Gothaer

Fragebogen für Unternehmen zur Gothaer Cyber-Versicherung

Stand: Mai 2022

118041 – 05.2022

1. Versicherungsnehmer

Name und Rechtsform der Gesellschaft (Versicherungsnehmerin)

Anschrift der Gesellschaft

Ansprechpartner im Unternehmen (Name, Telefon, E-Mail)

Webseite

Namen aller Tochtergesellschaften oder Zweigstellen
(Bitte fügen Sie eine gesonderte Liste bei, sofern der Platz nicht ausreicht)

Sind weitere mitzuversichernde Unternehmen (sofern keine Tochtergesellschaft) vorhanden?

Mitzuversichernde Unternehmen

Gesellschaftsrechtliches Verhältnis zum Versicherungsnehmer

2. Geschäftsbereich

Hinweis: Bitte berücksichtigen Sie bei der Beantwortung der nachstehenden Fragen alle zu versichernden Unternehmen in ihrer Gesamtheit. Sofern die Antworten nicht für alle zu versichernden Unternehmen gelten und/oder getrennte Systeme bestehen, bitten wir Sie um einen eigenen Fragebogen für das/die betreffende(n) Unternehmen.
(Bitte fügen Sie nach Möglichkeit ein aktuelles Firmen-Organigramm bei)

Betriebsbeschreibung

In welchen Geschäftsbereichen ist Ihr Unternehmen tätig? Wie viel Prozent des Umsatzes wird durch jeden Geschäftsbereich umgesetzt?

Geschäftsbereich (Betriebsart)	**Umsatzanteil in %**

3. Wirtschaftliche Kennzahlen

Bitte geben Sie die **konsolidierten**[1] Werte des letzten Geschäftsjahres an:

Geschäftsjahr:	**Gesamt**	**D**	**EWR (exkl. D)**	**USA**	**Sonstige**
Umsatz [Mio. EUR]					
Davon E-Commerce [Mio. EUR]					
Gewinn [Mio. EUR]					
Mitarbeiter					
Standorte					

[1] Zusammenfassung von Finanzzahlen der Jahresabschlüsse einzelner Unternehmen.

4. Kundenstruktur

Gibt es einzelne Kunden, mit denen Sie mehr als 10% Ihres Umsatzes erwirtschaften? ☐ ja ☐ nein

Wenn ja, welche?

Unternehmen	**Umsatzanteil in %**

Mit welchen der nachfolgenden Kunden / Unternehmensarten werden entsprechende Umsätze erzielt?

Kunden / Unternehmen / Branche	**Umsatzanteil in %**
Privatkunden	
Unternehmen der produzierenden Industrie	
Einzelhandel / Großhandel	
Finanzdienstleister	
Öffentlich rechtliche Unternehmen	
Rechtsanwälte / Steuerberater / Wirtschaftsprüfer u. ä.	
Sonstige Unternehmen	

5. IT-Organisation

5.1 Wie viele IT-Systeme sind im Einsatz?

Anzahl der Desktops .....

Anzahl Laptops .....

Anzahl Smartphones .....

Anzahl Server physisch ..... virtuell .....

Welche Art der Virtualisierung? .....

5.2 Ist der Einsatz von „Bring-your-own-device“ (BYOD) zulässig? ☐ ja ☐ nein

Wenn ja, besteht eine interne IT-Richtlinie zum sicheren Einsatz von BOYD? ☐ ja ☐ nein

Wenn ja, bestehen IT-technische Sicherungen wie z. B. eine Mobile Device Management Lösung (MDM) für den Einsatz von BYOD? ☐ ja ☐ nein

5.3 Werden in Ihrem Unternehmen Heim- oder Telearbeitsplätze angeboten und genutzt? ☐ ja ☐ nein

Wenn ja: Sind diese Arbeitsplätze auf dem gleichen Schutzniveau wie die Unternehmensarbeitsplätze? ☐ ja ☐ nein

5.4 Haben Sie eine eigene IT-Abteilung? ☐ ja ☐ nein

Anzahl der Mitarbeiter der IT-Abteilung .....

Wenn nein: Bitte nennen Sie den verantwortlichen Dienstleister für Ihre IT-Betreuung

.....

6. Datenstruktur/ Datensicherheit

6.1 Speichern oder verarbeiten Sie personenbezogene oder unternehmenssensible Daten? ☐ ja ☐ nein

Wenn Ja, wie viele Datensätze werden gespeichert? Mehrfach vorhandene Datensätze z. B. zu einer Person zählen dabei „einfach“. Bitte berücksichtigen Sie alle gespeicherten Datensätze, u. a. zu Mitarbeitern, Kunden, Lieferanten, Geschäftspartnern.

Personenbezogene oder unternehmenssensible Daten (z. B. Name, Adresse, sachliche Verhältnisse)
- ☐ 1–20.000 Datensätze
- ☐ 20.001–100.000 Datensätze
- ☐ 100.001–500.000 Datensätze
- ☐ 500.001–1 Mio. Datensätze
- ☐ über 1 Mio. Datensätze

davon besonders sensible Daten (z. B. Gesundheitsdaten, Daten zur ethnische Herkunft, Daten zur sexuelle oder religiöse Orientierung)
- ☐ 1–20.000 Datensätze
- ☐ 20.001–100.000 Datensätze
- ☐ 100.001–500.000 Datensätze
- ☐ 500.001–1 Mio. Datensätze
- ☐ über 1 Mio. Datensätze

davon Abrechnungsdaten (z. B. Kontoverbindungen, Kreditkartendaten, weitere elektronische Zahlungsdaten)
- ☐ 1–20.000 Datensätze
- ☐ 20.001–100.000 Datensätze
- ☐ 100.001–500.000 Datensätze
- ☐ 500.001–1 Mio. Datensätze
- ☐ über 1 Mio. Datensätze

Werden oben genannte Daten über internationale Grenzen versendet? ☐ ja ☐ nein

Wenn ja, wohin? .....

