HISCOX

Bitte per Telefax oder E-Mail an
Carl Rieck GmbH
Fax-Nr.: +49 (0)6074 69665 11
E-Mail: hiscox@carlrieck.de

CARL RIECK ASSECURADEUR

Hiscox CyberClear Fragebogen

Mit diesem Fragebogen möchten wir Sie und Ihr Unternehmen gerne kennenlernen. Aufgrund der von Ihnen gemachten Angaben besteht für keine Partei die Verpflichtung zum Abschluss eines Versicherungsvertrages. Nähere Erläuterungen zu cyberspezifischen* Begriffen finden Sie am Ende in den Hinweisen sowie in unserem Cyber-Glossar* unter www.hiscox.de/blog/cyber-glossar.

* Siehe Glossar am Ende des Fragebogens

Nachfolgende Fragen sind für die Gesamtheit aller mitzuversichernden Gesellschaften zu beantworten. Falls notwendig, verwenden Sie für weitere Details bitte ein Beiblatt.

I. GENERELLE INFORMATIONEN

Vermittlername | Vermittlernummer

1. Unternehmensangaben

Name | Website

Straße, Nr. | Tätigkeitsbeschreibung (Branche und Geschäftstätigkeit)

PLZ, Ort, Land

2. Unternehmenskennzahlen

Konsolidierte Kennzahlen für alle mitzuversichernden Gesellschaften aus dem letzten Geschäftsjahr

	Gesamt	davon EWR	davon USA/Kanada	davon restliche Länder
Umsatz in €				
davon Onlineumsatz in €				
Rohertrag in € (Umsatz - Wareneinsatz)				
Anzahl Mitarbeiter				
Anzahl Mitarbeiter mit Zugang zu E-Mails				
Anzahl Kunden				

Gesamtumsatz aktuelles Geschäftsjahr in €

Sind Sie Teil eines Konzerns mit einem Gesamtumsatz von über 100 Millionen Euro? ☐ Ja ☐ Nein

Sind Sie ein Franchiseunternehmen (Franchisenehmer oder -geber) ☐ Ja ☐ Nein

3. Mitzuversichernde Gesellschaften

Gibt es Tochtergesellschaften außerhalb des Europäischen Wirtschaftsraumes (EWR) und des Vereinigten Königreichs (UK) UND/ODER mitzuversichernde Gesellschaften im In- und Ausland? ☐ Ja ☐ Nein

Wenn „Ja“, sind diese mit Namen, Anschrift, Umsatz in € sowie der Tätigkeit in einer separaten Tabelle oder ggf. als Organigramm anzugeben.

4. Versicherungsumfang

Versicherungssumme	☐ € 500.000	☐ € 1.000.000	☐ € 3.000.000	☐ € 5.000.000	☐ € _____
Selbstbehalt	☐ € 5.000	☐ € 10.000	☐ € 25.000	☐ € 50.000	☐ € _____

Bitte per Telefax oder E-Mail an
Carl Rieck GmbH
Fax-Nr.: +49 (0)6074 69665 11
E-Mail: hiscox@carlrieck.de

Wünschen Sie über die Basis-Absicherung hinaus ein Angebot für die folgenden Zusatz-Bausteine?

Cyber-Betriebsunterbrechung On-Premises (Ziffer II.4.1.1. bis 4.1.3. CyberClear) für Daten und IT-Systeme in alleiniger Herrschaftsgewalt Ihres Unternehmens	☐ Ja
Cyber-Betriebsunterbrechung Cloud-Ausfall (Ziffer II.4.2. CyberClear) für Daten und IT-Systeme in der Herrschaftsgewalt eines externen Dienstleisters (z. B. externes Rechenzentrum, Cloud-Anbieter)?	☐ Ja
Cyber-Diebstahl (Ziffer II.2.7. CyberClear)	☐ Ja
Cyber-Betrug (Ziffer II.2.8. CyberClear)	☐ Ja
E-Discovery (Ziffer II.2.13. CyberClear)	☐ Ja
Cyber-Betriebsunterbrechung On-Premises bei technischen Problemen (Ziffer II.4.1.4. CyberClear)	☐ Ja

