HDI Versicherung AG
www.hdi.de

Risikoanalyse zur Cyberversicherung für tarifliche Risiken für Mitglieder des bft mit Jahresumsatz bis 10 Mio. EUR inkl. Erläuterungen

Partner-Nr. _____

Betreuer-Nr. _____

Vermittler-Nr./VP _____

Teil I: Risikoanalyse Seite 1 - 2
Teil II: Erläuterung zu den Risikofragen Seite 3 - 4

Interessent

☐ Frau ☐ Herr ☐ Firmierung Name/Vorname/Firmierung

_____

_____

Straße/Nr. _____

PLZ/Ort _____

Telefon _____

Mobil _____

Telefax _____

E-Mail _____

Internet _____

Zielgruppe _____ WZ-Code _____

Erstniederlassung bzw. Gründungsdatum _____

Büro Anschriften _____

Ist die Mitversicherung weiterer rechtlich selbstständiger Unternehmen gewünscht? ☐ ja ☐ nein

Bitte geben Sie den/die Namen und Anschrift/en an. Falls der Platz hier nicht ausreicht, fügen Sie bitte ein separates Blatt an.

Name _____ PLZ/Ort _____

Straße/Nr. _____

Wenn ja, umfassen die Antworten in diesem Fragebogen alle (mit)versicherten Unternehmen des Versicherungsnehmers? ☐ ja ☐ nein

Wenn nein, bitte für diese Unternehmen eine eigene Risikoanalyse einreichen

Tätigkeits-beschreibung

Branchengruppe _____ Jahresumsatz _____ davon aus Onlinegeschäften _____

Bei einem Umsatz größer 10.000.000 EUR reichen Sie bitte den HDI Cyber Risiko Checkup ein.

Tätigkeitsbeschreibung _____

Bei Umsätzen aus Online-Geschäften

Wir nutzen Dienstleister zum Betrieb unseres Webshops oder Payment Dienstleister zur Abwicklung aller eingehender bargeldlosen Zahlungsvorgänge ☐ ja ☐ nein

gewünschter Deckungs-umfang

Versicherungssumme in EURO	☐ 100.000	☐ 250.000	☐ 500.000	☐ 750.000	☐ 1.000.000	☐ _____
Selbstbeteiligung je Schadenfall in EURO	☐ 500	☐ 1.000	☐ 2.500	☐ _____		
Wartezeit bei Betriebsunterbrechung	☐ 12 Stunden	☐ _____				

Deckungserweiterungen

☒ **Cyber-Spionage** (beitragsfrei mitversichert)
Aufwendungen der rechtlichen Begutachtung sowie Minderung des Reputationsschadens auf Grund Spionage von Betriebs- und Geschäftsgeheimnissen durch einen Dritten.

☒ **Internet-Diebstahl – Sublimit VSU, max. 250.000 EUR** (beitragsfrei mitversichert)
Diebstahl von Geldern oder Waren bei Versicherten, Kommunikationskosten

☐ **Betriebsunterbrechnung durch Cloudausfall – Sublimit VSU, max. 250.000 EUR**
Betriebsunterbrechung durch den Ausfall einer beruflich und entgeldlich genutzten Cloud

☐ Betriebsunterbrechung durch technische Störungen - Sublimit 100.000 EUR

Risikofragen

1.Bearbeiten, speichern oder übermitteln Sie **weniger als** 20.000 Kreditkartendaten pro Jahr? ☐ ja ☐ nein

2. Werden vom Hersteller bereitgestellte Updates (z.B. Sicherheitspatches) unverzüglich eingespielt? ☐ ja ☐ nein

3. Setzen Sie Malwareschutz (z.B. in Form eines Antivirenprogramms) ein und wird dieser automatisch auf dem aktuellen Stand gehalten? ☐ ja ☐ nein

4. Sind alle Zugänge zum Internet durch Firewalls gesichert? ☐ ja ☐ nein

5. Erfolgt eine mindestens wöchentliche Datensicherung auf separaten Systemen oder Datensicherungsmedien? ☐ ja ☐ nein

6. Besitzt jeder Mitarbeiter nur die für die eigene Tätigkeit notwendigen Berechtigungen und passwortgeschützten individuellen Zugänge? (Hinweis: Administrative Zugänge werden ausschließlich zur Erledigung administrativer Tätigkeiten genutzt.) ☐ ja ☐ nein