6.2 Akzeptierten Sie oder mitversicherte Unternehmen bargeldlosen Zahlungsverkehr (Kreditkarte oder Maestro Card) ☐ ja ☐ nein

Wenn ja, speichern oder verarbeiten Sie diese Kreditkartendaten Dritter auf Ihren IT-Systemen (ggf. auch nur für kurze Zeit) ☐ ja ☐ nein

6.3 Müssen Sie Payment Card Industry (PCI) und Data Security Service (DSS) Anforderungen einhalten? ☐ ja ☐ nein

Wenn ja, welche Anforderungsstufe? ☐ 1 ☐ 2 ☐ 3 ☐ 4

6.4 Gibt es einen internen Datenschutzbeauftragten bzw. wird die Funktion durch einen externen Dienstleister/Datenschutzbeauftragten gewährleistet? ☐ ja ☐ nein

Bei externem DSB: Bitte nennen Sie den verantwortlichen Dienstleister für Ihre Betreuung im Bereich Datenschutz-Sicherheit.

.....

6.5 Existiert in Ihrem Unternehmen eine Aufstellung aller Systeme, Anwendungen und unterstützenden Infrastrukturen (z. B. Server, Datenbanken) die personengebundene oder sonstige sensible Informationen verarbeiten oder speichern? ☐ ja ☐ nein

6.6 Existiert innerhalb Ihres Unternehmens ein Löschkonzept nach DSGVO? ☐ ja ☐ nein

Existiert ein vollständiges Verzeichnis der Verarbeitungstätigkeiten nach DSGVO? ☐ ja ☐ nein

6.7 Erfolgt innerhalb Ihres Unternehmens eine Datenspeicherung von Dritten in Verbindung mit einer Vertraulichkeitsvereinbarung? ☐ ja ☐ nein

Sofern ja, sind diese mit Vertragsstrafen hinterlegt? ☐ ja ☐ nein

6.8 Sind innerhalb Ihres Unternehmens alle vertraulichen Daten auf Servern und Clients verschlüsselt abgespeichert? ☐ ja ☐ nein

Werden innerhalb Ihres Unternehmens alle vertraulichen Daten für die Übertragung verschlüsselt? ☐ ja ☐ nein

7. Extranet / Webseiten

7.1 Betreiben Sie ein Extranet oder Webseiten? ☐ ja ☐ nein

Wenn ja, hosten Sie diese Webseiten über einen Provider? ☐ ja ☐ nein

Provider: ..... ☐ teilweise

7.2 Betreiben Sie E-Commerce oder einen Onlineshop? ☐ B2B ☐ B2C ☐ nein

8. Externe Dienstleister

8.1 Setzen Sie für Ihr Unternehmen externe Dienstleister im Bereich IT-Dienstleistungen ein? ☐ ja ☐ nein

Wenn ja: Welche Dienstleistungen fallen darunter (z. B. Website, Wartung, Datensicherung, Zahlungsverkehrabwicklung)?

.....

Mit welchen IT-Dienstleistern arbeiten Sie zusammen?

.....

8.2 Gibt es bestehende Netzwerke oder gemeinsame Datenbanken zwischen Ihnen und einem Kunden/Zulieferer/Geschäftspartner? ☐ ja ☐ nein

8.3 Nutzen Sie Cloud-Computing / Software as a Service? ☐ ja ☐ nein

Wenn ja, mit welchem Cloud-Dienstleister? .....

Wenn ja, über welchen Serviceanbieter? .....

8.4 Gibt es Verfahrensvorschriften für Ihre Dienstleister in Bezug auf IT-Sicherheit und folgen diese einschlägigen Standards? ☐ ja ☐ nein ☐ teilweise

Gibt es hinsichtlich der von den Dienstleistern zu beachtenden Verfahrensvorschriften ein beschriebenes Verfahren und werden Service Level Agreements vereinbart? ☐ ja ☐ nein ☐ teilweise

Wird die Einhaltung der Verfahrensvorschriften für den Dienstleister überwacht? ☐ ja ☐ nein ☐ teilweise

9. IT-Abhängigkeit

9.1 Nennen Sie bitte die Ausfallzeit, nach der bei Ihrem Unternehmen ein signifikanter Schaden für Ihr Geschäft entsteht (nur für tatsächlich vorhandene Aktivitäten ausfüllen):

Anwendung oder Aktivität	Maximale Ausfallzeit, bevor ein negativer Einfluss auf Ihr Geschäft zu erwarten ist				
	bis 12 h	ab 12 h	ab 24 h	ab 48 h	ab 96 h
Produktion					
Logistik/Vertrieb/Handel					
Finanztransaktionen					
Sonstige					

9.2 Ist bei einem Ausfall der OT (Operational Technology) in ihrem Unternehmen eine Weiterführung der Produktion und Logistik auch manuell möglich? ☐ ja ☐ nein ☐ teilweise

10. Organisatorisches IT-Risikomanagement

10.1 Werden Security Audits oder Penetrationstests durchgeführt? ☐ ja ☐ nein

Wenn ja, werden dadurch gefundene Lücken geschlossen? ☐ ja ☐ nein

Wenn ja, wie häufig werden Security Audits / Penetrationstest durchgeführt?

