

Berkley Cyber Risk Protect Risikoerfassung für mittelständische Unternehmen

Bitte beziehen Sie sich bei Ihren Angaben auf die Versicherungsnehmerin inkl. Tochtergesellschaften.

Stammdaten zur Versicherungsnehmerin

Firmierung:			
Straße:		Postleitzahl:	Ort:
Mitarbeiteranzahl:		Mitarbeiteranzahl in der IT-Abteilung:	
Gründungsdatum:		Börsennotierung:	Ja <input type="checkbox"/> Nein <input type="checkbox"/>
Website(s):		Branche:	

Tätigkeitsbeschreibung

Finanzkennzahlen

Bitte die (konsolidierten) Kennzahlen in EUR angeben	Prognose lfd. Geschäftsjahr	Letztes Geschäftsjahr 20__
Umsätze insgesamt		
• davon in Deutschland/Österreich		
• davon in der EU, EWR und Schweiz		
• davon in USA/Kanada		
• davon Rest der Welt		
• Onlineumsätze		
Bilanzsumme		
Bruttojahresgewinn		
Rohertrag (Umsatz abzüglich Materialkosten/Einkaufspreis)		
IT-Budget		

Tochtergesellschaften

Bitte listen Sie alle Tochtergesellschaften und Niederlassungen außerhalb der EU/EWR auf (ggf. Zusatzblatt nutzen):

Firmierung	Land	Umsatz	Abweichende Tätigkeit zur VN

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, nämlich ca.:

Datenschutz

Es existiert eine schriftliche Datenschutzrichtlinie.	Ja	Nein
Die Datenschutzrichtlinie wird jährlich auf Konformität zu den geltenden Datenschutzregeln überprüft.	Ja	Nein
Die Datenschutzrichtlinie wurde durch einen externen Anwalt geprüft.	Ja	Nein
Es gibt einen unternehmensweiten Datenschutzbeauftragten (intern bzw. extern).	Ja	Nein
Alle Mitarbeiter sind im Umgang mit personenbezogenen Daten geschult, haben eine Vertraulichkeitserklärung unterschrieben oder eine entsprechende Regelung in Ihrem Arbeitsvertrag.	Ja	Nein
Es gibt Zugangsberechtigungen für Benutzer zu personenbezogenen Daten inkl. regelmäßiger Prüfung.	Ja	Nein
Vertrauliche Daten und personenbezogene Daten werden verschlüsselt:		
a) bei der Speicherung	Ja	Nein
b) bei der Übertragung (intern und extern)	Ja	Nein
Die Vorschriften der DSGVO bzw. vergleichbarer Bestimmungen werden vollständig erfüllt.	Ja	Nein
Es ist ein strukturierter Prozess zur Bearbeitung von Auskunftsrechten Betroffener sowie zur Löschung personenbezogener Daten i.S.d. DSGVO etabliert.	Ja	Nein
Informationen werden nach Schutzzielanforderungen (Vertraulichkeit, Integrität, Verfügbarkeit) klassifiziert.	Ja	Nein
Externe Dienstleister werden vor Beauftragung überprüft, dass die benötigten Sicherheitsanforderungen zum Datenschutz erfüllt werden.	Ja	Nein
Es wurde innerhalb der letzten 12 Monate eine Datenschutzfolgeabschätzung vorgenommen.	Ja	Nein
Mobile Endgeräte, Festplatten und Wechseldatenträger sind grundsätzlich verschlüsselt.	Ja	Nein
Der Verlust von Firmenhardware muss unverzüglich dem Unternehmen angezeigt werden.	Ja	Nein
Es ist eine Mobile Device Management-Lösung (MDM) implementiert und es ist möglich die Daten auf den mobilen Geräten aus der Ferne zu löschen.	Ja	Nein

Physische Sicherheit: Serverraum/Rechenzentrum

Kritische Systeme sind redundant ausgelegt (Aktiv-/Aktiv- oder Passiv-/Passiv- Architektur).	Ja	Nein
Für kritische Systeme ist eine unterbrechungsfreie Stromversorgung und Klimatisierung vorhanden.	Ja	Nein
Die unterbrechungsfreie Stromversorgung wird jährlich gewartet und getestet.	Ja	Nein
Physische Zugangskontrollen für Rechenzentren und Serverräume sind vorhanden.	Ja	Nein

