Anforderungen an IT-Sicherheit in Unternehmen - Allgemein

- **Definition von Rollen und Verantwortlichkeiten (bspw. Datenschutzbeauftragter)**

  Für die IT-Sicherheit und alle involvierten Prozesse muss ein leitender Angestellter ganzheitlich verantwortlich sein. Aus diesem Grund muss ein Verantwortlichkeits- und Rollenkonzept definiert und ein übergeordneter Ansprechpartner benannt werden.

- **Sensibilisierung und Schulung der Mitarbeiter zur Informations- und Cybersicherheit**

  Mitarbeiter mit Umgang von sensiblen Daten und Zugang zur (digitalisierten) technischen Steuerung (z.B. Steuerung über Netzwerke, Fernwartung) müssen regelmäßig zur Informationssicherheit und Cyber-Sicherheit geschult werden. Dies kann beispielsweise anhand monatlicher Newsletter mit aktuellen Informationen und jährlichen Grundlagenschulungen erfolgen.

- **Initiale, sichere Grundkonfiguration (Härtung)**

  Für das Computersystem muss eine sichere Grundfiguration (Härtung) gewährleistet sein. Dies bedeutet, dass nicht benötigte Anwendungsprogramme entfernt werden. Sinnvollerweise existiert eine Checkliste, anhand derer Systeme geprüft werden können.

- **Verwendung einer Anti-Schadcode-Software sowie einer Firewall**

  Auf allen Arbeitsplatzcomputern und Fileservern sowie mobilen Endgeräten muss eine geeignete Virenschutzsoftware/ Anti-Malware installiert sein, die zentral mittels Managementsoftware administriert wird und somit eine einheitliche Konfiguration und Aktualisierung gewährleistet.

- **Existenz eines geregelten Prozesses zum Patch-Management**

  Ein geregelter Prozess zum Patch- und Schwachstellenmanagement muss eingeführt werden. Alle Änderungen an Hard- und Softwarebeständen sowie deren Konfiguration sollen über das Patch- und Änderungsmanagement gesteuert und kontrolliert werden. Dafür müssen alle vorhandenen IT-Systeme und Anwendungen diesem unterstellt sein.

  Anmerkung/Ergänzung: Patches müssen unverzüglich installiert werden.

- **Erstellung und Aufbewahrung von Backups**

  Für die regelmäßige Erstellung und Funktionsprüfung von Backups muss ein geregelter Prozess zur Datensicherung definiert und umgesetzt werden. Dieses Konzept zur Datensicherung muss Datenwiederherstellbarkeit gewährleisten. Weiterhin müssen für die erstellten Backups Mindest-Aufbewahrungszeiten dokumentiert werden. Aufgrund des hohen Aufwands bei manueller Datensicherung wird die Backuperstellung mittels eines Tools empfohlen.

  Anmerkung/Ergänzung: mindestens wöchentliche Datenvollsicherung die getrennt vom IT-System gelagert wird.

- **Überwachung externer Zugänge zum Netzwerk**

  Ein Prozess zur Vergabe von externen Zutritten auf das Firmengelände sowie die Vergabe von Zugängen zum firmeninternen Netzwerk muss definiert werden, um mit einer funktionierenden Zutritts- und Zugangskontrolle zu gewährleisten, dass Datenverarbeitungssysteme nicht von Unbefugten genutzt werden können. Dies verlangt auch das Bundesdatenschutzgesetz (BDSG) in Nr. 2 der Anlagen zu § 9 Satz 1.

- **Schutz von Datenübertragung über ungesicherte Netze (bspw. Internet)**

  Sensible Daten müssen bei Übertragung über offene Netze (bspw. Internet) mit anerkannten Verschlüsselungsverfahren geschützt werden.

- **Existenz einer Richtlinie zur Passwortsicherheit**

  Für die Erstellung von und den Umgang mit Passwörtern muss eine einheitliche Richtlinie erstellt werden.

- **Zugang zu sicherheitsrelevanten Bereiche (Serverraum, Archiv etc.)**

  Zur physischen Sicherung eines Gebäudes muss ein Sicherheitskonzept mit Zutrittsbeschränkungen und zusätzlichen Zutrittskontrollen für sicherheitsrelevante Bereichen (bspw. Serverräumen, Archiv, Gebäudetechnik) erstellt und umgesetzt werden.