Fragebogen Zurich Cyberversicherung

Die Fragen sind vollständig und wahrheitsgemäss zu beantworten. Werden erhebliche Gefahrstatsachen verschwiegen oder unrichtig mitgeteilt (Verletzung der Anzeigepflicht), kann die Zürich Versicherungs-Gesellschaft AG (Zurich) den Vertrag kündigen (sofern zustande gekommen). Zudem erlischt in diesem Fall die Leistungspflicht von Zurich für bereits eingetretene Schäden, soweit deren Eintritt oder Umfang durch die nicht oder unrichtig angezeigte erhebliche Gefahrstatsache beeinflusst worden ist (Art. 6 VVG [Bundesgesetz über den Versicherungsvertrag]).

Für den Zweck dieses Fragebogens bezieht sich der Begriff «Versicherungsnehmer» auf die Gesamtheit aller zu versichernden Unternehmen inklusive aller Tochtergesellschaften.
Falls Antworten nur für Teile der zu versichernden Unternehmensgruppe zutreffen, ist dies entsprechend zu vermerken.

Sollte der Platz für die Beantwortung bestimmter Fragen nicht ausreichen, verwenden Sie bitte ein separates Blatt.

Angaben zum Versicherungsnehmer (Anschrift)

Name des Versicherungsnehmers

Strasse | Branche

PLZ, Ort | Mitarbeiter CH | Ausland

Homepage(s) | Umsatz (abgeschlossenen Geschäftsjahr) CHF

Haben Sie Niederlassungen im Ausland oder sind Sie die Tochtergesellschaft einer Muttergesellschaft welche im Ausland domiziliert ist? (Falls weitere, bitte mittels einer seperaten Liste zustellen oder Organigramm zustellen.)

☐ Ja ☐ Nein

Firmenname

Strasse | PLZ, Ort, Land

Wie teilt sich der Umsatz prozentual auf die folgenden Länder/Regionen auf?

CH % | EU % | US % | Rest der Welt %

1 Angaben zu sensiblen Daten

Personenbezogene und Medizinische Daten

1.1 Von wie vielen Personen, ausser Mitarbeitern, speichern oder verarbeiten Sie Daten wie Adresse, Name, Email oder Telefonnummer?

☐ Keine ☐ <1'000 ☐ <10'000
☐ <100'000 ☐ >100'000

1.2 Von wie vielen Personen, ausser Mitarbeitern, speichern oder verarbeiten Sie Gesundheitsdaten?

☐ Keine ☐ <1'000 ☐ <10'000
☐ <100'000 ☐ >100'000

1.3 Verschlüsseln Sie Daten auf den Festplatten Ihrer Endgeräte und Servern?

☐ Ja, für die Endgeräte ☐ Ja, für die Server ☐ Nein

1.4 Erfüllen Sie bereits folgende Pflichten in Zusammenhang mit dem revidierten DSG (zutreffende anwählen):

☐ Datenverarbeitungsinventar vorhanden und jährlich geprüft

☐ Schriftlicher Prozess vorhanden zur Meldung von Datenverlusten

☐ Datenschutz-Folgenabschätzung vorhanden

Kreditkartendaten

1.5 Ermöglichen Sie Kunden oder Geschäftspartnern das Bezahlen mit Kreditkarte?

☐ Ja ☐ Nein

1.6 Falls Sie solche Bezahlungen ermöglichen, lagern Sie die Verarbeitung von Kreditkartendaten und Zahlungen vollständig zu einem externen Anbieter aus, so dass Kreditkartendaten nie in Klartext auf dem Firmennetzwerk oder IT Systemen sind (Point-to-Point encryption)?

☐ Nein

☐ Ja, bei dem folgenden Anbieter:

2 Wie schützen Sie sich vor einem IT Betriebsunterbruch

2.1 Wieviel von dem Umsatz wurde durch e-Commerce/Webshops/ Online Vertrieb erzielt?

_____ %

Falls Geschäft über e-Commerce/Webshop/Online Vertrieb besteht:

2.2 Wird der Webshop/Online Vertrieb durch einen Partner betrieben?

- ☐ Nein, ich betreibe den Webshop komplett selber
- ☐ Ja, der Webshop ist eine Software as a Service Lösung von:

_____

2.3 Wie wird Ihr Webshop/Online Lösung von Angreifern und Unterbrüchen geschützt?

- ☐ Web Application Firewall (WAF)
- ☐ Distributed Denial of Service (DDos) Schutz
- ☐ Vulnerability Scans oder Penetrations Tests
- ☐ Web Server ist/sind nicht mit dem internen System verbunden

Einfluss Betriebsunterbruch

2.4 Wieviel Prozent ihrer üblichen Kundenaufträge/Bestellungen/ Buchungen/Termine können Sie in einer Woche neu annehmen, auch wenn ihre IT eine Woche lang ausfällt?

