HISCOX
WISSEN VERSICHERT.

Bitte per Telefax oder E-Mail an Hiscox
Fax-Nr.: 089/54 58 01-199
E-Mail: hiscox.underwriting@hiscox.de

Hiscox CyberClear Fragebogen

Mit diesem Fragebogen möchten wir Sie und Ihr Unternehmen gerne kennenlernen. Aufgrund der von Ihnen gemachten Angaben besteht für keine Partei die Verpflichtung zum Abschluss eines Versicherungsvertrages. Nähere Erläuterungen zu cyberspezifischen Begriffen finden Sie am Ende in den Hinweisen sowie in unserem Cyber-Glossar unter www.hiscox.de/blog/cyber-glossar.

Nachfolgende Fragen sind für die Gesamtheit aller mitzuversichernden Gesellschaften zu beantworten. Falls notwendig verwenden Sie für weitere Details bitte ein Beiblatt.

I. GENERELLE INFORMATIONEN

Vermittlername | Vermittlernummer

1. Unternehmensangaben

Name | **Website**

Straße, Nr. | Tätigkeitsbeschreibung (Branche und Geschäftstätigkeit)

PLZ, Ort, Land

2. Unternehmenskennzahlen

Konsolidierte Kennzahlen für alle mitzuversichernden Gesellschaften aus dem letzten Geschäftsjahr

	Gesamt	davon EWR/UK	davon USA/Kanada	davon restliche Länder
Umsatz in €				
davon Onlineumsatz in €				
Rohertrag in €				
Anzahl Mitarbeiter				
Anzahl Mitarbeiter *mit Zugang zu E-Mails*				
Anzahl Kunden				
Gesamtumsatz aktuelles Geschäftsjahr in €				

3. Mitzuversichernde Gesellschaften

Gibt es Tochtergesellschaften außerhalb des Europäischen Wirtschaftsraumes (EWR) und dem Vereinigtem Königreich (UK) UND/ODER mitzuversichernde Gesellschaften im In- und Ausland? ☐ Ja ☐ Nein

Wenn „Ja" sind diese mit Namen, Anschrift, Umsatz in €, sowie der Tätigkeit in einer separaten Tabelle oder ggf. als Organigramm anzugeben.

4. Versicherungsumfang

Versicherungssumme	☐ € 500.000	☐ € 1.000.000	☐ € 3.000.000	☐ € 5.000.000	☐ €
Selbstbehalt	☐ € 5.000	☐ € 10.000	☐ € 25.000	☐ € 50.000	☐ €

Sie wünschen ein Angebot für die folgenden Zusatz-Bausteine:

Cyber-Betrug (Ziffer II.2.8. CyberClear) ☐ Ja

E-Discovery (Ziffer II.2.13. CyberClear) ☐ Ja

Vertragsstrafen wegen verzögerter Leistungserbringung (Ziffer II.3.5.3. CyberClear) ☐ Ja

Falls ja, fügen Sie bitte den entsprechenden Teil der vertraglichen Vereinbarung diesem Fragebogen an.

Cyber-Betriebsunterbrechung bei Cloud-Ausfall (Ziffer II.4.8. CyberClear) ☐ Ja

Cyber-Betriebsunterbrechung bei Technischen Problemen (Ziffer II.4.9. CyberClear) ☐ Ja

HISCOX
WISSEN VERSICHERT.

Bitte per Telefax oder E-Mail an Hiscox
Fax-Nr.: 089/54 58 01-199
E-Mail: hiscox.underwriting@hiscox.de

1. Zusatz-Baustein Cyber-Betrug

Diese Fragen sind nur zu beantworten, wenn die Erweiterung Cyber-Betrug gewünscht wird.