7. Haben Sie alle vom Hersteller voreingestellten Passwörter auf allen Geräten in Ihrem Netzwerk (z.B. Telefonanlagen, Anrufbeantwortern, Drucker, Router, IoT-Geräte) geändert? ☐ ja ☐ nein

8. Erfolgt der Zugriff auf die interne IT-Infrastruktur über öffentliche oder drahtlose Netze ausschließlich verschlüsselt? ☐ ja ☐ nein

9. Es werden **keine** automatisierten Produktionssysteme (ICS) genutzt? ☐ ja ☐ nein

Sollten Sie eine der Fragen mit "nein" beantwortet haben, bitten wir Sie in der Anlage hierzu nähere Angaben zu machen. Vielen Dank.

Vorversicherung

☐ keine Vorversicherung ☐ bei HDI, Versicherungs-Nr. _____

☐ anderweitig, Name des Versicherers und VS-Nr.: _____

Aus den letzten 5 Jahren sind keine Schäden durch eine Daten- oder Cyberrechtsverletzung, Hacker-Angriff, Denial-of-Service- Angriff oder Cyber-Erpressung bekannt und Ihnen sind auch keine Umstände bekannt, die zu einem Cyber-Versicherungsfall führen könnten. ☐ ja ☐ nein

Anzahl der Schäden und Aufwendungen _____

Keine Aufsichtsbehörde, staatliche Stelle oder Verwaltungsbehörde hat Klage gegen den Versicherungsnehmer oder eine mitversicherte Person eingereicht, Ermittlungen eingeleitet oder Auskünfte angefordert, was den Umgang mit sensiblen Daten angeht. ☐ ja ☐ nein

Geben Sie auch alle Fälle an, die ohne eine Zahlung (zu Ihren Gunsten) geschlossen wurden.
Bitte beachten Sie: Bei einer Falschangabe ist der Versicherer zum Rücktritt wegen vorvertraglicher Anzeigepflichtverletzung berechtigt.

Ablauf der Vorversicherung _____

☐ Kündigung durch Versicherungsnehmer ☐ Kündigung durch Versicherer

Prämienzahlung/ Vertragslaufzeit

Versicherungsbeginn: _____ 0 Uhr Versicherungsablauf: _____ 0 Uhr Nächste Prämienfälligkeit: _____

Prämie zahlbar: ☐ jährlich ☐ 1/2-jährlich (3 % Zuschlag)

Wichtiger Hinweis

Bitte beachten Sie, dass der Versicherer seine Entscheidung über die Annahme des Antrags auf die wahrheitsgemäße Erklärung stützt. Unwahre oder unvollständige Angaben können den Versicherer zum Rücktritt vom Vertrag berechtigen, unter Umständen sogar zur Anfechtung wegen arglistiger Täuschung, die den Versicherungsschutz rückwirkend (von Anfang an) entfallen lässt.

Ort/Datum _____ Unterschrift ✗ _____

Nähere Angaben zu den Risikofragen

Zu Frage _____ _____

Zu Frage _____ _____

Zu Frage _____ _____

Zu Frage _____ _____

Zu Frage _____ _____

Zu Frage _____ _____

Erläuterungen zu den Risikofragen

Installieren Sie Updates für kritische IT-Systeme und -Anwendungen („Security Patches) unverzüglich?

Patches werden veröffentlicht, um ein oder mehrere Probleme (z.B. Schließen von Sicherheitslücken) einer Software zu beheben. Beinhalten Patches neue Funktionen der Software, wird von einem Update gesprochen.
Mit der Veröffentlichung von Sicherheits-Updates werden auch die zugrunde liegenden Software-Schwachstellen der allgemeinen Öffentlichkeit bekannt. Dadurch steigt das Risiko des Betriebs nicht aktueller Software. Besonderes Augenmerk ist dabei auf verwendete Standardsoftware (z.B. Adobe Reader, Internetbrowser und MS Office) zu legen.
Durch den Hersteller bereitgestellte Patches und Updates sollten unverzüglich eingespielt werden. Nicht mehr unterstützte Software muss zeitnah auf einen aktuellen Stand umgestellt werden.
In besonders geschäftskritischen Bereichen ist es üblich, Updates zunächst einer Prüfung zu unterziehen, um Probleme im Betrieb auszuschließen. In diesem Fall ist anstelle eines automatischen Updates ein zeitnahes Umsetzen je nach Kritikalität des Updates angemessen.