☐ Jedes halbe Jahr ☐ Jährlich ☐ 2-Jährlich ☐ Unregelmäßig ☐ Längere Abstände

Wenn ja, existieren betriebsinterne Vorgaben nach welchen Kriterien Security Audits / Penetrationstests zu wiederholen sind? ☐ ja ☐ nein

10.2 Sind in Ihrem Unternehmen Prozesse zum Informationssicherheits-Risikomanagement etabliert? ☐ ja ☐ nein ☐ teilweise

Wenn ja, unterliegt das IT-Risikomanagement einer regelmäßigen Überarbeitung und zusätzlichen Neubewertung nach Änderungen im Unternehmen? ☐ ja ☐ nein

10.3 Ist in Ihrem Unternehmen ein ISMS (Informationssicherheit-Management-System) etabliert? ☐ ja ☐ nein

10.4 Sind in Ihrem Unternehmen die Verantwortlichkeiten für den Bereich Informationssicherheit klar geregelt? Z. B. über einen CISO (Chief Information Security Officer) oder einen ISB (Informationssicherheitsbeauftragter) ☐ ja ☐ nein

Wenn nein: Bitte nennen Sie den verantwortlichen Dienstleister für Ihre Betreuung im Bereich Informationssicherheit.

.....

10.5 Sind in Ihrem Unternehmen interne Richtlinien / Anweisungen zu Wahrung / Sicherstellung von Datensicherheit / -schutz und Vertraulichkeit etabliert? ☐ ja ☐ nein ☐ teilweise

Wenn ja, sind diese Richtlinien/ Anweisungen für jeden betroffenen Mitarbeiter zugänglich? ☐ ja ☐ nein

Wenn ja, wird die Einhaltung der firmeninternen Handlungsanweisungen in Bezug auf die IT-Sicherheit und Datenschutz überwacht? ☐ ja ☐ nein

10.6 Werden in Ihrem Unternehmen Mitarbeiter in Bezug auf IT-Sicherheit und Datenschutz regelmäßig, mindestens aber jährlich, sensibilisiert bzw. geschult? ☐ ja ☐ nein

Wenn ja, wie geschieht dies? .....

Wenn ja, erfolgen im Rahmen oder im Nachgang der Schulungsmaßnahmen Phishing-Tests? ☐ ja ☐ nein

Wenn ja, erfolgen die Schulungsmaßnahmen für neue Mitarbeiter Ihres Unternehmens mindestens innerhalb der ersten 6 Monate nach Unternehmenseintritt? ☐ ja ☐ nein

10.7	Verwendet Ihr Unternehmen aktuelle Sicherheits- und Verschlüsselungstechnologien, sowie technische Schutzmaßnahmen- und verfahren? Erfüllen diese anerkannte industrielle Normen/ Standards?	☐ ja ☐ nein ☐ teilweise
10.8	Wurden physische Sicherheitszonen für IT- und datensicherheitsrelevante Bereiche definiert?	☐ ja ☐ nein ☐ teilweise
	Wenn ja, sind sicherheitsrelevante Bereiche aus öffentlichen Zonen nicht zugänglich und werden technisch überwacht? Erfolgt die Vergabe von Zutrittsberechtigungen zentral und werden Externe begleitet?	☐ ja ☐ nein
	Wenn ja, werden die Wirksamkeit der physischen Sicherheitszonen und die Prozesse regelmäßig überprüft?	☐ ja ☐ nein
10.9	Werden anerkannte Standards/Normen in Ihrem Unternehmen erfüllt oder sind aktuell in der Umsetzung (Bspw. ISO 27001, ISO 22301, TISAX)?	☐ ja ☐ nein
	Wenn ja, welche?	
10.10	Wird ihr Unternehmen regelmäßig und aktiv über (aktuelle) Schwachstellen und Bedrohungen in der IT-Sicherheit informiert (z. B. über CERT-Mitgliedschaft)?	☐ ja ☐ nein
10.11	Entsprechen die aktuellen Einstellungen Ihrer Active-Directory-Struktur den Empfehlungen des Herstellers?	☐ ja ☐ nein
10.12	Existiert innerhalb Ihres Unternehmens ein Change-Management-Prozess für kritische IT-Systeme?	☐ ja ☐ nein
10.13	Existieren innerhalb Ihres Unternehmens für sämtliche Benutzer von Systemen, Anwendungen und sonstiger Bürokommunikationssystemen personalisierte und eigene Benutzerkonten?	☐ ja ☐ nein
	Existieren innerhalb Ihres Unternehmens für Systemadministratoren privilegierte Benutzerkonten für deren administrative Aufgaben, sowie ein eigenes personalisiertes Benutzerkonto für den täglichen Zugriff?	☐ ja ☐ nein
10.14	Erfolgen Fernzugriffe auf ihr Unternehmensnetzwerk ausschließlich mit einer MFA (Multi-Faktor-Authentifizierung)	☐ ja ☐ nein
	Erfolgt der Zugang zu privilegierten Benutzerkonten mit einer eigenen MFA als zusätzlicher Schutz?	☐ ja ☐ nein
10.15	Existieren innerhalb Ihres Unternehmens eine Passwortrichtlinie welche komplexe Anforderungen an Passwörter fordert?	☐ ja ☐ nein
10.16	Existieren innerhalb Ihres Unternehmens ein Prozess für die Löschung/ Widerruf von Benutzer- und Zugriffsrechten bei bestimmten Ereignissen, insb. Abteilungswechsel, Kündigung eines Mitarbeiters, Dienstleisters oder Lieferanten?	☐ ja ☐ nein
10.17	Erfolgen innerhalb Ihres Unternehmens bei höheren Überweisungen besondere Sicherheitsmaßnahmen (z. B. 4-Augen-Prinzip, maximales Überweisungslimit, zusätzliche Freigabe durch ausführende Bank)?	☐ ja ☐ nein
	Wenn ja, welche Maßnahmen?	
10.18	Hat Ihr Unternehmen einen Notfallplan zur Wiederherstellung des Betriebes nach schwerwiegenden Störungen?	☐ ja ☐ nein
	Wenn ja: Wurde ein Probelauf des Notfallplans durchgeführt?	☐ ja ☐ nein
	Wenn ja: Beinhaltet der Notfallplan Ihres Unternehmens mindestens eine feste Aufgabenverteilung für die Behandlung eines Vorfalls und einen Kommunikationsplan für Kunden und andere Betroffene?	☐ ja ☐ nein
	Wenn ja: Wird der Notfallplan regelmäßig, mindestens aber alle 18 Monate aktualisiert?	☐ ja ☐ nein
	Wenn ja: Wird der Notfallplan regelmäßig, mindestens aber alle 2 Jahre, in einer Notfallübung (Probelauf) durch die handelnden Personen in Ihrem Unternehmen getestet?	☐ ja ☐ nein