1.1. Wie viele Mitarbeiter (neben der Geschäftsführung bzw. des Vorstands) dürfen im Namen Ihres Unternehmens eigenständig Überweisungen tätigen bzw. bei einer Bank anweisen? _____ Mitarbeiter

1.2. Sie haben folgende Sicherungsmaßnehmen umgesetzt, um sich gegen betrügerische Überweisungen zu schützen:

(Zutreffendes bitte ankreuzen)

- ☐ Verpflichtendes Vier-Augen-Prinzip per Anweisung ab einer Überweisungshöhe von € _____
- ☐ Technisch erzwungenes Vier-Augen-Prinzip ab einer Überweisungshöhe von € _____
- ☐ Zwei-Faktor-Authentisierung zur Anmeldung ins Online-Banking
- ☐ Zwei-Faktor-Authentisierung zur Überweisungsfreigabe ab einer Überweisungshöhe von € _____
- ☐ Verpflichtende Überprüfung beim Zahlungsempfänger bei neuen oder geänderten Kontoinformationen
- ☐ Weitere Maßnahmen (zum Beispiel bei Auslandsüberweisungen): _____

2. Zusatzbaustein Cyber-Betriebsunterbrechung bei Cloud-Ausfall

Diese Fragen sind nur zu beantworten, wenn die Erweiterung Cyber-Betriebsunterbrechung bei Cloud-Ausfall gewünscht wird.

2.1. Welche kritischen Geschäftsprozesse haben Sie in die Cloud bzw. ein externes Rechenzentrum ausgelagert?

_____

2.2. Die Cloud bzw. das externe Rechenzentrum, in das kritische Geschäftsprozesse ausgelagert sind, erfüllt folgende Standards:

(Zutreffendes bitte ankreuzen)

- ☐ Vertraglich zugesicherte Verfügbarkeit (SLA) von mindestens 99,9% (entspricht Tier Level 3 oder höher)
- ☐ Geo-Redundanz in zwei Rechenzentren (entspricht Tier Level 3 oder höher)
- ☐ Zertifizierung nach ISO27001, BSI IT-Grundschutz oder BSI C5

3. Zusatzbaustein Cyber-Betriebsunterbrechung bei Technischen Problemen

Diese Frage ist nur zu beantworten, wenn die Erweiterung Cyber- Betriebsunterbrechung bei Technischen Problemen gewünscht wird.

3.1. Werden kritische Systemänderungen wie die Installation und Veränderung von Software vor der Ausführung im Live-System erfolgreich in einer Testumgebung eingespielt? ☐ Ja ☐ Nein

5. Zusatzfragen

Können Ihre Kunden bei Ihnen mit Kreditkarte zahlen? ☐ Ja ☐ Nein

Falls ja, dann beantworten Sie bitte die Fragen zur Kreditkartenzahlung auf Seite 1 des Zusatzfragebogens.

Generieren Sie Onlineumsätze über Ihre Website? ☐ Ja ☐ Nein

Falls ja, dann beantworten Sie bitte die Fragen zum Online Shop auf Seite 2 des Zusatzfragebogens.

Betreiben Sie Industrie-Steuerungsanlagen mithilfe automatisierter Kontrollsysteme (ICS/SCADA) z.B. Produktion, Leitstände/Leitwarten, Gebäudeleittechnik oder Logistik? ☐ Ja ☐ Nein

Falls ja, dann beantworten Sie bitte die Fragen zu Industrie-Steuerungsanlagen auf Seite 3 des Zusatzfragebogens.

II. DATEN

1. Datenschutz

1.1. Bitte kreuzen Sie die Spanne der sensiblen personenbezogenen **Datensätze** (nach Art. 9 DSGVO) an, die Ihr Unternehmen sammelt, verarbeitet und speichert (ein **Datensatz** kann dabei mehrere Daten zu einer Person enthalten):

(Zutreffendes bitte ankreuzen)

- ☐ 0 – 20.000
- ☐ 20.001 – 100.000
- ☐ 100.001 – 250.000
- ☐ 250.001 – 500.000
- ☐ 500.001 – 1.000.000
- ☐ > 1.000.000

Bei Datenmengen größer 1.000.000 bitten wir um eine genauere Aufschlüsselung (in 1. bis 4.) und die konkrete Anzahl.

1.2. Sind die besonderen personenbezogenen Daten in Ihrem Unternehmen sowohl „in transit“ (z.B. beim Versenden von Emails) als auch „at rest“ (bei der Speicherung auf Speichermedien und Clients außerhalb von Servern) zu jeder Zeit mit einer Schlüssellänge von mindestens AES 256bits oder einem vergleichbaren Verfahren gespeichert? ☐ Ja ☐ Nein

1.3. Sind bei Ihnen formelle Prozesse und schriftliche Richtlinien umgesetzt, die den Schutz, die Aufbewahrung sowie das Löschen von personenbezogenen Daten regeln? ☐ Ja ☐ Nein

HISCOX
WISSEN VERSICHERT.

