Fragebogen zum Abschluss einer ERGO Cyber-Versicherung für Unternehmen mit einem Umsatz bis 50 Mio. Euro

(Für Unternehmen mit einem Umsatz über 50 Mio. Euro bitte Fragebogen 50078021 verwenden.)

Agenturinformationen

Name des Vermittlers

Agenturnummer

Bitte senden Sie den Fragebogen an das Gruppenpostfach: **VHCD@ergo.de**

I. Allgemeine Informationen zum Versicherungsnehmer

1. Name des Antragstellers, ggfs. Rechtsform:

Anrede: ☐ Herr ☐ Frau ☐ Firma ☐ keine

Titel, Vorname, Zuname/Firma

2. Anschrift:

Straße/Hausnummer

PLZ/Ort

Website (verpflichtende Eingabe und ohne www.)

3. Tochterunternehmen/Niederlassung:

(weitere ggf. auf separater Anlage, bitte benennen Sie uns auch die Standorte mit Sitz im europäischen oder außereuropäischen Ausland)

4. Branche/Unternehmenstätigkeit:

5. Anzahl Mitarbeiter:

6. Jahresumsatz: (in Euro letztes Geschäftsjahr)

II. Angaben zum Versicherungsumfang

7. Gewünschte Versicherungsleistungen:

pauschale Entschädigungsgrenze in Euro (z. B.):	Selbstbeteiligung in Euro
☐ 100.000	
☐ 300.000	☐ 1.000
☐ 500.000	☐ 2.500
☐ 1.000.000	☐ 5.000
☐ Andere:	☐ 10.000

Zusatzbaustein Cyber-Prävention: ☐ Ja ☐ Nein

Die Leistungsinhalte der Pakete können Sie der Tabelle auf der letzten Seite entnehmen.

☐ Komfort:	☐ Premium:
Für diesen Baustein wird ein Zuschlag von 20% auf die Jahresnettoprämie berechnet, mindestens jedoch 150,00 Euro, maximal 3.000 Euro.	Für diesen Baustein wird ein Zuschlag von 20% auf die Jahresnettoprämie berechnet, mindestens jedoch 300,00 Euro, maximal 3.000 Euro.

Daten des Ansprechpartners für Perseus:

Name: E-Mail-Adresse:

Telefonnummer:

8. Vorschäden:

Gab es in Ihrem Unternehmen in den letzten 5 Jahren Umstände oder Schäden, welche Gegenstand des hier gewünschten Versicherungsschutzes gewesen wären? ☐ Ja ☐ Nein

Falls ja, bitte ausfüllen:

Datum

Ursache des Schadens

Höhe des Schadens

Welche Maßnahmen wurden eingeleitet, um künftige Schäden dieser Art zu vermeiden?

III. Wichtige Mitteilung zu den Folgen einer Anzeigepflichtverletzung

Werden die im Risikofragebogen gestellten Fragen, soweit sie für die Übernahme der Gefahr erheblich sind, nicht wahrheitsgemäß oder nicht vollständig beantwortet, können wir den Vertrag unter Einhaltung einer Frist von einem Monat kündigen. Bei Vorsatz oder grober Fahrlässigkeit können wir sogar von dem Vertrag zurücktreten. Sie haben dann von Anfang an keinen Versicherungsschutz, es sei denn, durch die Verletzung der Anzeigepflicht ist uns kein Nachteil entstanden. Unser Rücktritts- und Kündigungsrecht ist – außer bei Vorsatz – ausgeschlossen, wenn wir den Vertrag auch bei Kenntnis der nicht angezeigten Umstände, wenn auch zu anderen Bedingungen, geschlossen hätten. Die Vertragsanpassung, etwa in Form eines Risikoausschlusses oder einer Beitragserhöhung, wird auf unser Verlangen rückwirkend, bei einer von Ihnen nicht zu vertretenden Pflichtverletzung ab der laufenden Versicherungsperiode wirksam. Durch die rückwirkende Einfügung eines Risikoausschlusses kann Ihr Versicherungsschutz für einen eingetretenen oder zukünftigen Versicherungsfall ebenfalls entfallen.

