afm unternehmensgruppe assekuranz-finanz-makler

MRH TROWE

Risikoerfassung Cyber-Versicherung

1 Allgemeine Angaben	
Firma:	
Anschrift:	
Internetadresse:	
Sind weitere Unternehmen als Mitversicherte zu berücksichtigen, die keine Tochtergesellschaften sind?	☐ nein ☐ ja Bitte fügen Sie uns ein aktuelles Organigramm bei.

Hinweis: Bitte beantworten Sie die nachstehenden Fragen für die Gesamtheit der zu versichernden Unternehmen. Sofern sich für die einzelnen Mitzuversichernden unterschiedliche Aussagen ergeben, beantworten Sie diese Abschnitte für die betreffen-den Unternehmen bitte jeweils separat.

Sofern Sie Standorte außerhalb des Europäischen Wirtschaftsraumes betreiben, wünschen Sie lokale Deckungen? (Falls nicht erfolgt die Deckung per Bilanzschutzklausel)	☐ nein ☐ ja
Beschreibung der Geschäftstätigkeit Ihres Unternehmens und etwaiger mitzuversichernder Gesellschaften *Bitte ggf. separates Beiblatt beifügen.*	

Bitte geben Sie nachfolgend die Umsatzdaten Ihres Unternehmens – inkl. mitzuversichernder Unternehmen – des letzten abgeschlossenen Geschäftsjahres an:

Umsatz insgesamt:				EUR
Deutschland:				EUR
Restlicher EWR:				EUR
UK/Schweiz:				EUR
USA / Kanada:				EUR
Rest der Welt: (Bitte um Angabe der jeweiligen Länder)				EUR
Umsatz aus online-Verkäufen oder online-Dienstleistungen:				EUR
Nur bei Tätigkeit „Finanzdienstleister“: Bilanzsumme:				EUR
Bitte geben Sie die Anzahl an Mitarbeitern an:	Vollzeit:		Teilzeit:	
Anzahl der technischen Endpoints (z.B. Server, Laptop, Desktop-PC; Nicht dazu zählen: Handy oder Tablett)				

IT-Verantwortlicher:	Ansprechpartner Vor- und Zuname: E-Mailadresse:	
Unterhalten sie oder eines ihrer Tochterunternehmungen Aktivitäten in Ländern, die mit Handels- oder Wirtschaftssanktionen der EU, der UN, nationalen Beschränkungen und US-amerikanischen Gesetzen und Bestimmungen belegt sind, wie z.B. Iran, Kuba, Syrien, Nordkorea, Nordsudan, Russland, Ukraine, Weißrussland, Venezuela in der Krim oder in den Regionen Luhansk und/oder Donezk?		☐ nein ☐ ja
Können Sie bestätigen, dass Sie ihren Hauptsitz in Deutschland haben und dass es sich bei Ihnen nicht um eine Tochtergesellschaft, einen Franchisenehmer oder eine kleinere Einheit einer größeren Organisation mit einem Umsatz von über 100 Mio. EUR handelt?		☐ nein ☐ ja

