Bitte per Telefax oder E-Mail an Hiscox
Fax-Nr.: 089/54 58 01-199
E-Mail: hiscox.underwriting@hiscox.de

Hiscox
Cyber Zusatzfragebogen

I. Zusatzfragen Kreditkartendaten

Nur zu beantworten, wenn Sie Frage I.5.1. des Cyber Fragebogens mit „Ja“ beantwortet haben.

1. Speichern, verarbeiten oder übermitteln Sie selbst Kreditkartendaten? ☐ Ja ☐ Nein

   Wenn **nein**, an welchen Payment Service Provider haben Sie den Zahlungsprozess ausgelagert? _____

2. Über welche Wege akzeptieren Sie Kreditkartendaten? **(Zutreffendes bitte ankreuzen)**

   ☐ Bestellung über Brief, Telefax oder Telefon (Mail Order, Telephone Order - MOTO)
   ☐ E-Commerce (Online)
   ☐ Physische Kartenzahlung vor Ort (Point of Sale - PoS)

3. Welche Art der Validierung nutzt Ihr Unternehmen, um den Payment Card Industry Data Security Standard (PCI DSS) einzuhalten?

   ☐ Keine
   ☐ Jährliche Selbstauskunft
   ☐ Jährliches Audit

   Es werden zusätzliche Sicherheits-Scans durch zertifizierte Dienstleister durchgeführt? ☐ Ja ☐ Nein

4. Wie viele Kreditkartentransaktionen verarbeiten Sie oder Ihr Dienstleister in Ihrem Auftrag pro Jahr?

   ☐ 0 – 20.000
   ☐ 20.001 – 100.000
   ☐ 100.001 – 250.000
   ☐ 250.001 – 500.000
   ☐ 500.001 – 1.000.000
   ☐ 1.000.001 – 6.000.000
   ☐ > 6.000.000

HISCOX

Bitte per Telefax oder E-Mail an Hiscox
Fax-Nr.: 089/54 58 01-199
E-Mail: hiscox.underwriting@hiscox.de

II. Zusatzfragen Online Shop

Nur zu beantworten, wenn Sie Frage I.5.2. des Cyber Fragebogens mit „Ja“ beantwortet haben.

ONLINEUMSÄTZE IN €	Letztes Geschäftsjahr	Schätzung aktuelles Geschäftsjahr
Gesamtonlineumsatz		
davon über eigene Website		
davon über Drittanbieter, wie Amazon, eBay, Etsy		

1. Welche Hosting-Strategie verfolgen Sie für Ihren Online Shop?

☐ Sie betreiben Ihren Online-Shop selbst auf Ihren eigenen Servern

☐ Sie nutzen einen externen Hosting-Anbieter, der Ihnen das Betriebssystem bereitstellt

☐ Sie nutzen einen externen Hosting-Anbieter, der Ihnen die komplette Anwendung bereit stellt und diese auch pflegt

2. Wie ist die Software und Netzwerkumgebung Ihres Online Shops umgesetzt?

☐ Die Software ist immer auf dem aktuellsten Stand und Sicherheitsupdates werden unmittelbar eingespielt

☐ Sie nutzen ausschließlich Standard-Software. Wenn ja, welche? _____

☐ Sie nutzen Standard-Software mit individuell programmierten Erweiterungen

☐ Sie nutzen ausschließlich individuell programmierte und individuell gewartete Software

Ist die Zuständigkeit für die Wartung und Pflege des System vertraglich geregelt? ☐ Ja ☐ Nein

☐ Es besteht eine Anbindung an folgende Back-End-Systeme:

☐ ERP ☐ CRM ☐ Produktionssteuerung ☐ Sonstige _____

3. Wie schnell würde der Umsatz Ihres Unternehmens durch einen Cyber-Vorfall oder einen Ausfall / eine Störung des IT-Systems beeinträchtigt?

☐ < 8 Stunden ☐ < 24 Stunden ☐ < 3 Tage ☐ < 1 Woche ☐ ≥ 1 Woche

4. Wie schnell können Sie Ihr IT-System nach einem Cyber-Vorfall oder einem Ausfall / einer Störung wieder in Notbetrieb nehmen (Wiederanlaufzeit)?

☐ < 8 Stunden ☐ < 24 Stunden ☐ < 3 Tage ☐ < 1 Woche ☐ ≥ 1 Woche

HISCOX

Bitte per Telefax oder E-Mail an Hiscox
Fax-Nr.: 089/54 58 01-199
E-Mail: hiscox.underwriting@hiscox.de

III. Zusatzfragen Industrie-Steuerungsanlagen (ICS/SCADA)

Nur zu beantworten, wenn Sie Frage I.5.3. des Cyber Fragebogens mit „Ja“ beantwortet haben.

1. Folgende Schutzmaßnahmen haben Sie für die Absicherung Ihrer Anlagen umgesetzt: **(Zutreffendes bitte ankreuzen)**

- ☐ Fernzugriffe sind nicht möglich
- ☐ Konfigurierung ausschließlich in einem separierten Netzwerk (Segmentierung)
- ☐ Zugriffsrechte nur für ICS/SCADA-Verantwortliche
- ☐ Ausschließliche Nutzung sicherer VPN-Verbindungen bei Fernzugriffen
- ☐ Durchgehende Protokollierung der Fernzugriffe
- ☐ Fernzugriffe nur mittels Zwei-Faktor-Authentifizierung möglich
- ☐ Dauerhafte Überwachung und bedarfsgerechte An- und Abschaltung der Fernzugriffsrechte
- ☐ Sonstige _____

2. Folgende Härtungsmaßnahmen für ICS/SCADA und beteiligte Systeme (wie Terminals) haben Sie umgesetzt:
(Zutreffendes bitte ankreuzen)

- ☐ Keine entsprechenden Maßnahmen umgesetzt
- ☐ Regelmäßiges Einspielen von Sicherheitsupdates
- ☐ Dokumentierte und erprobte Prozesse zum Einspielen von Sicherheitsupdates
- ☐ Deaktivierung ungenutzter Schnittstellen

3. Werden spezielle IT-Sicherheitsprüfungen wie Penetrations-Tests der Industrie-Steuerungsanlagen durchgeführt? Wenn ja: ☐ Ja ☐ Nein

- ☐ Interne Prüfung
- ☐ Prüfung durch einen externen Berater
  - Wann war die Letzte? _____
  - In welchem Turnus werden diese wiederholt? _____

4. Wie schnell würde der Umsatz Ihres Unternehmens durch einen Cyber-Vorfall oder einen Ausfall / eine Störung des IT-Systems beeinträchtigt?

☐ < 8 Stunden ☐ < 24 Stunden ☐ < 3 Tage ☐ < 1 Woche ☐ ≥ 1 Woche

5. Wie schnell können Sie Ihr IT-System nach einem Cyber-Vorfall oder einem Ausfall / einer Störung wieder in Notbetrieb nehmen (Wiederanlaufzeit)?

☐ < 8 Stunden ☐ < 24 Stunden ☐ < 3 Tage ☐ < 1 Woche ☐ ≥ 1 Woche