| Geschäftszahl: | | | In den Spalten "nein", "ja" und "trifft nicht zu / irrelevant" durch den Eintrag eines "x" die jeweils zutreffende Antwort wählen. | nein | ja | trifft nicht zu / irrelevant | Kurze Kommentare der Beraterin / des Beraters (Eingabe von Freitext mit 277 Zeichen möglich) |
|---|---|---|---|---|---|---|---|
| **betriebliche Hardware** | **1** | **Regelung des Zuganges zu betrieblicher Hardware** | | | | | |
| **betriebliche Hardware** | 1-1 | | Sind Räume mit betrieblicher EDV-Ausstattung gesichert? | | | | |
| **betriebliche Hardware** | 1-2 | | Verfügen Sie über Überwachungseinrichtungen (Zutrittssysteme, Videoüberwachung, etc.)? | | | | |
| **betriebliche Hardware** | 1-3 | | Wurden Zugangsberechtigungen festgelegt? | | | | |
| **betriebliche Hardware** | 1-4 | | Gibt es Sicherheitsvorkehrungen bei Reinigungs- und Wartungsarbeiten? | | | | |
| **betriebliche Hardware** | 1-5 | | Gibt es Sicherheitsvorkehrungen bei Telearbeit (Netzwerkzugang von außen) | | | | |
| **Datenzugriff** | **2** | **Regelung des Zugriffes auf Daten** | | | | | |
| **Datenzugriff** | 2-1 | | Gibt es ein Benutzeridentifikations- und ein Passwortverfahren für technische Geräte? | | | | |
| **Datenzugriff** | 2-2 | | Verfügen Sie über Systeme zur Protokollierung von Zugriffen auf Daten und deren Kontrolle? | | | | |
| **Datenzugriff** | 2-3 | | Verfügen Sie über eine Dokumentation der Eingabeverfahren? | | | | |
| **Datenzugriff** | 2-4 | | Sind automatische Bildschirmsperren (Passwortschutz bei Arbeitspausen) aktiviert? | | | | |
| **Datenzugriff** | 2-5 | | Sind automatische Zugangssperren bei wiederholten Anmelde-Fehlversuchen aktiviert? | | | | |
| **Datenzugriff** | 2-6 | | Gibt es individuelle Benutzerkonten für MitarbeiterInnen? | | | | |
| **Datenzugriff** | 2-7 | | Werden Datenträger verschlüsselt, insbesonders jene mit personenbezogenen Daten? | | | | |
| **Datenzugriff** | 2-8 | | Gibt es ein Berechtigungskonzept und ein Verfahren für die Vergabe von Zugriffsrechten auf Basis des Betriebssystems? | | | | |
| **Datenzugriff** | 2-9 | | Verfügen Sie über einen Schutz vor unberechtigten Zugriffen auf IT-Systeme (Firewall, etc.)? | | | | |
| **Datenzugriff** | 2-10 | | Werden mobilde Datenträger verwaltet, damit bekannt ist, wo diese sich gerade befinden um Verluste etc. zu entdecken? | | | | |
| **Datenzugriff** | 2-11 | | Gibt es ein Verfahren zur Datenlöschung im Sinne der DSGVO | | | | |
| **Datenzugriff** | 2-12 | | Erfolgt die Entsorgung von alten Datenträgern, Fehldrucken mit sensiblen Informationen etc. auf einem sicheren Weg? | | | | |
| **Datenzugriff** | 2-13 | | Gibt es eine interne Regelung für das Kopieren von Datenträgern? (zB Wer darf, wer nicht, ...) | | | | |
| **Datenzugriff** | 2-14 | | Gibt es schriftliche Regelungen für den Umgang mit mobile Devices (USB-Sticks, externe Festplatten, Tablets, Smartphones)? | | | | |
| **Datenzugriff** | 2-15 | | Ist die Fernwartung von Servern und PCs so geregelt, dass Sie entweder über einen Verarbeitervertrag verfügen oder jederzeit Fernwartungen nachvollziehen können und die Geheimhaltung durch den Dienstleister sicher gestellt ist? | | | | |
| **Datenweitergabe** | **3** | **Regelungen zur Weitergabe von Daten und Zugängen** | | | | | |
| **Datenweitergabe** | 3-1 | | Ist ein sicherer Transport analoger Datenträger sicher gestellt? (Boten, Post, etc.) | | | | |
