

# Informationsmappe

## **Gothaer Cyber-Versicherung**

für den Multikanalvertrieb der Gothaer Allgemeine Versicherung AG

Stand: Oktober 2018

## Inhaltsverzeichnis

	Das Cyber-Team	3
	Zeichnungskapazitäten	4
	Angebotseinholung / Vertragsabschluss	5
	Entscheidungshilfe zur Ermittlung einer Versicherungssumme für kleinere und mittlere Unternehmen bis EUR 10 Mio. Umsatz	6
	Highlights der Bedingungen	8
	Vertragsverlängerung	14
	Schadenbeispiele	14
	Dienstleisterübersicht	17
	Fragen & Antworten	18
	Glossar	21
	Die Gothaer als starker Partner	26

Die Gothaer Allgemeine Versicherung AG verfügt über ein erfahrenes Team an Cyber-Experten. Dieses Team hat seinen zentralen Sitz in Köln.

**Leitung**

<b>Frank Huy</b> Dipl. Betriebswirt	Leitung Produktmanagement Haftpflicht/Financial Lines/Gruppenunfall
Telefon 0221 308-33384 E-Mail frank_huy@gothaer.de	

**Underwriting/  
Produktmanagement**

<b>Udo G. Wegerhoff</b> Dipl.-Ing.	Produktmanagement & Underwriting Cyber
Telefon 0221 308-31307 E-Mail udo_wegerhoff@gothaer.de	

<b>Oliver Schulze, LL.M.</b> Rechtsanwalt	Produktmanagement & Underwriting Cyber
Telefon 0221 308-31266 E-Mail oliver_schulze@gothaer.de	

<b>Vanessa Bittner</b> M.Sc. (Versicherungswesen)	Underwriting Cyber
Telefon 0221 308-31836 E-Mail vanessa_bittner@gothaer.de	

<b>Tobias Treutlein</b> M.Sc. (Wirtschaftswissenschaften)	Underwriting Cyber
Telefon 0221 308-31818 E-Mail tobias_treutlein@gothaer.de	

**Besuchs- und  
Postanschrift**

Gothaer Allgemeine Versicherung AG  
Komposit Industriekunden  
Produktmanagement  
Gothaer Allee 1  
50969 Köln

## Zeichnungskapazitäten

Die Gothaer Allgemeine Versicherung AG zeichnet Cyber-Risiken grundsätzlich auf Basis der jeweils aktuellsten Versicherungsbedingungen zur Gothaer Cyber-Versicherung für Gewerbekunden (inkl. Zielgruppenkonzepte) sowie Industriekunden. In diesem Rahmen zeichnet die Gothaer Grunddeckungen und Exzedenten als Führungs- und Beteiligungsgeschäft.

### Cyber-Versicherung für Gewerbekunden inkl. Zielgruppenkonzepte (bis EUR 10 Mio. Jahresumsatz)

Vertragsgrundlage	Deckungssummen bis	Maximierung	Vertragslaufzeit
AVB zur Gothaer Cyber-Versicherung für Gewerbekunden/ Zielgruppenkonzepte (Stand 10.2018)	2.500.000 EUR	• 1-fach p.a.	• 1 Jahr

### Cyber-Versicherung für Industriekunden (ab EUR 10 Mio. Jahresumsatz)

Vertragsgrundlage	Deckungssummen bis	Maximierung	Vertragslaufzeit
AVB zur Gothaer Cyber-Versicherung (Stand 10.2018)	10.000.000 EUR im Einzelfall höhere Deckungssummen möglich	• 1-fach p.a.	• 1 Jahr

### Zeichnungsfähige Risiken

Die Gothaer Versicherung zeichnet Cyber-Risiken, 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

Hier ist eine Zeichnung nicht möglich.