Existiert innerhalb Ihres Unternehmens eine physische Notfallkontaktliste für Cyber-Security-Vorfälle? ☐ ja ☐ nein

10.19 Werden BCM-Maßnahmen / -Übungen durchgeführt (Stromabschaltung, Redundanztests etc.)? ☐ ja ☐ nein

11. Technisches IT-Risikomanagement

11.1 Hat Ihr Unternehmen eine flächendeckende, unternehmensweite, einheitliche Schnittstellenkontrolle (z. B. bei USB Ports)? ☐ ja ☐ nein ☐ teilweise

Wenn ja, für welche Systeme? .....

Wenn ja, werden Netzwerke in Bezug auf das Hinzufügen und Entfernen von Teilnehmern automatisch überwacht bzw. alternativ das unautorisierte Zufügen oder Löschen von Teilnehmern verhindert? ☐ ja ☐ nein

Wenn ja, ist beim Einsatz mobiler Datenträger der Datentransport zwischen IT-Systemen, die nicht miteinander vernetzt sind, gemäß Unternehmensrichtlinie geregelt? ☐ ja ☐ nein ☐ teilweise

Wie wird dies umgesetzt? .....

11.2 Wird in Ihrem Unternehmen eine MDM (Mobile-Device-Management) Lösung eingesetzt (inkl. BYOD) und besteht die Möglichkeit die Daten der mobilen Endgeräte aus der Ferne zu löschen? ☐ ja ☐ nein

Werden die mobilen Endgeräte alle verschlüsselt (z. B. Bitlocker)? ☐ ja ☐ nein

11.3 Ist im Unternehmen ein Patch-Management Prozess etabliert? ☐ ja ☐ nein

Wenn ja, wie wird dieser umgesetzt? .....

Wenn ja, ist sichergestellt, dass Ihr Unternehmen Informationen über alle kritischen Updates zeitnah erhält? ☐ ja ☐ nein

Wenn ja, gibt es einen Prozess, nach dem kritische Systemaktualisierungen getestet, freigegeben und eingebracht werden und ist dieser Prozess dokumentiert und erprobt? ☐ ja ☐ nein

Erfolgt innerhalb Ihres Unternehmens das Einspielen von Sicherheitsupdates zeitnah, mind. 30 Tagen nach Erscheinen des Herstellerupdates? ☐ ja ☐ nein

Erfolgt im Vorfeld des Patching eine Testung der Updates in einer isolierten Umgebung? ☐ ja ☐ nein

11.4 Setzt Ihr Unternehmen auf allen Endgeräten regelmäßig aktualisierte und funktionsfähige Antivirenprogramme ein? ☐ ja ☐ nein

Bitte nennen Sie Hersteller und Produkte:

.....

.....

Wie werden diese administriert?

.....

11.5 Setzt Ihr Unternehmen an allen Zugängen zu Ihrem Netzwerk bzw. allen Netzwerkknotenpunkten regelmäßig aktualisierte und funktionsfähige Firewall-Systeme ein? ☐ ja ☐ nein

Bitte nennen Sie Hersteller und Produkte:

.....

.....

Wie werden diese administriert?

.....

Werden die Programme / Systeme nach Herstellerangaben konfiguriert? ☐ ja ☐ nein

11.6 Ist Ihr Netzwerk segmentiert, so dass kritische Bereiche von weniger kritischen Bereichen getrennt sind? ☐ ja ☐ nein ☐ teilweise

Wenn ja, erfolgt die Netzwerktrennung auf Basis der Kritikalität mindestens in administrative Netze, Verwaltungsnetze und operative IT-Netze? ☐ ja ☐ nein ☐ teilweise

11.7 Sind Ihre IT-Systeme an externe Netzwerke (Internet etc.) angeschlossen? ☐ ja ☐ nein

11.8 Ist in Ihrem Unternehmen eine Endpoint Protection Plattform (EPP) im Einsatz? ☐ ja ☐ nein

11.9 Werden zusätzlich IDS/IPS Systeme (Angriffs Entdeckungssystem / Angriffs Präventionssystem) eingesetzt und erfolgen regelmäßige Auswertungen der Protokollierung? ☐ ja ☐ nein

11.10 Wird in Ihrem Unternehmen ein SIEM (Security Information and Event Management) System eingesetzt und können die Alarmmeldungen zeitnah bearbeitet werden? ☐ ja ☐ nein

11.11 Wird in Ihrem Unternehmen ein SOC (Security Operation Center) eingesetzt und werden die Meldungen und Ergebnisse durch geschulte interne Mitarbeiter oder durch spezialisierte externe Dienstleisterüberwacht und ausgewertet? ☐ ja ☐ nein

Wenn ja, durch welche IT-Dienstleister?

