CyberSchutz

Risikoerfassungsbogen CyberSchutz für kleine und mittlere Unternehmen.

Grunddaten

Firmenname

Nettojahresumsatz

Was macht ihr Betrieb/Unternehmen?

Existiert eine Betriebsstätte im Ausland?

Allgemeine Erfassung des Geschäfts- und Risikofeldes		
	Ja	**Nein**
Eine Infrastruktur für Online-Handel (eCommerce) wird betrieben.	☐	☐
Eine vernetzte Steuerungstechnik (ICS - Industrial Control System) wird genutzt.	☐	☐
Eine oder mehrere der nachfolgenden besonders sensiblen personenbezogene Daten Dritter werden gespeichert oder verarbeitet: 1. rassische, ethnische Herkunft 2. politische Meinungen, religiöse oder weltanschauliche Überzeugungen 3. Gewerkschaftszugehörigkeit 4. genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person 5. Gesundheitsdaten 6. Daten zum Sexualleben, der sexuellen Orientierung einer natürlichen Person 7. Geschäftsgeheimnisse 8. Finanz- und Steuerdaten	☐	☐
Ein oder mehrere Dienstleister zur Auftragsverarbeitung (im Sinne von Art. 28 DSGVO) werden genutzt. Hierzu zählen beispielsweise Hosting-Server bzw. Hosting Services, Email-Provider, Abrechnungsdienstleister usw.	☐	☐
Die Nutzung privater Geräte in der Unternehmens-IT ist gestattet.	☐	☐

PROVINZIAL

Schutzmaßnahmen 1 Diese Fragen sind **immer** zu beantworten.	Ja	Nein
Einzelne Nutzer und Befugnisebenen werden unterschieden.	☐	☐
Für User und Administratoren werden individuelle Passwörter vergeben. Der Zugang zu jedem System ist nur mit Passwort möglich.	☐	☐
Die individuellen Zugänge sämtlicher Nutzer werden mit ausreichend komplexen Passwörtern gesichert. Der regelmäßige Wechsel der Passwörter wird organisatorisch vorgesehen oder technisch erzwungen.	☐	☐
Administrative Zugänge sind ausschließlich den Administratoren und ausschließlich zur Erledigung administrativer Tätigkeiten vorbehalten. Die alltägliche Nutzung der Systeme findet ohne Admin-Privilegien statt.	☐	☐
Geräte, die über das Internet erreichbar oder im mobilen Einsatz sind, sind mit einem zusätzlichen Schutz vor unberechtigtem Zugriff versehen (z. B. Firewall, 2-Faktor-Authentifizierung bei Servern, Verschlüsselung von Datenträgern mobiler Geräte, Diebstahlsicherung oder ähnlich wirksame Maßnahmen).	☐	☐
Die informationsverarbeitenden Systeme verfügen über einen Schutz gegen Schadsoftware, der automatisch auf dem aktuellen Stand gehalten wird (z. B. Virenscanner, Application Firewall, Code Signing oder ähnliche wirksame Maßnahmen).	☐	☐
Es wird sichergestellt, dass alle Systeme auf aktuellem Stand sind und Sicherheitsupdates/-patches automatisch oder zeitnah installiert werden.	☐	☐
Der Schutz vor dem Verlust der wichtigsten Unternehmensdaten erfolgt durch eine mindestens wöchentliche vollständige Datensicherung (Backup).	☐	☐
Das Backup wird einem regelmäßigen Funktionstest unterzogen.	☐	☐
Die Datensicherungsmedien werden physisch getrennt von den gesicherten Systemen aufbewahrt (z. B. externen Speichermedium, Cloud-Lösungen).	☐	☐
Auf Originale und Backup kann nicht gleichzeitig zugegriffen werden.	☐	☐

Schutzmaßnahmen 2

Die Fragen sind nur zu beantworten, wenn die **Infrastruktur für einen Online-Handel** betrieben wird, **vernetzte Steuerungstechnik** genutzt wird **und/oder besonders sensible personenbezogene Daten** gespeichert und/oder verarbeitet werden. Zudem müssen diese Fragen von Unternehmen mit einem **Jahresnettoumsatz von über 2 Mio. Euro** beantwortet werden.

	Ja	Nein
Es gibt einen Verantwortlichen für die IT-Sicherheit.	☐	☐
Es gibt einen Verantwortlichen für die Einhaltung datenschutzrechtlicher Vorgaben.	☐	☐
Alle internen und externen Mitarbeiter werden regelmäßig über Maßnahmen zur Informationssicherheit geschult und sind verpflichtet diese einzuhalten.	☐	☐
Zugänge zur IT-Infrastruktur werden konsequent nur gewährt, wenn sie für die Aufgabenerfüllung notwendig sind.	☐	☐
Administrative Zugänge werden regelmäßig auf Ihre Notwendigkeit geprüft.	☐	☐
Der Zugriff auf die interne IT-Infrastruktur über öffentliche oder drahtlose Netze erfolgt ausschließlich verschlüsselt.	☐	☐
Es existiert eine zentrale Steuerung für die Installation von Sicherheits-Patches für die gesamte IT (Server, Arbeitsrechner, mobile Geräte...).	☐	☐
Das IT-Netzwerk besitzt unterschiedliche Sicherheitszonen nach Kritikalität.	☐	☐
Sensible Daten (z. B. personenbezogene Daten und Geschäftsgeheimnisse) werden nur auf verschlüsseltem Weg versandt.	☐	☐
Regelmäßige Risikoanalysen für besonders kritische IT-Systeme werden durchgeführt.	☐	☐
Ein IT-Notfall- und -Wiederanlauf-Konzept ist schriftlich fixiert und Verantwortliche dafür sind benannt.	☐	☐
Die private Nutzung in der Unternehmens-IT ist in betrieblichen/individualvertraglichen Vereinbarungen festgehalten.	☐	☐

Sonderfragen VSV

Diese Fragen sind nur zu beantworten, wenn der Vertrauensschaden-Baustein gewünscht wird.

