Basler Versicherungen

Risikoerfassungsbogen zur Cyberversicherung

für Unternehmen bis 10 Mio. Euro Jahresumsatz

Versicherungsnehmer

Name und Adresse

Telefon | Homepage | E-Mail

1. Vorvertragliche Situation (bitte auch ohne eine bestehende Vorversicherung/Cyberversicherung ausfüllen)

1.1 Derzeitiger Versicherer/VS-Nr. (falls vorhanden):

Gekündigt? ☐ Nein ☐ Ja, durch

1.2 Schadenverlauf der letzten fünf Jahre (auch nicht versicherte Vorfälle – unabhängig von einer bestehenden Vorversicherung):

Jahr	Art	ggf. Zahlungen	ggf. Reserven

2 Betriebsbeschreibung des Unternehmens/Branche (ggf. bitte Prospekte beifügen)

3 Allgemeine Informationen

3.1	Jahresumsatz im letzten Geschäftsjahr	davon Online-Handel
Deutschland		
USA/Kanada:		
übriges Ausland:		

3.2 Anzahl Mitarbeiter

3.3 Auslandsaktivitäten, z. B. Niederlassungen, Export, Teilnahme und Besuch von Messen, Montage etc. (insbesondere USA/Kanada)

3.4 Wie hoch sind Ihre geschätzten jährlichen Ausgaben in Euro für die IT-Sicherheit? EUR

4. Weitere Angaben zum Betrieb

4.1	Betreiben Sie eine eigene Infrastruktur für Online-Handel (e-Commerce)?	☐ Ja – bitte Anhang/Zusatzfragen ausfüllen	☐ Nein
4.2	Speichern und verarbeiten Sie Daten von Dritten ?	☐ Ja – bitte Anhang/Zusatzfragen ausfüllen	☐ Nein
4.3	Nutzen Sie einen Dienstleister zur Auftragsdatenverarbeitung nach § 11 BDSG?	☐ Ja – bitte Anhang/Zusatzfragen ausfüllen	☐ Nein
4.4	Ist die Nutzung privater Geräte in Ihrer Unternehmens-IT gestattet?	☐ Ja – bitte Anhang/Zusatzfragen ausfüllen	☐ Nein
4.5	Nutzen Sie automatisierte Produktionssysteme (ICS)?	☐ Ja – bitte Anhang/Zusatzfragen ausfüllen	☐ Nein

BAS 8291 06.17

5. Fragen zu Schutzmaßnahmen

5.1 Zugangssicherung

5.1.1	Ist für jeden Nutzer und Administrator eine benutzerindividuelle Kennung/Zugang mit Passwort vergeben? Ist für den Zugang zu jedem System eine Benutzerkennung und ein Passwort notwendig?	☐ Ja	☐ Nein
5.1.2	Haben Sie Mindestanforderungen an die Passwortqualität sämtlicher Mitarbeiter und Systeme? Werden diese technisch erzwungen?	☐ Ja	☐ Nein
5.1.3	Sind administrative Zugänge ausschließlich Administratoren und ausschließlich zur Erledigung administrativer Tätigkeiten vorbehalten? Findet die alltägliche Nutzung Ihrer Systeme ohne Admin-Privilegien statt?	☐ Ja	☐ Nein
5.1.4	Werden Zugänge für Ihre IT-Infrastruktur konsequent nur gewährt, wenn sie für die Aufgabenerfüllung notwendig sind?	☐ Ja	☐ Nein
5.1.5	Werden administrative Zugänge regelmäßig nach einem festgelegten Turnus auf deren Notwendigkeit überprüft?	☐ Ja	☐ Nein
5.1.6	Haben Sie Geräte, die über das Internet erreichbar oder im mobilen Einsatz sind, mit einem zusätzlichen Schutz vor unberechtigtem Zugriff versehen?	☐ Ja	☐ Nein

