württembergische

Fragebogen

Die Cyber-Police.
Das Plus für mehr Datensicherheit.

Versicherungsnehmer/Interessent

Interessent/Gesprächspartner	Vermittler-Nr.
Straße und Hausnummer	Vermittler – Name/Gesprächspartner
PLZ, Ort	Versicherungsschein-Nr,
Telefon/Fax	Kunden-Nr.
E-Mail	Homepage

1. Allgemeine Unternehmensinformationen

Nennen Sie die konkrete Firmierung aller zu versichernden Unternehmen:

Beschreiben Sie kurz Ihre Geschäftstätigkeit und die einzelnen Geschäftsbereiche:

Nennen und beschreiben Sie die Top-3-Arten von Daten (bspw. Gesundheits-, Adress-, Zahlungs-, Buchhaltungs-, Konstruktions- oder Kalkulationsdaten):

1. _____

2. _____

3. _____

Gesamtumsatz des letzten Geschäftsjahres

Umsatz gesamt in EUR _____

davon USA/Kanada in EUR _____

Gewünschte Versicherungssumme in EUR

☐ 125.000 ☐ 1.000.000
☐ 250.000 ☐ 2.000.000
☐ 500.000

Anzahl der Beschäftigten: _____

2. Elektronischer Zahlungsverkehr

Wie hoch ist der Umsatzanteil des Online-Handels (E-Commerce)? _____ %

Erfüllt Ihr Unternehmen die Vorgaben des Payment Card Industry Data Security Standards (PCI-Standard)? ☐ ja ☐ nein
Bitte fügen Sie das aktuelle Zertifikat über die PCI-Compliance Ihres Unternehmens bei.

Händlerkategorie Ihres Unternehmens nach PCI-Standard ist ☐ Level 1 ☐ Level 2 ☐ Level 3 ☐ Level 4

Werden Bank- oder Kreditkartendaten in Ihrem Netzwerk gespeichert?
☐ ja (verschlüsselt)
☐ ja (unverschlüsselt)
☐ nein

3. Ausgelagerte IT-Prozesse/Externe IT-Dienstleister

Werden in Ihrem Unternehmen IT-Prozesse ausgelagert/an externe IT-Dienstleister gegeben? ☐ ja ☐ nein

Wenn ja, welche Prozesse und an wen?

1. _____

2. _____

3. _____

Existiert eine Vereinbarung über die Freistellung der externen IT-Dienstleister gegen Schadenersatzansprüche? ☐ ja ☐ nein
Wenn ja, bitte Kopie der Freistellungsvereinbarung/des Dienstleistungsvertrags beifügen.

4. Risiko-Bewertung

Ab wann führt eine Nichtverfügbarkeit von Daten bzw. IT-Systemen zu signifikanten Ausfällen? Daten: _____ Tage

IT-Systeme: _____ Tage

Verarbeiten Sie Daten Dritter im Rahmen von Auftragsdatenverarbeitung oder Funktionsübertragung? ☐ ja ☐ nein

Wenn ja, wie hoch ist der Umsatzanteil? ☐ < 20 % ☐ 20% – 50% ☐ > 50 %

Welche Anzahl personenbezogener Datensätze (z. B. Adressdaten) ist in Ihren IT-Systemen gespeichert? Anzahl: _____

Verarbeiten Sie außerhalb der Lohnbuchhaltung Daten im Sinne des BDSG § 3 Abs. 9? ☐ ja ☐ nein
Hierunter fallen Angaben über Gesundheit, rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit oder Sexualleben.

Vertreiben Sie Waren und/oder Dienstleistungen über Webanwendungen? ☐ ja ☐ nein

Wenn ja, über
- ☐ kommerziellen Plattform-Anbieter (z. B. Amazon Marketplace, ebay)
- ☐ kommerziellen Webseiten-Hoster (z. B. Strato, 1&1, Hetzner-Online)
- ☐ eigene, selbstbetreute Server auf Basis
  - ☐ kommerzieller Webshop-Software
  - ☐ freier Webshop-Software
  - ☐ eines selbst entwickelten Webshops (bspw. über IT-Dienstleister)

