HISCOX

Bitte per Telefax oder E-Mail an
ALT + PARTNER
Fax-Nr.: 03142-21240
E-Mail: office@alt-partner.at

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

Hiscox
Cyber Zusatzfragebogen

I. Zusatzfragen Kreditkartendaten

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

1. Über welche Wege akzeptieren Sie Kreditkartendaten? **(Zutreffendes bitte ankreuzen)** **Anteil der Transaktionen**

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

2. Haben Sie die Speicherung, Verarbeitung und/oder Übermittlung von Kreditkartendaten vollständig an einen Payment Service Provider ausgelagert? ☐ Ja ☐ Nein

- Wenn ja, an welchen? _____
- Wenn nein, sind Sie PCI compliant? ☐ Ja ☐ Nein

3. 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 – 2.000.000
- ☐ 2.000.001 – 3.000.000
- ☐ 3.000.001 – 4.000.000
- ☐ 4.000.001 – 5.000.000
- ☐ 5.000.001 – 6.000.000
- ☐ > 6.000.000

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. Haben Sie Ihre Online Shop Systeme und Anwendungen redundant aufgestellt? ☐ Ja ☐ Nein

HISCOX

Bitte per Telefax oder E-Mail an
ALT + PARTNER
Fax-Nr.: 03142-21240
E-Mail: office@alt-partner.at

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

3. 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 Systems vertraglich geregelt? ☐ Ja ☐ Nein

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

☐ ERP ☐ CRM ☐ Produktionssteuerung ☐ Sonstige

4. Betreiben Sie eine Web Application Firewall (WAP) mit einem individuellen Regelwerk, das nicht legitimierte Anfragen aktiv blockiert? ☐ Ja ☐ Nein

5. Sie haben folgende Schutzmaßnahmen gegen Hochlastsituationen, wie Distributed-Denial-of-Service Angriffe (DDoS) umgesetzt: **(Zutreffendes bitte ankreuzen)**

☐ DDoS Schutzfunktionen (Mitigation) an der eigenen Firewall sind aktiviert

☐ Rückgriff auf ein Content Delivery Network (CDN) bzw. Hochverfügbarkeitsanbieter, wie beispielsweise Akamay, AWS oder Cloudflare ist eingerichtet

☐ Trennung von Shop und Website

☐ Secure Shell (SHH) für Admin Zugriffe, damit diese auch bei Überlast noch Zugang haben

☐ Kontinuierliche Überwachung der Seitenbesuche und Lastspitzen (Monitoring)

☐ Regelmäßige Last-Tests und Festlegung von Lastlimits (inkl. sich daraus ergebende Prozessbegrenzungen und Vorhalten mindestens der dreifachen Anfragereserven zum Normalprozess)

☐ Mögliche reaktive Entkopplung der Back-End-Systeme

☐ Abgestimmte und erprobte Reaktionspläne speziell für Denial-of-Service-Angriffe

6. Wurde in der Vergangenheit ein Penetrationstest speziell für Ihre Webanwendungen durchgeführt? ☐ Ja ☐ Nein

Wenn ja, wann zuletzt? _____

Welche identifizierten Maßnahmen wurden danach noch nicht umgesetzt? _____

7. Passwörter werden ausschließlich als sicherer kryptographischer Hashwert (SHA-256 mit „Salz“) gespeichert? ☐ Ja ☐ Nein

Wenn nein, wie speichern Sie Passwörter in Ihrer Datenbank? _____

8. 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
ALT + PARTNER
Fax-Nr.: 03142-21240
E-Mail: office@alt-partner.at

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

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? _____
  - Welche identifizierten Maßnahmen wurden danach noch nicht umgesetzt? _____

4. Haben Sie eine Analyse durchgeführt, wie schnell und wie gravierend der Ausfall Ihrer ICS/SCADA Systeme Ihren Umsatz beeinflussen würde (Business Impact Analyse)? ☐ Ja ☐ Nein

5. 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

6. 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

Sofern Sie an mehreren Standorten ICS/SCADA Systeme betrieben, lassen Sie uns bitte eine Übersicht der einzelnen Standorte mit Tätigkeit, Umsatz und Rohertrag zukommen.