5.2 Datensicherung

5.2.1	Schützen Sie sich vor dem Verlust der wichtigsten Unternehmensdaten durch eine mindestens wöchentliche Datensicherung?	☐ Ja	☐ Nein
5.2.2	Werden Ihre Datensicherungsmedien physisch getrennt von den gesicherten Systemen aufbewahrt?	☐ Ja	☐ Nein
5.2.3	Werden der unberechtigte Zugriff auf die Datensicherungen sowie deren nachträgliche Manipulation durch technische Maßnahmen verhindert?	☐ Ja	☐ Nein
5.2.4	Stellen Sie durch regelmäßige Tests nach einem festgelegten Turnus sicher, dass Ihre Datensicherung und -wiederherstellung funktionieren?	☐ Ja	☐ Nein

5.3 Sicherheitsupdates und Schutz vor Schadsoftware

5.3.1	Stellen Sie sicher, dass alle Systeme auf aktuellem Stand sind und installieren Sie Sicherheitsupdates automatisch oder zeitnah?	☐ Ja	☐ Nein
5.3.2	Wird die Installation von Sicherheits-Patches für Ihre IT zentral gesteuert?	☐ Ja	☐ Nein
5.3.3	Verfügen alle informationsverarbeitenden Systeme über einen Schutz gegen Schadsoftware, der automatisch auf dem aktuellen Stand gehalten wird (z.B. Virenscanner, Code Signing, Application Firewall oder ähnlich wirksame Maßnahmen)?	☐ Ja	☐ Nein

5.4 Verantwortlichkeiten

5.4.1	Gibt es einen Verantwortlichen für die IT-Sicherheit?	☐ Ja	☐ Nein
5.4.2	Gibt es einen Verantwortlichen für die Einhaltung datenschutzrechtlicher Vorgaben?	☐ Ja	☐ Nein
5.4.3	Werden alle internen und externen Mitarbeiter regelmäßig über Maßnahmen zur Informationssicherheit geschult? Sind sie verpflichtet, diese einzuhalten?	☐ Ja	☐ Nein
5.4.4	Ist Ihr IT-Notfall- und -Wiederanlauf-Konzept schriftlich fixiert und benennt es Verantwortliche?	☐ Ja	☐ Nein

5.5 Schutzmaßnahmen

5.5.1	Erfolgt der Zugriff auf Ihre interne IT-Infrastruktur über öffentliche oder drahtlose Netze ausschließlich verschlüsselt?	☐ Ja	☐ Nein
5.5.2	Ist Ihr IT-Netzwerk nach Kritikalität der Systeme in unterschiedliche Zonen aufgeteilt?	☐ Ja	☐ Nein
5.5.3	Werden sensible Daten (z.B. personenbezogene Daten und Geschäftsgeheimnisse) bei Datenversand verschlüsselt?	☐ Ja	☐ Nein
5.5.4	Führen Sie für besonders kritische IT-Systeme regelmäßig Risikoanalysen nach einem festgelegten Turnus durch?	☐ Ja	☐ Nein

Ort und Datum

Unterschrift

Anhang

Zusatzfragebogen

Zusatzfragen bitte nur ausfüllen, wenn eine der o. g. Fragen 4.1 bis 4.5 mit „ja“ beantwortet wurde

1 E-Commerce (nur auszufüllen, wenn Frage 4.1 mit „ja“ beantwortet wurde)

1.1 Wird der Webshop selbstständig administriert und betrieben? ☐ Ja ☐ Nein

1.2 Speichern Sie Kreditkartendaten? ☐ Ja ☐ Nein

1.3 Nutzen Sie einen Payment-Dienstleister zu Abwicklung aller eingehenden bargeldlosen Zahlungsvorgänge? ☐ Ja ☐ Nein

2 Datenverarbeitung (nur auszufüllen, wenn Frage 4.2 mit „ja“ beantwortet wurde)

2.1 Verarbeiten Sie Daten, die besonderen gesetzlichen Verschwiegenheitspflichten unterliegen, wie z. B. Gesundheitsdaten?