Überprüfen Sie die rechtliche Zulässigkeit der Veröffentlichung von digitalen Medieninhalten? ☐ ja ☐ nein

Nutzen Sie Betriebssysteme (auch auf Servern) die vom Hersteller nicht mehr gewartet oder unterstützt werden? ☐ ja ☐ nein

5. Organisatorische Aspekte von IT-Sicherheit und Datenschutz

Gibt es einen Datenschutzbeauftragten für Ihr Unternehmen (auch extern)? ☐ ja ☐ nein

Existieren schriftliche Datenschutzrichtlinien in Ihrem Unternehmen? ☐ ja ☐ nein

Gibt es einen Verantwortlichen für organisatorische und präventive IT-Sicherheit? ☐ ja ☐ nein

Sind alle internen und externen Mitarbeiter hinsichtlich der vorgegebenen internen Richtlinien/Anweisungen informiert und verpflichtet? ☐ ja ☐ nein

Dürfen Mitarbeiter mit privaten Systemen auf Daten und IT-Systeme des Unternehmens zugreifen? ☐ ja ☐ nein

Dürfen Mitarbeiter eigenständig Software installieren? ☐ ja ☐ nein

Dürfen Mitarbeiter nicht firmeneigene Datenträger (z.B. USB-Sticks) an Firmenhardware anschließen? ☐ ja ☐ nein

Verwenden Sie ein Web-Filtersystem (Zugriffsbeschränkungen im Internet)? ☐ ja ☐ nein

6. Präventive Maßnahmen

Ist für jeden Nutzer und Administrator ein(e) benutzerindividuelle(r) Kennung/Zugang vergeben? ☐ ja ☐ nein

Ist für jeden Nutzer und Administrator ein benutzerindividuelles Passwort vergeben? ☐ ja ☐ nein

Vorgegebenes Änderungsintervall _____ Wochen (nach Ablauf erfordert Zugang ein neues Passwort)

Wie viele Personen haben Administratorenrechte? Anzahl: _____

Wird der benutzerindividuelle Zugang beim Ausscheiden eines Mitarbeiters gesperrt? ☐ ja ☐ nein

Welche mobilen Geräte werden genutzt? (Bitte Zutreffendes ankreuzen)	Welche Maßnahmen existieren für die angegebenen Geräte? Zugriffsschutz/Passwort	Verschlüsselung	Option Fernlöschung
☐ Laptops	☐	☐	☐
☐ Tablets	☐	☐	☐
☐ Smartphones	☐	☐	☐
☐ Externe Festplatten (auch Back-up-Medien)	☐	☐	
☐ USB-Sticks	☐	☐	
☐ DVDs	☐	☐	
☐ Keine mobilen Geräte	☐	☐	

Nutzen Sie eine Antivirensoftware und ist die automatische Update-Funktion aktiviert? ☐ ja ☐ nein

Nutzen Sie zusätzlich zu Ihrem Internet-Zugangs-Router (z. B. DSL-Router) ein weiteres Gerät als Firewall? ☐ ja ☐ nein

Werden sensible Daten (z. B. personenbezogene Daten) bei Datenversand verschlüsselt? ☐ ja ☐ nein

Sofern Sie WLAN nutzen, haben Sie hierfür mindestens eine WPA2-Verschlüsselung eingerichtet? ☐ ja ☐ nein ☐ keine WLAN-Nutzung

Gibt es physische Zutrittsbeschränkungen zu Ihren Servern? ☐ ja ☐ nein

Ist sichergestellt, dass Sicherheitspatches unverzüglich installiert werden? ☐ ja ☐ nein

Erfolgt die Installation zentral über das gesamte IT-System (durch Softwareverteilung)? ☐ ja ☐ nein

Gibt es Vorgaben zur sicheren Entsorgung von Papier, Datenträgern (z. B. Festplatten, USB-Sticks) etc.? ☐ ja ☐ nein
Wenn ja, welche? Bitte erläutern Sie.

Wie häufig sichern Sie Ihre Daten?