## Angebotseinholung / Vertragsabschluss

Die Absicherung über eine Gothaer Cyber-Versicherung erhalten Sie grundsätzlich über eine individuelle Angebotserstellung durch einen unserer Cyber-Underwriter. Kleine und mittlere Unternehmen (KMU) können unter den benannten Voraussetzungen hiervon abweichend per Antragsverfahren eine Cyber-Versicherung erhalten. Beide Prozessabläufe skizzieren wir nachfolgend:

### Antragsverfahren (Gewerbe und Zielgruppenkonzepte)

- !** Geeignet für alle Unternehmen,
- deren (konsolidierter) Umsatz max. EUR 10 Mio. beträgt und
  - die alle Fragen des Antrages entsprechend der gekennzeichneten Vorgaben positiv beantworten können.

#### Benötigte Unterlagen:

Deckungsantrag zur Gothaer Cyber-Versicherung für Gewerbekunden

#### 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 der Versicherungsnehmerin gewünschten Umfang.

### Individuelles Underwriting (Unternehmen ab EUR 10 Mio. 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 unserem Dienstleister Infraforce GmbH durchgeführt wird und i. d. R. maximal 45 Minuten dauert, werden offene gebliebene Fragestellungen auf Grundlage der bis dahin vorliegenden Risikoinformationen (z. B. Risikofragebogen) geklärt. Hierfür stellt die Gothaer einen eingerichteten virtuellen Telefonkonferenzraum zur Verfügung. Als stille Beobachter nehmen i. d. R. ein Mitarbeiter der Gothaer Risk Management GmbH sowie der zuständige Underwriter an dem Interview teil. Im Anschluss erhält die Fachabteilung eine Auswertung des Interviews und erstellt unter Berücksichtigung der daraus gewonnenen Erkenntnisse ein verbindliches Angebot für eine Cyber-Versicherung.

#### Kurzbeschreibung Risikodialog

Bei einem Risikodialog besuchen Spezialisten der Infraforce GmbH sowie der zuständige Underwriter persönlich das zu versichernde Unternehmen. Neben der Klärung offener Fragestellungen erfolgt zumeist eine Besichtigung der Serverräume oder IT-Technik. Zusätzlich kann die Infraforce GmbH noch einen Schwachstellen-scan am Computersystem des zu versichernden Unternehmens durchführen. Im Anschluss erhält die Fachabteilung eine Auswertung des Risikodialogs sowie des Schwachstellenscans und erstellt unter Berücksichtigung der daraus gewonnenen Erkenntnisse ein verbindliches Angebot für eine Cyber-Versicherung.



## Entscheidungshilfe zur Ermittlung einer Versicherungssumme für kleinere und mittlere Unternehmen bis EUR 10 Mio. Umsatz

Die Ermittlung einer ausreichenden Cyber-Versicherungssumme gestaltet sich für die meisten Unternehmen in der Regel schwierig, da nur schwer vorherzusehen ist, welche versicherten Positionen im Versicherungsfall beim Versicherungsnehmer tatsächlich entstehen. Das nachfolgend beschriebene Vorgehen soll hierzu eine Unterstützung bzw. Entscheidungshilfe zur Ermittlung einer passenden Cyber-Versicherungssumme geben, die mindestens gewählt werden sollte.

### **Parameter Betriebsunterbrechung**

Im Cyber-Gewerbeprodukt der Gothaer ist im Betriebsunterbrechungsbaustein eine Haftzeit von drei Monaten festgelegt. Diese Haftzeit von 3 Monaten bestimmt somit den maximalen Zeitraum für einen möglichen versicherten Gewinnausfall sowie für die versicherten Kosten aus einer Betriebsunterbrechung.

Als Berechnungsbasis kann nun der Gewinn aus dem Vorjahr (mindestens aber 2 % vom Umsatz) herangezogen werden und von zwölf auf drei Monate heruntergerechnet werden (3/12 Jahr entsprechen 25 % eines Jahres). Hieraus ergibt sich eine Größenordnung von 25 % des Jahresgewinns zuzüglich eines Kostenzuschlags für die versicherten Kosten. Der genannte Kostenzuschlag kann bei diesem vereinfachten Verfahren nur als pauschale Annahme mit einfließen (z. B. mit einem Wert von 0,5 % bis 3 % des Jahresumsatzes). Insgesamt sollte jedoch eine Größenordnung von EUR 50.000 nicht unterschritten werden.