| **Datenweitergabe** | 3-2 | | Ist ein sicherer elektronischer Datenversand sicher gestellt? (zB Anhänge in E-Mails) | | | | |

| Geschäftszahl: | | | In den Spalten "nein", "ja" und "trifft nicht zu / irrelevant" durch den Eintrag eines "x" die jeweils zutreffende Antwort wählen. | nein | ja | trifft nicht zu / irrelevant | Kurze Kommentare der Beraterin / des Beraters (Eingabe von Freitext mit 277 Zeichen möglich) |
|---|---|---|---|---|---|---|---|
| Datenweitergabe | 3-3 | | Erfolgt die Auswahl von Auftragnehmern mit Zugriffsberechtigungen unter Berücksichtigung der DSGVO bzw. deren Qualifikation zur Einhaltung der DSGVO? | | | | |
| Datenweitergabe | 3-4 | | Erfolgt die Weitergabe von Zugriffsberechtigungen an Subunternehmen im Sinne der DSGVO? | | | | |
| Datenweitergabe | 3-5 | | Gibt es eine schriftliche Regelung für Auftragnehmer mit Datenzugang im Sinne der DSGVO (Geheimhaltungsvereinbarung oder Verarbeitervertrag)? | | | | |
| Datenweitergabe | 3-6 | | Werden Kontrollmaßnahmen durch eine/einen Datenschutzkoordinatorin/en durchgeführt? | | | | |
| Datensicherung | 4 | **Regelungen zur Umsetzung einer "Datensicherung" zzgl. Datensicherheit** | | | | | |
| Datensicherung | 4-1 | | Sind Brandschutz- und Wasserschutzmaßnahmen vorhanden? | | | | |
| Datensicherung | 4-2 | | Verfügen Sie über eine unterbrechungsfreie Stromversorgung für neuralgische IKT Geräte? (USV) | | | | |
| Datensicherung | 4-3 | | Werden Sicherungsdatenträger sicher und störungsfrei aufbewahrt? | | | | |
| Datensicherung | 4-4 | | Wurden Backup-Verfahren eingeführt, die den Anforderungen des Betriebes entsprechen? | | | | |
| Datensicherung | 4-5 | | Ist der Einsatz von Cloud-Lösungen geregelt und sind Sie sich der damit verbundenen Sicherheitsrisiken bewusst? | | | | |
| Datensicherung | 4-6 | | Ist ein Virenschutz auf allen Geräten eingeführt? | | | | |
| Datensicherung | 4-7 | | Erfolgen Funktionstests und Überprüfungen der Wiederherstellbarkeit des Backups? | | | | |
| Datensicherung | 4-8 | | Gibt es einen Notfallplan für externe (oder interne) Angriffe oder für Extremsituationen wie Schäden durch Feuer, Wasser etc. um eine Weiterführung des Betriebes sicher zu stellen? | | | | |
| org Maßnahmen | 5 | **Regelungen der organisatorischen Datenschutz- und Sicherungsmaßnahmen** | | | | | |
| eMail | 5-1 | | Gibt es innerbetriebliche Regelungen zur Datensicherheit? | | | | |
| eMail | 5-3 | | Sind die organisatorischen Maßnahmen zum Schutz personenbezogener Maßnahmen konform mit der Datenschutz-Grundverordnung? | | | | |
| eMail | 5-4 | | Erfolgt eine interne Kontrolle der Datenverarbeitungen? | | | | |
| eMail | 5-5 | | Die stichprobenartige Überprüfung von Protokollen und Login-Daten erfolgt regelmässig durch einen Professionisten? | | | | |
| eMail | 5-6 | | Ist die Vertretung von, mit der EDV befassten, MitarbeiterInnen im Urlaub- und Krankheitsfall geregelt? | | | | |
| eMail | 5-7 | | Sind Ihre elektronischen Zutrittssysteme separat abgesichert? (zB Schlüsselkarten, etc.) | | | | |
| IT-Betreuung | 6 | **Regelung der externen/internen IT-Betreuung** | | | | | |
| IT-Betreuung | 6-1 | | Verfügt der Dienstleister/Mitarbeiter über Qualifizierungsnachweise (Zertifikate zB incite, WIFI, ...) | | | | |