Risikomanagement

Es gibt regelmäßige Mitarbeiterschulungen/Trainings zum Thema Informationssicherheit, Datenschutz sowie Informationen über aktuelle Gefahrenpotenziale (z.B. Trojaner, Phishing, Ransomware).	Ja	Nein
Es gibt zusätzlich rollenbezogene/zielgruppenbezogene Sensibilisierungs-/Schulungsmaßnahmen (z.B. für Admins, Entwickler, Führungskräfte).	Ja	Nein
Es werden regelmäßige Phishing-Tests durchgeführt.	Ja	Nein
Mitarbeiter können verdächtige E-Mails als „Phishing-Angriff“ zur Prüfung melden.	Ja	Nein
Es existiert eine unternehmensweite Informationsrichtlinie bzw. Leitlinien im Umgang mit Informationssystemen, die an alle Mitarbeiter kommuniziert ist.	Ja	Nein

Es wurden unternehmenskritische Informationssysteme identifiziert und geeignete Kontrollinstrumente implementiert.	Ja	Nein
Es besteht ein verpflichtendes 4-Augen-Prinzip bei Überweisungen/Auszahlungen ab 25.000 EUR.	Ja	Nein
Es wurden geeignete Maßnahmen getroffen, um unautorisierte Warenlieferungen zu vermeiden.	Ja	Nein
Bei Telekommunikationsanlagen wurden voreingestellte Passwörter und Pins geändert.	Ja	Nein
Es besteht eine zwingende 2-Faktor Authentifizierung bei Anmeldung im Online-Banking und bei Überweisungsfreigaben.	Ja	Nein
Es werden regelmäßig Penetrationstests durchgeführt. Datum des letzten Tests: _____	Ja	Nein
Die identifizierten Schwachstellen werden in Anhängigkeit der Kritikalität behoben.	Ja	Nein
Ein zertifiziertes Informationsmanagementsystem (ISMS) z.B. nach ISO 27001 ist implementiert.	Ja	Nein
Ihr Unternehmen erhält regelmäßig Informationen zu Bedrohungen, Sicherheitslücken, Schwachstellen.	Ja	Nein

IT-Schutzmaßnahmen

Auf allen IT-Systemen ist eine aktuelle Anti-Virus Software installiert, deren Aktualisierung zentral überwacht wird.	Ja	Nein
Es gibt einen zentralen/automatisierten Prozess zum Aufspielen von Patches, Updates, Firmware, Software, etc. nach Herstellervorgaben.	Ja	Nein
Kritische Systemänderungen, Updates und Patches werden in einer Testumgebung geprüft, bevor diese in die „Live“-Umgebung eingespielt werden.	Ja	Nein
Wie schnell werden kritische Patches unternehmensweit verteilt? _____		
Patchinstallationen können durch den Besitzer nicht aufgeschoben werden. Falls dies möglich ist, wie lange? _____	Ja	Nein
Es werden mindestens täglich <u>vollständige</u> Backups durchgeführt.	Ja	Nein
Backups werden regelmäßig geprüft – inkl. Wiederherstellungstest.	Ja	Nein
Backups sind vom Firmennetzwerk getrennt.	Ja	Nein
Backups sind verschlüsselt.	Ja	Nein
Es werden mehrere Backup-Strategien angewendet wie z.B. Cloud Backups und lokale Backups.	Ja	Nein
Der Zugriff auf Backups erfolgt mittels Authentifizierungsmechanismus außerhalb des Active Directory.	Ja	Nein
Die Integrität von Backups kann vor der Wiederherstellung getestet werden, um Malware auszuschließen.	Ja	Nein
Es gibt eine schriftliche Passwort-Policy inkl. Vorgaben zur Komplexität und zeitlichen Gültigkeit (max. 90 Tage). Alternativ wird dies technisch erzwungen.	Ja	Nein
Sämtliche Standard-/Initial-Passwörter wurden geändert und durch komplexe Passwörter ersetzt.	Ja	Nein
Zugangsberechtigungen basieren auf Anwenderrollen nach dem Prinzip „need to know“ und es gibt einen Prozess der die Vergabe von Berechtigungen regelt.	Ja	Nein
Es gibt einen Prozess zur Einrichtung, Löschung, Sperrung oder Anpassung von Berechtigungen und Wiederherstellung von inventarisierten Informationen im Falle der Einstellung/Kündigung von Mitarbeitern, internen Jobwechseln sowie bei Kündigung externer Dritter mit Zugangsberechtigungen (z.B. Lieferanten bzw. Fernwartungszugänge).	Ja	Nein
Administrative Zugänge werden ausschließlich zur Erledigung administrativer Tätigkeiten genutzt. Für die alltägliche Nutzung (insbesondere Surfen im Internet und E-Mail-Kommunikation) wird ein Benutzerkonto ohne Admin-Rechte verwendet.	Ja	Nein