Bitte per Telefax oder E-Mail an Hiscox
Fax-Nr.: 089/54 58 01-199
E-Mail: hiscox.underwriting@hiscox.de

2. Datenverarbeitung

2.1. Sind Sie im Rahmen der Auftragsdatenverarbeitung für Dritte tätig? ☐ Ja ☐ Nein

2.2. Nutzen Sie Dienstleister zur Auftragsverarbeitung von personenbezogenen Daten? ☐ Ja ☐ Nein

Nr.	Name des Dienstleisters	E-Mail	Hosting	Abrechnung	Sonstige	Sofern Haftungsfreistellungen vereinbart, in welcher Form?
1.		☐	☐	☐		
2.		☐	☐	☐		
3.		☐	☐	☐		

Wenn genutzt bitte in der Tabelle aufführen, wenn nicht bitte mit Ziffer II.3 fortfahren (ggf. auf separatem Blatt).

2.3. Halten sich Ihre Dienstleister mindestens an das Datenschutzniveau aus Ihrem Unternehmen und überprüfen Sie dies regelmäßig durch Auditierungen?

☐ Nein bzw. unbekannt ☐ Ja, wir lassen uns dies regelmäßig durch eine Selbstauskunft bestätigen ☐ Ja, wir überprüfen dies regelmäßig durch die Prüfung eines Auditors ☐ Ja, unser Dienstleister ist zertifiziert. Benennung Zertifikat: _____

2.4. Regeln Sie in Ihren Dienstleistungsverträgen die Verfügbarkeit, Updates und das Beheben von Sicherheitslücken? ☐ Ja ☐ Nein

3. Mitarbeitersensibilisierung

3.1. Sensibilisieren Sie alle Ihre Mitarbeiter zur Erkennung und Vermeidung von Betrugsmaschen, wie Phishing und CEO-Fraud?

☐ Nein, bisher nicht ☐ Ja, unregelmäßig ☐ Ja, mindestens jährliche Wiederholung

3.2. Führen Sie zusätzlich bei all Ihren Mitarbeitern einen regelmäßigen Phishing-Test durch?

☐ Nein, bisher nicht ☐ Ja, mindestens jährliche Wiederholung ☐ Ja, mindestens quartalsweise Wiederholung

III. INFORMATIONSSICHERHEITS-MANAGEMENT

1. ISMS Zertifizierung

1.1. Ist in Ihrem Unternehmen ein Informationssicherheits-Management-System (ISMS) etabliert? ☐ Ja ☐ Nein
Wenn ja, von wem wird das ISMS überprüft und angepasst?

☐ Eigene IT-Abteilung ☐ Interne(r) Informationssicherheitsbeauftragte(r) ☐ Sonstige _____

1.2. Sind Sie nach einem der folgenden Standards oder Normen zertifiziert? ☐ Ja ☐ Nein

Wenn vorhanden, bitte angeben und mit Teil IV. fortfahren.

☐ VdS 3473 ☐ ISO27001 ☐ IT-Grundschutz ☐ Anforderung nach BSI C5

Bis wann ist diese Zertifizierung gültig? _____ Ist eine Verlängerung beabsichtigt? ☐ Ja ☐ Nein

2. Technische Sicherheitsmaßnahmen

2.1. Patch-Management-Prozess

Spielen Sie Sicherheitsupdates durchgehend auf Ihren kritischen IT-Systemen, einschließlich Firewalls und Virenschutz, ein?

☐ Nein, nicht durchgehend ☐ Ja, automatisch ☐ Ja, manuell ☐ Ja, manuell und zeitnah (spätestens nach 30 Tagen)

Werden diese Patches vor der Ausführung im Live-System erfolgreich in einer Testumgebung eingespielt? ☐ Ja ☐ Nein

HISCOX
WISSEN VERSICHERT.