5. Zusatzfragen

Können Ihre Kunden bei Ihnen mit Kreditkarte zahlen? **Falls ja, dann beantworten Sie bitte die Fragen zur Kreditkartenzahlung auf Seite 1 des Zusatzfragebogens.**	☐ Ja	☐ Nein
Generieren Sie Onlineumsätze über Ihre Website? **Falls ja, dann beantworten Sie bitte die Fragen zum Onlineshop auf Seite 1 & 2 des Zusatzfragebogens.**	☐ Ja	☐ Nein
Betreiben Sie Industrie-Steuerungsanlagen mithilfe automatisierter Kontrollsysteme (ICS/SCADA) z. B. in Produktion oder Logistik? **Falls ja, dann beantworten Sie bitte die Fragen zu Industrie-Steuerungsanlagen auf Seite 3 des Zusatzfragebogens.**	☐ Ja	☐ Nein

II. DATEN

1. Datenschutz

1.1. Bitte kreuzen Sie die Spanne der sensiblen personenbezogenen Datensätze* (nach Art. 9 DSGVO) an, die Ihr Unternehmen sammelt, verarbeitet und speichert (ein Datensatz kann dabei mehrere Daten zu einer Person enthalten):

(Zutreffendes bitte ankreuzen)

☐ 0 – 20.000 ☐ 20.001 – 100.000 ☐ 100.001 – 250.000

☐ 250.001 – 500.000 ☐ 500.001 – 1.000.000 ☐ > 1.000.000

Bei Datenmengen größer 1.000.000 bitten wir um eine genauere Aufschlüsselung (in 1. bis 4.) und die konkrete Anzahl.

1.2. Sind die besonderen personenbezogenen Daten in Ihrem Unternehmen sowohl „in transit“ (z. B. beim Versenden von E-Mails) als auch „at rest“ (bei der Speicherung auf Speichermedien und Clients außerhalb von Servern) zu jeder Zeit mit einer Schlüssellänge von mindestens AES* 256 Bit oder einem vergleichbaren Verfahren gespeichert?	☐ Ja	☐ Nein
1.3. Sind bei Ihnen formelle Prozesse und schriftliche Richtlinien umgesetzt, die den Schutz, die Aufbewahrung sowie das Löschen personenbezogenen Daten regeln?	☐ Ja	☐ Nein

Bitte per Telefax oder E-Mail an
Carl Rieck GmbH
Fax-Nr.: +49 (0)6074 69665 11
E-Mail: hiscox@carlrieck.de

2. Datenverarbeitung

2.1. Sind Sie im Rahmen der Auftragsdatenverarbeitung für Dritte tätig? ☐ Ja ☐ Nein

2.2. Nutzen Sie Dienstleister zur Auftragsverarbeitung von personenbezogenen Daten? ☐ Ja ☐ Nein

Nr.	Name des Dienstleisters	E-Mail	Hosting	Abrechnung	Sonstige	Sofern Haftungsfreistellungen vereinbart, in welcher Form?
1.		☐	☐	☐		
2.		☐	☐	☐		
3.		☐	☐	☐		

Wenn genutzt, bitte in der Tabelle aufführen, wenn nicht, bitte mit Teil 2.3 fortfahren (ggf. auf separatem Blatt).

2.3. Halten sich Ihre Dienstleister mindestens an das Datenschutzniveau aus Ihrem Unternehmen und überprüfen Sie dies regelmäßig durch Auditierungen?

- ☐ Nein bzw. unbekannt
- ☐ Ja, wir lassen uns dies regelmäßig durch eine Selbstauskunft bestätigen
- ☐ Ja, wir überprüfen dies regelmäßig durch die Prüfung eines Auditors
- ☐ Ja, unser Dienstleister ist zertifiziert. Benennung Zertifikat:

2.4. Regeln Sie in Ihren Dienstleistungsverträgen die Verfügbarkeit, Updates und das Beheben von Sicherheitslücken? ☐ Ja ☐ Nein

3. Mitarbeitersensibilisierung

3.1. Sensibilisieren Sie alle Ihre Mitarbeiter zur Erkennung und Vermeidung von Betrugsmaschen, wie Phishing* und CEO-Fraud*?

