

Berkley Cyber Risk Protect

Verlängerungsfragebogen zu Ihrer Cyber-Versicherung

Unser Cyber-Verlängerungsfragebogen dient dazu, einen Überblick über Veränderungen in Ihrem Unternehmen zu erhalten. Bitte beziehen Sie sich bei den Angaben auf die Versicherungsnehmerin inkl. Tochtergesellschaften.

Überprüfung der Stammdaten der Versicherungsnehmerin

Firmierung:			
Straße:		Postleitzahl:	Ort:
Anzahl an Mitarbeitenden:		davon Mitarbeitende in der IT-Abteilung:	
Davon Mitarbeitende mit PC-Arbeitsplatz:		Branche:	
Website(s):		Börsennotierung:	Ja Nein

Betriebs-/ Produktbeschreibung

Konsolidierte Finanzkennzahlen

Konsolidierte Kennzahlen in EUR	Abgeschlossenes Geschäftsjahr in EUR	Prognose laufendes Geschäftsjahr in EUR
Umsätze insgesamt		
• davon in Deutschland/ Österreich		
• davon in der EU, EWR und Schweiz		
• davon in USA/ Kanada		
• davon Rest der Welt		
• Onlineumsätze/ e-commerce (über eigene Website generiert)		
Bilanzsumme (insbesondere bei Finanzdienstleistern)		
Bruttojahresgewinn		
Rohertrag (Umsatz abzüglich Materialkosten/ Einkaufspreis)		
IT-Budget		

Unternehmensprofil

Gibt es neue oder abweichende Geschäftstätigkeiten, bzw. sind diese in den nächsten 12 Monaten geplant? Falls ja, bitte Details:

Ja Nein

Veränderungen/ Verschlechterungen/ negative Abweichungen zu den uns überlassenen Risikoinformationen aus dem Vorjahr (Fragebogen, Risikobericht, etc.)

Gab es in den letzten 12 Monaten relevante Veränderungen, insbesondere Verschlechterungen/ negative Abweichungen, bzw. sind Veränderungen geplant (bezogen auf den vorherigen Fragebogen, Risikobericht, unterjährig mitgeteilte Risikoinformationen, etc.)?

Falls ja, bitte Details:

Ja Nein

Anzahl personenbezogener Daten im Unternehmen

1 – 20.000 Datensätze	20.001 - 100.000 Datensätze
100.001 - 500.000 Datensätze	500.001 - 1.000.000 Datensätze
über 1.000.000 Datensätze	Andere:

Nutzen Sie bei den **Ja-/Nein-Fragen** gerne die pdf-Kommentar-Funktion, wenn Sie uns etwas mitteilen möchten.

So geht's: Im pdf rechte Maustaste klicken, "Kommentar hinzufügen" auswählen, Kommentar schreiben, "Beitragen" auswählen, Fenster schließen und den Kommentar-Icon mit der Maus an die entsprechende Stelle im Fragebogen ziehen.

Auflagen gemäß der aktuellen Police

Sind alle Auflagen der aktuellen Police innerhalb der vereinbarten Fristen vollständig umgesetzt worden und werden dauerhaft fortgeführt? **Wenn nein:** Welche Auflagen sind nicht fristgerecht umgesetzt worden und bis wann erfolgt eine vollständige Umsetzung?

Ja Nein

Datenschutz

Vertrauliche Daten und personenbezogene Daten werden verschlüsselt:

a) bei der Speicherung	Ja	Nein
b) bei der Übertragung (intern und extern)	Ja	Nein

Die Datenschutzrichtlinie wird jährlich auf Konformität zu den geltenden Datenschutzregeln überprüft und notwendige Anpassungen zeitnah umgesetzt.	Ja	Nein
--	----	------

Die Vorschriften der DSGVO bzw. vergleichbarer Bestimmungen werden vollständig erfüllt.	Ja	Nein
---	----	------

Bitte kommentieren Sie Ihre NEIN-Antworten:

IT-Schutzmaßnahmen

Es gibt eine kontinuierliche Bestandsaufnahme der eingesetzten Soft-/ Hardware inkl. Schwachstellenanalyse.	Ja	Nein
---	----	------

Es existiert eine Firewall zwischen internem Netzwerk und Internet. Die Firewall wird regelmäßig aktualisiert und angepasst sowie der Datenverkehr gefiltert und überwacht.	Ja	Nein
---	----	------