Jeder Admin verwendet für administrative Tätigkeiten ausschließlich ein benutzerindividuelles Admin-Konto.	Ja	Nein
Es erfolgt eine Härtung der IT-Systeme durch die Löschung bzw. Deaktivierung von Softwarebestandteilen oder Funktionen, die nicht benötigt werden.	Ja	Nein
Für PCs, Laptops, Server und mobile Endgeräte werden gesicherte Referenzkonfigurationen verwendet.	Ja	Nein
Mitarbeiter können ohne IT-Administratoren keine eigene Software installieren.	Ja	Nein
Es wurden geeignete Maßnahmen hinsichtlich der Verwendung von USB-Ports getroffen (automatische Verschlüsselung, Virensan, Verbot zur Einbindung von Fremdhardware, etc.).	Ja	Nein
Die Authentifizierung (SPF, DKIM, DMARC) ist durchgehend implementiert.	Ja	Nein
Externe Emails werden als solche gekennzeichnet.	Ja	Nein
Einsatz von Security Email Gateway (SEG).	Ja	Nein
Einsatz von Sandboxing zum Analysieren und Blockieren eingehender Email Anhänge mit böartigem Anhang.	Ja	Nein
Es werden Schwachstellenanalysen durchgeführt.	Ja	Nein

Netzwerksicherheit

Es existiert eine Firewall zwischen internem Netzwerk und Internet. Die Firewall wird regelmäßig angepasst sowie der Datenverkehr gefiltert und überwacht.	Ja	Nein
Firewall-Logdaten werden mindestens 60 Tage gespeichert.	Ja	Nein
Es sind Intrusion Detection Systeme (IDS) und Intrusion Prevention Systeme (IPS) implementiert. Diese werden regelmäßig aktualisiert und überwacht.	Ja	Nein
Alle internetfähigen IT-Systeme (z.B. E-Mail-Server) sind von ihrem vertrauenswürdigen Netzwerk getrennt.	Ja	Nein
Das Netzwerk ist nach Geschäftsfunktionen segmentiert (z.B. ist Datenverkehr zwischen verschiedenen Geschäftsfunktionen blockiert, außer es ist für bestimmte Anforderung 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 Anforderung notwendig)	Ja	Nein
Es wird eine regelmäßige Schwachstellenanalyse (Vulnerability Assessment) durchgeführt und sofern notwendig, werden entsprechende Maßnahmen eingeleitet.	Ja	Nein
Es existiert ein Incident- und Change-Management.	Ja	Nein
Sicherheitsvorfälle wie Virus, Zugriffsversuche, Datenverluste etc. werden protokolliert und überwacht.	Ja	Nein
Der RDP-Port wurde deaktiviert.	Ja	Nein
Der SMB-Port wurde deaktiviert.	Ja	Nein
Es wird ein schützender DNS-Dienst verwendet.	Ja	Nein
Es wird eine Webfilter-Lösung eingesetzt.	Ja	Nein
Eine EDR-Lösung (End Point Detection & Response) ist für alle kritischen Endpunkte/Server implementiert.	Ja	Nein
Bei allen End-Points sind die Administratorenrechte deaktiviert.	Ja	Nein
Der Datenverkehr zwischen internem und externem Netzwerk sowie dem Internet wird überwacht inkl. Anomalien im Netzwerk sowie Datentransfers.	Ja	Nein

Multifaktor-Authentifizierung (MFA)

Die Multifaktor-Authentifizierung (MFA) ist für folgende Bereiche unternehmensweit verpflichtend implementiert:

• Fernzugriff auf das Firmennetzwerk.	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.	Ja	Nein

Zertifizierungen

Wurden in den letzten 12 Monaten neue Zertifizierungen erreicht bzw. wurden vorhandene Zertifizierungen verlängert (z.B. ISO 27001, BSI Grundschutz)?	Ja	Nein
---	----	------

Falls ja, bitte Details:

