Cyber-Check

Versicherungsnehmer

Name und Adresse

Weitere mitversicherte Gesellschaften (inkl. ausländische Gesellschaften/Niederlassungen)

Telefon | Homepage | E-Mail

1 Vorvertragliche Situation

1.1 Derzeitiger Versicherer | VS-Nr.

Gekündigt? ☐ Nein ☐ Ja, durch

1.2 Schadenverlauf der letzten fünf Jahre (auch nicht versicherte Vorfälle – unabhängig von einer bestehenden Vorversicherung)

Jahr	Art	ggf. Zahlungen	ggf. Reserven

2 Betriebsbeschreibung des Unternehmens/Branche (inkl. der weiteren Gesellschaften/Niederlassungen)

3 Allgemeine Informationen

3.1

	Jahresumsatz im letzten Geschäftsjahr	davon Online-Handel
Gesamt		
davon Deutschland		
davon USA/Kanada		
davon übriges Ausland		

3.2 Wie hoch ist die Anzahl Ihrer Mitarbeiter? Insgesamt | In der IT

3.3 Wie hoch sind Ihre jährlichen Ausgaben? Für die IT EUR | Für die IT-Sicherheit EUR

3.4 Haben Sie eine Zertifizierung (wie ISO 27001, ISIS 12, VDS 10000er, IT-Grundschutz (BSI), etc.)? ☐ Ja ☐ Nein

Wenn ja, welche?

Fragen zu Schutzmaßnahmen

4 Zugangssicherung

4.1	Ist für den Zugang zu jedem System eine benutzerindividuelle Kennung/Zugang mit Passwort vergeben?	☐ Ja	☐ Nein
4.2	Haben Sie Mindestanforderungen an die Passwortqualität sämtlicher Mitarbeiter und Systeme?	☐ Ja	☐ Nein
	Wenn ja, werden diese technisch erzwungen?	☐ Ja	☐ Nein
4.3	Sind administrative Zugänge ausschließlich Administratoren und ausschließlich zur Erledigung administrativer Tätigkeiten vorbehalten?	☐ Ja	☐ Nein
4.4	Werden Zugänge für Ihre IT-Infrastruktur konsequent nur gewährt, wenn sie für die Aufgabenerfüllung notwendig sind?	☐ Ja	☐ Nein
4.5	Werden administrative Zugänge regelmäßig nach einem festgelegten Turnus auf deren Notwendigkeit überprüft?	☐ Ja	☐ Nein
4.6	Haben Sie Geräte, die über das Internet erreichbar oder im mobilen Einsatz sind, mit einem zusätzlichen Schutz vor unberechtigtem Zugriff versehen?	☐ Ja	☐ Nein

5 Datensicherung

5.1	Schützen Sie sich vor dem Verlust der wichtigsten Unternehmensdaten durch eine mindestens wöchentliche Datensicherung?	☐ Ja	☐ Nein
5.2	Werden Ihre Datensicherungsmedien physisch getrennt von den gesicherten Systemen aufbewahrt?	☐ Ja	☐ Nein
5.3	Werden der unberechtigte Zugriff auf die Datensicherungen sowie deren nachträgliche Manipulation durch technische Maßnahmen (z. B. Verschlüsselung) verhindert?	☐ Ja	☐ Nein
5.4	Stellen Sie durch regelmäßige Tests nach einem festgelegten Turnus sicher, dass Ihre Datensicherung und -wiederherstellung funktionieren?	☐ Ja	☐ Nein

6 Sicherheitsupdates und Schutz vor Schadsoftware

6.1	Stellen Sie sicher, dass alle Systeme auf aktuellem Stand sind und installieren Sie Sicherheitsupdates automatisch oder zeitnah (Patch-Management)?	☐ Ja	☐ Nein
6.2	Wird die Installation von Sicherheits-Patches für Ihre IT zentral gesteuert?	☐ Ja	☐ Nein
6.3	Verfügen alle informationsverarbeitenden Systeme über einen Schutz gegen Schadsoftware, der automatisch auf dem aktuellen Stand gehalten wird (z. B. Virenscanner, Code Signing, Application Firewall oder ähnlich wirksame Maßnahmen)?	☐ Ja	☐ Nein

7 Verantwortlichkeiten

7.1	Gibt es einen Verantwortlichen für die IT-Sicherheit?	☐ Ja	☐ Nein
7.2	Gibt es einen Verantwortlichen für die Einhaltung datenschutzrechtlicher Vorgaben?	☐ Ja	☐ Nein
7.3	Werden alle internen und externen Mitarbeiter über Maßnahmen zur Informationssicherheit geschult?	☐ Ja	☐ Nein
	Wenn ja, wie häufig? ☐ Einmalig ☐ Regelmäßig		
7.4	Besteht ein IT-Notfall- und -Wiederanlauf-Konzept?	☐ Ja	☐ Nein
	Wenn ja, ist dieses schriftlich fixiert und benennt es Verantwortliche?	☐ Ja	☐ Nein