### **Parameter Anzahl personenbezogene Datensätze**

Als mögliche weitere relevante Größenordnung kann die Anzahl der personenbezogenen Datensätze, die vom Unternehmen gespeichert oder „verwendet“ werden, herangezogen werden. Die Gesamtkosten (Benachrichtigungskosten etc.) im Falle einer Datenrechtsverletzung können sich nach derzeitigen Erkenntnissen durchaus auf zwischen EUR 50,- und EUR 150,- je personenbezogenen Datensatz belaufen.

### **Parameter Dienstleisterkosten**

Als mögliche Größenordnung für die Dienstleisterkosten, die in einem Schadenfall entstehen können, ist – je nach Branche oder Ausrichtung des Unternehmens – von sehr unterschiedlichen Beträgen auszugehen. Dies ist auch hier der Fall, da von sehr unterschiedlichen Szenarien und Einsatzbereichen sowie Einsatzzeiten der Dienstleister ausgegangen werden muss. Für den Gewerbebereich sollte je nach Risikoeinschätzung eine Mindestgrößenordnung von EUR 50.000,- bis EUR 250.000,- angesetzt werden.

### **Parameter Drittschäden**

Insbesondere für den Parameter Drittschäden ist eine angemessene Größenordnung für die Versicherungssumme sehr schwer abzuschätzen. Unter anderem vor dem Hintergrund der seit Mai 2018 in Kraft befindlichen EU-Datenschutzgrundverordnung ist es zum derzeitigen Zeitpunkt ungewiss, in welchen Höhen sich zukünftige Schadenersatzansprüche bewegen werden. Für diesen

Deckungsbaustein sollte zumindest eine sich am Umsatz und der Ausrichtung des Unternehmens orientierende entsprechende Größenordnung, beispielsweise 10 % vom Umsatz, zusätzlich berücksichtigt werden.

### Beispiele zur Ermittlung einer Mindest-Versicherungssumme

Beispiel 1:			
Branche:	Metall- und Werkzeugbau		
Umsatz:	EUR 7,0 Mio.		
Gewinn Vorjahr:	EUR 150.000		
Personenbezogene Datensätze:	750		
<b>Ermittlung Mindest-VS:</b>			
Betriebsunterbrechungsanteil:	25 % vom Jahresgewinn	→	EUR 37.500,-
	1,5 % vom Jahresumsatz	→	EUR 105.000,-
Personenbezogene Datensätze:	750 DS mit EUR 120,-/DS	→	EUR 90.000,-
Dienstleisterkosten Anteil:	Kleineres Risikopotential	→	EUR 80.000,-
Drittschadenanteil:	10% vom Jahresumsatz	→	EUR 700.000,-
Summe:		→	EUR 1.012.500,-
<b>Vorschlag für eine Mindest-Versicherungssumme:</b>			→ EUR 1.500.000,-

Beispiel 2:			
Branche:	Immobilienmakler		
Umsatz:	EUR 1,5 Mio.		
Gewinn Vorjahr:	EUR 200.000		
Personenbezogene Datensätze:	4.500		
<b>Ermittlung Mindest-VS:</b>			
Betriebsunterbrechungsanteil:	25 % vom Jahresgewinn	→	EUR 50.000,-
	2 % vom Jahresumsatz	→	EUR 30.000,-
Personenbezogene Datensätze:	4.500 DS mit EUR 120,-/DS	→	EUR 540.000,-
Dienstleisterkosten Anteil:	Kleineres Risikopotential	→	EUR 70.000,-
Drittschadenanteil:	10 % vom Jahresumsatz	→	EUR 150.000,-
Summe:		→	EUR 840.000,-
<b>Vorschlag für eine Mindest-Versicherungssumme:</b>			→ EUR 1.000.000,-

Die Zusammenstellung möglicher Parameter zur Ermittlung einer passenden Versicherungssumme wurde von der Gothaer Allgemeine Versicherung AG mit größtmöglicher Sorgfalt erstellt. Die Gothaer Allgemeine Versicherung AG übernimmt keinerlei Haftung etc. für Fälle, in denen eine auf dieser Basis gewählte Versicherungssumme in einem Schadenszenario nicht ausreichend ist.