- ☐ Keine: 0%
- ☐ Einige: Bis 33%
- ☐ Teilweise: 33%–66%
- ☐ Grossteil: Mehr als 66%

2.5 Wieviel Prozent Ihrer Kundenaufträge/Bestellungen/Buchungen/ Termine/Produktion können Sie in einer Woche noch abarbeiten/ erfüllen/bedienen, wenn Ihre IT eine Woche lang ausfällt?

- ☐ Keine: 0%
- ☐ Einige: Bis 33%
- ☐ Teilweise: 33%–66%
- ☐ Grossteil: Mehr als 66%

Business Continuity/Disaster Recovery Fähigkeiten

2.6 Sichern Sie alle Systeme und Daten mit Sicherheitskopien ab?

- ☐ Ja, mindestens täglich
- ☐ Ja, mindestens wöchentlich
- ☐ Ja, mindestens monatlich
- ☐ Nein

2.7 Lagern Sie Sicherheitskopien an einem Ort ausserhalb Ihres eigenen Netzwerks aus?

☐ Ja ☐ Nein

2.8 Haben Sie einen dokumentierten Prozess zur Wiederherstellung von Systemen aus Sicherheitskopien?

☐ Ja ☐ Nein

2.9 Testen Sie das Wiederherstellen dieser Systeme aus den Sicherheitskopien mindestens einmal jährlich?

☐ Ja ☐ Nein

2.10 Haben Sie einen schriftlichen Plan zur Aufrechterhaltung des Geschäftsbetriebs für den Fall, dass Ihre IT ausfällt?

☐ Ja ☐ Nein

3 Wie verwalten und pflegen Sie ihre IT?

Organisation

3.1 An wen rapportiert der IT Chef oder ist er Mitglied der Geschäftsleitung?

_____

3.2 Wie viele Mitarbeiter sind in Ihrer IT beschäftigt?

_____

3.3 Wie viele dieser Mitarbeiter sind für die IT Sicherheit zuständig?

_____

Risikoanalyse

3.4 Haben Sie eine Risiko- und Schwachstellen Analyse ihrer IT Sicherheit in den letzten drei Jahren durchgeführt (wie z. B. Penetration Tests/Vulnverability Scan oder Security Audits)?

- ☐ Ja und es wurden kritische Mängel gefunden und bereits adressiert.
- ☐ Ja und es wurden kritische Mängel gefunden, welche noch nicht adressiert oder in Umsetzung sind.
- ☐ Ja und es wurden keine kritische Mängel gefunden.
- ☐ Nein

Inventar

3.5 Verwalten Sie Ihre Endgeräte, Server und Anwendungen in einem Inventar System

- ☐ Ja, für Endgeräte
- ☐ Ja, für Anwendungen auf Endgeräten
- ☐ Ja, für Server
- ☐ Ja, für Serveranwendungen
- ☐ Nein

Endgeräte

3.6 Wie viele Endgeräte (Desktop und Notebooks) werden in Ihrem Unternehmen eingesetzt?

3.7 Diese Endgeräte und darauf installierte Anwendungen werden:

☐ selbst eingerichtet und gewartet.

☐ von folgendem externen Anbieter eingerichtet und gewartet:

3.8 Diese Endgeräte und darauf installierte Anwendungen werden mindestens **monatlich** mit kritischen Updates aktualisiert.

☐ Nein

☐ Ja, alle

☐ Ja, aber einige Endgeräte laufen mit Betriebssystemen, welche «out of support» sind und daher nicht mehr mit Updates aktualisiert werden können (z. B. Windows XP):

Netzwerk-Infrastrukturen

3.9 Die Netzwerkinfrastrukturen Ihres Unternehmens (Router, Access Gateways, Switches, Firewalls, etc.) werden:

☐ selbst eingerichtet und gewartet.

☐ von folgendem externen Anbieter eingerichtet und gewartet:

Server

3.10 Welche Server und Serveranwendungen betreiben und warten Sie selbst und welche werden von einem Dritten betrieben und gewartet?

Typ	Selbst betrieben?	Von Dritten/Cloud Anbieter betrieben und Name?	
☐ Email Server	☐ Ja ☐ Nein		☐ inklusive Backup Service
☐ File Server	☐ Ja ☐ Nein		☐ inklusive Backup Service
☐ CRM Server	☐ Ja ☐ Nein		☐ inklusive Backup Service
☐ ERP Server	☐ Ja ☐ Nein		☐ inklusive Backup Service
☐ Active Directory Server	☐ Ja ☐ Nein		☐ inklusive Backup Service
☐ Weitere	☐ Ja ☐ Nein		☐ inklusive Backup Service

3.11 Werden Server mindestens quartalsweise mit kritischen Updates aktualisiert?

☐ Nein

☐ Ja, alle

☐ Ja, aber die folgenden Server sind «out of support», und können nicht mehr aktualisiert werden:

3.12 Für Notfall-Updates, die gemäss Hersteller dringend und umgehend eingespielt werden müssen, bestehen für Server und Endgeräte Notfallprozesse um diese innerhalb von 48 Stunden einzuspielen (emergency patch)

☐ Ja ☐ Nein

Industrielle IT/Medizinische IT

3.13 Werden in Ihrem Unternehmen industrielle Anlagen zur Produktion, Fertigung, Logistik oder medizinische Geräte eingesetzt?