Es gibt einen kontinuierlichen und formalisierten Prozess zum Aufspielen von Patches, Updates, Firmware, Software, etc. nach Herstellervorgaben bzw. die empfohlen Maßnahmen werden umgesetzt.	Ja	Nein
--	----	------

Patches/ Updates/ kritische Sicherheitslücken mit CVSS Score ab 7,0 bzw. BSI Bedrohungslage „orange und/oder „rot“ werden unverzüglich (72 Stunden) nach Herstellervorgaben geschlossen bzw. die empfohlen Maßnahmen werden umgesetzt. Alternative Dauer der Einspielung:	Ja	Nein
Patch-/ Updateinstallationen können durch den Benutzer nicht oder nur stark begrenzt (max. 12h) aufgeschoben werden.	Ja	Nein
Zugangsberechtigungen basieren auf Anwenderrollen nach dem Prinzip der niedrigsten Berechtigung und es gibt einen Prozess, der die Vergabe von Berechtigungen regelt. Nicht mehr benötigte Zugänge werden unverzüglich gelöscht/gesperrt.	Ja	Nein
Es werden mindestens täglich vollständige Backups durchgeführt und regelmäßig (mind. quartalsweise) geprüft – inkl. Wiederherstellungstest.	Ja	Nein
Es werden mehrere Backup Strategien angewendet wie Cloud Backups und lokale Backups.	Ja	Nein
Backups sind vom Firmennetzwerk getrennt.	Ja	Nein
Backups sind verschlüsselt oder unveränderlich (immutable).	Ja	Nein
Die Integrität von Backups kann vor der Wiederherstellung getestet werden, um Malware auszuschließen.	Ja	Nein
Es sind RPOs (Recovery Point Objectives) für alle kritischen Daten definiert.	Ja	Nein
Das Netzwerk ist nach Geschäftsfunktionen segmentiert (z.B. ist Datenverkehr zwischen verschiedenen Geschäftsfunktionen blockiert, außer für bestimmte Anforderungen notwendig).	Ja	Nein
Das Netzwerk ist nach geografischen Aspekten segmentiert (z.B. ist Datenverkehr zwischen Büros und verschiedenen Standorten blockiert, außer es ist für bestimmte Anforderungen notwendig).	Ja	Nein
Administrative Zugänge/ privilegierte Benutzerkonten werden ausschließlich zur Erledigung dieser Tätigkeiten genutzt. Für die alltägliche Nutzung (insbesondere Surfen im Internet, Email-Kommunikation) wird ein Benutzer-Konto ohne Admin/ privilegierte-Rechte verwendet.	Ja	Nein
Jeder Admin verwendet für administrative Tätigkeiten ausschließlich ein benutzerindividuelles Admin-Konto.	Ja	Nein
Die Erstellung von neuen oder die Änderung von bestehenden Admin-Accounts ist gegen Missbrauch geschützt und wird kontinuierlich überwacht.	Ja	Nein
Es sind Intrusion Detection Systeme (IDS) und Intrusion Prevention Systeme (IPS) implementiert. Diese werden regelmäßig aktualisiert und überwacht.	Ja	Nein
Eine EDR-Lösung (End Point Detection & Response) ist auf allen Endpunkten/Servern/ Clients aktiviert.	Ja	Nein
Eine XDR-Lösung (Extended Detection & Response) ist auf allen kritischen Endpunkten/Servern/ Clients implementiert.	Ja	Nein
Accounts werden nach einer bestimmten Anzahl an ungültigen Anmeldeversuchen temporär gesperrt.	Ja	Nein
Es gibt dokumentierte Prozesse wie neue Unternehmen in die IT-Infrastruktur und Sicherheitsrichtlinien integriert werden. Netzwerke/Systeme/Anwendungen werden erst nach Erreichen eines vergleichbaren Sicherheitsniveaus integriert.	Ja	Nein

Bitte kommentieren Sie Ihre NEIN-Antworten:

Multifaktor-Authentifizierung (MFA)

Die Multifaktor-Authentifizierung (MFA) ist für folgende Bereiche unternehmensweit implementiert:		
• Fernzugriff auf das Firmennetzwerk inkl. VPN.	Ja	Nein
• Privilegierte/Administratoren Benutzerkonten.	Ja	Nein
• Fernzugriff auf Cloud-basierte Anwendungen wie Office 365 oder Microsoft Azure.	Ja	Nein

- | | | |
|--|----|------|
| • Fernzugriff auf E-Mails inkl. Cloud-basierter E-Mail-Systeme (sofern keine VPN-Verbindung genutzt wird). | Ja | Nein |
|--|----|------|