IV. Zusatzinformationen bei Umsatz bis 10 Millionen Euro

9. Speichern Sie weniger als 20.000 personenbezogene Datensätze*?

☐ Ja ☐ Nein

*Ein Kunde ist ein Datensatz.

V. Zusatzinformationen bei Umsatz ab 10 Millionen Euro

Im folgenden Kapitel werden Fachbegriffe benutzt. Diese sind mit einem Sternchen* markiert. Eine entsprechende Erläuterung finden Sie auf der letzten Seite im Glossar.

Wie viele Datensätze (Kunden und Mitarbeiter) sind auf Ihren IT-Systemen gespeichert?

☐ Personenbezogene Daten — Anzahl der Datensätze

☐ Personenbezogene Gesundheitsdaten — Anzahl der Datensätze

☐ Kreditkartendaten — Anzahl der Datensätze

ERGO

1. Awareness-Schulungen
Welche Anforderungen erfüllen Ihre Weiterbildungen zum Thema Informationssicherheit (Awareness Schulungen)?

- ☐ Die Schulungen sind verpflichtend für alle Mitarbeiter mit Zugang zu IT-Systemen
- ☐ Es wird geprüft und dokumentiert, dass die Schulungen mindestens jährlich durchgeführt werden; bei Neueinstellungen innerhalb der ersten 3 Monate
- ☐ Die Schulung umfasst mindestens die Themen: Social Engineering, Informationen über Cyber-Bedrohungen und Grundlagen der IT-Sicherheit
- ☐ Zusätzlich zur Schulung werden Phishing-Kampagnen* jährlich durchgeführt
- ☐ Keine der genannten Anforderungen wird erfüllt

2. Kennwortrichtlinie
Welche Voraussetzungen erfüllt Ihre Kennwortrichtlinie?

- ☐ Mindestens 8 Zeichen bestehend aus mindestens einem Buchstaben, einer Ziffer und einem Sonderzeichen
- ☐ Alle Mitarbeiter verwenden einen Passwort Safe bzw. Passwort Manager*
- ☐ Keine Voraussetzung ist komplett erfüllt oder es gibt keine Richtlinie

3. Segmentierung
Welche Bereiche werden in Ihrem Netzwerk segmentiert?

- ☐ Demilitarisierte Zone (DMZ)*
- ☐ hochkritische Bereiche (z.B. Produktion (OT) oder Point of Sales; sofern vorhanden)
- ☐ Standorte (sofern vorhanden)
- ☐ Clients und Server
- ☐ keine Segmentierung vorhanden

4. Altsysteme (End of Life)
Wie schützen Sie Altsysteme, die nicht mehr vom Hersteller mit Sicherheitsupdates versorgt werden?

- ☐ keine Altsysteme vorhanden
- ☐ Altsysteme sind in einem separatem Netzwerk (keine Verbindung zu allen anderen Netzwerken)
- ☐ Netzwerksegmentierung inkl. Firewall*
- ☐ Überwachung des Datenverkehrs*
- ☐ Altsysteme haben keinen Internetzugang
- ☐ Eine vollständige Ablösung der Altsysteme ist geplant bis zum: _____
- ☐ keine der vorgegebenen Antworten passt oder es sind keine Gegenmaßnahmen vorhanden

5. Notfallplan
Welche Anforderungen erfüllt Ihr Plan zur Reaktion auf kritische Informationssicherheitsvorfälle (Notfallplan)?