8 Schutzmaßnahmen

8.1	Erfolgt der Zugriff auf Ihre interne IT-Infrastruktur über öffentliche oder drahtlose Netze ausschließlich verschlüsselt?	☐ Ja	☐ Nein
8.2	Ist Ihr IT-Netzwerk nach Kritikalität (Wichtigkeit) der Systeme in unterschiedliche Zonen aufgeteilt?	☐ Ja	☐ Nein
8.3	Werden sensible Daten (z.B. personenbezogene Daten und Geschäftsgeheimnisse) bei Datenversand verschlüsselt?	☐ Ja	☐ Nein
8.4	Führen Sie für besonders wichtige/notwendige (kritische) IT-Systeme regelmäßig Risikoanalysen nach einem festgelegten Turnus durch?	☐ Ja	☐ Nein
8.5	Werden Security Audits, Schwachstellenanalysen (vulnerability assessment) und/oder Penetrationstests durchgeführt?	☐ Ja	☐ Nein
	Wenn ja, in welchem Umfang?		

9 Datenverarbeitung

9.1	Verarbeiten Sie Daten, die besonderen gesetzlichen Verschwiegenheitspflichten unterliegen, wie z. B. Gesundheitsdaten?	☐ Ja	☐ Nein
	Wenn ja, welche?		
9.2	Verarbeiten oder speichern Sie Geschäftsgeheimnisse von Dritten?	☐ Ja	☐ Nein
9.3	Verarbeiten oder speichern Sie Finanz- oder Steuerdaten von Dritten?	☐ Ja	☐ Nein
9.4	Sind Sie im Bereich der Datenauftragsverarbeitung tätig?	☐ Ja	☐ Nein
	Wenn ja, in welchem Umfang?		

10 E-Commerce

10.1	Betreiben Sie einen eigenen E-Commerce Online-Handel (eCommerce)?	☐ Ja	☐ Nein

Wenn ja:

10.1.1	Wird der Webshop selbstständig administriert und betrieben?	☐ Ja	☐ Nein
10.1.2	Speichern Sie Kreditkartendaten?	☐ Ja	☐ Nein
	Wenn ja, wie viele?		
10.1.3	Nutzen Sie einen Payment-Dienstleister zu Abwicklung aller eingehenden bargeldlosen Zahlungsvorgänge?	☐ Ja	☐ Nein
10.1.4	Unterliegen Sie den Anforderungen der Payment Card Industry (PCI) und dem Data Security Service (DSS)?	☐ Ja	☐ Nein

11 Dienstleister

11.1	Arbeiten Sie mit externen Dienstleistern zusammen, die mit Ihrem Netzwerk verbunden sind oder die Daten in Ihrem Auftrag verarbeiten oder erhalten?	☐ Ja	☐ Nein

Wenn ja:

11.1.1	Der Dienstleister ist in folgenden Bereichen für uns tätig:		
	Dienstleister		
	Dienstleistung		
11.1.2	Existiert ein Dienstleistungsvertrag, in dem Verfügbarkeit, Updates und das Beheben von Sicherheitslücken geregelt sind?	☐ Ja	☐ Nein
11.1.3	Ist Ihr Dienstleister zertifiziert?	☐ Ja	☐ Nein
11.1.4	Unternehmen Sie regelmäßig eine unabhängige Qualitätssicherung?	☐ Ja	☐ Nein
11.1.5	Haben Sie Ihren Dienstleister von der Haftung freigestellt?	☐ Ja	☐ Nein
	Wenn ja, in welchen Fällen?		
11.1.6	Unterliegt Ihr Dienstleister dem einheitlichen Datenschutzrecht der Europäischen Union?	☐ Ja	☐ Nein

12 Nutzung privater Geräte

12.1	Ist die Nutzung privater Geräte in Ihrer Unternehmens-IT gestattet?	☐ Ja	☐ Nein

Wenn ja:

12.1.1	Befinden sich die privaten Geräte in einem getrennten Netzwerk-Segment?	☐ Ja	☐ Nein
12.1.2	Haben die privaten Geräte Zugriff auf geschäftliche Dienste oder Infrastruktur?	☐ Ja	☐ Nein

13 Automatisierte Produktionssysteme (ICS)

13.1	Nutzen Sie automatisierte Produktionssysteme (ICS)?	☐ Ja	☐ Nein

Wenn ja:

