HDI Versicherung AG
www.hdi.de

Cyber Risiko Check Up
Risikoanalyse für Firmen und Freie Berufe bis 20 Mio. € Umsatz - inkl. Erläuterungen

Partner-Nr. _____

Betreuer-Nr. _____

Vermittler-Nr./VP _____

Allgemeine Informationen

☐ Frau ☐ Herr ☐ Firmierung Name/Vorname/Firmierung _____

Straße/Nr. _____

PLZ/Ort _____

Branche _____

Mitarbeiterzahl _____

Rechtsform _____

Telefon _____

Mobil _____

Telefax _____

E-Mail _____

Internet _____

Ansprechpartner im Unternehmen _____

Funktion _____

Telefon _____

E-Mail _____

Konsolidierte Unternehmenskennzahlen

Jahresumsatz

Gesamtumsatz des Antragsstellers und mitzuversichernden Unternehmen: _____ EUR

- davon Umsatz außerhalb Deutschlands (inkl. Export): _____ EUR
- davon Umsatz in USA (inkl. Export): _____ EUR
- davon Umsatzanteil aus dem E-Commerce: _____ EUR

Elektronischer Zahlungsverkehr

Speichern und verarbeiten Sie Kreditkartendaten? ☐ ja ☐ nein Wenn ja, wie viele? _____

Betreiben Sie einen Webshop? ☐ ja ☐ nein ☐ ☐

gewünschter Versicherungsschutz

Versicherungssumme in EURO ☐ 100.000 ☐ 250.000 ☐ 500.000 ☐ 750.000 ☐ 1 Mio. ☐ 2 Mio. ☐ _____

Selbstbetbehalt je Schadenfall in EURO ☐ 500 ☐ 1.000 ☐ 2.500 ☐ 5.000 ☐ _____

Wartezeit bei Betriebsunterbrechung ☐ 12 Stunden ☐ _____

Optionale Bausteine

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

☐ **Cyber Betriebsunterbrechung durch technische Störung – Sublimit VSU, max. 250.000 EUR**
Cyber Betriebsunterbrechung in Folge einer technischen Störung durch, z.B. Über- und Unterspannung, Überhitzung oder unterlassenes IT-Systemupgrade

☐ **Cyber Security Baustein:**
Jährlicher Check der IT-Systeme zur Ermittlung des aktuellen Sicherheitsniveaus und Erhalt von Verbesserungspotenzialen

Ohne ausdrückliche Benennung sind als rechtlich selbständige Tochtergesellschaften existierende Gesellschaften innerhalb der Bundesrepublik Deutschland mitversichert, sofern keine abweichende Tätigkeit vorliegt.

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 _____

Straße/Nr. _____ PLZ/Ort _____

Wenn ja, umfassen die Antworten in diesem Fragebogen alle (mit)versicherten Unternehmen / Abteilungen des Versicherungsnehmers? (Wenn nein, bitte für diese Unternehmen eine eigene Risikoanalyse einreichen) ☐ ja ☐ nein

7003031500-202410

Risikofragen

1. Unternehmensorganisation im Umgang mit Daten

1.1 Haben Sie einen Verantwortlichen für die Informationssicherheit? ☐ ja ☐ nein

1.2 Haben Sie einen Datenschutzbeauftragten (sofern für Ihr Unternehmen gesetzlich verpflichtend)? ☐ ja ☐ nein

1.3 Haben Sie eine Datenschutzrichtlinie etabliert, deren Inhalt und Einhaltung regelmäßig geprüft wird? Wird in dem Zuge auch eine Klassifizierung der Daten vorgenommen? ☐ ja ☐ nein ☐ teilweise

(Falls „teilweise" gewählt, erläutern Sie bitte die ergriffenen Maßnahmen. Falls es keine weitere Erläuterung gibt, wird die Frage als „nein" gewertet.)