afm unternehmensgruppe assekuranz-finanz-makler

MRH TROWE

Risikoerfassung Cyber-Versicherung

2 Versicherungsbedarf	
Versicherungssumme	☐ 1.000.000 EUR ☐ 2.000.000 EUR ☐ 3.000.000 EUR ☐ 5.000.000 EUR
Selbstbeteiligung	☐ 10.000 EUR ☐ 25.000 EUR ☐ 50.000 EUR ☐ 100.000 EUR ☐ 250.000 EUR
Gewünschter Versicherungsbeginn:	
Assistance (24h-Hotline, Forensik, Rechtsberatung, PR-Beratung)	Basisschutz
Wiederherstellungskosten Kosten, die notwendig sind, um IT-Systeme, Daten und Betriebsprozesse nach einem Cyberangriff oder Datenverlust wiederherzustellen. Dazu gehören z.B. Kosten für die Wiederherstellung von Daten aus Backups, die Reparatur von beschädigter Software sowie die Arbeitskosten für IT-Spezialisten, die diese Wiederherstellungen durchführen.	Basisschutz
Betriebsunterbrechung Absicherung der finanziellen Verluste, die ein Unternehmen erleidet, wenn der Geschäftsbetrieb aufgrund eines Cyberangriffs oder eines IT-Ausfalls vorübergehend stillsteht.	Basisschutz
Erpressungsgeld Lösegeldzahlungen, die an Cyberkriminelle geleistet werden müssen, um verschlüsselte Daten freizugeben oder die Veröffentlichung sensibler Informationen zu verhindern.	☐ nein ☐ ja
Cyber-Haftpflicht Kosten, die entstehen, wenn Dritte durch einen Cyberangriff geschädigt werden und Ansprüche geltend machen. Dazu gehören z. B. Schadenersatzforderungen, Rechtskosten und Kosten für die Verteidigung gegen Klagen.	☐ nein ☐ ja
Cyber-Betrug Finanzielle Verluste, die durch betrügerische Aktivitäten im Internet entstehen. (Identitätsdiebstahl etc.)	☐ nein ☐ ja
Vertragsstrafen aufgrund Lieferausfällen Finanzielle Strafen oder Gebühren, die ein Unternehmen zahlen muss, wenn es aufgrund eines Cyberangriffs oder IT-Ausfalls seine vertraglichen Lieferverpflichtungen nicht einhalten kann. Diese Strafen können in Verträgen mit Kunden oder Partnern festgelegt sein.	☐ nein ☐ ja
Vertragliche Schadenersatzansprüche Forderungen, die Dritte erheben können, wenn durch einen Cyberangriff vertraglich vereinbarte Leistungen nicht erfüllt, werden können.	☐ nein ☐ ja
Vertragsstrafen aufgrund Geheimhaltungspflichtverletzungen Finanzielle Strafen, die auferlegt werden, wenn vertrauliche Informationen unautorisiert offengelegt oder missbraucht werden.	☐ nein ☐ ja
PCI-DSS Vertragsstrafen PCI-DSS (Payment Card Industry Data Security Standard) Vertragsstrafen sind Geldstrafen, die Unternehmen auferlegt werden, wenn sie gegen die Sicherheitsstandards zur Verarbeitung von Kreditkartendaten verstoßen.	☐ nein ☐ ja
Technische Probleme & Systemfehler Als technische Probleme oder Systemausfall gelten sämtliche ungeplante sowie ungewollte Ausfälle oder wesentlichen Beeinträchtigung des Computersystems eines versicherten Unternehmens.	☐ nein ☐ ja
Betriebsunterbrechung nach Cloud-Ausfall Absicherung der finanziellen Verluste, die ein Unternehmen erleidet, wenn der Geschäftsbetrieb aufgrund eines Cyberangriffs oder eines IT-Ausfalls bei einem Cloud-Dienstleister vorübergehend stillsteht.	☐ nein ☐ ja

Risikoerfassung Cyber-Versicherung

3 Umfang der Verarbeitung und Speicherung personenbezogener Daten

Welche sensiblen Informationen werden im Rahmen Ihres Unternehmens gesammelt, verarbeitet und gespeichert? Wie viele Datensätze liegen jeweils vor?
Bitte Zutreffendes ankreuzen. **Mehrfach vorhandene Datensätze zu einer Person zählen „einfach“**.
Bitte berücksichtigen Sie Datensätze zu Kunden, Lieferanten, Dienstleistern und Mitarbeitern.

Personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Falls mehr als 1.000.000 Datensätze vorhanden, bitte um genaue Angabe.	☐ 0 Datensätze ☐ 1 – 20.000 Datensätze ☐ 20.001 – 100.000 Datensätze ☐ 100.001 – 500.000 Datensätze ☐ 500.001 – 1.000.000 Datensätze ☐ _____ Datensätze
davon besonders sensible Daten: Angaben über die ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben Falls mehr als 1.000.000 Datensätze vorhanden, bitte um genaue Angabe.	☐ 0 Datensätze ☐ 1 – 20.000 Datensätze ☐ 20.001 – 100.000 Datensätze ☐ 100.001 – 500.000 Datensätze ☐ 500.001 – 1.000.000 Datensätze ☐ _____ Datensätze

Bitte spezifizieren Sie die Art dieser besonders sensiblen Daten:

4 Umfang und Art der Kreditkartentransaktionen

Akzeptieren Sie Kreditkartenzahlungen? falls ja, bitte nachstehende Fragen beantworten:	☐ nein ☐ ja
Wie viele Kreditkartendaten (PCI-Daten) sammeln, speichern oder verarbeiten Sie? Falls mehr als 1.000.000 Datensätze vorhanden, bitte um genaue Angabe.	☐ 0 Datensätze ☐ 1 – 20.000 Datensätze ☐ 20.001 – 100.000 Datensätze ☐ 100.001 – 500.000 Datensätze ☐ 500.001 – 1.000.000 Datensätze ☐ _____ Datensätze

Wer verarbeitet und speichert die Kreditkartendaten?
☐ Dienstleister, und zwar:
☐ unser Unternehmen selbst

Falls Ihr Unternehmen selbst Kreditkartendaten verarbeitet, bitte nachstehende Fragen beantworten:

Finden die aktuell geltenden Payment Card Industry Data Security Standards (PCI DSS) bei Ihnen Anwendung?	☐ nein ☐ ja
Was für eine gültige PCI Compliance Zertifizierung haben Sie?	☐ Keine ☐ PCI-Level 1 ☐ PCI-Level 2 ☐ PCI-Level 3 ☐ PCI-Level 4

5 Umfang und Art der Auslagerung auf externe IT-Dienstleister und Cloud- Dienstleister

Nutzt Ihr Unternehmen Cloud-Dienste oder externe Rechenzentren?	☐ nein ☐ ja

Wenn „ja“, geben Sie nachfolgend bitte Namen und Sitz des Dienstleisters, sowie eine kurze Beschreibung von Art und Umfang des fremdvergebenen Arbeitsinhalts.