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

... 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 (zum Beispiel 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 Gewebekunden und Zielgruppenkonzepte

Der nachfolgende Überblick nennt die wichtigsten Highlights der Versicherungsbedingungen:

#### Produkt

- Versicherungssumme, Selbstbehalte und Sublimits je nach Umsatz auswählbar
- Weltweiter Versicherungsschutz
- Alle Branchen (außer Banken, Versicherungen, Kreditkartenunternehmen, Online Plattformen/Marktplätze, Rechenzentren, Telekommunikation-DL, Cloud-Service-Provider, Krankenhäuser, Krankenkassen, Auskunfteien, Datenhändler) versicherbar
- Kombiniertes 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
- Alle Deckungsinhalte sind immer pauschal mitversichert
- Folgende Deckungsinhalte stehen mit einem Sublimit zur Verfügung:
  - Cyber-Diebstahl (Basiswert mit Erhöhungsoption)
  - Bedienfehler (Basiswert mit Erhöhungsoption)
  - Unter- und Überspannung, elektromagnetische Störung (Basiswert mit Erhöhungsoption)
  - Geldbußen nach EU-DSGVO (Basiswert mit Erhöhungsoption)
  - Erpressungsgelder (Basiswert mit Erhöhungsoption)
  - Betriebsunterbrechung durch Cloud-Ausfall (Basiswert mit Erhöhungsoption)
  - Kosten für Datenüberwachungsdienstleistungen (10 % der VS)
  - PCI-DSS-Vertragsstrafen (10 % der VS)
  - Sachschäden am Computersystem (fester Wert)
  - 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.

**Für verkammerte Berufe: 10% Nachlass bei vorhandener Gothaer-VSH-Police.  
Die Pflichtversicherung der Vermögensschadenhaftpflicht bleibt erhalten.**

### Gothaer Cyber-Versicherung für Industriekunden

Der nachfolgende Überblick nennt die wichtigsten Highlights dieser Versicherungsbedingungen:

#### Produkt

- Modulares Deckungskonzept – Bausteine optional wählbar
- Versicherungssumme, Selbstbehalte und Sublimits variabel
- Weltweiter Versicherungsschutz
- Kombiniertes 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.

Gothaer Cyber-Versicherung für Industriekunden					
Drittschäden (Haftpflicht)	Eigenschaden (Assistanceleistungen)	Betriebsunterbrechung	Vertragsstrafe	Erpressung	Erweiterte Eigenschäden
obligatorisch		optional	optional	optional	optional
Unterschiedliche Deckungsauslöser/Trigger je Deckungselement					
Unterschiedliche Limits/Sublimits/SB's je Deckungselement					

#### 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.

Im Folgenden werden die wesentlichen Versicherungselemente im Überblick dargestellt:

### **Drittschäden (Haftpflichtversicherung)**

- **Haftpflichtversicherung:**

- Prüfung der Haftpflichtfrage
- Abwehr unberechtigter Schadenersatzansprüche
- Freistellung des Versicherten von berechtigten Schadenersatzansprüchen
- Geldmittel, zu deren Hinterlegung der Versicherte verpflichtet ist, zum Beispiel in einen Consumer-Redress-Fund zur Entschädigung von Ansprüchen von Verbrauchern

- **Versicherungsschutz für behördl. Verfahren wegen Datenrechtsverletzungen:**

Kosten, die dem Versicherten durch die Abwehr von gegen ihn wegen einer Datenrechtsverletzung eingeleiteter Straf-, Ordnungswidrigkeits- oder sonstiger behördlicher Verfahren 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, sofern hieraus eine Freistellungsverpflichtung des Versicherten gegenüber diesem Unternehmen besteht.

- **Rechtsschutz:**

Kostenersatz für die außergerichtliche und gerichtliche Abwehr der von einem Dritten geltend gemachten Ansprüche (insb. 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 ggü. 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:**

... 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.

- **Kosten im Zusammenhang mit Benachrichtigungspflichten:**

... für notwendige und angemessene Kosten, die dadurch entstehen, dass der Versicherte aufgrund einer Datenrechtsverletzung gesetzliche oder behördliche Benachrichtigungspflichten erfüllen muss.

