Richtlinien für PCs

Übersicht

Dieser Artikel bestimmt die Sicherheitsrichtlinien die bei der Arbeit mit dem jeweiligen Gerätetyp umzusetzen sind.

Firmencomputer

Für alle Firmencomputer (Endgeräte) müssen folgende Richtlinien am Gerät aktiviert bzw. kontrolliert werden:

- Sperrung des Gerätes mit Kennworteingabe nach 10 Minuten
- Gerät ist Mitglied des Azure AD und die Anmeldung findet über das Microsoft Firmenkonto statt
- Das Gerät wurde mit BitLocker verschlüsselt; Der Key wird im Azure-AD und 1Password-Vault der IT-Abteilung gespeichert
- Administrative Tätigkeiten dürfen ausschließlich von einem Firmengerät aus durchgeführt werden.

Eine VPN Verbindung besteht nicht, da kein stationäres Firmennetzwerk genutzt wird und nur SaaS-Anwendungen genutzt werden.

Persönliche Computer und Smartphones (BYOD)

Für alle Benutzer, die mit Ihrem persönlichen Computer auf Firmenressourcen zugreifen, gilt folgendes:

- Der Zugriff auf Firmenressourcen (Dokumente, E-Mails, Passwörter, ...) oder die Verarbeitung personenbezogener Daten ist nur auf einem Firmengerät gestattet.
- Alle Arbeiten müssen auf Firmengeräten getätigt werden
- Die Datenverarbeitung auf dem Datenträger oder im Arbeitsspeicher eines Privatgerätes ist nicht gestattet.