11.12 Werden innerhalb Ihres Unternehmens Altsysteme (Legacy-Systeme) betrieben, für welche der jeweilige Hersteller keine Updates mehr zur Verfügung stellt (z. B. Windows 7, Windows XP)? ☐ ja ☐ nein

Wenn ja, werden diese Systeme ausschließlich in einer komplett isolierten Umgebung betrieben und sind von sonstigen Systemen/Netzwerken/ Internet getrennt? ☐ ja ☐ nein

Wenn keine Isolierung existiert:
Bitte beschreiben Sie Art, Anzahl und Aufgaben der vorhandenen Altsysteme und die von ihnen getroffenen Schutzmaßnahmen.

11.13 Gibt es in Ihrer Infrastruktur IT-Systeme, die nicht durch die genannten Schutzmechanismen geschützt werden? ☐ ja ☐ nein

Wenn ja, welche Systeme werden nicht geschützt? Begründen Sie bitte, warum diese Systeme nicht geschützt werden:

11.14 Erfolgt innerhalb Ihres Unternehmens eine regelmäßige, mind. tägliche Back-up-Sicherung aller geschäftskritischen Systeme? ☐ ja ☐ nein

Ist ein Prozess beschrieben, wie Back-ups zu erstellen, aufzubewahren und regelmäßig zu testen sind? ☐ ja ☐ nein ☐ teilweise

Welches Verfahren innerhalb des Back-up-Prozesses wendet ihr Unternehmen an (z. B. Vollbackup, inkrementelles Back-up, differenzielles Back-up)?

Welche Back-up Medien werden innerhalb Ihres Unternehmens verwendet (z. B. externe Festplatte, Band, Online-Cloud, NAS)?

Hat ihr Unternehmen ein vollständiges Back-up (offline) auf separierten Systemen gespeichert, welches nicht älter als 1 Woche ist? ☐ ja ☐ nein

Sofern kein Offline-Back-up existiert:
Erfolgt das Backup außerhalb des Active-Directory Ihres Unternehmens (Authentifizierung-Schutzmechanismus)? ☐ ja ☐ nein

Erfolgt innerhalb Ihres Unternehmens das Back-up nach der 3-2-1 Regel? ☐ ja ☐ nein

Erfolgt innerhalb Ihres Unternehmens eine Verschlüsselung der Back-ups? ☐ ja ☐ nein

Werden Restore-Tests regelmäßig durchgeführt? ☐ ja ☐ nein

Nutzt Ihr Unternehmen ein Redundanzsystem für alle Computernetzwerke? ☐ ja ☐ nein

Sind die Back-up-Systeme räumlich / physisch voneinander getrennt? ☐ ja ☐ nein

Wenn ja, bitte beschreiben Sie die Trennung der Systeme möglichst genau:

.....

11.15 Werden in Ihrer IT-Infrastruktur Industrial Control Systeme (ICS) wie SCADA-Systeme oder DCS betrieben? ☐ ja ☐ nein

Wenn ja,

a) Befinden sich die IC-Systeme in einem separierten Netzwerk mit eingeschränkten Zugriffsmöglichkeiten? ☐ ja ☐ nein

b) Erfolgt der Fernzugriff auf die IC-Systeme ausschließlich auf verschlüsseltem Weg und/oder mittels einer Multi-Faktor-Authentifizierung? ☐ ja ☐ nein

11.16 Erfolgt die Freigabe von Fernwartungszugänge ausschließlich durch legitimierte Mitarbeiter Ihres Unternehmens? ☐ ja ☐ nein

Sofern nicht, welches Verfahren setzt ihr Unternehmen ein?

.....

Wird eine Fernwartung durchgehend durch legitimierte Mitarbeiter Ihres Unternehmens begleitet und überwacht? ☐ ja ☐ nein

12. Vorschäden / Verfahren

12.1 Hatten Sie Schäden / Vorfälle innerhalb der letzten 5 Jahre in den folgenden Bereichen, oder sind Ihrem Unternehmen oder Ihnen Umstände bekannt welche zu einem Schaden oder einem Schadenersatzanspruch in den folgenden Bereichen führen könnten? ☐ ja ☐ nein

- Allgemeine Datenschutzverletzung (z. B. Diebstahl vertraulicher Daten)
- Behördliche Untersuchung eines Datenschutzvorfalles
- Beschwerden (z. B. von Mitarbeitern) aufgrund von Datenschutzverletzungen
- Unbefugtes Eindringen (hacken) Ihrer IT-Infrastruktur oder Applikationen
- Ausfall eines Teils Ihrer IT-Infrastruktur oder Applikationen aufgrund eines unbefugten Eindringens
- Umsatzausfälle oder sonstige erhebliche Kosten verursacht durch unbefugtes Eindringen in Ihre IT-Infrastruktur oder Applikationen
- Angedrohte oder tatsächliche Handlungen von Dritten gegen Daten, Programme oder die IT-Infrastruktur in Verbindung mit einer Aufforderung zur Zahlung von Erpressungsgeld

Wenn ja, welche Vorfälle / Schäden gab es und wie hoch waren die jeweiligen Kosten?