| IT-Betreuung | 6-2 | | Gibt es Vertretungsregelungen oder Notfallvorsorgen für den Fall der Nichtverfügbarkeit des Admins? | | | | |
| IT-Betreuung | 6-3 | | Werden bei der Beendigung der Tätigkeit als IT-Administrator dessen Zugangsmöglichkeiten gesperrt? | | | | |
| IT-Betreuung | 6-4 | | Gibt es dokumentierte Regelungen für Wartungs- und Reparaturarbeiten? | | | | |

| Geschäftszahl: | | | In den Spalten "nein", "ja" und "trifft nicht zu / irrelevant" durch den Eintrag eines "x" die jeweils zutreffende Antwort wählen. | nein | ja | trifft nicht zu / irrelevant | Kurze Kommentare der Beraterin / des Beraters (Eingabe von Freitext mit 277 Zeichen möglich) |
|---|---|---|---|---|---|---|---|
| IT-Betreuung | 6-5 | | Sind die Administrations-Kennungen (Benutzerdaten und Kennwörter) vor Zugriffen Dritter geschützt? | | | | |
| IT-Betreuung | 6-6 | | Wird Ihr System mittels Monitoring-Systeme (MDM) überwacht? | | | | |
| IT-Betreuung | 6-7 | | Ist der Administratorfür die laufende Aktualisierung der Dokumentation verantwortlich? | | | | |
| IT-Betreuung | 6-8 | | Wurden "Auto-Update-Mechanismen" aktiviert/eingerichtet? | | | | |
| **WLAN** | **7** | **Regelungen zum Schutz von WLANs** | | | | | |
| WLAN | 7-1 | | Erfolgte nachweislich eine sichere Basiskonfiguration Ihres Accesspoint oder WLAN-Routers (Einhaltung der WLAN-Sicherheitsstandards)? | | | | |
| WLAN | 7-2 | | Ist sichergestellt, dass die Mitarbeitern das betriebliche WLAN mit privaten Geräten nicht benutzen können? | | | | |
| WLAN | 7-3 | | Ist sichergestellt, dass Gäste/Besucher/private Endgeräte in einem separaten WLAN abgetrennt werden und so keinen Zugriff auf Unternehmensdaten haben? | | | | |
| WLAN | 7-4 | | Sind Ihre Mitarbeiter darauf geschult, die Zugangsdaten des WLANs nicht an Dritte weiter zu geben? | | | | |
| WLAN | 7-5 | | Führen Sie eine regelmäßige Überprüfung der im WLAN angemeldeten Benutzer und Endgeräte durch? | | | | |
| **Firewall** | **8** | **Regelungen zur sicheren Einrichtung einer Firewall** | | | | | |
| Firewall | 8-1 | | Ist eine sichere Grundkonfiguration dieser Firewall dokumentiert und sicher gestellt? | | | | |
| Firewall | 8-2 | | Werden regelmäßig Updates und Patches (Firmware) auf dem Gerät eingespielt? | | | | |
| Firewall | 8-3 | | Ist die Administrationsschnittstelle geschützt? | | | | |
| Firewall | 8-4 | | Erfolgt die Absicherung von grundlegenden Internetprotokollen? | | | | |
| Firewall | 8-5 | | Haben Sie geeignete Filterregelungen am Paketfilter eingerichtet? | | | | |
| Firewall | 8-6 | | Sind Reaktionszeiten für den Fall des Ausfalles der Firewall mit internem Personal bzw. externen Dienstleistern geregelt? | | | | |
| Firewall | 8-7 | | Wurde eine Betriebsdokumentation erstellt und wird diese laufend aktualisiert? | | | | |
| **VPN** | **9** | **Regelungen zum Schutz von Fernzugriffen** | | | | | |
| VPN | 9-1 | | Ist ein externer Zugriff mittels VPN eingerichtet? | | | | |
| VPN | 9-2 | | Wurde eine Sicherheitsrichtlinie zur VPN-Nutzung erstellt? | | | | |
| VPN | 9-3 | | Werden nicht mehr benötigte VPN-Zugänge gesperrt? | | | | |
| VPN | 9-4 | | Werden Zugriffsvorgänge über die VPN-Zugänge protokolliert und regelmäßig geprüft? | | | | |
| **Organisation & Personal** | **10** | **Regelungen zur Schulung von MitarbeiterInnen** | | | | | |