- **Kosten für Kommunikations- und Public-Relations-Maßnahmen:**

... für notwendige und angemessene Kosten für Kommunikations- und Public-Relations-Maßnahmen des Versicherten, ... 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 der Betroffenen zu überprüfen.

- **Kosten der Wiederherstellung von Daten und Programmen:**

... im Falle eines Hacker-Angriffs auf das Computersystem des Versicherten ... zur Feststellung,

- ob Daten und Programme, wiederhergestellt, erneut erfasst oder neu erhoben werden können,
- zur Entfernung von Schadsoftware und
- zur Wiederherstellung des früheren, betriebsbereiten Zustandes der Daten und Programme ...

- **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. Auch mitversichert ist die Betriebsunterbrechung bei der VN durch einen Ausfall der Cloud-Services oder der Computersysteme eines namentlich benannten Dienstleisters.

- **PCI-DSS-Vertragsstrafen:**

... für die Abwehr unberechtigter und die Freistellung von berechtigten Forderungen zur Zahlung von Vertragsstrafen, die von einem der im PCI Security Standards Council zusammengeschlossenen 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
- Verletzung von Persönlichkeitsrechten infolge Missbrauch des Computersystems
- Hacker-Angriff durch eine mitversicherte Person

**Cyber-Diebstahl:**

- bei Manipulation der Webseite oder daran angeschlossener Datenbanken und Programme
- bei Manipulation des Online Bankings oder von Online-Zahlungssystemen versicherter Unternehmen
- Diebstahl oder Veränderung von Daten, welche zur Teilnahme am Zahlungsverkehr befähigen
- Unberechtigte Nutzung der Telefonanlage

**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.

- **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:** 12 Monate

- **Nachmeldefrist:** 24 Monate

Die oben aufgeführten Versicherungsinhalte erheben keinen Anspruch auf Vollständigkeit und dienen ausschließlich Informationszwecken. Als rechtsverbindlich gelten allein die im Einzelfall schriftlich vereinbarten Bedingungen nebst Versicherungsschein.



## Vertragsverlängerung

Grundsätzlich beträgt die Vertragslaufzeit 12 Monate.

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



## 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 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 Schadenersatzansprüche gegenüber dem IT-Systemhaus melden.

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 mittels einer 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 Schadenersatzansprüche 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
- 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 Schadenersatzansprüchen 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 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
- Betriebsunterbrechung



## Dienstleisterübersicht

Die Gothaer arbeitet im Rahmen der Cyber-Versicherung mit zentralen, spezialisierten Dienstleistungsunternehmen (z. B. Infraforce GmbH) zusammen. Im Bedarfsfalle 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.

		Dienstleister (Auszug)
	Risikoermittlung, Risikodialog, Schwachstellenanalyse Ermittlung/Beratung Präventionsmaßnahmen	Infraforce GmbH (mit Kooperationspartner TÜV)
	24/7/365 Hotline, Forensik, Schadenermittlung, Sicherheitstechnische Dienstleistungen, Wiederherstellung	
	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 & Antworten

Nachfolgende Fragen und Antworten 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, die 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 direkten oder indirekten 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.

### **Was 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 (inkl. Zielgruppenkonzepte) ist direkt über das Antragsmodell ohne vorherige Angebotserstellung abschließbar. Im Industriesegment über EUR 10 Mio. Jahresumsatz erfolgt eine Angebotserstellung nach Bewertung des Risikos im Rahmen des individuellen Underwriting.

### **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 u. a. an der Größe und Internationalität des Unternehmens, der Branche sowie 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 Bedingungenwerke ist jedoch möglich.

**Besteht Versicherungsschutz für direkte Geldverluste?**

Es besteht Versicherungsschutz für unmittelbare Vermögensschäden durch

- eine Manipulation der Webseite 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 (CEO-Fraud oder Business Email Compromise) Fälle 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 bspw. wöchentlich, monatlich oder quartalsweise durchgeführt werden). Genaue Ausgestaltung und 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-Marktplätzen“ 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 über 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.