Bitte per Telefax oder E-Mail an Hiscox
Fax-Nr.: 089/54 58 01-199
E-Mail: hiscox.underwriting@hiscox.de

2.2. Umgang mit Altsystemen

Nutzen Sie noch Software für die vom Hersteller keine Sicherheitsupdates mehr bereitgestellt werden? (Wenn „Ja“ Zutreffendes bitte ankreuzen): ☐ Ja ☐ Nein

- ☐ Alle betroffenen Systeme sind identifiziert und wurden nach Kritikalität bewertet
- ☐ Vorhandensein eines zeitnahen Migrationsplans für diese Systeme (bis (_____)
- ☐ Nutzung eines verlängerten Hersteller-Supports
- ☐ Ausschließlicher Betrieb der restlichen Systeme in einer isolierten Netzwerkumgebung ohne direkten Internetzugang und mit durchgehender Kontrolle des Datenverkehrs

Wenn keine Isolierung gegeben bitte erläutern, welche zusätzlichen Schutzmaßnahmen (wie End-Point-Security) Sie für die übrigen Systeme getroffen haben und um welche Software es sich handelt. _____

2.3. Cyber-Diebstahl

Sie haben eine Telefonanlage ohne Anrufbeantworter mit PIN-Zugang oder haben bei Ihren Telefonanlagen und Anrufbeantwortern die Passwörter & PINs von der Werkseinstellung geändert. ☐ Ja ☐ Nein

Wenn die Antragsfrage mit „Nein“ beantwortet wird, wird Ziffer II.2.7. der CyberClear Bedingungen (Cyber-Diebstahl) vom Versicherungsschutz ausgeschlossen.)

2.4. Verantwortlichkeit IT-Sicherheit

Wer ist in Ihrem Unternehmen für das Thema IT-Sicherheit verantwortlich?

- ☐ Es gibt noch keine dedizierte Rolle
- ☐ Informationssicherheitsbeauftragte(r) (ISB)
- ☐ Head of Information Security, CISO o.ä. mit regelmäßigem Reporting an die Geschäftsleitung
- ☐ Sonstige _____

2.5. Netzwerksegmentierung

An mindestens folgenden Stellen halten Sie Firewallstrukturen bzw. Filtersysteme in Ihrem Netz vor: (Zutreffendes bitte ankreuzen)

- ☐ An allen Netzübergängen zum Internet
- ☐ Auf allen Clients (Desktop-Computer, Laptops und Terminals)
- ☐ Zwischen Clients und Servern
- ☐ Zwischen Standorten bzw. ein gibt nur einen Standort
- ☐ Zwischen Steuerungsanlagen und dem Büro-Netz bzw. solche Verbindungen sind gar nicht vorhanden
- ☐ Nutzung einer demilitarisierten Zone (DMZ)
- ☐ Nutzung einer Web Application Firewall (WAF)

2.6. Rechtekonzept

Ihr Rechtekonzept erfüllt folgende Mindestanforderungen: (Zutreffendes bitte ankreuzen)

- ☐ Nutzung eines zentralen Authentisierungs- und Autorisierungsdienstes
- ☐ Ausschließlich benutzerindividuelle Zugänge für alle Mitarbeiter mit Zugriffsbeschränkungen für das jeweilige Rollenprofil
- ☐ Prozess zur regelmäßigen Überprüfung der Zugriffsrechte sowie Sperrung der Konten von ausgeschiedenen Mitarbeitern
- ☐ Administrative Zugänge werden ausschließlich zur Erledigung administrativer Tätigkeiten genutzt. Für die alltägliche Nutzung (insbesondere Surfen im Internet und E-Mail Kommunikation) wird ein Benutzer-Konto ohne Admin-Rechte verwendet
- ☐ Jeder Administrator verwendet für administrative Tätigkeiten ausschließlich ein benutzerindividuelles Administrator-Konto
- ☐ Zugänge zu Notfallkonten sind stark abgesichert (wie 2FA oder komplexe Passwörter mit mindestens 12 Zeichen) und die Zugangsmittel sind sicher hinterlegt (wie einem Safe)

2.7. Fernzugriff

Sie nutzen bei allen Fernzugriffsmöglichkeiten auf Ihr IT-System sowie Cloud-Diensten mindestens eine Zwei-Faktor-Authentisierung (2FA)? ☐ Ja ☐ Nein

Wenn „Nein“ bitte separat erläutern, für Fernzugriffe auf welche Systeme 2FA nicht umgesetzt wird und welche anderweiten Sicherheitsmaßnahmen (wie Protokollierung, Beobachtung, Freischaltung) genutzt werden. _____

HISCOX
WISSEN VERSICHERT.

