

CHECKLISTE FÜR SICHERE ENDPOINT SECURITY

ALLES AUF EINEN BLICK

SICHER IM HOME-OFFICE

Mobile- und Home-Office sind die Arbeitsplatzmodelle der Zukunft. Sie bieten neue Chancen für Arbeitgebende und Arbeitnehmende – allerdings auch neue Risiken für die IT-Sicherheit. Sogenannte „Endpoints“ wie Laptops, Smartphones und mit der Unternehmens-IT verbundene Programme bieten Cyber-Kriminellen neue Angriffspunkte.

Wir zeigen euch in einfachen Schritten, was Arbeitgebende und Arbeitnehmende für eine sichere Endpoint Security tun können.

» UNTERNEHMEN

ARBEITSEQUIPMENT STELLEN

- Richtiger Umgang mit Equipment muss vermittelt werden
- Security-Awareness-Schulungen geben

VERHALTENSRICHTLINIEN MITGEBEN

- Wie gehe ich mit Firmendaten um?
- Wer hat welche Kompetenzen?
- Wem darf ich welche Informationen zur Verfügung stellen?

PASSWÖRTER

- Vorgaben nicht zu komplex
- Wichtig: Multifaktor-Authentifikation einrichten
- Häufige Passwortwechsel werden NICHT empfohlen
- Passwort-Manager zur Verfügung stellen

TECHNISCHE PRÄVENTIVMAßNAHMEN

- Virenschutz
- Anti-Spam-Filter
- Regelmäßiges Einspielen von Updates
- Cloud-Lösungen konfigurieren
- Daten verschlüsseln

» MITARBEITENDE

SECURITY-AWARENESS (REGELMÄßIG)

- Erkennen und Umgang mit Spam-Mails
- Externe URLs vorher auf Vertraulichkeit überprüfen
- Sicherer Gebrauch von externen Datenträgern, z.B. USB

UMGANG MIT MOBILEN NETZWERKEN

- Kenne ich den Ursprung meines Hotspots?

PASSWÖRTER IM HOME-OFFICE

- Passwörter nach Möglichkeit nicht aufschreiben (Passwort-Manager nutzen!)
- Passwort sollte gut zu merken sein
- Beim Entfernen vom Arbeitsplatz, den Desktop mit einem Passwort schützen oder abmelden