☐ Nein, wir verwenden keine solche Geräte.

☐ Ja, diese Anlagen werden selbst bewirtschaftet und gewartet.

☐ Ja, diese Anlagen werden von folgendem externen Anbieter eingerichtet und gewartet:

3.14 Falls Sie solche Anlagen und Geräte einsetzten, werden diese von der restlichen betrieblichen IT getrennt betrieben (Network Segregation).

☐ Ja ☐ Nein

3.15 Falls Sie solche Anlagen und Geräte einsetzen, haben diese einen Remote-Zugriff für Hersteller oder Mitarbeiter?

- ☐ Es besteht kein Remote-Zugriff
- ☐ Es besteht Remote-Zugriff ohne Zugriffschutz
- ☐ Es besteht Remote-Zugriff via Benutzername und Passwort
- ☐ Es besteht Remote-Zugriff via Multifaktor-Authentisierung

4 Wie verwalten Sie den Zugang von Benutzern auf Ihre Systeme?

Benutzerverwaltung und Rechtevergabe

4.1 Hat jeder Benutzer einen eigenen Account?

☐ Ja ☐ Nein

4.2 Haben Sie technisch erzwungene Passwortrichtlinien zur Sicherstellung von starken Passwörtern und mindestens quartalsweisem Passwortwechsel?

☐ Ja ☐ Nein

4.3 Wird immer verhindert, dass Benutzer Programme auf Endgeräten installieren können?

☐ Ja ☐ Nein

4.4 Gibt es ein Berechtigungskonzept wonach unterschiedliche Benutzer unterschiedliche Anwendungs-Zugriffsrechte haben?

☐ Ja ☐ Nein

4.5 Sind Fernzugriffe auf das Firmennetzwerk möglich?

- ☐ Nein
- ☐ Ja, die Verbindung erfordert Benutzername und Passwort und ist mit privaten Computern möglich (Bring Your Own Device)
- ☐ Ja, die Verbindung erfordert Benutzername und Passwort und den Einsatz eines Firmencomputers.
- ☐ Ja, die Verbindung erfordert Multifaktor-Authentisierung

4.6 Wie werden die Zugriffsberechtigungen für Systemadministratoren verwaltet?

- ☐ Systemadministratoren haben Admin-Accounts und loggen sich mittels Benutzername und Passwort ein
- ☐ Systemadministratoren haben Admin-Accounts, welche von einem zentralen Zugriffsmanagementsystem verwaltet werden. Um auf eine Ressource zuzugreifen, erfordert dieses
  - ☐ die Eingabe von Benutzername und Passwort.
  - ☐ die Eingabe von Benutzername und Passwort und einen zweiten Faktor.

5 Wie schützen Sie Ihre IT vor unerlaubtem Eindringen von aussen

Network Access Control

5.1 Können sich nur zugelassene und registrierte Geräte mit dem Netzwerk verbinden?

☐ Ja ☐ Nein

Firewalls

5.2 Haben Sie eine Firewall/Proxy Lösung für Endgeräte und Server welche regelmässig aktualisiert wird?

- ☐ Ja, diese wird intern gewartet.
- ☐ Ja, diese wird durch einen externen Dienstleister gewartet.
- ☐ Nein

Antivirus und EDR

5.3 Haben Sie eine Antivirus Lösung auf allen Endgeräten und Servern installiert, welche regelmässig aktualisiert wird?

☐ Ja ☐ Nein

5.4 Haben Sie eine EDR (Endpoint Detection and Response)-Lösung (z. B. Microsoft Defender) im Einsatz?

- ☐ Ja, für Endgeräte
- ☐ Ja, für Server
- ☐ Ja und Warnungen werden von der Monitoring Lösung erfasst
- ☐ Nein

Intrusion Detection und Monitoring

5.5 Werden Netzwerkereignisse, Systemausfälle und Sicherheitsereignisse in einem Monitoring System überwacht?

- ☐ Ja, durch die interne IT
  - ☐ Zu Bürozeiten
  - ☐ 24/7 mit Pikettdienst
- ☐ Ja, durch einen externen Partner für Monitoring und Security Operations Services (SOC)
  - ☐ Zu Bürozeiten
  - ☐ 24/7 mit Pikettdienst
- ☐ Nein

Training

5.6 Absolvieren alle IT Nutzer ein Training zum sicheren Umgang mit der IT?

- ☐ Ja, beim Firmeneintritt
- ☐ Ja, das Training muss mindestens jährlich wiederholt werden
- ☐ Ja, und das Training beinhaltet zusätzlich Phishing Simulationen
- ☐ Nein

Zahlungsanweisungen

5.7 Prüfen Sie bei Rechnungen oder Zahlungsanweisungen ob sich die Bankverbindungen des Rechnungsstellers geändert haben?