Bitte kommentieren Sie Ihre NEIN-Antworten:

Cyber-Krisenmanagement

Folgende Sicherheitsmaßnahmen sind unternehmensweit vorhanden und wurden erfolgreich getestet:

- | | | |
|---|----|------|
| • Physischer IT-Notfallplan (BCP). | Ja | Nein |
| • Physischer Wiederanlaufplan (DRP). | Ja | Nein |
| • Redundante Auslegung kritischer Systeme. | Ja | Nein |
| • Krisenreaktionsplan in Bezug auf Datenschutzvorfälle. | Ja | Nein |
| • Die Kontaktdaten der Cyber-Krisenhotline von W. R. Berkley und das Vorgehen zur Schadenmeldung sind in den IT-Notfallplan integriert. | Ja | Nein |

Bitte kommentieren Sie Ihre NEIN-Antworten:

Operations Technology (OT)

Wird OT verwendet (sofern OT nicht verwendet wird, ist die Beantwortung der folgenden Fragen nicht notwendig)?	Ja	Nein
--	----	------

Ist die teilweise Aufrechterhaltung mittels Notbetrieb möglich?	Ja	Nein
---	----	------

Ist dieses Szenario bereits erfolgreich getestet worden?	Ja	Nein
--	----	------

Wie lange ist der Notbetrieb bis zum vollständigen Stillstand der Produktion/ Logistik möglich	Ja	Nein
--	----	------

Sofern OT um Einsatz ist, werden folgende Schutzmaßnahmen sind durchgehend umgesetzt:

- | | | |
|---|----|------|
| • Fernzugriffe sind nicht möglich. | Ja | Nein |
| • Fernzugriffe erfordern eine VPN-Verbindung. | Ja | Nein |
| • Fernzugriffe erfordern MFA. | Ja | Nein |
| • Fernzugriffe werden durchgehend protokolliert. | Ja | Nein |
| • Kontinuierliche Überwachung und bedarfsgerechte An-/ Abschaltung von Fernzugriffen. | Ja | Nein |
| • Schnittstellen an Terminals sind deaktiviert. | Ja | Nein |
| • OT befindet sich in einem separierten Netzwerk. | Ja | Nein |
| • Zugriffsrechte bestehen ausschließlich für die berechtigten User, die diese zwingend benötigen. | Ja | Nein |
| • Externe Wartungszugänge sind besonders gesichert (Freigabe, etc.). | Ja | Nein |
| • Produktionssysteme werden nach herstellervorgaben gepatched. | Ja | Nein |
| • Es sind Workarounds für nicht patchbare/ nicht unterstützbare Systeme, z.B. durch restriktives Application-Whitelisting für Produktions-IT implementiert. | Ja | Nein |
| • Produktionssysteme und -anwendungen sind vollwertig in die Backupstrategie integriert. | Ja | Nein |

Bitte kommentieren Sie Ihre NEIN-Antworten:

Outsourcing: Nutzung von externen IT-Dienstleistern, IT-Services und Cloud-Services

Externe Dienstleister werden regelmäßig (mind. jährlich) überprüft, dass diese die erforderlichen Sicherheitsanforderungen bzw. Mindeststandards zum Datenschutz und IT-/ Cyber-Sicherheit erfüllen.	Ja	Nein
Es existiert eine schriftliche Outsourcing-Vereinbarung inkl. Sicherheitsanforderungen, die von diesem Dienstleister einzuhalten ist.	Ja	Nein
Es besteht ein Service Level Agreement (SLA) inkl. Vertragsstrafen, die bei Nichteinhaltung durch den Dienstleister zu zahlen sind.	Ja	Nein
Es bestehen <u>keine</u> Freistellungs- und/oder haftungsbegrenzende Vereinbarungen mit den externen Dienstleistern.	Ja	Nein

Bitte kommentieren Sie Ihre NEIN-Antworten:

End-of-life, end-of-Service, legacy Systeme

Werden End-of-life (EoL), end-of-Service (EoS) oder Legacy Systeme verwendet?	Ja	Nein
Es erfolgt eine kontinuierliche Bestandsaufnahme und Bewertung nach Kritikalität von EOL/EOS-Assets sowie Ableitung und Umsetzung von Sicherheitsmaßnahmen.	Ja	Nein
Es gibt einen Migrationsplan. Wenn ja: bis	Ja	Nein
Es wird ein verlängerter Herstellersupport verwendet.	Ja	Nein
Betrieb in einem separierten Netzwerk.	Ja	Nein
Es besteht kein direkter Internetzugang.	Ja	Nein
Durchgehende Kontrolle des Datenverkehrs.	Ja	Nein