2. Absicherung der IT-Systeme

2.1 Werden im Rahmen eines Patch-Management-Verfahrens vom Hersteller bereitgestellte Sicherheitsupdates zeitnah eingespielt? ☐ ja ☐ nein

2.2 Setzen Sie einen Schutz gegen Schadsoftware (z.B. Antivirensoftware) ein, der automatisch auf dem aktuellen Stand? gehalten wird? ☐ ja ☐ nein ☐ teilweise

(Falls „teilweise" gewählt, erläutern Sie bitte die ergriffenen Maßnahmen. Falls es keine weitere Erläuterung gibt, wird die Frage als „nein" gewertet.)

2.3 Nicht mehr unterstütze Software (End-of-Life) wird nicht betrieben ☐ ja ☐ nein ☐ teilweise

(Falls „teilweise" gewählt, erläutern Sie bitte die ergriffenen Maßnahmen. Falls es keine weitere Erläuterung gibt, wird die Frage als „nein" gewertet.)

3. Netzwerksicherheit

3.1 Sind Ihre IT-Systeme mit einem zusätzlichen Schutz gegen unberechtigten Zugriff (z.B. Firewall) ausgerüstet, wenn diese über das Internet (z.B. Server) erreichbar sind oder es sich um Mobilgeräte handelt ? ☐ ja ☐ nein ☐ teilweise

(Falls „teilweise" gewählt, erläutern Sie bitte die ergriffenen Maßnahmen. Falls es keine weitere Erläuterung gibt, wird die Frage als „nein" gewertet.)

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

(Falls „teilweise" gewählt, erläutern Sie bitte die ergriffenen Maßnahmen. Falls es keine weitere Erläuterung gibt, wird die Frage als „nein" gewertet.)

4. Umgang mit Daten

4.1 Werden mobile Speichermedien oder Datenträger mit sensiblen Daten verschlüsselt? ☐ ja ☐ nein ☐ teilweise

(Falls „teilweise" gewählt, erläutern Sie bitte die ergriffenen Maßnahmen. Falls es keine weitere Erläuterung gibt, wird die Frage als „nein" gewertet.)

4.2 Werden sensible Informationen vernichtet, wenn die Geräte / Datenträger nicht mehr verwendet werden? ☐ ja ☐ nein

4.3 Wie oft führen Sie eine Datensicherung durch? ☐ täglich ☐ wöchentlich ☐ > wöchentlich ☐ nie

4.4 Erfolgt die Datensicherung auf separaten Systemen oder Datensicherungsmedien? ☐ ja ☐ nein

4.5 Wird regelmäßig geprüft (mind. jährlich), dass eine Rücksicherung bei Bedarf einwandfrei durchgeführt werden kann? ☐ ja ☐ nein ☐ teilweise

(Falls „teilweise" gewählt, erläutern Sie bitte die ergriffenen Maßnahmen. Falls es keine weitere Erläuterung gibt, wird die Frage als „nein" gewertet.)

5. Zugangs- und Zugriffskontrolle

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

(Falls „teilweise" gewählt, erläutern Sie bitte die ergriffenen Maßnahmen. Falls es keine weitere Erläuterung gibt, wird die Frage als „nein" gewertet.)

5.2 Haben Sie eine Passwortrichtlinie implementiert, die die Verwendung von langen und komplexen Passwörtern in Ihrem Unternehmen durchsetzt? ☐ ja ☐ nein ☐ teilweise

(Falls „teilweise" gewählt, erläutern Sie bitte die ergriffenen Maßnahmen. Falls es keine weitere Erläuterung gibt, wird die Frage als „nein" gewertet.)

5.3 Besitzen alle Nutzer individuelle, passwortgeschützte Zugänge und unterscheidet das betriebene IT-System in unterschiedliche Befugnisebenen? ☐ ja ☐ nein ☐ teilweise

(Falls „teilweise" gewählt, erläutern Sie bitte die ergriffenen Maßnahmen. Falls es keine weitere Erläuterung gibt, wird die Frage als „nein" gewertet.)