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

Überträgt Ihr Unternehmen IT- oder datenverarbeitungsbezogene Geschäftsaufgaben, Prozesse, Dienstleistungen (vollständig oder teilweise) an Dritte bzw. nutzt Cloud Services?	Ja	Nein
---	----	------

• Rechenzentren	Ja	Nein
• Managed Security	Ja	Nein
• Datenverarbeitung-/Datenspeicherung	Ja	Nein
• Anwendungsmanagement	Ja	Nein
• Alert Monitoring	Ja	Nein
• Backup and storage	Ja	Nein
• Cloud Services	Ja	Nein
• Andere/weitere: _____		

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
--	----	------

Cyber-Krisenmanagement

Es existiert ein Krisenreaktionsplan mit folgenden Regelungen:

• Bei Störungen ist die Aufrechterhaltung/der Wiederanlauf betriebsnotwendiger Systeme festlegt.	Ja	Nein
• Kommunikationsplan für Betroffene.	Ja	Nein
• Feste Aufgabenverteilung für die Behandlung des Vorfalls im Unternehmen.	Ja	Nein
• Alternative Outsourcing-Kapazitäten für den Fall eines Ausfalls eines Outsourcing Dienstleisters im Bereich unternehmenskritischer Bereiche.	Ja	Nein
• Die Kontaktdaten der Cyber-Krisenhotline von Berkley Deutschland und das Vorgehen zur Schadenmeldung werden in den Krisenreaktionsplan übernommen.	Ja	Nein

Es existiert ein Business Continuity Plan (BCP).	Ja	Nein
Es existiert eine Notfall-/Disaster Recovery Plan (DRP).	Ja	Nein
Der Krisenreaktionsplan, BCP und/oder der DRP wird regelmäßig getestet und aktualisiert.	Ja	Nein
Es ist sichergestellt, dass auf Vorfälle, auch an Wochenenden oder nachts (Helpdesk/CERT Verfügbarkeit für Vorfälle 24/7), zeitnah reagiert werden kann.	Ja	Nein

Operations Technology (OT)

Wie schnell führt eine Nichtverfügbarkeit Ihrer Systeme zu signifikanten Auswirkungen auf Ihre Geschäftstätigkeit?						
Sofort	nach 6h	nach 12h	nach 24h	nach 48h	_____	
Die fortlaufende Produktion/Logistik ist bei Ausfall der IT-Systeme vollständig manuell und offline möglich.					Ja	Nein
• Falls ja: Über welchen Zeitraum, bevor der Geschäftsbetrieb zu einem kompletten Stillstand kommt? _____						
• Wie würden die Produktion und die Logistik in diesem Fall fortgeführt? _____						
• Ist dieses Notfall-Szenario bereits getestet worden?					Ja	Nein
Bei einem IT-bedingten Produktionsausfall kann auf ein Lager an Fertigprodukten zurückgegriffen werden.					Ja	Nein
• Falls ja, über welchen Zeitraum ist dies möglich, bevor es zu Lieferengpässen, bis hin zu einem kompletten Auslieferungstillstand kommt? _____						
Folgende Schutzmaßnahmen sind durchgehend implementiert:						
• Schnittstellen an Terminals sind deaktiviert.					Ja	Nein
• OT befindet sich in einem separierten Netzwerk.					Ja	Nein
• Zugriffsrechte bestehen ausschließlich für die entsprechenden User.					Ja	Nein
• 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
• Externe Wartungszugänge sind besonders gesichert (Freigabe, zeitbasiert etc.).					Ja	Nein
• Produktionssysteme werden regelmäßig gepatched.					Ja	Nein
• Malwareschutz wird eingesetzt wo möglich.					Ja	Nein
• Es sind Workarounds für nicht patchbare/nicht unterstützte Systeme, z.B. durch restriktives Application-Whitelisting für Produktions-IT (z. B. Supervisory Control and Data Acquisition (SCADA) oder Human Machine Interface (HMI)) implementiert.					Ja	Nein
• Produktionssysteme sind in das Backup integriert.					Ja	Nein
• Es werden regelmäßige Backups von Systemen und Anwendungen der Produktions-IT durchgeführt.					Ja	Nein
• Es existiert eine Umgangsrichtlinie mit Lieferanten von Drittsystemen innerhalb Ihrer Produktions-IT.					Ja	Nein