Bitte kommentieren Sie Ihre NEIN-Antworten:

IT-Roadmap/ Pläne für das nächste Geschäftsjahr (bitte kurze Beschreibung/Auflistung)

Hinweis

Der Unterzeichner erklärt, die obenstehenden Fragen vollständig und wahrheitsgemäß beantwortet zu haben, keine für diese Übernahme/ Fortführung dieser Versicherung wichtigen Aspekte verschwiegen oder nicht richtig wiedergegeben zu haben und verpflichtet sich, Änderungen, die sich vor oder nach dem Abschluss des Vertrages bzw. Vertragsverlängerung ergeben, unverzüglich und ohne Aufforderung dem Versicherer mitzuteilen (vgl. §§19 ffVVG).

Diese ausgefüllte Erklärung und die eventuellen Anlagen werden Bestandteil des Versicherungsvertrages. Mit Unterschrift(en) wird bestätigt, dass vorstehende Angaben vollständig und richtig sind. Der Versicherer ist berechtigt, im Schadenfall sämtliche Angaben zu überprüfen und bei Falschangaben den Versicherungsschutz zu versagen. Die von uns im Verlängerungsfragebogen abgefragten Risikoinformationen sind für uns wesentlich für die Risikobewertung und Fortführung bzw. Anpassung des Versicherungsvertrages. Auf die Rechtsfolgen der Verletzung der gesetzlichen Anzeigepflicht (Seite 7) wird hingewiesen.

Datenschutz

Die Versicherungsnehmerin willigt ein, dass der Versicherer im erforderlichen Umfang Daten, die sich aus den Antragsunterlagen oder der Vertragsdurchführung (Prämien, Versicherungsfälle, Risiko-/Vertragsänderungen) ergeben, an Rückversicherer und Unternehmen der Berkley Gruppe sowie falls erforderlich an (externe) Dienstleister zur Beurteilung des Risikos und der Ansprüche an andere Versicherer/Gutachter/Rechtsanwälte/ Krisendienstleister etc. übermitteln darf. Diese Einwilligung gilt auch unabhängig vom Zustandekommen des Versicherungsvertrages sowie für entsprechende Prüfungen bei anderweitig beantragten Versicherungsverträgen und bei künftigen Anträgen.

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

Unsere aktuelle Datenschutzerklärung finden Sie unter: <https://www.berkleyeurope.com/datenschutz#deutschland>

Bitte beachten Sie die gesonderte Mitteilung über die Folgen einer Verletzung der vorvertraglichen Anzeigepflicht im Anschluss an diesen Fragebogen.

Ort, Datum

Unterschrift eines Repräsentanten der
Versicherungsnehmerin i.S.d.
Versicherungsbedingungen

Firmenstempel

Gesonderte Mitteilung über die Folgen einer Verletzung der vorvertraglichen Anzeigepflicht

Gemäß § 19 Absatz 1 VVG hat der Versicherungsnehmer „bis zur Abgabe seiner Vertragserklärung die ihm bekannten Gefahrumstände, die für den Entschluss des Versicherers, den Vertrag mit dem vereinbarten Inhalt zu schließen, erheblich sind und nach denen der Versicherer in Textform gefragt hat, dem Versicherer anzuzeigen. Stellt der Versicherer nach der Vertragserklärung des Versicherungsnehmers, aber vor Vertragsannahme Fragen im Sinn des Satzes 1, ist der Versicherungsnehmer auch insoweit zur Anzeige verpflichtet.“

Gemäß § 19 Absatz 5 Seite 1 VVG stehen dem Versicherer Rechte wegen einer Verletzung der vorvertraglichen Anzeigepflicht nur zu, „wenn er den Versicherungsnehmer durch gesonderte Mitteilung in Textform auf die Folgen einer Anzeigepflichtverletzung hingewiesen hat.“

Deshalb weisen wir Sie auf die nachstehenden gesetzlichen Regelungen über die Folgen einer Anzeigepflichtverletzung hin:

§ 19 VVG (Anzeigepflicht)

(2) Verletzt der Versicherungsnehmer seine Anzeigepflicht nach Absatz 1, kann der Versicherer vom Vertrag zurücktreten.