5.4 Werden einem Mitarbeiter beim Ausscheiden aus dem Unternehmen sämtliche Rechte entzogen? ☐ ja ☐ nein ☐ teilweise

(Falls „teilweise" gewählt, erläutern Sie bitte die ergriffenen Maßnahmen. Falls es keine weitere Erläuterung gibt, wird die Frage als „nein" gewertet.)

6. Zusatzfragen für Unternehmen aus den Branchen Unternehmensberatung / Ingenieurwesen / Marketing und Werbung / Erbringung von Beratungsleistungen auf dem Gebiet der Informationssicherheit

6.1 Es wird KEINE Softwareentwicklung für Dritte betrieben? ☐ ja ☐ nein

6.2 Sie bieten KEINE "as a Service" Dienstleistungen an oder hosten KEINE Dienste für Dritte? ☐ ja ☐ nein

7. Produktions-IT (OT)

7.1 Werden automatisierte Produktionssysteme (ICS) genutzt? ☐ ja ☐ nein

Wenn ja:

7.2 Ist es möglich, die Produktion bei einem Ausfall der Produktions-IT manuell fortzusetzen? ☐ ja ☐ nein ☐ teilweise

(Falls „teilweise" gewählt, erläutern Sie bitte die ergriffenen Maßnahmen. Falls es keine weitere Erläuterung gibt, wird die Frage als „nein" gewertet.)

7.3 Befinden sich die Produktionssysteme in einem separierten Netzwerk mit eingeschränkten Zugriffsmöglichkeiten? ☐ ja ☐ nein

7.4 Erfolgt der Fernzugriff auf die Produktionssysteme ausschließlich auf verschlüsseltem Weg? ☐ ja ☐ nein ☐ teilweise

(Falls „teilweise" gewählt, erläutern Sie bitte die ergriffenen Maßnahmen. Falls es keine weitere Erläuterung gibt, wird die Frage als „nein" gewertet.)

7.5 Sind die Prozesse zur Wiederherstellung eines betriebsbereiten Zustandes dokumentiert und werden sie regelmäßig erprobt? Gibt es einen Wiederanlaufplan? ☐ ja ☐ nein ☐ teilweise

(Falls „teilweise" gewählt, erläutern Sie bitte die ergriffenen Maßnahmen. Falls es keine weitere Erläuterung gibt, wird die Frage als „nein" gewertet.)

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

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 ✗ _____

Angaben zu weiteren mitzuversichernder rechtlich selbständiger Unternehmen

_____

_____

_____

Nähere Angaben zu den Risikofragen

Zu Frage _____ _____

_____

Zu Frage _____ _____

_____

Zu Frage _____ _____

_____

Zu Frage _____ _____

_____

Erläuterungen zu den Risikofragen

1. Unternehmensorganisation im Umgang mit Daten

1.1 Haben Sie einen Verantwortlichen für die Informationssicherheit?

Unter dem Begriff „Informationssicherheit" definiert man alle technischen und organisatorischen Maßnahmen, die die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen und somit im Unternehmen befindliche Informationen schützen. Bei der Vertraulichkeit muss gewährleistet werden, dass Informationen ausschließlich von befugten Benutzern / Mitarbeitern eingesehen und verwaltet werden können. Die Integrität soll sicherstellen, dass Daten nicht unbemerkt verändert oder manipuliert werden können. Die Verfügbarkeit dient dazu, dass Risiko von Systemausfällen minimiert wird und die gewünschten Informationen den Benutzern beim Abruf auch zur Verfügung stehen.
Um die Informationssicherheit im Unternehmen zu gewährleisten, sollte es in dem Bereich einen Verantwortlichen geben. In größeren Unternehmen hat diese Verantwortlichkeit z.B. ein Chief Information Security Officer „CISO" oder ein Informationssicherheitsbeauftragter „ISB". In kleinen Unternehmen kann der Verantwortliche z.B. IT-Leiter, Geschäftsführer sein. Wichtig ist jedoch, dass es einen definierten Ansprechpartner in diesem Bereich gibt. Der Verantwortliche für die Informationssicherheit kann u.a. folgende Aufgaben im Unternehmen haben: Schulung von Mitarbeitern, Umsetzung von Sicherheitsmaßnahmen, Einhaltung regulativer Anforderungen, Audits, Beratung der Geschäftsführung, Untersuchung sicherheitsrelevanter Vorfälle.