Setzen Sie Malwareschutz (z.B. in Form eines Antivirenprogramms) ein?

Malwareschutz kann zum Beispiel in Form eines Antivirenprogramms umgesetzt werden und dient dem Schutz vor Schadsoftware. Dabei ist es enorm wichtig, dass das Programm stets auf dem aktuellen Stand gehalten wird, da sich die Angriffslage ständig verändert und neue Schadsoftware entwickelt wird. Dieser Schutz sollte auf sämtlichen vom Versicherten betriebenen Hard- und Softwaresystemen sowie Endgeräten eingesetzt und aktiviert werden. Eine automatische Aktualisierung sollte sichergestellt sein. Auch hier gilt, dass vom Hersteller nicht mehr unterstützte Software zeitnah auf den aktuellen Stand umgestellt werden sollte.

Möglichkeiten sind handelsübliche Antivirenprogramme oder auch die betriebssystemeigene Schutzsoftware (z.B. Windows Defender).
Server oder Geräte, die mit dem Internet direkt oder indirekt verbunden sind, sind dort einem allgemeinen und ständigen Angriffsrisiko ausge¬setzt und unterliegen daher höheren Schutzanforderungen als stationäre Bürorechner.

Sind alle Zugänge zum Internet durch Firewalls gesichert?

Sämtliche IT-Systeme sollten durch eine Firewall geschützt werden. Eine Firewall schützt IT-Systeme vor Angriffen oder unbefugten Zugriffen, in dem Sie den Netzwerkzugriff analysieren, weiterleiten oder blockieren kann. Eine Personal- / Desktop-Firewall sollte auf allen mit dem Internet verbundenen Geräten installiert, aktiviert und aktualisiert sein. Je nach Unternehmensgröße kann die vorinstallierte Firewall von gängigen Betriebssystemen (Windows, MacOS) ausreichend sein.

Erfolgt eine mindestens wöchentliche Datensicherung auf separaten Systemen oder Datensicherungsmedien?

Ohne Datensicherung ist eine Wiederherstellung der Betriebsbereitschaft kaum möglich. Ein nachhaltiger Datenverlust bedeutet darüber hinaus nicht selten eine lang dauernde Betriebsunterbrechung. Es sollte mindestens eine wöchentliche Sicherung aller Daten (Vollsicherung) stattfinden. Idealerweise werden geschäftskritische / sensible Daten täglich gesichert.
Wenn Backup-Systeme dauerhaft mit den Zielsystemen verbunden sind, besteht das Risiko, dass sie bei einem Angriff ebenfalls zu Schaden kommen. Daher sind diese an einem geschützten Ort und ohne Netzzugriff aufzubewahren.
Backups sollten außerdem vor Manipulation oder unbefugtem Zugriff geschützt werden. Wenn Backups nachträglich vom betroffenen System oder vom Angreifer verändert werden können, besteht das Risiko, dass sie ebenfalls zu Schaden kommen.
Eine regelmäßige Überprüfung der Wiederherstellung stellt sicher, dass diese auch im Ernstfall vollständig funktioniert. Findet eine solche regelmäßige Prüfung nicht statt, sind aufgrund des unerprobten Vorgangs Probleme durch Unvollständigkeit oder Verzögerungen bei der Wiederherstellung wahrscheinlicher. Die Lebensdauer eines Datenträgers ist begrenzt. Ebenso können Systemausfälle oder andere Gründe dazu führen, dass Daten nicht ordnungsgemäß dupliziert wurden.

Besitzt jeder Mitarbeiter nur die für die eigene Tätigkeit notwendigen Berechtigungen und passwortgeschützten individuellen Zugänge?
(Hinweis: Administrative Zugänge werden ausschließlich zur Erledigung administrativer Tätigkeiten genutzt.)