Teilsicherung (nur die seit letzter Sicherung geänderten Dateien) ☐ täglich ☐ wöchentlich ☐ _____

Vollsicherung (alle Dateien) ☐ täglich ☐ wöchentlich ☐ _____

Anzahl der verfügbaren Sicherungsgenerationen? Anzahl: _____

Erfolgt eine zentrale Datensicherung? ☐ ja ☐ nein

Wie oft wird die Verwendbarkeit der Datensicherung getestet? ☐ mindestens halbjährlicher Turnus ☐ nie ☐ mindestens jährlicher Turnus ☐ _____

Die Auslagerung der Datensicherung erfolgt ☐ in einem Datensicherungsschrank ☐ an einem anderen Ort ☐ in einem anderen Raum im selben Gebäude

Ist ein schriftlich fixiertes IT-Notfall-/Wiederanlaufkonzept vorhanden? ☐ ja ☐ nein

7. Produktionsmaschinen (nur auszufüllen, falls Produktionsmaschinen im Einsatz sind)

Nutzen Sie auf Produktionsanlagen Betriebssysteme, die vom Hersteller nicht mehr gewartet oder unterstützt werden (z. B. Windows XP)?	☐ ja	☐ nein
Die Steuerungssysteme von Produktionsanlagen befinden sich in einem eigenen, vollständig separierten Netzwerk?	☐ ja	☐ nein
Ein Fernzugriff auf die Steuerungssysteme von Produktionsanlagen ist ausschließlich mittels 2-Faktor-Authentifizierung möglich?	☐ ja	☐ nein
Der Fernzugriff auf Steuerungssysteme von Produktionsanlagen erfolgt ausschließlich auf verschlüsseltem Weg?	☐ ja	☐ nein

8. Vorversicherung/Vorschäden/Bisherige Vorfälle

Bestand oder besteht eine Vorversicherung gegen Cyber-Gefahren? ☐ ja ☐ nein

Wenn ja, bitte geben Sie an:

Versicherer _____ Versicherungsschein-Nr. _____ Gekündigt durch ☐ VN ☐ Versicherer

Kam es infolge oder aufgrund eines Angriffs auf das IT-System Ihres Unternehmens oder im Online-Banking in den letzten 5 Jahren zu ☐ ja ☐ nein

– einem Datenverlust?
– einem Datendiebstahl?
– einer Datenveränderung?
– einer Unterbrechung des Betriebsablaufs?
– einem Ausfall des IT-Systems?

Wenn ja, bitte erläutern Sie den Hergang des Vorfalls und welche Maßnahmen danach ergriffen wurden.

Hat eine Aufsichts- oder Justizbehörde in den letzten 5 Jahren gegen Ihr Unternehmen wegen des Vorwurfs einer Datenschutzverletzung eine Untersuchung eingeleitet oder Ihr Unternehmen gebeten, Informationen und/oder Daten zur Verfügung zu stellen? ☐ ja ☐ nein

Wenn ja, bitte erläutern Sie.

Hat Ihr Unternehmen in den letzten 5 Jahren eine Beschwerde von Kunden, Mitarbeitern und/oder externen Dienstleistern wegen der Verletzung von personenbezogenen oder vertraulichen Informationen und/oder Daten erhalten? ☐ ja ☐ nein

Wurde bislang ein Schadenersatzanspruch gegen Sie aufgrund eines Datenmissbrauchs erhoben?

Wenn ja, bitte erläutern Sie.

Ort, Datum	Unterschrift des Antragstellers/Versicherungsnehmers

Bitte verwenden Sie ggf. ein Beiblatt, sollte der Platz für Ihre Antworten hier nicht ausreichen.

Hinweise zur IT-Sicherheit

Ein angemessenes IT-Sicherheitskonzept ist die Voraussetzung für eine wirksame Reduzierung der Gefahr von Störungen des betrieblichen Ablaufs. Für die Absicherung des Restrisikos haben Sie über die Cyber-Police einen exzellenten Versicherungsschutz. Um die Gefahr einer Betriebsstörung von vornherein zu reduzieren, empfehlen wir Ihnen untenstehende Maßnahmen und zusätzlich die Einschaltung eines qualifizierten IT-Dienstleisters:

Organisatorische Maßnahmen

- Datensicherheit ist Chefsache.
- IT-Risiken müssen klar kommuniziert werden. Sensibilisieren Sie Ihre Mitarbeiter.
- Verwenden Sie für jeden Nutzer und Administrator benutzerindividuelle, ablaufende Passwörter. Schützen Sie auch Ihre Daten auf mobilen Geräten mit einem Passwort. Sperren Sie Rechner und mobile Geräte bei Inaktivität automatisch.
- Datenschutz: Achten Sie auf die sichere Entsorgung von Papier und Datenträgern (Festplatten, USB-Sticks etc.).