1.2 Haben Sie einen Datenschutzbeauftragten (sofern für Ihr Unternehmen gesetzlich verpflichtend)?

Oftmals tun sich Unternehmen schwer Datenschutz von der Informationssicherheit zu unterscheiden. Das liegt unter anderem daran, dass sich die beiden Bereiche häufig überschneiden. Der wohl größte Unterschied ist, dass es sich bei der Umsetzung des Datenschutzes um strenge gesetzliche Anforderungen handelt. Der Datenschutz dient dabei vorwiegend dem Schutz der Bürger, in dem seine personenbezogenen Daten durch regulative Anforderungen geschützt werden müssen und nur unter besonderen Voraussetzungen (z.B. gesetzlicher Grund oder freiwillige Einwilligung) von Unternehmen verarbeitet werden dürfen. Die Informationssicherheit sorgt sich hingegen vermehrt um im Unternehmen verarbeitete Informationen und vertritt sowie schützt somit das Unternehmen.
Der Datenschutzbeauftragte ist für die Einhaltung des Datenschutzes, also dem Schutz von im Unternehmen verarbeiteten personenbezogenen Daten, zuständig und kann entweder ein interner oder externer Mitarbeiter sein. Durch die Einführung der DSGVO bestehen strengere Anforderungen an den Datenschutz. In drei Fällen benötigt ein Unternehmen einen Datenschutzbeauftragen, (I) wenn sich mindestens zehn Personen ständig mit der (automatisierten) Verarbeitung personenbezogener Daten beschäftigen, (II), wenn das Unternehmen personenbezogene Daten geschäftsmäßig erhebt oder verarbeitet oder (III) wenn das Unternehmen besonders sensible Daten (z.B. Gesundheitsdaten) verarbeitet.

1.3 Haben Sie eine Datenschutzrichtlinie etabliert, deren Inhalt und Einhaltung regelmäßig geprüft wird? Wird in dem Zuge auch eine Klassifizierung der Daten vorgenommen?

Der Datenschutz dient dem Schutz vor der missbräuchlichen Verarbeitung personenbezogener Daten sowie den Schutz des Rechts auf informationelle Selbstbestimmung. Bei der Einhaltung des Datenschutzes ist eine etablierte und gelebte Datenschutzrichtlinie essenziell.
Eine Datenklassifizierung ist sinnvoll, damit intern ein Bewusstsein und Überblick geschaffen wird, welche Daten im Unternehmen vorhanden sind und wie schützenswert diese sind. Erst wenn bekannt ist, welche Daten vertraulich sind, können diese auch angemessen geschützt werden. Außerdem gibt es Compliance-Anforderungen und gesetzliche Regulierungen nach denen bestimmte Daten, wie Kreditkarteninformationen oder personenbezogene Daten geschützt werden müssen.

2. Absicherung der IT-Systeme

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

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 zeitnah 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 au-tomatischen Updates ein zeitnahes Umsetzen je nach Kritikalität des Updates angemessen.

2.2 Setzen Sie Malwareschutz (z.B. in Form eines Antivirenprogramms) auf sämtlichen Gerä-ten ein und halten Sie diesen automatisch auf dem aktuellen Stand?

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 ausgesetzt und unterliegen daher höheren Schutzanforderungen als stationäre Bürorechner.

