axelion

Checklist

Cyber Security

Organisation

- [ ] Im Unternehmen ist die Rolle und Verantwortung des CISO klar definiert.
- [ ] Es ist ein Disaster Recovery Plan für den Worstcase-Fall vorhanden.
- [ ] Die IT wird kontinuierlich auf Schwachstellen geprüft.
- [ ] Für den Ereignisfall besteht eine Cyber-Security-Versicherung.

Faktor Mensch

- [ ] Die Mitarbeitenden werden kontinuierlich geschult.
- [ ] Der Affinitätsgrad der Mitarbeitenden wird laufend überprüft.

Zugriffskonzepte

- [ ] Es besteht ein funktions- / rollenbasiertes Berechtigungskonzept für Administratoren und User.
- [ ] Clientcomputer für IT-User besitzen keine Installationsrechte.
- [ ] Die Zugriffs-Authentifizierung erfolgt über MFA (Multi-Faktor-Authentifizierung).
- [ ] Die Passwortkomplexität entspricht den aktuellen Sicherheitsempfehlungen.

Backup & Disaster Recovery

- [ ] Das Backup-Konzept basiert auf der 3-2-1-1-0 Regel.
- [ ] Das Backup-Konzept erfüllt betriebliche und gesetzliche Anforderungen.
- [ ] Die zu sichernden Daten wurden definiert.

IT-Infrastruktur

- [ ] Sämtliche ICT-Komponenten werden laufend und zeitnah mit Patches versorgt.
- [ ] Es wird eine Patchmanagement-Lösung verwendet.
- [ ] Client- und Serversysteme werden durch Antivirus-Lösungen geschützt.
- [ ] Auf der Firewall sind Intrusion Prevention (IPS) und Deep Packet Inspection (DPI) aktiviert.
- [ ] Firewall-Regeln werden laufend überprüft und die externen Zugriffe sind bekannt.
- [ ] Es wird ein Spam Gateway genutzt.
- [ ] Ein Web Content Filter ist aktiviert.