Präventive Maßnahmen

- Öffentliche WLAN-Netze sind unsicher. Geben Sie keine vertraulichen Daten wie Passwörter und Kontodaten ein, solange Sie einen öffentlichen Netzwerkzugang nutzen.
- Schützen Sie Ihren Server im Idealfall durch eine physische Zutrittsbeschränkung zum Server-Raum.
- Prüfen Sie, ob Sie digitale Medieninhalte (beispielsweise Bilder) veröffentlichen dürfen.

Absicherung des IT-Netzwerkes

- Schützen Sie Ihren elektronischen Firmenzugang durch eine für Ihr Unternehmen geeignete Firewall, durch VPN-Zugänge oder ähnliches. Im Idealfall als eigenständige Hardware-Firewall, die nicht im DSL-Router integriert ist.
- Richten Sie für Ihr WLAN mindestens eine WPA2-Verschlüsselung ein

Umgang mit mobilen Geräten

- Schalten Sie bei mobilen Geräten (Smartphone, Tablet, Laptop etc.) die Bluetooth- oder WLAN-Funktion Ihres Endgerätes nur ein, wenn Sie diese bewusst zur Kommunikation einsetzen.
- Schließen Sie keine USB-Sticks, SD-Karten und andere Speichermedien von nicht vertrauenswürdigen Quellen an einen Rechner an.

Schutz vor Schadsoftware

- Verwenden und aktualisieren Sie regelmäßig Ihre Antivirensoftware. Lassen Sie den Virenscanner im Hintergrund laufen. Dateien werden so bei Zugriff gescannt.
- Verwenden Sie Software und Links nur aus vertrauenswürdigen Quellen. Gehen Sie mit Downloads von Programmen, Bildschirmschonern und Daten-Dateien aus dem Internet sorgsam um. Sie können Trojaner und Viren enthalten.
- Übernehmen Sie sicherheitsrelevante Patches der Softwarehersteller über die automatische Updatefunktion.

Sicherung der Daten

- Sichern Sie mindestens einmal wöchentlich auf einem separaten Datenträger. Überschreiben Sie die wöchentliche Datensicherung frühestens nach vier Wochen.
- Um zusätzliche Sicherheit zu gewährleisten, sollte darüber hinaus je Quartal mindestens eine Sicherung auf einem separaten Datenträger durchgeführt werden. Überschreiben Sie die längerfristige Datensicherung frühestens nach vier Quartalen.
- Die Sicherungsdatenträger müssen eindeutig gekennzeichnet sein und der Zeitpunkt der Datensicherung nachvollziehbar dokumentiert werden.
- Die Sicherungsdatenträger sollten mit einem Passwort geschützt werden. Die Sicherungsdatenträger sollten nur zur Datensicherung mit dem Netzwerk verbunden werden und ansonsten vom Netzwerk getrennt sein.
- Testen Sie den Notfall: Können die gesicherten Daten auch wieder auf die Anlage zurückgespielt werden?
- Lagern Sie Ihre Sicherungsdatenträger in einem anderen Gebäude oder in einem geeigneten Datensicherungsschrank.

Bitte beachten Sie, dass dieser Maßnahmenkatalog keinen Anspruch auf Vollständigkeit oder Allgemeingültigkeit erhebt. Die Einhaltung dieser Maßnahmen verringert zwar die Möglichkeit einer Störung Ihres IT-Systems, völlig ausschließen lässt sich diese Gefahr jedoch nicht.

! Erst ein mit Ihrem qualifizierten IT-Dienstleister erstelltes Sicherheitskonzept bietet Ihnen in Verbindung mit unserer Cyber-Police den maximalen Schutz vor wirtschaftlichen Nachteilen bei einem Cyber-Vorfall.