Remote/außerhalb des Büros arbeiten

Es wird sichergestellt, dass die IT-Sicherheitsmaßnahmen und Datenschutzregelungen auch remote eingehalten werden.	Ja	Nein
Es gibt eine schriftliche Richtlinie/festgelegte Vorgehensweise für remote arbeitende Mitarbeiter. In diesem Kontext gibt es Regelungen zu IT-Sicherheit und zum Umgang mit elektronischen/physischen Daten.	Ja	Nein
Die Verbindung zum Firmennetzwerk erfolgt ausschließlich über abgesicherte Zugangsmöglichkeiten (VPN, Citrix, VDI, etc.).	Ja	Nein
Alle Endgeräte verfügen über ein aktuelles Betriebssystem und Endpoint Protection.	Ja	Nein
Infolge des remote Arbeitens kommt es zu <u>keiner</u> Einschränkung bei:	Ja	Nein
• IDS/IPS	Ja	Nein
• Malware-/Virenerkennung	Ja	Nein
• Backups	Ja	Nein
• EDR-Tools	Ja	Nein
• Patchmanagement	Ja	Nein
Mitarbeiter nutzen ausschließlich Firmengeräte.	Ja	Nein
Sofern „bring your own device“ (BYOD) Geräte verwendet werden:	Ja	Nein
• BYOD Geräte sind in das MDM eingebunden.	Ja	Nein
• Verlust der BYOD Geräte muss gemeldet werden.	Ja	Nein
• Fernlöschung der Unternehmensdaten ist möglich.	Ja	Nein
• Für BYOD-Geräte gelten die IT-/Datenschutzanforderungen wie bei Firmengeräten.	Ja	Nein

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

Werden End-of-life (EoL), end-of-Service (EoS) oder Legacy Systeme verwendet?	Ja	Nein
Sofern dies der Fall ist, wurden folgende Schutzmaßnahmen implementiert:	Ja	Nein
• Es erfolgt eine kontinuierliche Bestandsaufnahme/Überprüfung nach Kritikalität von EOL/EOS-Assets.	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

Elektronischer Zahlungsverkehr (Payment Card Industry)

Speichert, verarbeitet oder übermittelt Ihr Unternehmen/ein externer Dienstleister Kreditkartendaten?	Ja	Nein
• Es wird der aktuell geltende Payment Card Industry Data Security Standard (PCI DSS) im Unternehmen bzw. beim Dienstleister eingehalten.	Ja	Nein
• Durchschnittliches Transaktionsvolumen in EUR: _____		
• Abgewickelte Anzahl an Zahlungen pro Jahr: _____		
• Die Speicherung, Verarbeitung oder Übermittlung von Kreditkartendaten wurde an einen zertifizierten Dienstleister ausgelagert. Name des externen Dienstleisters: _____	Ja	Nein

Aktuelle Themen

Ukraine, Russland, Belarus

- | | | |
|---|----|------|
| • Bestehen Tochtergesellschaften, Vertriebsbüros, Geschäftsbeziehungen etc. in der/in die Ukraine, nach/in Belarus oder Russland? | Ja | Nein |
|---|----|------|

Wenn ja, in welchem Land und beschreiben Sie dies bitte näher (u.a. reiner Export, Vertriebsniederlassung, Produktion, etc.):

Wie hoch ist der Umsatz bzw. Export in diesen Ländern? _____

- | | | |
|--|----|------|
| Bestehen Abhängigkeiten zu Kunden, Lieferanten, Investoren oder Auftraggebern? | Ja | Nein |
|--|----|------|

Falls eine lokale Präsenz in diesen Ländern besteht: Welche Maßnahmen ergreifen Versicherte, um sicherzustellen, dass die lokale IT-Infrastruktur vor Störungen, Unterbrechungen und Kompromittierungen geschützt ist?

