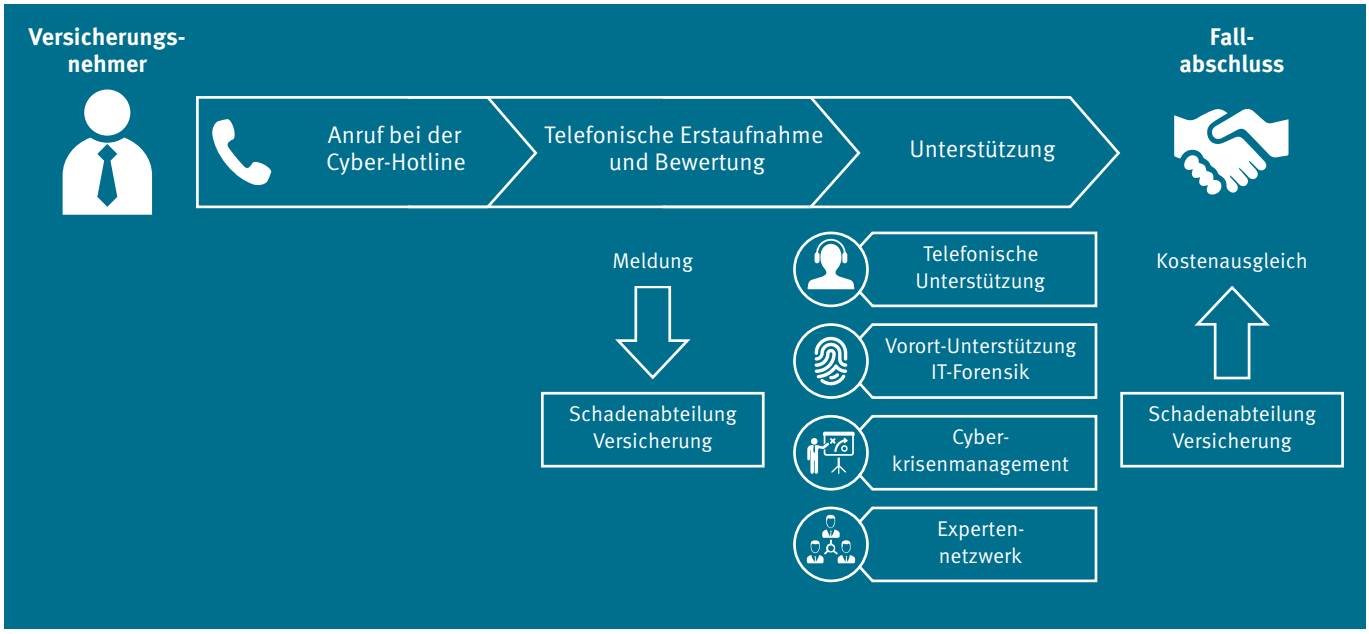
Grundsätzlich beträgt die Vertragslaufzeit 12 Monate.

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 Schadensbeispiele 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 IT-Systemhauses. Ziel sind die Arbeitsplätze der Administratoren, welche die Kundensysteme (Netzwerke, Server) überwachen und administrieren. Der Angriff richtet keinen erkennbaren Schaden an der IT-Umgebung an, jedoch werden in großem Umfang Kundendaten gestohlen. Diese Daten werden anschließend im Darknet zum Verkauf angeboten, woraufhin die betroffenen Kunden Schadensersatzansprüche gegenüber dem IT-Systemhaus anmelden.

Leistungen unter der Gothaer 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 Kunden

Datenabgriff bei Lebensmittelproduzenten mit Kundenclub:
Es erfolgt ein Angriff über eine nicht geschlossenen 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 Gothaer 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-Sicherheitsverletzung

DDoS-Attacke auf Versandhaus:
Das Computersystem eines versicherten Unternehmens wird von einem Dritten zum Angriff auf ein Online-Versandhaus mittels einer Distributed-Denial-of-Service-Attacke benutzt. Dadurch kommt es bei dem Online-Versandhaus zu einer mehrstündigen Betriebsunterbrechung, da die Internetseite nicht mehr erreichbar ist. Das Versandhaus macht Schadensersatzansprüche gegenüber dem versicherten Unternehmen geltend.

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

Hacker-Angriff

Computer-Virus 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 Gothaer Cyber-Versicherung:
- Soforthilfe durch die 24/7/365-Cyber-Hotline
- Kosten für IT-Forensik
- Kosten für die Wiederherstellung der Daten
- Kosten der Betriebsunterbrechung
- Lösegeld

Computer-Virus 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 Kunden werden vom Hacker im Darknet zum Kauf angeboten, woraufhin sich betroffene Kunden mit Schadensersatzansprüchen melden. Zudem verlangen verschiedene Kreditkartenanbieter wegen Verstößen gegen PCI-Standards Vertragsstrafen.

Leistungen unter der Gothaer Cyber-Versicherung:
- Soforthilfe durch die 24/7/365-Cyber-Hotline
- Kosten für IT-Forensik
- Kosten für den Einsatz eines Krisenmanagers
- Haftpflichtansprüche der betroffenen Kunden
- 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 Gothaer 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 Gothaer 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 über eine separate, nur für Gothaer Kunden bestehende Cyber-Hotline-Nummer. Diese Hotline-Nummer wird bei Vertragsabschluss zur Verfügung gestellt.