Risikoerfassung Cyber-Versicherung

Welche der oben aufgeführten Fremdleistungen sind geschäftskritisch, d.h. der Ausfall welcher Fremdleistung führt bei Ihnen zu einer Betriebsunterbrechung? *Bitte spezifizieren.*	
Haben Sie vertraglich vereinbart, dass permanent mindestens eine der folgenden Zertifizierungen vorzuhalten ist: Tier Level 3-4 oder ISO27001?	☐ nein ☐ ja
Gibt es einen geregelten Prozess bei der Auslagerung von IT-Dienstleistungen sowie Datenverarbeitung an externe Dienstleister und werden die geschlossenen Verträge durch die Rechtsabteilung, sowie durch die IT-Sicherheit geprüft und freigegeben?	☐ nein ☐ ja
Werden von ihrem Unternehmen Regressverzichtsvereinbarungen/Haftungsfreistellungen in den vertraglichen Vereinbarungen mit den Drittanbietern vereinbart?	☐ nein ☐ ja
Der Ausfall welchen Systems sehen Sie als Ihr größtes Risiko?	
6 Unternehmensorganisation und -führung zur Informations- und Datenverarbeitung sowie Krisenmanagement	
Ist eine Verantwortlichkeit für Cybersicherheit etabliert (z.B. CISO)?	☐ nein ☐ ja
Ist eine Datenschutzrichtlinie vorhanden?	☐ nein ☐ ja
Der physische Zutritt zu Servern in Ihrem Unternehmen ist eingeschränkt?	☐ nein ☐ ja
Ist ein vollständiges Verzeichnis der Verarbeitungstätigkeiten gemäß den anwendbaren Datenschutzgesetzen vorhanden?	☐ nein ☐ ja
Sind organisatorische Maßnahmen etabliert, um den Geschäftsbetrieb fortzuführen, falls die IT ausfällt (BCM)?	☐ nein ☐ ja
Existiert ein Notfallplan, der bei Störungen die Aufrechterhaltung bzw. den Wiederanlauf von betriebsnotwendigen Systemen festlegt und ist dieser auch bei einem IT-Ausfall verfügbar?	☐ nein ☐ ja
Wenn ja, umfasst dieser Plan folgende Elemente? IT- und Datenschutzvorfälle, Sofortmaßnahmen, Verantwortlichkeiten, Kontaktdaten für externe Unterstützung, einen Wiederanlaufplan.	☐ nein ☐ ja
Wird dieser Notfallplan regelmäßig überprüft und aktualisiert?	☐ nein ☐ ja
Führen Sie regelmäßig (mind. Jährlich) Desaster Recovery-Tests durch?	☐ nein ☐ ja
Führen Sie regelmäßig (mind. monatlich) Scans von außen auf Ihr Netzwerk durch, um unzulässige offene Ports und möglich Schwachstellen zu erkennen?	☐ nein ☐ ja
Gibt es einen Prozess zur Erkennung und Dokumetierung von Aufälligkeiten in internen Netzwerken, um Incidents frühzeitig zu erkennen? Hierzu gehört die Generierung, Speicherung (über mindestens 8 Wochen) und Auswertung von Logfiles.	☐ nein ☐ ja
Haben Sie Regeln zum sicheren Umgang mit der Unternehmens-IT für alle Benutzer verbindlich und schriftlich dokumentiert?	☐ nein ☐ ja
Haben Sie eine formelle Richtlinie zur Informationssicherheit entwickelt und implementiert, die unternehmensweit und dauerhaft für alle Mitarbeiter und relevante externe Dritte verfügbar ist?	☐ nein ☐ ja
Dürfen Mitarbeiter private Geräte für dienstliche Zwecke nutzen?	☐ nein ☐ ja
Falls Ja, gibt es eine dokumentierte BYOD-Policy und Sicherheitsvorkehrungen zur Erkennung von Schadsoftware auf den privaten Geräten bei Nutzung im Unternehmen?	☐ nein ☐ ja
Falls es mit nicht vom Unternehmen verwalteteten Geräten externen Zugriff auf interne Daten gibt, ist der Zugang so beschränkt, dass die Daten selbst nicht auf das Gerät übertragen werden, sondern nur eine Ansicht dargestellt wird? (z.B. Terminalserver-Lösung)	☐ nein ☐ ja
Haben Sie ein Mobile Device Management eingerichtet?	☐ nein ☐ ja
Sind auf allen mobilen Geräten gespeicherten, als intern klassifizierte Daten verschlüsselt?	☐ nein ☐ ja
Können alle mobilen Endgeräte remote gesperrt und gelöscht werden?	☐ nein ☐ ja