Bitte per Telefax oder E-Mail an Hiscox
Fax-Nr.: 089/54 58 01-199
E-Mail: hiscox.underwriting@hiscox.de

2.8. Richtlinien

Sie haben eine IT-Sicherheitsrichtlinie umgesetzt, in der die folgenden Elemente geregelt werden: **(Zutreffendes bitte ankreuzen)**

☐ Wir haben keine schriftliche IT-Sicherheitsrichtlinie
☐ Alle Standardnutzer und Standardpasswörter werden durch starke individuelle Daten ersetzt
☐ Definierte Mindestanforderungen an die Passwortstärke
☐ Regelung oder Verbot der privaten Nutzung der dienstlichen IT-Infrastruktur
☐ Vorhalten eines aktuellen Netzplans (Strukturplan des IT-Systems)

2.9. Angriffserkennung

a. Welche Maßnahmen haben Sie zur Erkennung von Angriffen und Sicherheitsvorfällen implementiert?
(Zutreffendes bitte ankreuzen)

☐ Wir haben keine entsprechenden Maßnahmen implementiert
☐ Automatische Auswertung von Protokolldaten
☐ Angriffserkennungssystem (Intrusion-Detection und -Prevention)
☐ Schutzmaßnahmen gegen unerwünschten Datenabfluss (Data Loss Prevention)
☐ System zum Umgang mit sicherheitsrelevanten Ereignissen (Security Information und Event Management (SIEM))
☐ Nutzung eines (managed) Securitiy Operations Centers (SOC)
Ist sichergestellt, dass bei Feststellung unmittelbar eine Bewertung und Lösung umgesetzt wird? ☐ Ja ☐ Nein

b. Über welchen Zeitraum werden Protokolldaten gespeichert?

☐ Weniger als 90 Tage ☐ Mindestens 90 Tage ☐ Mindestens 90 Tage und mindestens an zwei Stellen

2.10. Schwachstellenerkennung

a. Wurde in der Vergangenheit eine automatische Schwachstellenanalyse (Vulnerability assessment) durchgeführt?

☐ Nein ☐ Ja, unregelmäßig ☐ Ja, mindestens jährlich

b. Wurde in der Vergangenheit ein manueller Penetrationstest durchgeführt?

☐ Nein ☐ Ja, unregelmäßig ☐ Ja, mindestens jährlich
Wenn ja, wann zuletzt? (_____)

2.11. Mobile-Device-Management (MDM)

Sie haben eine Mobilgeräteverwaltung implementiert, das die folgenden Schutzmaßnahmen umsetzt: **(Zutreffendes bitte ankreuzen)**

☐ Wir haben kein MDM umgesetzt ☐ Fernlöschung der Geräte ☐ Sichere VPN Verbindung (beschränkt, protokolliert, autorisiert)

☐ Verschlüsselung (Full-disk-encryption) ☐ Abgetrennte Container für dienstliche Daten auf mobilen Geräten ☐ Es gibt eine Bring-Your-Own-Device-Policy (BYOD) - Regelung zur dienstlichen Nutzung privater Geräte

3. Datensicherung

Ihre Datensicherungsstrategie erfüllt folgende Mindestanforderungen: (Zutreffendes bitte ankreuzen)

☐ Mindestens einmal tägliche Durchführung einer vollständigen automatischen Datensicherung

☐ Einzelne (zum Beispiel versehentlich gelöschte) Dateien können für einen Zeitraum von einem Monat problemlos im Regelbetrieb wiederhergestellt werden

☐ Ständiges Vorhandensein von mindestens einer vollständigen Offline-Datensicherung, die jeweils nicht älter als eine Woche ist ODER Nutzung einer Cloud-Back-Up-Lösung verpflichtend mit Zwei-Faktor-Authentisierung (2FA) für eine mehrfache vollständige Datensicherung

☐ Erfolgreiche, mindestens jährliche vollständige Wiederherstellungstests aus der Offline-Datensicherung oder dem Cloud-Back-Up

☐ Anwendung der 3-2-1 Backup-Strategie

HISCOX
WISSEN VERSICHERT.