- | | | |
|---|----|------|
| Wird Software/Dienstleistung von Kaspersky im Unternehmen eingesetzt? | Ja | Nein |
|---|----|------|

Ergänzende Fragen zu gravierenden Sicherheitslücken

1. Hat die Versicherungsnehmerin eine Folgen-/Risikoabschätzung für folgende Ereignisse durchgeführt?

- | | | |
|---|----|------|
| • Apache Log4j Sicherheitslücke (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) | Ja | Nein |
| • Microsoft Exchange Server On Premise (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065) | Ja | Nein |
| • Kaseya VSA (CVE-2021-30116) | Ja | Nein |
| • Druckerspools auf Microsoft Systemen (CVE 2021-34527 und CVE 2021-1675) | Ja | Nein |

2. Verwendet die Versicherungsnehmerin einen der betroffenen Softwarecodes, Produkte oder Anwendungen, die in einem dieser Ereignisse identifiziert wurden, und wurden alle betroffenen Softwarecodes, Produkte oder Anwendungen identifiziert? (Zutreffendes bitte ankreuzen)

- | | | |
|---|----|------|
| • Apache Log4j Sicherheitslücke (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) | Ja | Nein |
| • Microsoft Exchange Server On Premise (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065) | Ja | Nein |
| • Kaseya VSA (CVE-2021-30116) | Ja | Nein |
| • Druckerspools auf Microsoft Systemen (CVE 2021-34527 und CVE 2021-1675) | Ja | Nein |

3. Wurden alle CVEs (Common Vulnerabilities and Exposures), die diesen Schwachstellen zugewiesen sind, behoben?

- | | | |
|---|----|------|
| • Apache Log4j Sicherheitslücke (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) | Ja | Nein |
| • Microsoft Exchange Server On Premise (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065) | Ja | Nein |
| • Kaseya VSA (CVE-2021-30116) | Ja | Nein |
| • Druckerspools auf Microsoft Systemen (CVE 2021-34527 und CVE 2021-1675) | Ja | Nein |

4. Hat die Versicherungsnehmerin eine forensische Analyse eingeleitet, um einen IOC (Indicator of Compromise) zu identifizieren, der aus der/den festgestellten Sicherheitslücke(n) resultiert?

Ja Nein

5. Wurden bei der forensischen Analyse eines der folgenden Produkte IOCs festgestellt?

• Apache Log4j Sicherheitslücke (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105)	Ja	Nein
• Microsoft Exchange Server On Premise (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065)	Ja	Nein
• Kaseya VSA (CVE-2021-30116)	Ja	Nein
• Druckerspooler auf Microsoft Systemen (CVE 2021-34527 und CVE 2021-1675)	Ja	Nein

6. Falls IOCs identifiziert wurden, hat die Versicherungsnehmerin identifizierte Schadsoftware im Computersystem der Versicherungsnehmerin für die folgenden Produkte beseitigt und entfernt?

• Apache Log4j Sicherheitslücke (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105)	Ja	Nein
• Microsoft Exchange Server On Premise (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065)	Ja	Nein
• Kaseya VSA (CVE-2021-30116)	Ja	Nein
• Druckerspooler auf Microsoft Systemen (CVE 2021-34527 und CVE 2021-1675)	Ja	Nein

7. Hat die Versicherungsnehmerin ein vom Hersteller veröffentlichtes Patch/Software-Update/work-around im Zusammenhang mit einem der oben ausgeführten Ereignisse erfolgreich angewendet?

Ja Nein

8. Bitte beschreiben Sie kurz wie Sie generell mit derartigen Sicherheitslücken (auch zukünftig) umgehen?

Schadenhistorie und bekannte Umstände in Bezug auf die Cyber-Versicherung

Sind Ihnen aus den letzten 5 Jahren Umstände, Inanspruchnahmen, Beschwerden oder Schäden bekannt, die zu einem Versicherungsfall unter den Versicherungsschutz dieser Cyber-Versicherung führen könnten?	Ja	Nein
--	----	------

Dies sind u.a. Hacker-Angriffe, interne/externe Ermittlungen und Untersuchungen in Bezug auf Datenschutzverletzungen, Vorfälle durch Schadprogramme, Cyber-Erpressungen, Bedienfehler, technische Probleme, Datenverluste, ungeplante Betriebsunterbrechungen sowie Schadenersatzansprüche von Dritten in Bezug auf Datenrechtsverletzungen oder drohenden/anhängigen Verfahren von Datenschutzbehörden.

Bitte listen Sie alle tatsächlichen oder potenziellen Umstände/Schäden inklusive Beschreibung auf (insbesondere Datum; Beschreibung der Umstände; Beschreibung der getroffenen Gegenmaßnahmen; Finanzieller Aufwand/Schaden):

Hinweis zum Datenschutz

Unsere aktuelle Datenschutzerklärung finden Sie unter: <https://www.berkleyversicherung.de/datenschutz/>

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 Gefahrsicherung 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.