☐ Nein ☐ Ja, und zwar _____

_____

_____

2.2 Verarbeiten oder speichern Sie Geschäftsgeheimnisse von Dritten? ☐ Ja ☐ Nein

2.3 Verarbeiten oder speichern Sie Finanz- oder Steuerdaten von Dritten? ☐ Ja ☐ Nein

3 Dienstleister (nur auszufüllen, wenn Frage 4.3 mit „ja“ beantwortet wurde)

3.1 Der Dienstleister ist in folgenden Bereichen für uns tätig:

Dienstleister _____

Dienstleistung _____

3.2 Existiert ein Dienstleistungsvertrag, in dem Verfügbarkeit, Updates und das Beheben von Sicherheitslücken geregelt sind? ☐ Ja ☐ Nein

3.3 Ist Ihr Dienstleister zertifiziert? Unternehmen Sie regelmäßig eine unabhängige Qualitätssicherung? ☐ Ja ☐ Nein

3.4 Haben Sie Ihren Dienstleister von der Haftung freigestellt?

☐ Nein ☐ Ja, und zwar in folgenden Fällen _____

_____

_____

3.5 Unterliegt Ihr Dienstleister dem einheitlichen Datenschutzrecht der Europäischen Union? ☐ Ja ☐ Nein

4 Nutzung privater Geräte (nur auszufüllen, wenn Frage 4.4 mit „ja“ beantwortet wurde)

4.1 Befinden sich die privaten Geräte in einem getrennten Netzwerk-Segment? ☐ Ja ☐ Nein

4.2 Haben die privaten Geräte Zugriff auf geschäftliche Dienste oder Infrastruktur? ☐ Ja ☐ Nein

5 Automatisierte Produktionssysteme (ICS) (nur auszufüllen, wenn Frage 4.5 mit „ja“ beantwortet wurde)

5.1 Befinden sich die IC-Systeme in einem separierten Netzwerk mit eingeschränkten Zugriffsmöglichkeiten? ☐ Ja ☐ Nein

5.2 Ist ein Fernzugriff auf die IC-Systeme wenn, dann nur mittels 2-Faktor-Authentifizierung möglich? ☐ Ja ☐ Nein

5.3 Wird für Systeme, die an ICS beteiligt sind, insbesondere auch Terminals, die Einhaltung besonderer Härtungsmaßnahmen sichergestellt? ☐ Ja ☐ Nein

5.4	Sind die Prozesse zum regelmäßigen und unplanmäßigen Einspielen von Sicherheitsupdates dokumentiert und erprobt?	☐ Ja	☐ Nein
5.5	Wird der Zugriff auf IC-Systeme an zentraler Stelle protokolliert und überwacht?	☐ Ja	☐ Nein
5.6	Sind Ihre mobilen an dem ICS beteiligten Geräte vor unberechtigtem Zugriff durch Verschlüsselung und Passwörter geschützt?	☐ Ja	☐ Nein
5.7	Erfolgt der Fernzugriff auf IC-Systeme ausschließlich auf verschlüsseltem Weg?	☐ Ja	☐ Nein
5.8	Werden Ihre Datensicherungsmedien physisch getrennt von den gesicherten Systemen aufbewahrt?	☐ Ja	☐ Nein
5.9	Sind die Prozesse zur Wiederherstellung eines betriebsbereiten Zustandes dokumentiert und werden sie regelmäßig erprobt?	☐ Ja	☐ Nein
5.10	Stellen Sie durch regelmäßige Tests nach einem festgelegten Turnus sicher, dass Ihre Datensicherung und -wiederherstellung funktionieren?	☐ Ja	☐ Nein
5.11	Ist die Nutzung privater Geräte im ICS-Segment gestattet?	☐ Ja	☐ Nein

Ort und Datum

Unterschrift