Dienstleistungen

- Risikoermittlung, Risikodialog, Schwachstellenanalyse, Ermittlung/Beratung Präventionsmaßnahmen
- 24/7/365-Hotline, Forensik, Schadenermittlung, sicherheitstechnische Dienstleistungen, Wiederherstellung
- Präventionsmaßnahmen, Sensibilisierung von MA in Datenschutz und Cybersicherheit
- Ergänzung der Risikoanalyse
- Krisenberatung, Public-Relations-Beratung
- Datenüberwachungsdienstleistungen
- IT-/Cyber-Rechtsberatung, BDSG/DSGVO – Beratung, Benachrichtigungen

Fragen und Antworten

Nachfolgende Fragen entstehen häufig im Zusammenhang mit einer Cyber-Versicherung. Selbstverständlich sind viele weitere individuelle Themenkomplexe denkbar. Die Antworten auf individuelle Fragen erhalten Sie von den Cyber-Experten der Gothaer.

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.

Wie kann ich ein Angebot zur Gothaer Cyber-Versicherung erhalten?

Die Gothaer Cyber-Versicherung für Gewerbekunden sowie für Unternehmen bis EUR 50 Mio. Umsatz ist direkt über das Antragsmodell ohne vorherige Angebotserstellung abschließbar. Im Industriesegment über 50 Mio. Euro Jahresumsatz erfolgt eine Angebotserstellung nach Bewertung des Risikos im Rahmen des individuellen Underwritings.

Wie wird der Versicherungsbeitrag errechnet?

Im vereinfachten Antragsverfahren stehen im Rahmen eines Beitragstableaus festgelegte Versicherungssummen mit festen Versicherungsbeiträgen zur Auswahl.

Im individuellen Underwriting wird der Versicherungsbeitrag im Rahmen der Risikoprüfung durch die Cyber-Experten der Gothaer einzelfallabhängig ermittelt. Die Höhe des Beitrags bemisst sich dabei unter anderem an der Größe und Internationalität des Unternehmens, der Branche sowie an den im Unternehmen etablierten organisatorischen und technischen IT-Sicherheitsmechanismen/-standards.

Wer zahlt den Versicherungsbeitrag?

Der Beitrag wird vom Versicherungsnehmer entrichtet.

Ist in der Gothaer Cyber-Versicherung eine „Innovationsklausel" enthalten?

In den gegenwärtig relevanten Produkten der Gothaer ist eine Innovationsklausel derzeit nicht berücksichtigt. Eine Umstellung auf neu erschienene Bedingungswerke ist jedoch möglich.

Besteht Versicherungsschutz für direkte Geldverluste?

Es besteht Versicherungsschutz für unmittelbare Vermögensschäden durch

- eine Manipulation der Website oder daran angeschlossener Datenbanken und Programme eines versicherten Unternehmens (z. B. des Angebotstools, des Web-Shops oder der Kundendatenbank)
- eine 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
- eine 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?

Nach vorheriger Abstimmung mit der Fachabteilung besteht für größere Unternehmen und Industriekonzerne im Schadenfall die Möglichkeit, auch auf eigene IT-Dienstleister zurückzugreifen.

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

Was ist unter der regelmäßigen Sensibilisierung oder Schulung der Mitarbeiter 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-Spezialisten 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). Die genaue Ausgestaltung und der Umfang bleiben an dieser Stelle unberücksichtigt.

Welche Mitarbeiter 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 0000 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 befindliche 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 zu 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 Daten bestand 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. Diese gilt auch für cloud basierte 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 Daten 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 den Verantwortlichen 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 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.

Computer-Virus

Computer-Virus bezeichnet ein Schadprogramm, welches sich zum Teil unkontrolliert im Computersystem ausbreitet. Wesentliches Merkmal eines Computer-Virus ist die Fähigkeit, sich selbstständig über weitere Computersysteme zu vervielfältigen und zu verbreiten. Hierfür verbirgt sich der Computer-Virus 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 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 (sog. Rechnernetz). Je nach gewähltem Inhalt existieren mehrere dieser Rechnernetze, in welchen eine verschlüsselte Datenübertragung zwischen den Teilnehmern 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 und Empfänger 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 Ab-sicherung der Schnittstellen im Netzwerk verstanden. Ziel ist 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 Mitarbeiter auf ein bestimmtes Medium übertragen dürfen

EU-Datenschutzgrundverordnung (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 den Kunden 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 Kunden 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 Computer-Viren, Trojaner oder Ransomware), die es dem Benutzer 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 potenzielle Angreifer in das Unternehmensnetzwerk eindringen könnten.

Pharming

Pharming ist eine Betrugsmethode, welche auf der Grundidee des Phishings beruht. Bei diesem Verfahren wird der Anwender 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 des Anwenders 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 Zugriff auf bestimmte Programme erhalten. Die Software sowie die zugehörige IT-Infrastruktur werden hierbei nicht mehr beim Anwender 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 Internet) 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 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 Cyber-Versicherung für Unternehmen

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

117230 – 07.2023