2.3 Nicht mehr unterstützte Software (End-of-Life) wird nicht betrieben?

Wenn eine Software ihr "End-of-Life" erreicht, bedeutet dies normalerweise, dass der Hersteller keine Updates, Patches oder technischen Support mehr bereitstellt. Das Betreiben solcher Software kann zu Sicherheitsrisiken führen, da bekannte Fehler und Schwachstellen nicht behoben werden.

3. Netzwerksicherheit

3.1 Sind Ihre IT-Systeme mit einem zusätzlichen Schutz gegen unberechtigten Zugriff (z.B. Firewall) ausgerüstet, wenn diese über das Internet (z.B. Server) erreichbar sind oder es sich um Mobilgeräte handelt??

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 Unterneh-mensgröße kann die vorinstallierte Firewall von gängigen Betriebssystemen (Windows, Ma-cOS) ausreichend sein.

3.2. 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 gespeicherten 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.

4. Umgang mit Daten

4.1 Werden mobile Speichermedien oder Datenträger mit sensiblen Daten angemessen verschlüsselt?

Zu den sensiblen oder vertrauenswürdigen Informationen zählen u.a. personenbezogene Daten (Art. 4 DSGVO), Gesundheitsdaten & Privatgeheimnisse (§203 StGB) sowie interne und externe Betriebsgeheimnisse.
Personenbezogenen Daten umfassen bspw. Name, Anschrift, Geburtsdatum von natürlichen Personen. Unter den Geheimnisschutz fallen Gesundheitsdaten (Patientenakte) & weitere Privatgeheimnisse. Diese sind besonders schützenswert. Als interne Betriebsgeheimnisse werden sämtliche Interna deklariert, die nicht an Dritte herausgegeben werden dürfen. Beispiele dafür sind Bilanzdaten, Informationen zur Geschäftsstrategie. Externe Betriebsgeheimnisse berücksichtigen Informationen über Dritte (z.B. Kunden), die nicht öffentlich zugänglich sind und die es daher zu schützen gilt (z.B. Finanzinformationen, Schwachstellen oder Patente).
Da sensible Informationen angemessen geschützt werden müssen, benötigen die mobilen Speichermedien oder Datenträger eine Verschlüsselung. Mobile Geräte oder Datenträger können im Fall eines Diebstahls oder Verlusts in fremde Hände geraten. Ein einfacher Passwortschutz reicht dann nicht mehr aus, um Angreifer am Auslesen der darauf gespeicherten Daten zu hindern. Eine Verschlüsselung aller mobilen Datenträger ist daher erforderlich.

4.2 Werden sensible Informationen vernichtet, wenn die Geräte / Datenträger nicht mehr verwendet werden?

Bevor Medien / Datenträger vernichtet werden, muss unbedingt sichergestellt werden, dass gespeicherte Informationen unwiderruflich gelöscht sind. Wichtig ist hierbei, dass die Informationen unter keinen Umständen wiederherstellbar sind.
Das hat den Hintergrund, dass in vielen Unternehmen nicht mehr benötigte Geräte und Datenträger über den Müll entsorgt werden. Jedoch kommt es vor, dass Dritte (z.B. externe Mitarbeiter, Wirtschaftsspione) Müll von Unternehmen durchsuchen. Daher ist es wichtig, dass Informationen auf den Geräten vor der Entsorgung unwiderruflich vernichtet werden.

4.3 Wie oft führen Sie eine Datensicherung durch?

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.

4.4 Erfolgt die Datensicherung auf separaten Systemen oder Datensicherungsmedien?

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.

4.5 Wird eine regelmäßig geprüft (min. jährliche), dass eine Rücksicherung bei Bedarf einwandfrei durchgeführt werden kann?

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.

5. Zugangs- und Zugriffskontrolle

5.1 Haben Sie alle vom Hersteller voreingestellten Passwörter auf allen Geräten in Ihrem Netzwerk (z.B. Telefon, 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. Wer-den diese nicht geändert, können oftmals gängige Sicherheitsanforderungen für Passwort-sicherheit 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.