☐ Nein, bisher nicht ☐ Ja, unregelmäßig ☐ Ja, mindestens jährliche Wiederholung

3.2. Führen Sie zusätzlich bei all Ihren Mitarbeitern einen regelmäßigen Phishing-Test durch?

☐ Nein, bisher nicht ☐ Ja, mindestens jährliche Wiederholung ☐ Ja, mindestens quartalsweise Wiederholung

III. INFORMATIONSSICHERHEITS-MANAGEMENT

1. ISMS-Zertifizierung

1.1. Ist in Ihrem Unternehmen ein Informationssicherheits-Management-System (ISMS) etabliert? ☐ Ja ☐ Nein
Wenn ja, von wem wird das ISMS überprüft und angepasst?

☐ Eigene IT-Abteilung ☐ Interne(r) Informationssicherheitsbeauftragte(r) ☐ Sonstige

1.2. Sind Sie nach einem der folgenden Standards oder Normen zertifiziert? ☐ Ja ☐ Nein

Wenn vorhanden, bitte angeben und mit Teil IV. fortfahren.

☐ VdS 3473 ☐ ISO27001 ☐ IT-Grundschutz ☐ Anforderung nach BSI C5

Bis wann ist diese Zertifizierung gültig? Ist eine Verlängerung beabsichtigt? ☐ Ja ☐ Nein

2. Technische Sicherheitsmaßnahmen

2.1. Patch-Management-Prozess

Spielen Sie Sicherheitsupdates durchgehend auf Ihren kritischen IT-Systemen, einschließlich Firewalls und Virenschutz, ein?

☐ Nein, nicht durchgehend ☐ Ja, automatisch ☐ Ja, manuell ☐ Ja, manuell und zeitnah (spätestens nach 30 Tagen)

Werden Patches zu kritischen Sicherheitslücken (CVSS-Score* von mind. 8,0) innerhalb von 14 Tagen nach Veröffentlichung auf den betroffenen Systemen installiert? ☐ Ja ☐ Nein

Werden Patches grundsätzlich vor der Ausführung im Live-System erfolgreich in einer Testumgebung eingespielt? ☐ Ja ☐ Nein

2.2. Umgang mit Altsystemen ☐ Ja ☐ Nein

Nutzen Sie noch Software, für die vom Hersteller keine Sicherheitsupdates mehr bereitgestellt werden?

(Wenn „Ja“, Zutreffendes bitte ankreuzen):

☐ Alle betroffenen Systeme sind identifiziert und wurden nach Kritikalität bewertet

☐ Vorhandensein eines zeitnahen Migrationsplans für diese Systeme (vollständige Migration aller Altsysteme bis)

☐ Nutzung eines verlängerten Hersteller-Supports (bis)

☐ Ausschließlicher Betrieb der restlichen Systeme in einer getrennten Netzwerkumgebung* ohne direkten Internetzugang und mit durchgehender Kontrolle des Datenverkehrs*

Wenn keine Netzwerktrennung gegeben ist, erläutern Sie bitte, welche zusätzlichen Schutzmaßnahmen (wie z. B. End-Point-Security) für die übrigen Systeme getroffen wurden und um welche Software es sich handelt.

2.3. Verantwortlichkeit IT-Sicherheit

Wer ist in Ihrem Unternehmen für das Thema IT-Sicherheit verantwortlich?

☐ Es gibt noch keine dedizierte Rolle

☐ Informationssicherheitsbeauftragte(r) (ISB)

☐ Head of Information Security, CISO o. Ä. mit regelmäßigem Reporting an die Geschäftsleitung

☐ Geschäftsführer oder IT-Leiter

2.4. Netzwerktrennung

An mindestens folgenden Stellen halten Sie Firewallstrukturen bzw. Filtersysteme in Ihrem Netz vor:

(Zutreffendes bitte ankreuzen)

☐ An allen Netzübergängen zum Internet

☐ Auf allen Clients (Desktop-Computer, Laptops und Terminals)

☐ Zwischen Clients und Servern

☐ Zwischen allen Standorten bzw. es gibt nur einen Standort

☐ Zwischen Steuerungsanlagen / Operational Technologie (OT) und dem Büro-Netz bzw. solche Verbindungen sind gar nicht vorhanden

☐ Nutzung einer demilitarisierten Zone (DMZ)

☐ Nutzung einer Web Application Firewall (WAF)