<b>Backup</b>	Backup bezeichnet das Kopieren von Dateien und deren Archivierung auf separaten Systemen, um die Wiederherstellung der Originaldaten nach Zerstörung, Beschädigung oder Verlust zu ermöglichen.
<b>Bring-your-own-device (BYOD)</b>	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 u. a. personenbezogene Daten bzw. vertrauliche Daten auf privaten Geräten gespeichert werden und diese in der Regel nicht über die gleichen Schutzmaßnahmen verfügen wie Unternehmensgeräte.
<b>Chief Information Security Officer (CISO)</b>	CISO bezeichnet den Verantwortlichen für die Informationssicherheit des Unternehmens. Hauptaufgaben sind u. a. die Sicherstellung des Datenschutzes sowie das Aufstellen von Richtlinien und Zielen für die IT-Sicherheit.
<b>Client</b>	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.
<b>Cloud-Computing</b>	Cloud-Computing beschreibt die bedarfsorientierte Bereitstellung von IT-Ressourcen wie Server oder Software-Anwendungen zur Datenverarbeitung durch externe Anbieter über das Internet.
<b>Computer-Virus</b>	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 weiter zu verbreiten. Hierfür verbirgt sich der Computer-Virus in Dateien die z. B. über USB-Sticks oder E-Mail-Anhänge weiter verbreitet werden können.
<b>Consumer-Redress-Fund</b>	Unternehmen können in Folge 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 Zwecke als auch illegale Anwendungsgebiete 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 Webserver 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 verbundenen Angriff durch 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. Ziel ist sowohl die Sicherstellung des Datenschutzes als auch die Abwehr von Angriffen über externe Speichermedien. Einige zu berücksichtigende Punkte sind u. a.

- 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 gleichen Zuge wurde auch das Bundesdatenschutzgesetz (BDSG-neu) an die neue Verordnung durch Umsetzung der Öffnungsklauseln angepasst.

## **Firewall**

Eine Firewall ist ein Sicherungssystem (Soft- und/oder Hardware), welches ein lokales Netzwerk gegen unberechtigte Verbindungsversuche aus dem Internet schützt.

<b>Goodwill-Coupons</b>	Goodwill-Coupons werden den Kunden aus Kulanz für entstandene Unannehmlichkeiten zur Verfügung gestellt. Diese beinhalten meist Rabatte bzw. Gutscheine für Dienstleistungen oder Produkte des herausgebenden Unternehmens. Es wird hiermit die Intention verfolgt, Reputationsverluste bei den Kunden zu minimieren.
<b>Industrial Control System (ICS)</b>	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‘).
<b>Intrusion Detection System (IDS)</b>	Intrusion Detection Systeme sind Netzwerkanalyseprogramme, welche selbstständig auf das Unternehmensnetzwerk gerichtete Angriffe 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.
<b>Intrusion Prevention System (IPS):</b>	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 direkt dahinter geschaltet und analysiert den Datenverkehr in Echtzeit.
<b>Malware</b>	Malware ist ein Oberbegriff für jegliche Arten von Schadsoftware (beispielsweise Computer-Viren, Trojaner oder Ransomware), die es dem Benutzer ermöglichen unerwünschte oder schädigende Funktionen auszuführen.
<b>Patch</b>	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 oder Update.
<b>Payment Card Industry – Data Security Standard (PCI-DSS)</b>	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.
<b>Penetrationstest</b>	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.
<b>Pharming</b>	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.