5.2 Haben Sie eine Passwortrichtlinie implementiert, die die Verwendung von langen und komplexen Passwörtern in Ihrem Unternehmen durchsetzt?

Mittlerweile existieren zahlreiche Methoden, um Passwörter durch wahlloses Ausprobieren von Zeichenkombinationen herauszufinden. Bei so genannten „Brute-Force-Angriffe" pro-bieren 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 vor-gehen. 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
- 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

5.3 Besitzen alle Nutzer individuelle, passwortgeschützte Zugänge und unterscheidet sich das betriebene IT-System in unterschiedlichen Befugnisebenen?

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 weitrei-chenden 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 Tä-tigkeit notwendigen Berechtigungen ausgestattet ist. Besitzen Mitarbeiter weitreichende Berechtigungen, als notwendig, kann nie vollständig ausgeschlossen, dass diese beabsich-tigt oder unbeabsichtigt missbraucht werden. Das Teilen von Accounts (sog. Shared User Ac-counts) sollte unterbunden werden und birgt zahlreiche Risiken. Laut Art. 32 DSGVO müssen Benutzer bei Anmeldungen an Datenverarbeitungssystemen eindeutig identifiziert und au-thentisiert werden, um eine ausreichende Vertraulichkeit und Integrität der Daten zu gewähr-leisten. 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. Wur-de 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 Pass-wort mehreren Mitarbeitern mitgeteilt werden. Dabei besteht die Gefahr, dass das Passwort durch Dritte ausgespäht werden. Außerdem müssen sich mehrere Leute das gleiche Passwort merken, weshalb oftmals einfache Passwörter gewählt werden.

5.4 Werden einem Mitarbeiter beim Ausscheiden aus dem Unternehmen sämtliche Rechte entzogen?

Systemzugänge, Kennwörter und Berechtigungen dürfen nach dem Ausscheiden des Mitar-beiters aus dem Unternehmen (Ende des Beschäftigungszeitraums) nicht mehr zur Verfügung stehen. Auch Zugangskarten sowie überlassene Geräte (Laptop, Mobiltelefon etc.) sind vom ehemaligen Mitarbeiter zurückzuverlangen. Da das Ausscheiden von Mitarbeitern nicht immer mit beidseitigem Verständnis vonstattengeht, sollten diesem Mitarbeiter Zugänge und Be-rechtigungen umgehend entzogen werden, um unbeabsichtigte oder beabsichtige schadhafte Handlungen durch den Mitarbeiter auszuschließen. Es sollte stets sichergestellt werden, das ausschließlich Mitarbeiter des Unternehmens noch Zugänge besitzen, um die IT und das ge-samte Unternehmen zu schützen.

6. Zusatzfragen für Unternehmen aus den Branchen Unternehmensberatung/Ingenieurwesen/Marketing und Werbung/Erbringung von Dienstleistungen auf dem Gebiet der Informationstechnologie

6.1 Es wird KEINE Softwareentwicklung für Dritte betrieben?

Hierunter fällt die Entwicklung von Software deren Nutzung für andere Unternehmen oder Personen bestimmt ist. Dies können u.a. benutzerdefinierte Softwarelösungen, Anwendungen oder Websites sein.

6.2 Sie bieten KEINE "as a Service" Dienstleistungen an oder Sie hosten KEINE Dienste für Dritte?

"As a Service" bedeutet, dass Dienstleistungen über das Internet bereitgestellt werden, normalerweise gegen eine Abonnementgebühr. Viele Unternehmen bieten Dienste und Hosting-Services für andere Unternehmen oder Personen an. Beispiele dafür sind Software as a Service (SaaS), bei dem Softwareanwendungen über das Internet bereitgestellt und genutzt werden können, Infrastructure as a Service (IaaS), bei dem Unternehmen Zugriff auf technische Infrastruktur wie Server, Speicherplatz und Netzwerkressourcen erhalten, oder Platform as a Service (PaaS), bei dem eine Entwicklungsplattform über das Internet bereitgestellt wird, um Anwendungen zu entwickeln und bereitzustellen. Durch das Hosten von Diensten für Dritte stellt ein Unternehmen seine technische Infrastruktur zur Verfügung, damit andere Unternehmen oder Personen Anwendungen oder Websites auf ihren Servern betreiben können.