2.5. Rechtekonzept

Ihr Rechtekonzept erfüllt folgende Mindestanforderungen:

(Zutreffendes bitte ankreuzen)

- ☐ Nutzung eines zentralen Authentisierungs- und Autorisierungsdienstes*
- ☐ Ausschließlich benutzerindividuelle Zugänge für alle Mitarbeiter mit Zugriffsbeschränkungen für das jeweilige Rollenprofil
- ☐ Prozess zur regelmäßigen Überprüfung der Zugriffsrechte sowie Sperrung der Konten ausgeschiedener Mitarbeiter nach max. 3 Monaten
- ☐ Administrative Zugänge werden ausschließlich zur Erledigung administrativer Tätigkeiten genutzt. Für die alltägliche Nutzung (insbesondere Surfen im Internet und E-Mail-Kommunikation) werden ausschließlich Benutzer-Konten ohne Admin-Rechte verwendet
- ☐ Jeder Administrator verwendet für administrative Tätigkeiten ausschließlich ein benutzerindividuelles Administrator-Konto
- ☐ Alle vorhandenen Cloud-Administrationskonten sind mit einer Zwei-Faktor-Authentifizierung abgesichert
- ☐ Zugänge zu Notfallkonten sind stark abgesichert (wie 2FA oder komplexe Passwörter mit mindestens 24 Zeichen) und die Zugangsmittel sind sicher hinterlegt (z. B. in einem Safe)

2.6. Absicherung von Fernzugriffen*

2.6.1. Fernzugriffe auf Ihr IT-System*

Gibt es Fernzugriffsmöglichkeiten auf Ihr IT-System oder auf externe Cloud-Dienste? ☐ Ja ☐ Nein

Wenn JA, beantworten Sie bitte die folgenden Fragen:
Die Absicherung von Fernzugriffsmöglichkeiten auf Ihr IT-System sowie Ihre Cloud-Dienste erfüllt folgende Anforderungen:
(Zutreffendes bitte ankreuzen)
Nutzung einer VPN-Verbindung, die die folgenden Voraussetzungen erfüllt:

- ☐ Einsatz aktueller kryptografischer Verfahren
- ☐ Einsatz von IPSec bzw. TLS-/SSL-Verschlüsselung*
- ☐ Durchgehende Nutzung einer Zwei- oder Mehr-Faktor-Authentifizierung (2FA oder MFA)*
- ☐ Nutzung anderweitiger Sicherheitsmaßnahmen (Nutzung von Zertifikaten, Kontrolle der IP-Adressen, Protokollierung, Beobachtung, Freischaltung etc.)

(Bitte erläutern Sie diese Maßnahmen separat)

2.6.2. Fernzugriffe auf IT-Systeme von Kunden

Gibt es Fernzugriffsmöglichkeiten auf die IT-Systeme Ihrer Kunden? ☐ Ja ☐ Nein

Wenn JA, bitte beantworten Sie die folgenden Fragen:

Werden diese Fernzugriffe durch den Einsatz zusätzlicher Sicherheitsmechanismen kontrolliert (z. B. durch den Einsatz von Zertifikaten, zeitbasierten Zugangskontrollen oder MFA)? ☐ Ja ☐ Nein

Sofern keine Sicherheitsmechanismen derzeit implementiert sind: haben Sie Ihren Kunden empfohlen, derartige Kontrollen für den Fernzugriff zeitnah einzuführen? ☐ Ja ☐ Nein

Verwalten Sie für Ihre Kunden die Zugriffsrechte (Erstellung, Löschung oder Änderung von Benutzerzugriffsrechten und Konten etc.), z. B. durch die Verwendung von Active Directory? ☐ Ja ☐ Nein

2.7. Richtlinien

Sie haben eine IT-Sicherheitsrichtlinie umgesetzt, in der die folgenden Elemente geregelt werden:
(Zutreffendes bitte ankreuzen)

- ☐ Wir haben keine schriftliche IT-Sicherheitsrichtlinie
- ☐ Alle Standardnutzer und Standardpasswörter werden durch starke individuelle Daten ersetzt
- ☐ Definierte Mindestanforderungen an die Passwortstärke*
- ☐ Regelung oder Verbot der privaten Nutzung der dienstlichen IT-Infrastruktur
- ☐ Vorhalten eines aktuellen Netzplans (Strukturplan des IT-Systems)
- ☐ Die automatische Ausführung von Makros in Office-Dokumenten ist deaktiviert