| Organisation & Personal | 10-1 | | Sind Reaktionen auf Verletzungen der Sicherheitsvorgaben in Ihrem Betrieb definiert und geschult? | | | | |

| Geschäftszahl: | | | In den Spalten "nein", "ja" und "trifft nicht zu / irrelevant" durch den Eintrag eines "x" die jeweils zutreffende Antwort wählen. | nein | ja | trifft nicht zu / irrelevant | Kurze Kommentare der Beraterin / des Beraters (Eingabe von Freitext mit 277 Zeichen möglich) |
|---|---|---|---|---|---|---|---|
| Organisation & Personal | 10-2 | | Werden Fremdpersonen in sensiblen Bereichen beaufsichtigt und begleitet? | | | | |
| Organisation & Personal | 10-3 | | Erfolgt eine geregelte (dokumentierte) Einarbeitung/Einschulung neuer Mitarbeiter? | | | | |
| Organisation & Personal | 10-4 | | Haben Sie eine Rollenbeschreibung der Arbeitsplätze? | | | | |
| Organisation & Personal | 10-5 | | Gibt es eine geregelte (dokumentierte) Verfahrensweise beim Weggang eines Mitarbeiters? | | | | |
| Organisation & Personal | 10-6 | | Werden Ihre Mitarbeiter regelmäßig auf IT-sicherheitsrelevante Verfahren geschult? | | | | |
| Organisation & Personal | 10-7 | | Erfolgt eine Sensibilisierung Ihrer Mitarbeiter hinsichtlich Informationssicherheit? | | | | |
| Organisation & Personal | 10-8 | | Werden Ihre Mitarbeiter im sicheren Umgang mit IT-Systemen geschult? | | | | |
| Organisation & Personal | 10-9 | | Gibt es eine schriftliche Richtlinie zur sicheren IT-Nutzung? | | | | |
| Organisation & Personal | 10-10 | | Gibt es Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal? (inkl. Putzpersonal) | | | | |
| Organisation & Personal | 10-11 | | Haben Sie eine schriftliche Verschwiegenheits-/Vertraulichkeitsvereinbarung mit Ihren Mitarbeitern? | | | | |
| **Mobile Devices** | **11** | **Regelungen zum Umgang mit mobilen Endgeräten** | | | | | |
| Mobile Devices | 11-1 | | Ist eine sichere Grundkonfiguration für mobile Geräte sichergestellt? | | | | |
| Mobile Devices | 11-2 | | Ist die Verwendung eines erweiterten Zugriffsschutz (Passwort statt PIN) sichergestellt? | | | | |
| Mobile Devices | 11-3 | | Erfolgen regelmäßige Updates von Betriebssystem und Applikationen? | | | | |
| Mobile Devices | 11-4 | | Wurden nichtbenutzte Kommunikationsschnittstellen deaktiviert (Ortungsdienste, ...)? | | | | |
| Mobile Devices | 11-5 | | Gibt es schriftliche Richtlinien zur Benutzung von betrieblichen Mobilen Endgeräten? | | | | |
| Mobile Devices | 11-6 | | Ist die Auswahl und Freigabe von Applikationen vor der Installation sichergestellt? | | | | |
| Mobile Devices | 11-7 | | Gibt es eine Definition von erlaubten Informationen (Dateien, Kontakte, eMail-Konten) auf mobilen Geräten? | | | | |
| Mobile Devices | 11-8 | | Ist sichergestellt, dass bei betrieblicher Nutzung von privaten Endgeräten eine explizite/schriftliche Regelung vorliegt? | | | | |
| Mobile Devices | 11-9 | | Nutzen Sie zur Verwaltung der (betrieblichen) mobilen Endgeräte ein Mobile-Device-Management (MDM)? | | | | |
| Mobile Devices | 11-10 | | Ist die Nutzung von privaten Endgeräten für betriebliche Zwecke erlaubt? (Dulden = erlauben) | | | | |
| Mobile Devices | 11-11 | | Verwenden Sie auf dem mobilen Endgerät einen lokalen Virenschutz? | | | | |
| Mobile Devices | 11-12 | | Ist die "automatische Sperre" in den Einstellungen aktiviert? | | | | |
| Mobile Devices | 11-13 | | Ist die Möglichkeit einer Fernlöschung sichergestellt? | | | | |