<b>Phishing</b>	Phishing beschreibt den Versuch, mittels gefälschter Emails und/oder Webseiten Zugangsdaten (Benutzernamen und Passwörter) für bestimmte Dienste oder Webseiten zu erlangen. In den meisten Fällen handelt es sich um Zugangsdaten für Online-Banking oder Online-Shops, welche von den Angreifern im Anschluss missbräuchlich genutzt werden.
<b>Ransomware</b>	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 Blockierung der Anmeldung am Computersystem. Die Blockierung bzw. Sperrung wird erst gegen Zahlung eines entsprechenden Lösegeldes wieder aufgehoben.
<b>Restore-Tests</b>	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.
<b>Security-Audits</b>	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 auch im Unternehmen aufgestellte Richtlinien zum Thema IT-Sicherheit und Datenschutz analysiert.
<b>Security Information and Event Management (SIEM)</b>	SIEM-Systeme identifizieren sicherheitsrelevante Ereignisse meist auf Grundlage von systemrelevanten Sicherheitsmeldungen und Benutzerverhalten im Unternehmensnetzwerk (Sammlung von Protokollen, welche Trends und Muster anzeigen, die vom gewohnten Schema abweichen), bewerten diese Meldungen und informieren anschließend den Administrator, welcher diese Meldungen monitoren und ggf. erforderliche Gegenmaßnahmen einleiten kann. Sie übernehmen somit die Sicherheitsüberwachung im Netzwerk indem eine ganzheitliche Sicht auf die Sicherheit der IT gelegt wird.
<b>Social Engineering</b>	Im Rahmen von Social Engineering versuchen Angreifer den Anwender durch Vortäuschung einer persönlichen Beziehung zur Installation von Schadsoftware oder zur Informationsherausgabe zu bewegen.
<b>Software as a Service (SaaS)</b>	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 (bspw. Energieerzeugung, Wasserversorgung, etc.) eingesetzt (siehe auch ‚ICS‘).

**Trojaner**

Ein Trojaner ist ein Programm, welches einen böartigen oder schädlichen Programmcode beinhaltet und nach Installation im Hintergrund verdeckt unerwünschte Funktionen ausführt.

**Wurm**

Ein Computerwurm ist eine Art von Malware. Dieses sich selbst vervielfältigende Schadprogramm mit eigenständiger Programmroutine hat die Eigenschaft, sich ohne fremde Hilfe weiter zu verbreiten ohne dabei Dateien oder Bootsektoren zu infizieren.



## Die Gothaer als starker Partner

Mit über 3,5 Millionen Mitgliedern und Beitragseinnahmen von mehr als vier Milliarden Euro gehört die Gothaer zu den großen deutschen Versicherungskonzernen und ist einer der größten Versicherungsvereine auf Gegenseitigkeit in Deutschland. Durch qualitativ hochwertige Risiko- und Finanzkonzepte bietet die Gothaer ihren Kunden umfassende Lösungen, die über die reinen Versicherungs- und Vorsorgefragen hinausgehen.

Für noch mehr aktuelle Kompetenz, noch mehr Service und zusätzliche Sicherheit kooperiert die Gothaer mit leistungsstarken Partnerunternehmen, Verbänden und Interessengemeinschaften.

Dass die Gothaer Allgemeine Versicherung AG verlässlich und solide aufgestellt ist, bestätigen die Ratingergebnisse von Standard & Poor's (A-) und Fitch (A) zum wiederholten Male. Der Ausblick der Ratings ist weiterhin „stabil“.

Die Analysten lobten die starke Wettbewerbsposition des Gothaer Konzerns, die durch das gut diversifizierte Produkt- und Vertriebsportfolio getragen wird. Die Bestätigung der Ergebnisse reflektiert ebenso die starke und widerstandsfähige Kapitalausstattung der Gothaer.

Es ist schon etwas ganz Besonderes, wenn man auf fast zweihundert Jahre Erfahrung zurückblickt. In dieser Zeit hat der Gothaer Konzern den Versicherungsmarkt durch innovative Versicherungslösungen mitgestaltet und gemeinsam mit den Kolleginnen und Kollegen des Gothaer Exklusivvertrieb, die Herausforderungen des Marktes gemeistert.

Auf weiterhin gute Zusammenarbeit.

Gothaer Allgemeine Versicherung AG  
Komposit Industriekunden  
Produktmanagement  
Gothaer Allee 1  
50969 Köln



# Gothaer

**Gothaer**  
**Allgemeine Versicherung AG**  
**Gothaer Allee 1**  
**50969 Köln**

**Telefon 0221 308-00**  
**Telefax 0221 308-103**  
**[www.gothaer.de](http://www.gothaer.de)**