2.8. Angriffserkennung

Welche Maßnahmen haben Sie zur Erkennung von Angriffen und Sicherheitsvorfällen implementiert?
(Zutreffendes bitte ankreuzen)

- ☐ Wir haben keine entsprechenden Maßnahmen implementiert
- ☐ Speicherung von Protokolldaten über einen Zeitraum von mind. 90 Tagen
- ☐ Speicherung von Protokolldaten an zwei Stellen
- ☐ Automatische Auswertung von Protokolldaten
- ☐ Angriffserkennungssystem (Intrusion-Detection und -Prevention)
- ☐ Schutzmaßnahmen gegen unerwünschten Datenabfluss (Data Loss Prevention)
- ☐ System zum Umgang mit sicherheitsrelevanten Ereignissen (Security Information und Event Management (SIEM))
- ☐ Nutzung eines (Managed) Securitiy Operations Centers (SOC)
- ☐ Nutzen eines Endpoint Detection und Response Systems (EDR)
  - Welcher Anbieter?
  - Welcher Anteil des IT-Systems ist umfasst?
  - Wie ist diese gemanagt? ☐ intern ☐ extern

Ist sichergestellt, dass bei Feststellung unmittelbar eine Bewertung und Lösung umgesetzt wird? ☐ Ja ☐ Nein

Sonstige Maßnahmen zur Angriffserkennung (z. B. (Managed) Extended Detection und Response)

2.9. Schwachstellenerkennung

Wurde in der Vergangenheit eine automatische Schwachstellenanalyse (Vulnerability Assessment) oder ein manueller Penetrationstest durchgeführt?

☐ Nein ☐ Ja, unregelmäßig ☐ Ja, mindestens jährlich

2.10. Mobile-Device-Management (MDM)

Sie haben eine Mobilgeräteverwaltung implementiert, die die folgenden Schutzmaßnahmen umsetzt:
(Zutreffendes bitte ankreuzen)

- ☐ Wir haben kein MDM umgesetzt
- ☐ Fernlöschung der Geräte
- ☐ Sichere VPN-Verbindung (beschränkt, protokolliert, autorisiert)
- ☐ Verschlüsselung (full-disk encryption)
- ☐ Abgetrennte Container für dienstliche Daten auf mobilen Geräten
- ☐ Es gibt eine Bring-Your-Own-Device-Policy (BYOD) – Regelung zur dienstlichen Nutzung privater Geräte

Bitte per Telefax oder E-Mail an
Carl Rieck GmbH
Fax-Nr.: +49 (0)6074 69665 11
E-Mail: hiscox@carlrieck.de

3. Datensicherung

Ihre Datensicherungsstrategie erfüllt folgende Mindestanforderungen:
(Zutreffendes bitte ankreuzen)

☐ Mindestens tägliche Durchführung einer vollständigen automatischen Datensicherung*
☐ Einzelne (z. B. versehentlich gelöschte) Dateien können für einen Zeitraum von einem Monat problemlos im Regelbetrieb wiederhergestellt werden
☐ Nutzung einer Offline-Datensicherung* mit dauerhafter physischer Trennung von den IT-Systemen ODER
☐ Nutzung einer unveränderbaren Online-Datensicherung, auf welche die Administratoren nur mit einer von der betreffenden Domäne unabhängigen Zwei-Faktor-Authentifizierung* oder aus einer separaten Domäne zugreifen können
☐ Erfolgreiche, mindestens jährliche vollständige Wiederherstellungstests
☐ Anwendung der 3-2-1-Backup-Strategie*
☐ Vorhalten gestaffelter Langzeit-Backups, um Wiederherstellungszeitpunkte von vor mind. 90 Tagen erreichen zu können

4. Größe der IT-Infrastruktur

4.1. Wie viele (virtuelle und physische) Server betreiben Sie?

4.2. Über wie viele Clients/Endpoints verfügt Ihr IT-System?