Risikoerfassung Cyber-Versicherung

7 Netzwerksicherheit und Patch-Management	
Verfügen Sie über aktuelle technische Schutzmaßnahmen gegen unbefugten Zugriff durch Firewalls und Virenscanner, die automatisch aktualisiert werden?	☐ nein ☐ ja
Ist erweiterte Antimalware und Antivirus mit heuristischer Analyse im Einsatz?	☐ nein ☐ ja
Sind Netzwerk- und/oder Host-Firewall-Regeln implementiert, die die Verwendung von RDP über das Internet zur Anmeldung an Arbeitsstationen verhindern?	☐ nein ☐ ja
Ist der Übergang zum Internet durch eine DMZ abgesichert?	☐ nein ☐ ja
Ist ein IDS (Intrusion Detection System) oder IPS (Intrusion Prevention System) im Einsatz?	☐ nein ☐ ja
Wird ein Security-Operations-Center betrieben?	☐ nein ☐ ja
Falls ja, ist dieses 24/7 verfügbar?	☐ nein ☐ ja
Wird ein EDR (Endpoint Detection and Reaction) eingesetzt?	☐ nein ☐ ja
Falls Ja, die Software welchen Herstellers nutzen Sie?	
Haben alle Arbeitsplatzrechner eine Sicherheitssoftware mit Verhaltenserkennung und Exploit-Mitigation aktiviert um verdächtige Aktivitäten aktiv zu blockieren?	☐ nein ☐ ja
Werden Sicherheitsprotokolle in einer SIEM-Lösung gesammelt und kontinuierlich analysiert?	☐ nein ☐ ja
Wird Netzwerkverkehr auf Anomalien und poteziell verdächtigen Datentransfer überwacht?	☐ nein ☐ ja
Haben Sie einen Patch-Management-Prozess umgesetzt, welcher das durchgehende und unverzügliche Aufspielen von Patches regelt und können Benutzer die Installation nur für einen bestimmten Zeitraum aufschieben?	☐ nein ☐ ja
In welchem Zeitraum werden Emergency-Security-Patches aufgespielt?	☐ innerhalb von mind. 3 Tagen ☐ innerhalb von mind. 7 Tagen ☐ innerhalb von mind. 14 Tagen ☐ innerhalb von mind. 29 Tagen
Werden Altsysteme betrieben? Dies sind alle Betriebssysteme und Anwendungsprogramme, bei denen der Hersteller den Support eingestellt hat und eine Aktualisierung auch durch Drittanbieter nicht mehr erfolgen kann (end-of-life/end-of-support). (z.B. Windows 7, Windows XP etc.)	☐ nein ☐ ja
Falls „ja“, werden alle Altsysteme ausschließlich in einer komplett isolierten Umgebung betrieben oder durch geeigente Maßnahmen vor Zugriffen von außen gesichert?	☐ nein ☐ ja
Werden alle Security-Tools, welche regelmäßig Updates von Definitionen erfordern mindestens täglich aktualisiert?	☐ nein ☐ ja
Wird eine Sicherheitsfunktion verwendet, um den Zugriff von allen Arbeitsplatzrechnern auf bekannte schädliche URLs jederzeit zu blockieren?	☐ nein ☐ ja
Scannt eine Sicherheitsfunktion alle E-Mails auf bekannte schädliche Anhänge und Links / URLs?	☐ nein ☐ ja
Gibt es ein Quarantäne-Service für verdächtige E-Mails?	☐ nein ☐ ja
Überprüfen und entschärfen Sie bei eingehenden E-Mails Anhänge in einer Sandbox?	☐ nein ☐ ja
Wird bei eingehenden E-Mails ein Sender Policy Framework (SPF) erzwungen?	☐ nein ☐ ja
Sind Microsoft Office-Makros standardmäßig deaktiviert?	☐ nein ☐ ja
Haben Sie einen Überblick über alle Admin-Accounts und einen Prozess zu deren Verwaltung etabliert?	☐ nein ☐ ja
Verwenden alle IT-Benutzer (inkl. aller Admin-Accounts) ausschließlich individuelle IT-Benutzerkonten?	☐ nein ☐ ja