7. Produktions-IT (OT)

7.1 Werden automatisierte Produktionssysteme (ICS) genutzt?

ICS Systeme oder auch automatisierte Produktionssysteme sind automatisierte Anlagen für den Produktionsprozess. Dies kann z.B. eine Anlage zur visuellen Bewertung von Bauteilen oder aber auch eine Pulverbeschichtungsanlage mit Industrieroboter inkl. der automatischen Teilezuführung sein. 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.

7.2 Ist es möglich, die Produktion bei einem Ausfall der Produktions-IT manuell fortzusetzen?

Um die Abhängigkeit der Produktion von der IT zu betrachten, ist es entscheidend, ob die Produktion auch bei einem Ausfall der Produktions-IT fortzuführen ist. Kommt es zu einer Betriebsunterbrechung, wenn die Produktions-IT z.B. in Folge eines Hackerangriffs ausfällt, ist mit einem hohen Schaden für das Unternehmen zu rechnen.

7.3 Befinden sich die Produktionssysteme in einem separierten Netzwerk mit eingeschränkten Zugriffsmöglichkeiten?

Die Produktions-IT sollte sich stets in einem anderen Netzwerk befinden, als die sonstige IT im Unternehmen. Die sogenannte Netzwerksegmentierung ist entscheidend, um Schäden bzw. einen Stillstand der Produktion zu verhindern. Außerdem sollte die Produktions-IT, falls nicht unbedingt notwendig, keine Internetverbindung haben, um potenzielle Einfallstore zu mini-mieren. Weiterhin sollten aus diesem Grund nur wirklich notwendige Schnittstellen zu ande-ren Systemen bestehen. Sämtliche notwendige Schnittstellen sollten entsprechend gesichert sein, um eine Betriebsunterbrechung zu verhindern. Maschinen und Systeme in der Produkti-on haben oftmals eine lange Laufzeit und sind teilweise mit veralteter Software ausgestattet, für die der Herstellersupport eingestellt wurde. Auch dieser Aspekt stellt ein Cyberrisiko dar, weshalb sich die Produktions-IT in einem separierten Netzwerk befinden sollte.

7.4 Erfolgt der Fernzugriff auf die Produktionssysteme ausschließlich auf verschlüsseltem Weg?

Auf Grund der Spezialität der Maschinen und Systeme in der Produktion erfolgt die Wartung und Instandhaltung oftmals durch externe, spezialisierte Dienstleister. In dem Zusammenhang ist es nicht selten, dass eine Fernwartung durchgeführt wird. Dabei muss dem Dienstleister eine Verbindung zu den Produktionssystemen gewährt werden. Daher ist es wichtig, dass die Verbindung zum Netzwerk ausschließlich verschlüsselt stattfindet (z.B. über einen VPN-Zugang), um sämtliche Risiken zu minimieren. Generell sollte jeder Fernzugriff verschlüsselt sein, damit die Produktionssysteme vor einem unbefugten Zugriff geschützt sind.

7.5 Sind die Prozesse zur Wiederherstellung eines betriebsbereiten Zustandes dokumentiert und werden sie regelmäßig erprobt? Gibt es einen Wiederanlaufplan?

Trotz zahlreicher Sicherheitsmaßnahmen kann eine Betriebsunterbrechung nie vollständig ausgeschlossen werden. Daher sollte der Prozess der Wiederherstellung dokumentiert sein und regelmäßig erprobt bzw. überprüft werden. In dem Zuge ist ein Wiederanlaufplan sinn-voll, der regelt, welche Systeme und Geräte in welcher Reihenfolge gestartet werden, um den Betrieb schnellstmöglich wiederherzustellen.