



Checkliste

Zero Trust einführen

Zugriffsrechte analysieren

- ☐ Welche Systeme enthalten kritische oder sensible Daten?
- ☐ Wer hat aktuell Zugriff und ist dieser Zugriff noch gerechtfertigt?
- ☐ Gibt es gemeinsam Logins oder ungesicherte Adminstartor-Konten?

Identität absichern

- ☐ Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktivieren
- ☐ Starke Passwortsrichtlinien durchsetzen
- ☐ Regelmäßige Überprüfung und Löschung inaktiver Nutzerkonten

Endgeräte verwalten

- ☐ Firmengeräte registrieren und über MDM (Mobile Device Management) verwalten
- ☐ Sicherheitsrichtlinien (Updates, Virenschutz, Verschlüsselung) definieren
- ☐ Zugriff von privaten Geräten (BYOD) begrenzen oder absichern

Netzwerksegmentierung prüfen

- ☐ Gibt es eine Trennung zwischen internen, externen und Gast-Netzwerken?
- ☐ Können Angreifer sich im Netz lateral bewegen?
- ☐ Netzwerk-Zonen definieren und Kommunikationswege einschränken

Cloud- und SaaS-Zugriffe kontrollieren

- ☐ Single Sign-on (SSO) für Cloud-Dienste einführen
- ☐ Rechtevergabe in Cloud-Tools regelmäßig prüfen
- ☐ Nutzung unbekannter Dienste („Schatten-IT“) verhindern

Protokollieren und überwachen

- ☐ Login-Versuche, Systemzugriffe und Datenbewegungen protokollieren
- ☐ Anomalien automatisch erkennen lassen (SIEM – Security Information & Event Management)
- ☐ Regelmäßige Auswertung und Alarmierung einrichten

Mitarbeitende sensibilisieren

- ☐ Schulungen zu Phishing, Social Engineering und Passwortsicherheit anbieten
- ☐ Security-Guidelines verständlich und verbindlich kommunizieren
- ☐ Vorfälle offen ansprechbar machen (Fehlerkultur!)

Technische und organisatorische Maßnahmen dokumentieren

- ☐ IT-Sicherheitskonzept mit klaren Verantwortlichkeiten erstellen
- ☐ Maßnahmen- und Umsetzungsplan mit Prioritäten definieren
- ☐ Notfall- und Wiederherstellungspläne erarbeiten

Gefördert durch:



Bundesministerium
für Wirtschaft
und Energie

Mittelstand-
Digital 

aufgrund eines Beschlusses
des Deutschen Bundestages