Datum	Kurzbeschreibung	Status	Kosten	offene / erwartete Kosten	Sonstiges (Abschlussdatum)

Bitte senden Sie uns zusätzlich zu der Kurzbeschreibung eine ausführliche separate Stellungnahme zu den Vorfällen / Schäden sowie zu den daraus entstandenen Maßnahmen.

12.2 Sind behördliche Verfahren oder Ansprüche wegen Datenrechtsverletzungen gegen Sie einschlägig? ☐ ja ☐ nein

Datenweitergabe

Ich (Wir) bin (sind) damit einverstanden, dass die Gothaer im erforderlichen Umfang Daten, die sich aus den überlassenen Unterlagen oder der Vertragsdurchführung (Beiträge, Versicherungsfälle, Risiko-Vertragsänderungen) ergeben, an Rückversicherer und/oder andere Versicherer zur Beurteilung des Risikos und eventueller Ansprüche übermitteln oder dem Gesamtverband der Deutschen Versicherungswirtschaft e. V., Berlin, solche Daten zur Weitergabe an andere Versicherer zur Verfügung stellen. Ich (Wir) bin (sind) weiterhin damit einverstanden, dass die Gothaer im erforderlichen Umfang Daten, die sich aus den überlassenen Unterlagen oder der Vertragsdurchführung ergeben an ausgewählte Dienstleister der Gothaer zur Beurteilung des Risikos und eventueller Ansprüche übermitteln. Diese Einwilligung gilt auch unabhängig vom Zustandekommen des Vertrages sowie für entsprechende Prüfungen bei anderweitig beantragten Versicherungsverträgen und bei künftigen Anträgen.

Unterschrift(en)

Der/die Unterzeichner/-in(nen) bestätigt (bestätigen), vor Unterzeichnung dieses Fragebogens die beigefügte Mitteilung über die Folgen einer Verletzung der vorvertraglichen Anzeigepflicht nach dem anliegend Muster erhalten und zur Kenntnis genommen zu haben.

Der/die vertretungsberechtigte(n) Unterzeichner/-in(nen) erklärt (erklären) mit Wirkung für und gegen die Gesellschaft als Versicherungsnehmerin, ihre Tochterunternehmen und die zu versichernden Personen, die oben gestellten Fragen vollständig und wahrheitsgemäß beantwortet zu haben.

Dieser ausgefüllte Fragebogen und die eventuellen Anlagen sind Grundlage der Versicherung und werden deshalb Bestandteil eines etwaigen Versicherungsvertrags sein. Für den Fall, dass ein Versicherungsvertrag zustande kommt, gelten die in diesem Fragebogen und eventuellen Anlagen gemachten Angaben als vorvertragliche Angaben im Sinne der §§ 19 ff. Versicherungsvertragsgesetz (VVG).

Name und Position im Unternehmen

Im Namen (Versicherungsnehmerin)

Datum

Unterschrift des/der Vertretungsberechtigten

Widerrufsbelehrung

Abschnitt 1 — **Widerrufsrecht, Widerrufsfolgen und besondere Hinweise**

Widerrufsrecht

Sie können Ihre Vertragserklärung innerhalb einer Frist von 14 Tagen ohne Angabe von Gründen in Textform (z. B. Brief, Fax, E-Mail) widerrufen. Die Widerrufsfrist beginnt, nachdem Ihnen

- **der Versicherungsschein,**
- **die Vertragsbestimmungen,**
  einschließlich der für das Vertragsverhältnis geltenden Allgemeinen Versicherungsbedingungen, diese wiederum einschließlich der Tarifbestimmungen,
- **diese Belehrung,**
- **das Informationsblatt zu Versicherungsprodukten,**
- **und die weiteren in Abschnitt 2 ausgeführten Informationen**

jeweils in Textform zugegangen sind. Zur Wahrung der Widerrufsfrist genügt die rechtzeitige Absendung des Widerrufs. Der Widerruf ist zu richten an: Gothaer Allgemeine Versicherung AG, Gothaer Allee 1, 50969 Köln.

Widerrufsfolgen

Im Falle eines wirksamen Widerrufs endet der Versicherungsschutz und der Versicherer hat Ihnen den auf die Zeit nach Zugang des Widerrufs entfallenden Teil der Prämien zu erstatten, wenn Sie zugestimmt haben, dass der Versicherungsschutz vor dem Ende der Widerrufsfrist beginnt. Den Teil der Prämie, der auf die Zeit bis zum Zugang des Widerrufs entfällt, darf der Versicherer in diesem Fall einbehalten; dabei handelt es sich pro Tag um einen Betrag in Höhe von 1/360 der von Ihnen für ein Jahr zu zahlenden Prämie. Der Versicherer hat zurückzuzahlende Beiträge unverzüglich, spätestens 30 Tage nach Zugang des Widerrufs, zu erstatten. Beginnt der Versicherungsschutz nicht vor dem Ende der Widerrufsfrist, so hat der wirksame Widerruf zur Folge, dass empfangene Leistungen zurückzugewähren und gezogene Nutzungen (z. B. Zinsen) herauszugeben sind.

Besondere Hinweise

Ihr Widerrufsrecht erlischt, wenn der Vertrag auf Ihren ausdrücklichen Wunsch sowohl von Ihnen als auch vom Versicherer vollständig erfüllt ist, bevor Sie Ihr Widerrufsrecht ausgeübt haben.