Jeder Mitarbeiter sollte nur die für die eigene Tätigkeit notwendigen Berechtigungen und Zugänge erhalten. Somit kann unbefugtem Zugriff und Missbrauch von Rechten vorgebeugt werden. Lokale Administratorrechte sollten nur Administratoren besitzen, die diese weitreichenden Berechtigungen für die tägliche Arbeit benötigen. Diese stellen nicht nur eine Gefahr hinsichtlich unbeabsichtigter oder böswilliger Aktivitäten der Endnutzer (z.B. Installation von Schadsoftware, Konfiguration der Firewall) dar, sondern sind auch für Angreifer ausnutzbar. Wurde ein Account mit lokalen Administratorrechten kompromittiert, kann sich der Angreifer weitere Zugangsdaten beschaffen und sich durch das Firmennetz bewegen, um z.B. Zugriff zu weitere privilegierte Benutzerkonten zu erlangen. Somit kann der Angreifer im schlimmsten Fall Zugriff auf die gesamte IT-Infrastruktur bekommen und diesen ausnutzen.
Außerdem sollte jeder Mitarbeiter einen eigenen Account besitzen, der mit den für die Tätigkeit notwendigen Berechtigungen ausgestattet ist. Besitzen Mitarbeiter weitreichende Berechtigungen, kann nie vollständig ausgeschlossen, dass diese beabsichtigt oder unbeabsichtigt missbraucht werden. Das Teilen von Accounts (sog. Shared User Accounts) sollte unterbunden werden und birgt zahlreiche Risiken. Laut Art. 32 DSGVO müssen Benutzer bei Anmeldungen an Datenverarbeitungssystemen eindeutig identifiziert und authentisiert werden, um eine ausreichende Vertraulichkeit und Integrität der Daten zu gewährleisten. Wird dies nicht umgesetzt, besteht zum einen das Problem, dass die Zugriffsrechte der einzelnen Benutzer, je nach Aufgabenstellung oder Tätigkeitwechsel, innerhalb des Systems nicht differenziert vergeben werden können. Außerdem kann nicht nachvollzogen werden, wer wann auf welche Daten zugegriffen hat bzw. diese bearbeitet oder verändert hat. Wurde im Namen des geteilten Accounts eine für das Unternehmen ungewollte oder schädliche Handlung ausgeführt, kann nicht nachgewiesen werden, wer den festgestellten Missbrauch begangen hat. Auch Angreifer und Unbefugte nutzen diese Anonymität dieser Accounts gerne aus, um dem Unternehmen zu schaden. Weiterhin ist die Vertraulichkeit der Passwörter bei Shared User Accounts nicht gewährleistet. Bei einem Passwortwechsel muss das neue Passwort mehreren Mitarbeitern mitgeteilt werden. Dabei besteht die Gefahr, dass das Passwort durch Dritte ausgespäht wird. Außerdem müssen sich mehrere Leute das gleiche Passwort merken, weshalb oftmals einfache Passwörter gewählt werden.

Systeme ohne Authentifizierung können von Angreifern ohne Hindernis übernommen und kontrolliert werden. Daher sehen aktuelle Betriebssysteme grundsätzlich eine Authentifizierung vor. Benutzerindividuelle Kennungen sind darüber hinaus notwendig, um die Zugriffsrechte einzelner Accounts granular zu definieren und nachvollziehen zu können, welche angriffs- oder schadenrelevanten Tätigkeiten zu welchem Zeitpunkt von welchem Nutzer durchgeführt wurden. Sogenannte „Funktionsaccounts", also Log-in-Daten, die sich mehrere Personen teilen, dürfen nur an unkritischen Systemen und unkritischer Software verwendet werden. Als kritisch werden administrative bzw. vollständige Änderungs- und Löschrechte auf sensible Personendaten (Datenschutz) oder IT-Infrastruktur (z. B. Server) angesehen.
Zudem ist sicherzustellen, dass in den Betriebssystemen je Nutzer eigene Konten angelegt / genutzt werden (z. B. Windowskonto).

Mittlerweile existieren zahlreiche Methoden, um Passwörter durch wahlloses Ausprobieren von Zeichenkombinationen herauszufinden. Bei so genannten „Brute-Force-Angriffe" probieren leistungsstarke Computer automatisiert alle möglichen Zeichenkombinationen für ein Passwort aus. Durch die Automatisierung benötigen diese Computer bei einem Passwort von vier Zeichen weniger als eine Sekunde zum erraten. Bei sieben Zeichen dauert es 21 Stunden. Ab dem achten Zeichen sind es schon 84 Tage. Das neunte Zeichen verlängert die Dauer auf 22 Jahre. Weiterhin gibt es Angriffe, bei denen mit Hilfe von Passwortlisten versucht wird, ein unbekanntes Passwort zu ermitteln. Daher sollten auf einfache Wörter oder Namen verzichtet werden. Die zwei genannten Methoden zeigen, wie professionell heutzutage Angreifer vorgehen. Umso wichtiger wird die Verwendung eines komplexen Passworts. Allgemein gilt, dass die Verwendung eines komplexen, langen Passworts einen effektiveren Schutz liefert, als die Verwendung eines weniger komplexen Passworts, das regelmäßig geändert wird. Neben der Verwendung eines komplexen Passworts, sollte kein Passwort mehrfach verwendet werden. Wurde eine Anwendung oder ein Dienst kompromittiert, werden die hinterlegten Accounts oftmals veröffentlicht oder verkauft, wodurch sämtliche Accounts in Gefahr sind, bei denen Sie dasselbe Passwort verwendet haben.