IV. NOTFALLMANAGEMENT

1. Haben Sie kritische IT-Systeme* und Anwendungen für Ihr Unternehmen definiert?	☐ Ja	☐ Nein	
2. Haben Sie kritische IT-Systeme und Anwendungen redundant aufgestellt?	☐ Ja	☐ Nein	
3. Wie werden Ihre kritischen IT-Systeme und Anwendungen primär gehostet?	☐ intern	☐ extern	☐ gemischt
4. Haben Sie die für Ihr Unternehmen kritischen bzw. sensiblen Daten definiert?	☐ Ja	☐ Nein	

5. Es besteht ein schriftlich fixiertes Notfallkonzept, das folgende Mindestanforderungen erfüllt:
(Zutreffendes bitte ankreuzen)

☐ Wir haben noch kein Notfallkonzept
☐ Prozess zur Erkennung sowie zum Umgang mit Sicherheitsvorfällen (inkl. Datenschutzpannen)
☐ Geschäftsfortführungsplan (Business Continuity Plan)
☐ Wiederanlaufplan (Disaster Recovery Plan)
☐ Neben herkömmlichen Gefahren wie Brand, Stromausfall oder Unwetter sind auch explizit Cyber-Gefahren, wie ein Komplettausfall der IT-Systeme durch einen zielgerichteten Ransomware-Angriff, erfasst
☐ Regelmäßige inhaltliche Überprüfung (mindestens alle 2 Jahre) – letzter Termin:
☐ Regelmäßige praktische Tests (mindestens alle 2 Jahre) – letzter Termin:

6. Welcher Anteil am Umsatz kann auch bei Ausfall der kritischen IT-Systeme noch erwirtschaftet werden?
☐ < 10 % ☐ 10 - 25 % ☐ 25 - 50 % ☐ 50 - 75 % ☐ > 75 %

Bitte per Telefax oder E-Mail an
Carl Rieck GmbH
Fax-Nr.: +49 (0)6074 69665 11
E-Mail: hiscox@carlrieck.de

V. FRAGEN FÜR ZUSATZBAUSTEINE

1. Cyber-Diebstahl (Ziffer II.2.7. CyberClear) ☐ Ja ☐ Nein

Nutzen Sie eine analoge Telefonanlage ohne Anrufbeantworter ODER eine digitale Telefonanlage oder einen Anrufbeantworter (analog oder digital), deren Passwörter und PINs Sie von der Werkseinstellung geändert haben?

Wenn die Antragsfrage mit „Nein" beantwortet wird, kann der Zusatzbaustein Cyber-Diebstahl (Ziffer II.2.7.) nicht abgeschlossen werden.

2. Cyber-Betrug (Ziffer II.2.8. CyberClear)

Sie haben folgende Sicherungsmaßnahmen umgesetzt, um sich gegen betrügerische Überweisungen* zu schützen: (Zutreffendes bitte ankreuzen)

☐ Verpflichtendes Vier-Augen-Prinzip per Anweisung ab einer Überweisungshöhe von €_____

☐ Verpflichtende Überprüfung beim Zahlungsempfänger bei neuen oder geänderten Kontoinformationen

☐ Weitere Maßnahmen (z. B. bei Auslandsüberweisungen):_____

3. Cyber-Betriebsunterbrechung bei Cloud-Ausfall (Ziffer II.4.2. CyberClear)

Diese Fragen sind nur zu beantworten, wenn die Erweiterung Cyber-Betriebsunterbrechung bei Cloud-Ausfall gewünscht wird.

3.1. Welche kritischen Geschäftsprozesse haben Sie in die Cloud bzw. ein externes Rechenzentrum ausgelagert?

_____ _____

3.2. Die Cloud bzw. das externe Rechenzentrum, in das kritische Geschäftsprozesse ausgelagert sind, erfüllt folgende Standards: (Zutreffendes bitte ankreuzen)

☐ Einstufung mind. Tier Level 3 gem. TIA-942 (Telecommunications Infrastructure Standard for Data Centers)

☐ Zertifizierung nach ISO27001

4. Zusatzbaustein Cyber-Betriebsunterbrechung On-Premises bei technischen Problemen (Ziffer II.4.1.4. CyberClear)

Diese Frage ist nur zu beantworten, wenn die Erweiterung Cyber-Betriebsunterbrechung On-Premises bei technischen Problemen gewünscht wird.