Abschnitt 2 — **Auflistung der für den Fristbeginn erforderlichen weiteren Informationen**

Hinsichtlich der in Abschnitt 1 Satz 2 genannten weiteren Informationen werden die Informationspflichten im Folgenden im Einzelnen aufgeführt:

Informationspflichten bei allen Versicherungszweigen

Der Versicherer hat Ihnen folgende Informationen zur Verfügung zu stellen:

1. die Identität des Versicherers und der etwaigen Niederlassung, über die der Vertrag abgeschlossen werden soll; anzugeben ist auch das Handelsregister, bei dem der Rechtsträger eingetragen ist, und die zugehörige Registernummer;
2. die ladungsfähige Anschrift des Versicherers und jede andere Anschrift, die für die Geschäftsbeziehung zwischen dem Versicherer und Ihnen maßgeblich ist, bei juristischen Personen, Personenvereinigungen oder -gruppen auch den Namen eines Vertretungsberechtigten; soweit die Mitteilung durch Übermittlung der Vertragsbestimmungen einschließlich der Allgemeinen Versicherungsbedingungen erfolgt, bedürfen die Informationen einer hervorgehobenen und deutlich gestalteten Form;
3. die Hauptgeschäftstätigkeit des Versicherers;
4. die wesentlichen Merkmale der Versicherungsleistung, insbesondere Angaben über Art, Umfang und Fälligkeit der Leistung des Versicherers;
5. den Gesamtpreis der Versicherung einschließlich aller Steuern und sonstigen Preisbestandteile, wobei die Prämien einzeln auszuweisen sind, wenn das Versicherungsverhältnis mehrere selbständige Versicherungsverträge umfassen soll, oder, wenn ein genauer Preis nicht angegeben werden kann, Angaben zu den Grundlagen seiner Berechnung, die Ihnen eine Überprüfung des Preises ermöglichen;
6. Einzelheiten hinsichtlich der Zahlung und der Erfüllung, insbesondere zur Zahlungsweise der Prämien;
7. die Befristung der Gültigkeitsdauer der zur Verfügung gestellten Informationen, beispielsweise die Gültigkeitsdauer befristeter Angebote, insbesondere hinsichtlich des Preises;
8. Angaben darüber, wie der Vertrag zustande kommt, insbesondere über den Beginn der Versicherung und des Versicherungsschutzes sowie die Dauer der Frist, während der der Antragsteller an den Antrag gebunden sein soll;
9. das Bestehen oder Nichtbestehen eines Widerrufsrechts sowie die Bedingungen, Einzelheiten der Ausübung, insbesondere Namen und Anschrift derjenigen Person, gegenüber der der Widerruf zu erklären ist, und die Rechtsfolgen des Widerrufs einschließlich Informationen über den Betrag, den Sie im Falle des Widerrufs gegebenenfalls zu zahlen haben; soweit die Mitteilung durch Übermittlung der Vertragsbestimmungen einschließlich der Allgemeinen Versicherungsbedingungen erfolgt, bedürfen die Informationen einer hervorgehobenen und deutlich gestalteten Form;
10. a) Angaben zur Laufzeit des Vertrages;
    b) Angaben zur Mindestlaufzeit des Vertrages;

11. Angaben zur Beendigung des Vertrages, insbesondere zu den vertraglichen Kündigungsbedingungen einschließlich etwaiger Vertragsstrafen; soweit die Mitteilung durch Übermittlung der Vertragsbestimmungen einschließlich der Allgemeinen Versicherungsbedingungen erfolgt, bedürfen die Informationen einer hervorgehobenen und deutlich gestalteten Form;
12. die Mitgliedsstaaten der Europäischen Union, deren Recht der Versicherer der Aufnahme von Beziehungen zu Ihnen vor Abschluss des Versicherungsvertrags zugrunde legt;
13. das auf den Vertrag anwendbare Recht, eine Vertragsklausel über das auf den Vertrag anwendbare Recht oder über das zuständige Gericht;
14. die Sprachen, in denen die Vertragsbedingungen und die in diesem Abschnitt genannten Vorabinformationen mitgeteilt werden, sowie die Sprachen, in denen sich der Versicherer verpflichtet, mit Ihrer Zustimmung die Kommunikation während der Laufzeit dieses Vertrags zu führen;
15. einen möglichen Zugang für Sie zu einem außergerichtlichen Beschwerde- und Rechtsbehelfsverfahren und gegebenenfalls die Voraussetzungen für diesen Zu-gang; dabei ist ausdrücklich darauf hinzuweisen, dass die Möglichkeit für Sie, den Rechtsweg zu beschreiten, hiervon unberührt bleibt;
16. Name und Anschrift der zuständigen Aufsichtsbehörde sowie die Möglichkeit einer Beschwerde bei dieser Aufsichtsbehörde.

Ende der Widerrufsbelehrung

Weitere wichtige Hinweise für den Fall eines Widerrufs

Das Widerrufsrecht besteht gemäß § 8 Absatz 3 VVG nicht bei Verträgen mit einer Laufzeit von weniger als einem Monat. Soweit eine vorläufige Deckung erteilt wurde, endet diese mit dem Zugang des Widerrufs bei uns.

Widerrufen Sie einen Ersatzvertrag, so läuft Ihr ursprünglicher Versicherungsvertrag weiter.

Vorvertragliche Anzeigepflicht

Mitteilung nach § 19 Abs. 5 VVG über die Folgen einer Verletzung der gesetzlichen Anzeigepflicht

Damit wir Ihren Versicherungsantrag ordnungsgemäß prüfen können, ist es notwendig, dass Sie die beiliegenden Fragen wahrheitsgemäß und vollständig beantworten. Es sind auch solche Umstände anzugeben, denen Sie nur geringe Bedeutung beimessen.

Bitte beachten Sie, dass Sie Ihren Versicherungsschutz gefährden, wenn Sie unrichtige oder unvollständige Angaben machen. Nähere Einzelheiten zu den Folgen einer Verletzung der Anzeigepflicht können Sie der nachstehenden Information entnehmen.