Bitte per Telefax oder E-Mail an Hiscox
Fax-Nr.: 089/54 58 01-199
E-Mail: hiscox.underwriting@hiscox.de

IV. NOTFALLMANAGEMENT

1. Haben Sie kritische IT-Systeme und Anwendungen für Ihr Unternehmen definiert?	☐ Ja	☐ Nein	
2. Haben Sie kritische IT-Systeme und Anwendungen redundant aufgestellt?	☐ Ja	☐ Nein	
3. Wie werden Ihre kritischen IT-Systeme und Anwendungen primär gehostet?	☐ intern	☐ extern	☐ gemischt
4. Haben Sie die für Ihr Unternehmen kritischen bzw. sensiblen Daten definiert?	☐ Ja	☐ Nein	

5. Es besteht ein schriftlich fixiertes Notfallkonzept, das folgende Mindestanforderungen erfüllt: (Zutreffendes bitte ankreuzen)

☐ Wir haben noch kein Notfallkonzept	☐ Neben herkömmlichen Gefahren wie Brand, Stromausfall oder Unwetter sind auch explizit Cyber-Gefahren, wie ein Komplettausfall der IT-Systeme durch einen zielgerichteten Ransomware-Angriff, erfasst
☐ Prozess zur Erkennung sowie zum Umgang mit Sicherheitsvorfällen (inkl. Datenschutzpannen)	
☐ Geschäftsfortführungsplan	☐ Regelmäßige inhaltliche Überprüfung (mindestens alle 2 Jahre) – letzter Termin (_____)
☐ Wiederanlaufplan	☐ Regelmäßige praktische Tests (mindestens alle 2 Jahre) letzter Termin (_____)

V. VORSCHÄDEN

1. In den letzten fünf Jahren gab es keine Netzwerksicherheitsverletzungen (wie Hacker-Angriffe, Denial-of-Service-Angriffe oder Vorfälle durch Schadprogramme), Bedienfehler, Datenrechtsverletzungen oder Cyber-Erpressungen, die insgesamt bereits zu Schäden und Kosten von über EUR 1.000 geführt haben. Darüber hinaus sind Ihnen keine Umstände bekannt, die zu einem Schaden oder Kosten führen könnten.	☐ Ja	☐ Nein

Wenn die vorstehende Frage mit „Nein“ beantwortet wurde, bitten wir um Details zu jedem Vorfall.

- Was ist konkret passiert (Detailbeschreibung)?
- Welche einzelnen Kosten sind Ihnen durch den Vorfall entstanden?
- Kam es zu einem Systemausfall/Betriebsausfall (vollständig oder teilweise), und wenn ja wie lange?
- Welche Maßnahmen wurden ergriffen um solche Vorfälle zukünftig möglichst zu vermeiden?

Mit einer Vorversichereranfrage erkläre ich mich einverstanden!

Diese ausgefüllte Erklärung sowie eventuelle Anlagen werden bei Abschluss eines Vertrages Grundlage und Bestandteil des Versicherungsvertrages. Die Risikoangaben sind vorvertragliche Anzeigen. Hinsichtlich der Folgen bei der Verletzung vorvertraglicher Anzeigepflichten verweisen wir auf die Regelung des Versicherungsvertragsgesetzes (VVG).

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

Name	Position im Unternehmen	Unterschrift Geschäftsleitung oder befugten Vertreters/Firmenstempel	Datum

Hinweise zu den abgefragten IT-Schutzmaßnahmen im Regulierungsbogen

Frage I.4.1 Cyber-Betrug

Betrügerische Überweisungen	Meist durch Social Engineering, also gezielte Manipulation von Mitarbeitern, veranlasste Geld-zahlungen an Kriminelle, oft auch bekannt als Fake President oder CEO-Fraud.