13.1.1	Befinden sich die IC-Systeme in einem separierten Netzwerk mit eingeschränkten Zugriffsmöglichkeiten?	☐ Ja	☐ Nein
13.1.2	Ist ein Fernzugriff auf die IC-Systeme nur mittels 2-Faktor-Authentifizierung möglich?	☐ Ja	☐ Nein
13.1.3	Wird für Systeme, die an ICS beteiligt sind, insbesondere auch Terminals, die Einhaltung besonderer Härtungsmaßnahmen sichergestellt?	☐ Ja	☐ Nein
13.1.4	Sind die Prozesse zum regelmäßigen und unplanmäßigen Einspielen von Sicherheitsupdates dokumentiert und erprobt?	☐ Ja	☐ Nein
13.1.5	Wird der Zugriff auf IC-Systeme an zentraler Stelle protokolliert und überwacht?	☐ Ja	☐ Nein
13.1.6	Sind Ihre mobilen an dem ICS beteiligten Geräte vor unberechtigtem Zugriff durch Verschlüsselung und Passwörter geschützt?	☐ Ja	☐ Nein
13.1.7	Erfolgt der Fernzugriff auf IC-Systeme ausschließlich auf verschlüsseltem Weg?	☐ Ja	☐ Nein
13.1.8	Werden Ihre Datensicherungsmedien physisch getrennt von den gesicherten Systemen aufbewahrt?	☐ Ja	☐ Nein
13.1.9	Sind die Prozesse zur Wiederherstellung eines betriebsbereiten Zustandes dokumentiert und werden sie regelmäßig erprobt?	☐ Ja	☐ Nein
13.1.10	Stellen Sie durch regelmäßige Tests nach einem festgelegten Turnus sicher, dass Ihre Datensicherung und -wiederherstellung funktioniert?	☐ Ja	☐ Nein
13.1.11	Ist die Nutzung privater Geräte im ICS-Segment gestattet?	☐ Ja	☐ Nein

14 Gewünschter Versicherungsschutz

Sie können für jeden Hauptbaustein eine Versicherungssummenbegenzung individuell wählen. Die höchste Versicherungssummenbegrenzung entspricht der Versicherungssumme.

14.1 Cyber Kostenpositionen*

- ☐ 50.000 EUR
- ☐ 100.000 EUR
- ☐ 250.000 EUR
- ☐ 500.000 EUR
- ☐ 750.000 EUR
- ☐ 1.000.000 EUR
- ☐ 1.500.000 EUR
- ☐ Andere

14.2 Cyber Drittschadendeckung*

- ☐ 50.000 EUR
- ☐ 100.000 EUR
- ☐ 250.000 EUR
- ☐ 500.000 EUR
- ☐ 750.000 EUR
- ☐ 1.000.000 EUR
- ☐ 1.500.000 EUR
- ☐ Andere

14.3 Cyber Eigenschadendeckung*

- ☐ 50.000 EUR
- ☐ 100.000 EUR
- ☐ 250.000 EUR
- ☐ 500.000 EUR
- ☐ 750.000 EUR
- ☐ 1.000.000 EUR
- ☐ 1.500.000 EUR
- ☐ Andere

14.4 Selbstbehalt

- ☐ Selbstbehalt 500 EUR
- ☐ Selbstbehalt 1.000 EUR
- ☐ Selbstbehalt 2.500 EUR
- ☐ Andere

Der Selbstbehalt findet keine Anwendung für Abwehrkosten im Rahmen der Drittschadendeckung (Teil C AVB Cyber) und für forensische Untersuchungen (Teil B Ziffer 1 AVB Cyber).

14.5 Zeitlicher Selbstbehalt

- ☐ Selbstbehalt 6 Stunden
- ☐ Selbstbehalt 12 Stunden
- ☐ Selbstbehalt 24 Stunden
- ☐ Andere

14.6 ☐ Betriebsunterbrechung durch Ausfall des Dienstleisters mit 100.000 EUR (50.000 EUR beim Schutzbrief)*

14.7 ☐ Betriebsunterbrechung durch technische Probleme mit 100.000 EUR (50.000 EUR beim Schutzbrief)*

14.8 ☐ Cyber-Betrug mit 100.000 EUR (50.000 EUR beim Schutzbrief)*

Sofern gewünscht:

Bei Überweisungen über 10.000 EUR besteht ein verpflichtendes 4-Augenprinzip. Ebenso werden Mitarbeiter mit Überweisungsvollmacht mindestens halbjährlich zur Erkennung und Vermeidung von Betrugsmaschen, wie CEO-Fraud und Lieferanten-Betrug sensibilisiert. ☐ Ja ☐ Nein

*Versicherungssummenbegrenzung je Versicherungsfall und -jahr

Ort und Datum

Unterschrift