	Ja	Nein
Die Zuverlässigkeit aller Mitarbeiter, die mit Geld oder Finanzen im Allgemeinen umgehen, wird im Vorfeld anhand von Führungszeugnissen oder Referenzen überprüft. Es wird sichergestellt, dass keine Beschäftigte für unser Unternehmen tätig werden, die über negative Führungszeugnisse oder negative Referenzen verfügen.	☐	☐
Verträge mit Lieferanten oder Dienstleistern, die tätig sind, sind schriftlich fixiert.	☐	☐
Geld und Vermögensverfügungen (z. B. Überweisungen) einzelner Mitarbeiter unterliegen grundsätzlichen Regelungen (z. B. 4-Augen Prinzip, Vollmachten zur Höhe etc.).	☐	☐

Zusatzfragen eCommerce

Diese Fragen sind nur zu beantworten, wenn eine Infrastruktur für Online-Handel betrieben wird.

	Ja	Nein
Der Web-Shop wird nicht selbständig administriert und betrieben.	☐	☐
Es werden keine Kreditkartendaten gespeichert.	☐	☐
Es wird ein Payment-Dienstleister zur Abwicklung aller eingehenden bargeldlosen Zahlungsvorgänge genutzt.	☐	☐

Zusatzfragen vernetze Steuerungstechnik

Diese Fragen sind nur zu beantworten, wenn vernetzte Steuerungstechnik genutzt wird.

	Ja	Nein
IC-Systeme befinden sich in einem vollständig separierten Netzwerk mit eingeschränkten Zugriffsmöglichkeiten.	☐	☐
Ein Fernzugriff auf IC-Systeme ist nur mit 2-Faktor-Authentifizierung und verschlüsselt möglich.	☐	☐
Reguläre Arbeitsrechner werden nicht zur Administration oder Steuerung von vernetzten Produktionssystemen genutzt.	☐	☐
Die Prozesse zum regelmäßigen und unplanmäßigen Einspielen von Sicherheitsupdates sind dokumentiert und erprobt.	☐	☐
Zugriffe auf IC-Systeme werden an zentraler Stelle protokolliert und überwacht.	☐	☐
Mobile an dem ICS beteiligten Geräten werden durch Verschlüsselung und Passwörter vor unberechtigtem Zugriff geschützt.	☐	☐
Der Zugriff von privat genutzten Geräten im ICS-Segment wird nicht gestattet.	☐	☐
Die Datensicherungsmedien werden physisch getrennt von den gesicherten Systemen aufbewahrt.	☐	☐
Die Prozesse zur Wiederherstellung eines betriebsbereiten Zustandes sind dokumentiert und werden regelmäßig erprobt.	☐	☐
Durch regelmäßige Tests nach einem festgelegten Turnus wird sichergestellt, dass die Datensicherung- und wiederherstellung funktionieren.	☐	☐

Zusatzfragen private Geräte

Diese Fragen sind nur zu beantworten, wenn die Nutzung privater Geräte in der Unternehmens-IT gestattet ist.

	Ja	Nein
Private Geräte befinden sich in einem getrennten Netzwerk-Segment.	☐	☐
Private Geräte haben keinen Zugriff auf geschäftliche Dienste oder Infrastruktur.	☐	☐

Zusatzfragen zur Nutzung eines Dienstleisters zur Datenverarbeitung

Diese Fragen sind nur zu beantworten, wenn ein oder mehrere Dienstleister zur Datenverarbeitung genutzt wird bzw. werden.

	Ja	Nein
Es wird ein E-Mail-Provider zur Auftragsverarbeitung genutzt.	☐	☐
Es wird ein Hosting-Server bzw. Hosting-Service zur Auftragsverarbeitung genutzt.	☐	☐
Es wird ein Abrechnungsdienstleister zur Auftragsverarbeitung genutzt.	☐	☐
Es wird ein sonstiger Dienstleister zur Auftragsverarbeitung genutzt.	☐	☐
Es wird gewährleistet, dass der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen durchführt, sodass die Verarbeitung im Einklang mit den datenschutzrechtlichen Anforderungen erfolgt. Dies kann durch Selbstauskünfte, Audits oder Zertifikate erfolgen.	☐	☐
Es existiert ein Dienstleistervertrag, in dem Verfügbarkeit, Updates und das Beheben von Sicherheitslücken geregelt sind.	☐	☐
Der Dienstleister unterliegt dem einheitlichen Datenschutzrecht der Europäischen Union.	☐	☐

Datum, Unterschrift gesetzliche/-r Vertreter

VM GI 09/18