- ☐ Ist physisch vorhanden und den Schlüsselpersonen (insbesondere oberste Geschäftsleitung, IT-Leitung und Informations-sicherheits-/Datenschutzbeauftragter) bekannt
- ☐ Wird mindestens jährlich überprüft
- ☐ Wird mindestens jährlich in einer Notfall-Übung geprobt
- ☐ Notfallplan nicht vorhanden

6. Multi-Faktor-Authentifizierung (MFA)
Welche Zugänge/Systeme sichern Sie durch einen zweiten Faktor (2FA/MFA) ab?

- ☐ alle Cloud-Zugänge
- ☐ alle administrativen Systeme
- ☐ alle Fernzugriffe (ohne Site-to-Site) auf die eigenen IT-Systeme
- ☐ keine

VI. Unterschrift und Bestätigungen

Der/die Unterzeichner(in) erklärt mit Wirkung für und gegen die Gesellschaft als Versicherungsnehmer, ihre Tochterunternehmen/Niederlassungen, die obigen Fragen vollständig und wahrheitsgemäß beantwortet zu haben.

Dieser ausgefüllte Fragebogen und die eventuellen Anlagen sind Grundlage der Versicherung und werden deshalb Bestandteil eines etwaigen Versicherungsvertrags sein. Für den Fall, dass ein Versicherungsvertrag zustande kommt, gelten die in diesem Fragebogen und eventuellen Anlagen gemachten Angaben als vorvertragliche Angaben im Sinne der §§ 19 ff. VVG. Der Versicherungsschutz besteht frei von bekannten Ansprüchen/Schäden.

Datum	Antragsteller/Vertretungsberechtigter	Vermittler/ORGA

VII. Begriffserklärung/Glossar

1.	Bei **Phishing Kampagnen** werden E-Mails verschickt, die Phishing-Mails stark ähneln. Fällt ein Nutzer auf eine solche E-Mail rein, dann bekommt er einen Hinweis und eine entsprechende Schulung. Durch solche Kampagnen werden Mitarbeiter praxisnah geschult Phishing-Mails erkennen zu können.
2.	Ein Passwort Safe bzw. **Passwort Manager** dient zur sicheren Verwaltung von Passwörtern.
3.	Eine **Demilitarisierte Zone (DMZ)** bezeichnet man als den Bereich zwischen externen (z. B. Internet) und internen Netzwerken. Typischerweise ist diese Zone z. B. durch Firewalls besonders gesichert.
4.	Bei der **Netzwerksegmentierung** wird das Altsystem in einem extra Netzwerksegment betrieben. Das Segment ist mindestens durch eine **Firewall**, die sehr streng konfiguriert ist, geschützt. Bei der **Überwachung des Datenverkehrs** wird der aus- und eingehende Datenverkehr auf Anomalien untersucht. Dadurch kann ein Angriff schnellstmöglichst festgestellt werden.

VIII. Zusatzbedingungen für den Baustein „Cyber-Prävention“

Der Zusatzbaustein enthält insbesondere folgende Leistungen:

	Cyber-Prävention Komfort	**Cyber-Prävention Premium**
Onlinetraining (Cyber-Sicherheit, DSGVO)	✓	✓
Browser-Check	✓	✓
Blog, Newsletter, Glossar	✓	✓
Phishing-Kampagnen	✓	✓
Tools (E-Mail-Scanner, Datensicherheits-Check)	✓	✓
Reporting (IT-Sicherheits-Score, Phishing-Report)	✓	✓
Automatische Aktivierung der Mitarbeiter	✓	✓
Gefahrenwarnung bei akuten Cyber-Bedrohungen	✓	✓
Individualisierbarer Notfallplan	✓	✓
SB-Reduzierung um 50%, maximal um 2.500,00 EUR im ersten Schadensfall	✓	✗
Richtlinien und Leitfäden (Datensicherungsstrategie, Datenschutz, Social Media, u.a.)	✗	✓
Security Baseline Check **im Wert von 650 €**	✗	✓
SB-Verzicht um bis zu 5.000,00 EUR im ersten Schadensfall	✗	✓
Verzicht auf Einrede der groben Fahrlässigkeit bis 5.000,00 EUR	✗	✓
Verzicht auf Schadensfallkündigung	✗	✓