Welche vorvertraglichen Anzeigepflichten bestehen?

Sie sind bis zur Abgabe Ihrer Vertragserklärung verpflichtet, alle Ihnen bekannten gefahrerheblichen Umstände, nach denen wir in Textform gefragt haben, wahrheitsgemäß und vollständig anzuzeigen. Wenn wir nach Ihrer Vertragserklärung, aber vor Vertragsannahme in Textform nach gefahrerheblichen Umständen fragen, sind Sie auch insoweit zur Anzeige verpflichtet.

Welche Folgen können eintreten, wenn eine vorvertragliche Anzeigepflicht verletzt wird?

1. Rücktritt und Wegfall des Versicherungsschutzes

Verletzen Sie die vorvertragliche Anzeigepflicht, können wir vom Vertrag zurücktreten. Dies gilt nicht, wenn Sie nachweisen, dass weder Vorsatz noch grobe Fahrlässigkeit vorliegt. Bei grob fahrlässiger Verletzung der Anzeigepflicht haben wir kein Rücktrittsrecht, wenn wir den Vertrag auch bei Kenntnis der nicht angezeigten Umstände, wenn auch zu anderen Bedingungen, geschlossen hätten.

Im Fall des Rücktritts besteht kein Versicherungsschutz. Erklären wir den Rücktritt nach Eintritt des Versicherungsfalles, bleiben wir dennoch zur Leistung verpflichtet, wenn Sie nachweisen, dass der nicht oder nicht richtig angegebene Umstand

– weder für den Eintritt oder die Feststellung des Versicherungsfalles

– noch für die Feststellung oder den Umfang unserer Leistungspflicht

ursächlich war. Unsere Leistungspflicht entfällt jedoch, wenn Sie die Anzeigepflicht arglistig verletzt haben.

Bei einem Rücktritt steht uns der Teil des Beitrags zu, welcher der bis zum Wirksamwerden der Rücktrittserklärung abgelaufenen Vertragszeit entspricht.

2. Kündigung

Können wir nicht vom Vertrag zurücktreten, weil Sie die vorvertragliche Anzeigepflicht lediglich einfach fahrlässig oder schuldlos verletzt haben, können wir den Vertrag unter Einhaltung einer Frist von einem Monat kündigen.

Unser Kündigungsrecht ist ausgeschlossen, wenn wir den Vertrag auch bei Kenntnis der nicht angezeigten Umstände, wenn auch zu anderen Bedingungen, geschlossen hätten.

3. Vertragsänderung

Können wir nicht zurücktreten oder kündigen, weil wir den Vertrag auch bei Kenntnis der nicht angezeigten Gefahrumstände, wenn auch zu anderen Bedingungen, geschlossen hätten, werden die anderen Bedingungen auf unser Verlangen Vertragsbestandteil. Haben Sie die Anzeigepflicht fahrlässig verletzt, werden die anderen Bedingungen rückwirkend Vertragsbestandteil. Haben Sie die Anzeigepflicht schuldlos verletzt, werden die anderen Bedingungen erst ab der laufenden Versicherungsperiode Vertragsbestandteil.

Erhöht sich durch die Vertragsänderung der Beitrag um mehr als 10 % oder schließen wir die Gefahrabsicherung für den nicht angezeigten Umstand aus, können Sie den Vertrag innerhalb eines Monats nach Zugang unserer Mitteilung über die Vertragsänderung fristlos kündigen. Auf dieses Recht werden wir Sie in unserer Mitteilung hinweisen.

4. Ausübung unserer Rechte

Wir können unsere Rechte zum Rücktritt, zur Kündigung oder zur Vertragsänderung nur innerhalb eines Monats schriftlich geltend machen. Die Frist beginnt mit dem Zeitpunkt, zu dem wir von der Verletzung der Anzeigepflicht, die das von uns geltend gemachte Recht begründet, Kenntnis erlangen. Bei der Ausübung unserer Rechte haben wir die Umstände anzugeben, auf die wir unsere Erklärung stützen. Zur Begründung können wir nachträglich weitere Umstände angeben, wenn für diese die Frist nach Satz 1 nicht verstrichen ist. Wir können uns auf die Rechte zum Rücktritt, zur Kündigung oder zur Vertragsänderung nicht berufen, wenn wir den nicht angezeigten Gefahrumstand oder die Unrichtigkeit der Anzeige kannten.

Unsere Rechte zum Rücktritt, zur Kündigung und zur Vertragsänderung erlöschen mit Ablauf von fünf Jahren nach Vertragsschluss. Dies gilt nicht für Versicherungsfälle, die vor Ablauf dieser Frist eingetreten sind. Die Frist beträgt zehn Jahre, wenn Sie die Anzeigepflicht vorsätzlich oder arglistig verletzt haben.

5. Stellvertretung durch eine andere Person

Lassen Sie sich bei Abschluss des Vertrages durch eine andere Person vertreten, so sind bezüglich der Anzeigepflicht, des Rücktritts, der Kündigung, der rückwirkenden Vertragsänderung und der Ausschlussfrist für die Ausübung unserer Rechte die Kenntnis und Arglist Ihres Stellvertreters als auch Ihre eigene Kenntnis und Arglist zu berücksichtigen. Sie können sich darauf, dass die Anzeigepflicht nicht vorsätzlich oder grob fahrlässig verletzt worden ist, nur berufen, wenn weder Ihrem Stellvertreter noch Ihnen Vorsatz oder grobe Fahrlässigkeit zur Last fällt.