Risikoerfassung Cyber-Versicherung

Werden Admin-Accounts ausschließlich getrennt von regulären Nutzeraccounts und nur für Admin-Tätigkiten genutzt?	☐ nein ☐ ja
Ist der Zugriff auf Admin-Accounts durch MFA geschützt?	☐ nein ☐ ja
Werden Konten mit permanenten IT-Administrativen Berechtigungen nicht für den Internetzugriff oder andere allgemeine Aufgaben genutzt?	☐ nein ☐ ja
Werden alle Zugriffsrechte für alle Mitarbeiter und Dienstleister etc. unverzüglich entzogen bzw. das Benutzerkonto gesperrt, sobald die besitzende Person das Unternehmen verlässt bzw. die Vertragsbeziehung endet?	☐ nein ☐ ja
Existiert eine Passwortrichtlinie, welche komplexe Anforderungen an Passwörter regelt und technisch erzwingt (z.B. mind. 8 Zeichen + Ziffern + Sonderzeichen)?	☐ nein ☐ ja
Gibt es für Admin-Accounts eine gesonderte Passwortrichtlinie	☐ nein ☐ ja
Sind Richtlinien gegen die Wiederverwendung von Passwörtern festgelegt und geschult?	☐ nein ☐ ja
Werden Erfolgs- und Fehlerereignisse bei der Anmeldung protokolliert, gespeichert und überwacht?	☐ nein ☐ ja
Sind ‚sofern vorhanden, alle Fernzugriffe technisch durch Multifaktor-Authentifizierung abgesichert, sodass ein nicht autorisierter Zugriff verhindert wird? (hierunter zählen z.B. auch Webmaileinrichtungen)	☐ nein ☐ ja
Wird bei Fernzugriffen eine VPN-Verbindung technisch erzwungen?	☐ nein ☐ ja
Werden Fernwartungszugänge zusätzlich z. B. separat freigeschaltet, zeitlich begrenzt bzw. überwacht?	☐ nein ☐ ja ☐ Keine Fernwartungszugänge vorhanden
Sind Maßnahmen implementiert, um nur zugelassene und registrierte Geräte im Netzwerk zu erlauben? (z.B. Network Access Control)	☐ nein ☐ ja
Ist der Zugriff auf Wechselmedien über USB-Ports technisch unterbunden oder eingeschränkt?	☐ nein ☐ ja
Ist das Netzwerk nach Schutzbedarf segmentiert?	☐ nein ☐ ja

8 Datenhaltung und Back-Up	
Verfügen Sie über eine Übersicht aller im Unternehmen eingesetzter Soft- und Hardware?	☐ nein ☐ ja
Ist ein Datenschutzbeauftragter bestellt?	☐ nein ☐ ja
Gibt es in Ihrem Unternehmen ein Verzeichnis von Verarbeitungstätigkeiten im Sinne der DSGVO?	☐ nein ☐ ja
Gibt es in Ihrem Unternehmen Maßnahmen zum sicheren Löschen von Daten im Sinne der DSGVO?	☐ nein ☐ ja
Führen Sie eine mind. werktägliche Datensicherung Ihrer Systeme und Daten durch?	☐ nein ☐ ja Sondern:
Werden Back-Ups für mind. 6 Monate vorgehalten?	☐ nein ☐ ja