Frage II.1 Datenschutz

Besondere personenbezogene Daten	Besondere personenbezogene Daten sind 1. Sozialversicherungs-, Führerschein- und Ausweisdaten 2. Steuer und Finanzdaten, wie Bank- oder Kreditkartenkonten 3. Informationen zu Strafverfahren und Ordnungswidrigkeiten 4. Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben (Art. 9 DSGVO).
AES	Steht für Advanced Encryption Standard und ist ein symmetrisches Verschlüsselungsverfahren. 256Bits ist die Schlüssellänge

Frage III.2. Technische Sicherheitsmaßnahmen und Frage I.4.2 Cloud-Ausfall

Kritisch	IT-Systeme sind kritisch, sobald ein mehrtägiger Ausfall (3 Tage) zu einem Umsatzverlust führt.
Zeitnah	Ein Sicherheitsupdate ist dann zeitnah, wenn es schnellstmöglich innerhalb der bestehenden Prüfprozesse eingespielt wird. Dies sollte nicht länger als 30 Tage, bei kritischen Teilen allerdings deutlich kürzer, andauern.
IT-System	Zum IT-System zählen sowohl Geräte, Betriebssysteme als auch Anwendungen. Im Patch-Management-Prozess müssen also sowohl die Treiber auf Geräten wie Routern, als auch die Operating Systems (OS) auf Clients und Servern, sowie die darauf installierten Applikationen (kurz Apps) bzw. Computerprogramme wie ERP oder CRM Software berücksichtigt werden.
Isolierte Netzwerkumgebung	Eine isolierte Netzwerkumgebung kann über eine Segmentierung erreicht werden.
Steuerungsanlagen	Meint den Betrieb von Industrie-Steuerungsanlagen mithilfe automatisierter Kontrollsysteme (ICS/SCADA), wie Produktion, Leitstände/Leitwarten, Gebäudetechnik oder Logistik.
Datenverkehr	Mit durchgehender Kontrolle des Datenverkehrs ist gemeint, dass die Kommunikationsverbindungen (oder auch Netzwerk-Traffic) durch Filtersysteme wie Router mit ACL (Access Control List) oder Firewalls läuft.
Ausgelaufene Herstellerunterstützung	Auch engl. „End of Life“ trifft zum Beispiel auf Windows XP, Windows Server 2003, MacOS Sierra 10.12 oder Linux Ubuntu 12.04 und ältere Versionen zu.
Kritikalität	Dies ist ein relatives Maß für die Bedeutsamkeit eines Teiles des IT-Systems in Bezug auf die Konsequenzen, die eine Störung oder ein Funktionsausfall auf die Geschäftsprozesse hat.
Verlängerter Hersteller-Support	Für Windows 7 bzw. Windows Server 2008 wird dies beispielsweise als Extended Security Updates (ESU) bis 2023 kostenpflichtig bereitgestellt. Für Ubuntu 18.04 soll der Extended Security Maintanance (ESM) bis April 2023 bereitgestellt werden.
Authentisierungs- und Autorisierungsdienst	Am bekanntesten ist das Active Directory (AD) von Microsoft. Eine Alternative für Unix-Betriebssysteme ist Radius.
Fernzugriff	Zu Fernzugriffen zählen sowohl Remote-Zugänge für Homeoffice/Telearbeit, als auch Fernwartungen von Systemen und Anlagen

Frage III.3 Datensicherung

Vollständige Datensicherung	Vollständig bedeutet, dass eine Wiederherstellung aller kritischen Dateien und Anwendungen für den eigenen Geschäftsbetrieb möglich ist.
Offline-Datensicherung	Damit sichergestellt ist, dass bei einem nicht erfolgreichen Update eines Back-Up-Standes weiter-hin ein vollwertiges Back-Up verfügbar ist, empfiehlt es sich, zwei vollständige Datensicherungen physisch getrennt (offline) vom eigentlichen IT-System abzuspeichern. Mindestens eine vollständige Offline-Datensicherung, die nicht älter als eine Woche ist, sollte ständig vorhanden sein ,um sich effektiv vor Manipulation durch Angreifer zu schützen, die alle laufenden IT-Systeme unter ihre Kontrolle gebracht haben (wie Emotet).
3-2-1 Backup-Strategie	Diese Strategie besagt die vollständige Datensicherung immer mindestens in dreifacher Ausführung bereit zu halten. Dabei sollten mindestens zwei verschiedene Technologien (NAS, Storage, Bänder, Objektspeicher) zum Einsatz kommen und mindestens eine Datensicherung sollte außer des eigenen Zugriffs sein (Offline oder sichere Cloud).