(3) Das Rücktrittsrecht des Versicherers ist ausgeschlossen, wenn der Versicherungsnehmer die Anzeigepflicht weder vorsätzlich noch grob fahrlässig verletzt hat. In diesem Fall hat der Versicherer das Recht, den Vertrag unter Einhaltung einer Frist von einem Monat zu kündigen.

(4) Das Rücktrittsrecht des Versicherers wegen grob fahrlässiger Verletzung der Anzeigepflicht und sein Kündigungsrecht nach Absatz 3, Satz 2 sind ausgeschlossen, wenn er den Vertrag auch bei Kenntnis der nicht angezeigten Umstände, wenn auch zu anderen Bedingungen, geschlossen hätte. Die anderen Bedingungen werden auf Verlangen des Versicherers rückwirkend, bei einer vom Versicherungsnehmer nicht zu vertretenden Pflichtverletzung ab der laufenden Versicherungsperiode Vertragsbestandteil.

(5) Dem Versicherer stehen die Rechte nach den Absätzen 2 bis 4 nur zu, wenn er den Versicherungsnehmer durch gesonderte Mitteilung in Textform auf die Folgen einer Anzeigepflichtverletzung hingewiesen hat. Die Rechte sind ausgeschlossen, wenn der Versicherer den nicht angezeigten Gefahrumstand oder die Unrichtigkeit der Anzeige kannte.

(6) Erhöht sich im Fall des Absatzes 4, Satz 2 durch eine Vertragsänderung die Prämie um mehr als zehn Prozent

oder schließt der Versicherer die Gefahrabsicherung für den nicht angezeigten Umstand aus, kann der Versicherungsnehmer den Vertrag innerhalb eines Monats nach Zugang der Mitteilung des Versicherers ohne Einhaltung einer Frist kündigen. Der Versicherer hat den Versicherungsnehmer in der Mitteilung auf dieses Recht hinzuweisen.

§ 20 VVG (Vertreter des Versicherungsnehmers)

Wird der Vertrag von einem Vertreter des Versicherungsnehmers geschlossen, sind bei der Anwendung des § 19 Absatz 1 bis 4 und des § 21 Absatz 2 Satz 2 sowie Absatz 3 Satz 2 sowohl die Kenntnis und die Arglist des Vertreters als auch die Kenntnis und die Arglist des Versicherungsnehmers zu berücksichtigen. Der Versicherungsnehmer kann sich darauf, dass die Anzeigepflicht nicht vorsätzlich oder grob fahrlässig verletzt worden ist, nur berufen, wenn weder dem Vertreter noch dem Versicherungsnehmer Vorsatz oder grobe Fahrlässigkeit zu Last fällt.

§ 21 VVG (Ausübung der Rechte des Versicherers)

(1) Der Versicherer muss die ihm nach § 19 Absatz 2 bis 4 zustehenden Rechte innerhalb eines Monats schriftlich geltend machen. Die Frist beginnt mit dem Zeitpunkt, zu dem der Versicherer von der Verletzung der Anzeigepflicht, die das von ihm geltend gemachte Recht begründet, Kenntnis erlangt. Der Versicherer hat bei der Ausübung seiner Rechte die Umstände anzugeben, auf die er seine Erklärung stützt; er darf nachträglich weitere Umstände zur Begründung seiner Erklärung angeben, wenn für diese die Frist nach Satz 1 nicht verstrichen ist.

(2) Im Fall eines Rücktritts nach § 19 Absatz 2 nach Eintritt des Versicherungsfalles ist der Versicherer nicht zur Leistung verpflichtet, es sei denn, die Verletzung der Anzeigepflicht bezieht sich auf einen Umstand, der weder für den Eintritt oder die Feststellung des Versicherungsfalles noch für die Feststellung oder den Umfang der Leistungspflicht des Versicherers ursächlich ist. Hat der Versicherungsnehmer die Anzeigepflicht arglistig verletzt, ist der Versicherer nicht zur Leistung verpflichtet.

(3) Die Rechte des Versicherers nach § 19 Absatz 2 bis 4 erlöschen nach Ablauf von fünf Jahren nach Vertragschluss; dies gilt nicht für Versicherungsfälle, die vor Ablauf dieser Frist eingetreten sind. Hat der Versicherungsnehmer die Anzeigepflicht vorsätzlich verletzt, beläuft sich die Frist auf zehn Jahre.

§ 22 VVG (Arglistige Täuschung)

Das Recht des Versicherers, den Vertrag wegen arglistiger Täuschung anzufechten, bleibt unberührt.