4.1. Werden kritische Systemänderungen, wie die Installation und Veränderung von Software, vor der Ausführung im Live-System erfolgreich in einer Testumgebung eingespielt? ☐ Ja ☐ Nein

Bitte per Telefax oder E-Mail an
Carl Rieck GmbH
Fax-Nr.: +49 (0)6074 69665 11
E-Mail: hiscox@carlrieck.de

V. VORSCHÄDEN

Gab es in den letzten fünf Jahren Netzwerksicherheitsverletzungen (wie Hacker-Angriffe, Denial-of-Service-Angriffe oder Vorfälle durch Schadprogramme), Bedienfehler, Datenrechtsverletzungen oder Cyber-Erpressungen, die insgesamt bereits zu Schäden und Kosten von über € 1.000 geführt haben? Sind Ihnen darüber hinaus Umstände bekannt, die zu einem Schaden oder Kosten führen könnten? ☐ Ja ☐ Nein

Wenn die vorstehende Frage mit „Ja“ beantwortet wurde, bitten wir um Details zu jedem Vorfall.

- Was ist konkret passiert (Detailbeschreibung inkl. Datum)?
- Welche einzelnen Kosten sind Ihnen durch den Vorfall entstanden?
- Kam es zu einem Systemausfall/Betriebsausfall (vollständig oder teilweise), und wenn ja, wie lange?
- Welche Maßnahmen wurden ergriffen, um solche Vorfälle zukünftig möglichst zu vermeiden?

Mit einer Vorversichereranfrage erkläre ich mich einverstanden!

Diese ausgefüllte Erklärung 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 (VVG).

Mit Ihrer Unterschrift bestätigen Sie, dass vorstehende Angaben vollständig und richtig sind.

Name	Position im Unternehmen	Unterschrift Geschäftsleitung oder befugten Vertreters/Firmenstempel	Datum

Bitte per Telefax oder E-Mail an
Carl Rieck GmbH
Fax-Nr.: +49 (0)6074 69665 11
E-Mail: hiscox@carlrieck.de

Hinweise zu den abgefragten IT-Schutzmaßnahmen im Fragebogen

Besondere personenbezogene Daten	Besondere personenbezogene Daten sind 1. Sozialversicherungs-, Führerschein- und Ausweisdaten, 2. Steuer- und Finanzdaten, wie Bank- oder Kreditkartenkonten, 3. Informationen zu Strafverfahren und Ordnungswidrigkeiten, 4. Angaben über die ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben (Art. 9 DSGVO).
AES	Steht für Advanced Encryption Standard und ist ein symmetrisches Verschlüsselungsverfahren. 256 Bit ist die Schlüssellänge.
Phishing	Phishing bezeichnet die illegale Methode, über gefälschte Webseiten, per E-Mail oder Kurznachrichten persönliche Daten oder Anmeldedaten von Internetnutzern abzugreifen. Die Daten eines Benutzers werden dann für betrügerische Aktionen genutzt.
CEO-Fraud	Auch als Fake-President-Fraud (deutsch Geschäftsführer-Betrug) bezeichnet den Versuch, sich als Geschäftsführer oder Entscheidender auszugeben und dadurch Geldmengen zu erbeuten.
IT-System	Zum IT-System zählen sowohl Geräte, Betriebssysteme als auch Anwendungen. Im Patch-Management-Prozess müssen also sowohl die Treiber auf Geräten wie Routern als auch die Operating Systems (OS) auf Clients und Servern sowie die darauf installierten Applikationen (kurz Apps) bzw. Computerprogramme wie ERP oder CRM Software berücksichtigt werden.
CVSS Score	Ein international anerkannter Standard des National Institute of Standards and Technology zur Bewertung der Schwere von Software-Sicherheitslücken.
Ausgelaufene Herstellerunterstützung	Auch engl. „End of Life“, trifft z. B. auf Windows XP, Windows Server 2003, MacOS Sierra 10.12 oder Linux Ubuntu 12.04 und ältere Versionen zu.
Kritikalität	Dies ist ein relatives Maß für die Bedeutsamkeit eines Teiles des IT-Systems in Bezug auf die Konsequenzen, die eine Störung oder ein Funktionsausfall für die Geschäftsprozesse hat.
Verlängerter Hersteller-Support	Für Windows 7 bzw. Windows Server 2008 wird dies beispielsweise als Extended Security Updates (ESU) bis 2023 kostenpflichtig bereitgestellt. Für Ubuntu 18.04 soll der Extended Security Maintenance (ESM) bis April 2023 bereitgestellt werden.
Getrennte Netzwerkumgebung	Eine getrennte Netzwerkumgebung kann über eine Segmentierung (z. B. durch einzelne VLANs oder Netzwerk-Firewalls) erreicht werden.
Kontrolle des Datenverkehrs	Eine durchgehende Kontrolle des Datenverkehrs soll sicherstellen, dass die Kommunikationsverbindungen (oder auch Netzwerk-Traffic) durch Filtersysteme wie Router mit ACL (Access Control List) oder Firewalls abgesichert werden.
Steuerungsanlagen / Operational Technologie (OT)	Bei den Industrie-Steuerungsanlagen handelt es sich um Soft- und Hardware, die zur Steuerung und/oder Überwachung von physischen Geräten, industriellen Anlagen und Prozessen eingesetzt werden. Dies erfolgt i. d. R. mithilfe automatisierter Kontrollsysteme (ICS/SCADA) in den Bereichen wie Produktion, Leitstände/Leitwarten, Gebäudetechnik oder Logistik.
Authentisierungs- und Autorisierungsdienst	Am bekanntesten ist das Active Directory (AD) von Microsoft. Eine Alternative für Unix-Betriebssysteme ist Radius.
Fernzugriffe	Zu Fernzugriffen zählen sowohl Remote-Zugänge für Homeoffice/Telearbeit als auch Fernwartungen von Systemen und Anlagen.
TLS-/SSL-Verschlüsselung	Transport Layer Security (TLS, deutsch Transportschichtsicherheit) ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet. Secure Sockets Layer (SSL) ist umgangssprachlich bekannter, jedoch veraltet und die Vorgängerbezeichnung für das besagte Protokoll.