☐ Ja ☐ Nein

6 Welche Zwischenfälle hat es in der Vergangenheit gegeben?

Schadenerfahrung

6.1 Hat ihr Unternehmen in den letzten drei Jahren Systemeinbrüche, Datendiebstähle oder Datenverluste erlitten?

☐ Nein

☐ Ja, Beschreibung Vorfall, Massnahmen um weitere Fälle vorzubeugen

6.2 Wurde Ihnen oder Ihrem Unternehmen in den letzten drei Jahren eine Cyberversicherung oder eine Versicherung mit ähnlichem Inhalt abgelehnt oder gekündigt?

☐ Ja ☐ Nein

6.3 Sind Ihnen oder einem anderen (gegenwärtigen oder ehemaligen) Geschäftsleitungs- oder Managementmitglied, einem Mitarbeiter, Ihrem IT Dienstleister oder sonstigen Vertragspartner Umstände bekannt, welche zu einem Anspruch in Verbindung mit der vorliegend beantragten Versicherungsdeckung führen könnten?

☐ Ja ☐ Nein

7 Welche Veränderungen haben sich ergeben und welche Verbesserungen planen Sie?

7.1 Bitte erläutern Sie die Änderungen in den letzten 12 Monaten in Zusammenahng mit Ihren Geschäftsaktivitäten und IT-Sicherheit (Organisation, Schutzmassnamen, Monitoring und Wiederherstellung), sowie die geplanten Verbesserungen für die nächsten 12 Monate

8 Zusätzliche Bemerkungen und Antworten zu den Fragen 6.1, 6.2, 6.3 und 7.1

Schlusserklärung

Der Versicherungsnehmer erklärt, die in diesem Dokument enthaltenen Fragen nach bestem Wissen beantwortet zu haben. Weiter bestätigt er die Richtigkeit der darin deklarierten Tatsachen (Gefahrstatsachen). Er verpflichtet sich, Änderungen, die vor Beginn des definitiven Versicherungsschutzes eintreten, Zurich zu melden.

Der Versicherungsnehmer nimmt zur Kenntnis, dass Zurich im Zusammenhang mit dem Vertragsabschluss und der Vertragsabwicklung und zu weiteren Zwecken Daten bearbeitet, die sich auf natürliche Personen beziehen (Personendaten). Nähere Informationen zu dieser Bearbeitung finden sich in der Datenschutzerklärung von Zurich. Diese Datenschutzerklärung kann unter www.zurich.ch/datenschutz abgerufen oder unter Zürich Versicherungs-Gesellschaft AG, Datenschutz, Postfach, 8085 Zürich, datenschutz@zurich.ch bezogen werden.

Zurich behält sich vor, in diesem Zusammenhang und in den weiteren in der Datenschutzerklärung genannten Personendaten – ggf. einschliesslich von Gesundheitsdaten – an Dritte weiterzugeben.

Der Versicherungsnehmer willigt mit Abgabe dieser Erklärung ausdrücklich ein, dass Vor-, Mit- und Rückversicherer, andere Versicherer und weitere Stellen innerhalb von Zurich, Amtsstellen und weitere Dritte an Zurich im Zusammenhang mit Risiko- und Leistungs- bzw. Schadensprüfungen, zur Missbrauchsbekämpfung und zur Abwicklung des Versicherungsvertragsverhältnisses sachdienliche Auskünfte erteilen, insbesondere über den Schadenverlauf und über frühere oder parallele Versicherungen und Leistungen. Dies ist für die Vorbereitung bzw. Abwicklung des Versicherungsvertragsverhältnisses notwendig. Der Versicherungsnehmer entbindet alle diese Stellen für diesen Fall von einer etwaigen Schweigepflicht.

Der Versicherungsnehmer verpflichtet sich, Dritte, deren Personendaten er Zurich übermittelt, über die Bearbeitung ihrer Personendaten durch Zurich zu informieren.

Datum, Ort

Versicherungsnehmer

Name des Unterzeichnenden

Unterschrift

ZH29275d-2203

Zürich Versicherungs-Gesellschaft AG
Hagenholzstrasse 60, 8050 Zürich
Telefon 0800 80 80 80, www.zurich.ch

ZURICH