Risikoerfassung Cyber-Versicherung

Werden Sicherungsdatenträger so aufbewahrt, dass sie auf einem externen, von den sonstigen informationsverarbeitenden Systemen getrennten Medium sind? (in der Regel Offline-Datensicherung z.B. auf seperatem Medium oder Cloud-Backup mit MFA-Absicherung)	☐ nein ☐ ja
Wie und in welchem Turnus werden regelmäßige Wiederherstellungstests durchgeführt?	
Sind die Back-Up-Systeme vom Actice Directory getrennt?	☐ nein ☐ ja
Erfolgt grundsätzlich eine Verschlüsselung von sensiblen Daten, die auf Laptops und anderen mobilen Geräten gespeichert werden?	☐ nein ☐ ja
Wird unbefugter Zugriff auf personbezogene oder andere kritische Daten durch eine eingeschränkte Berechtigung ggf. zusätzlich durch Verschlüsselung verhindert?	☐ nein ☐ ja
Werden vergebene Berechtigungen regelmäßig überprüft?	☐ nein ☐ ja
9 Art und Umfang der Produktions-IT (sofern vorhanden)	
Werden Bereiche der Produktion durch eine automatisierte Prozesssteuerung betrieben oder unterstützt?	☐ nein ☐ ja
Ist eine Sicherheitspolitik formuliert und ein Sicherheitsmanagement etabliert?	☐ nein ☐ ja
Sind im Produktionsbereich Sicherheitszonen und -perimeter etabliert?	☐ nein ☐ ja
Gibt es Fernwartungszugänge durch Dritte in den Produktionsbereichen? Falls ja, werden diese Zugänge mittels MFA abgesichert?	☐ nein ☐ ja ☐ nein ☐ ja
Gibt es Fernzugriffe durch Ihre Mitarbeiter auf Ihre OT-Anlagen? Falls ja, werden diese Zugänge mittels MFA abgesichert?	☐ nein ☐ ja ☐ nein ☐ ja
Sind Ihre OT-Anlagen vom Internet segmentiert?	☐ nein ☐ ja
Werden, sofern vorhanden, Schutzmaßnahmen wie EDR und SOC auch auf die Produktionsumgebung angewendet?	☐ nein ☐ ja
10 Betrugsprävention	
Ist bei Banküberweisungen ab einem Betrag von 10.000 EURO ein 4-Augen-Prinzip vorgeschrieben?	☐ nein ☐ ja
Führen Sie für Ihre Mitarbeiter regelmäßig (mind. jährlich) verpflichtende Maßnahmen zur Awareness im Umgang mit Internet, IT und Daten durch?	☐ nein ☐ ja
Müssen Mitarbeiter mind. jährlich ein (Web-based) Training zu Cyber-Sicherheit absolvieren?	☐ nein ☐ ja
Führen Sie regelmäßig Phishing-Simulationen durch?	☐ nein ☐ ja
Werden E-Mails von außerhalb der Organisation auch als solche gekennzeichnet?	☐ nein ☐ ja
11 Schaden	
Kam es in den letzten fünf Jahren im Zusammenhang mit einem Cyber- oder Datenschutz-Vorfall im Unternehmen zu • der Einleitung einer Klage, eines Auskunfts- oder Ermittlungsverfahrens durch eine Aufsichtsbehörde oder öffentliche Stelle, • der Geltendmachung eines Schadenersatzanspruches durch einen Dritten, • finanziellen Verlusten (Computerbetrug)?	☐ nein ☐ ja
Ist Ihnen ferner ein Umstand bekannt, der Sie ein Eintreten dieser Fälle vermuten lässt?	☐ nein ☐ ja
Kam es in den letzten fünf Jahren in Ihrem Unternehmen zu einer Netzwerksicherheitsverletzung?	☐ nein ☐ ja
Wenn „Ja“, bitte jeweils Beschreibung der Vorfälle auf einem Beiblatt inkl. Schadenhöhe und lessons learned.	

Risikoerfassung Cyber-Versicherung

Weitere Unterlagen
Falls vorhanden bitte folgende Dokumente beifügen: - Organigramm - Notfallplan - Umsatzallokation

Wichtig: Bitte beantworten Sie die Fragen vollständig und richtig, sonst ist der Versicherungsschutz gefährdet. Dieser ausgefüllte Fragebogen, sowie eventuelle Anlagen werden bei Abschluss eines Vertrages Grundlage und Bestandteil des Versicherungsvertrages. Die Risikoangaben sind vorvertragliche Anzeigen. Hinsichtlich der Folgen bei der Verletzung vorvertraglicher Anzeigepflichten verweisen wir auf die Regelung des Versicherungsvertragsgesetzes (§19 VVG).
Mit Ihrer Unterschrift bestätigen Sie, dass vorstehende Angaben vollständig und richtig sind.

_____	_____	_____
(Ort)	(Datum)	*(Unterschrift Unternehmensrepräsentant)*