Zwei- oder Mehr-Faktor-Authentifizierung (2FA oder MFA)	Bei einem Log-in mit einer Zwei- oder Mehr-Faktor-Authentifizierung (2FA oder MFA) benötigt man – neben dem Benutzernamen und Passwort – noch eine oder mehrere weitere eindeutige Informationen. Oft ist das eine zusätzliche Ziffernfolge. Per App oder SMS wird der Einmalcode auf Anforderung gesendet. So kann der Zugriff auf Accounts mit geleakten Passwörtern und Zugangsdaten verhindert werden.
Passwortstärke	Informationen zum Thema Passwortsicherheit erhalten Sie vom Bundesamt für Sicherheit in der Informationstechnik (z. B. unter www.bsi.bund.de).
Vollständige Datensicherung	Vollständig bedeutet, dass eine Wiederherstellung aller kritischen Dateien und Anwendungen für den eigenen Geschäftsbetrieb möglich ist.
Offline-Datensicherung	Damit sichergestellt ist, dass bei einem nicht erfolgreichen Update eines Backup-Standes weiterhin ein vollwertiges Backup verfügbar ist, empfiehlt es sich, zwei vollständige Datensicherungen physisch getrennt (offline) vom eigentlichen IT-System abzuspeichern. Mindestens eine vollständige Offline-Datensicherung, die nicht älter als eine Woche ist, sollte ständig vorhanden sein, um sich effektiv vor Manipulation durch Angreifer zu schützen, die alle laufenden IT-Systeme unter ihre Kontrolle gebracht haben (wie Emotet).
3-2-1-Backup-Strategie	Diese Strategie fordert, die vollständige Datensicherung immer mindestens in dreifacher Ausführung bereitzuhalten. Dabei sollten mindestens zwei verschiedene Technologien (NAS, Storage, Bänder, Objektspeicher) zum Einsatz kommen und mindestens eine Datensicherung sollte außer des eigenen Zugriffs sein (offline oder sichere Cloud).
Kritische IT-Systeme	IT-Systeme sind kritisch, sobald ein mehrtägiger Ausfall (3 Tage) zu einem Umsatzverlust führt.
Betrügerische Überweisungen	Meist durch Social Engineering, also gezielte Manipulation von Mitarbeitern, veranlasste Geldzahlungen an Kriminelle, auch bekannt als Fake-President oder CEO-Fraud.