Gemäß BSI sollten Passwörter folgenden Kriterien entsprechen:

- Länge: Mindestens acht Zeichen haben
- Verwendung von Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen
- Vermeidung von Passwörtern aus gängigen Passwortlisten oder dem Wörterbuch
- Vermeidung der Wiederverwendung der letzten Passwörter
- Keine Mehrfachverwendung von Passwörtern (für jedes IT-System bzw. jede Anwendung muss ein eigenständiges Passwort verwendet werden)
- Passwörter müssen gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht
- Passwörter müssen so sicher wie möglich gespeichert werden

Haben Sie alle vom Hersteller voreingestellten Passwörter auf allen Geräten in Ihrem Netzwerk (z.B. Telefonanlagen, Anrufbeantwortern, Drucker, Router, IoT-Geräte) geändert?

Standardpasswörter stellen ein erhebliches Sicherheitsrisiko dar und sollten vor der ersten Nutzung geändert werden. Idealerweise wird die Änderung technisch erzwungen. Diese Passwörter folgen einer definierten Logik und können sogar wiederholend vorkommen. Werden diese nicht geändert, können oftmals gängige Sicherheitsanforderungen für Passwortsicherheit nicht erfüllt werden. Aus diesen Gründen stellen Standardpasswörter eine enorme Schwachstelle dar und sind ein beliebtes Ziel für Angreifer. Durch die Vernetzung der Geräte (z.B. Drucker, Router) bieten sie ein beliebtes Einfallstor für Angreifer, die auf diesem Weg oftmals auch auf weitere Teile des Netzwerks zugreifen.

Erfolgt der Zugriff auf die interne IT-Infrastruktur über öffentliche oder drahtlose Netze ausschließlich verschlüsselt?

Öffentliche WLAN-Netzwerke, z.B. in Hotels, Konferenzzentren oder Restaurants, stellen oft eine unverschlüsselte drahtlose Verbindung zwischen dem mobilen Gerät und dem Router dar und können von lokalen Angreifern passiv mitgeschnitten oder aktiv manipuliert werden. Nach Beendigung der Verbindung sollte das Netzwerk außerdem aus der Liste der gespei-

cherten WLAN-Netzwerke gelöscht werden, um ein unbewusstes, automatisches Einwählen zu verhindern. Der Zugriff auf kritische Systeme oder der Austausch von vertraulichen Daten darf daher nur über verschlüsselte und authentifizierte Kanäle erfolgen. Dies kann z.B. mittels eines VPN (Virtuelles privates Netzwerk) erreicht werden. Ein VPN ist ein sicherer Tunnel zwischen zwei oder mehreren Geräten und bietet die Möglichkeit von außen (z.B. mit einem Laptop) auf ein bestehendes Netzwerk (z.B. Unternehmensnetzwerk) zuzugreifen. Mit Hilfe eines VPNs kann sichergestellt werden, dass die Kommunikation zum bestehenden Netzwerk nicht mitgelesen wird. Außerdem besteht so die Möglichkeit von außen auf unternehmensinterne Laufwerke zuzugreifen. Darüber hinaus kann der Zugriff auf Laufwerke, die auf dem unternehmenseigenen Server liegen und nur innerhalb des Unternehmensnetzwerks verfügbar sein sollen, ermöglicht werden.

Es werden keine automatisierte Produktionssysteme (ICS) genutzt?

ICS-Systeme sind automatisierte Anlagen für den Produktionsprozess. Oftmals sind diese Anlagen von den eigentlichen IT-Systemen entkoppelt. Es ist aber ein Trend der Vernetzung zu verzeichnen, was mit einem erhöhten Cyberrisiko einhergeht.

7003001260-202206