Schutz privilegierter Zugriffe (PIM)

Ausgangssituation

Ein Unternehmen nutzt Microsoft Entra ID PIM (Privileged Identity Management)
Es gibt verschiedene Identitäten, die zeitweise administrative Aufgaben erledigen müssen.

Eure Aufgabe ist es, Rollen sinnvoll und sicher zuzuweisen.

Aufgabe 1: Rollenbeispiele erarbeiten

1. Wählt 3–4 Administratorrollen aus Microsoft 365 / Entra ID.
2. Beschreibt kurz, wofür diese Rolle genutzt wird.
3. Entscheidet, ob die Rolle:
    - nie dauerhaft
    - nur über PIM
    - nur für sehr wenige Personen vergeben werden sollte

Aufgabe 2: Identitäten analysieren & zuordnen

Ordnet jeder Identität einer Kategorie zu, bewertet das Risiko und entscheidet euch für Schutzmaßnahmen:

Identität	Kategorie	Typisches Risiko	Schutzmaßnahme
Interner IT-Admin			
Externer Berater			
Backup-Tool			

Aufgabe 3 – PIM-Entscheidung treffen

Szenario 1 – Interner Mitarbeiter

- **Benutzer**: IT-Admin
- **Aufgabe**: Benutzer anlegen & zurücksetzen
- **Dauer**: regelmäßig, aber nicht permanent

Fragen:

- Welche Rolle?
- Wie hoch ist das Risiko?
- PIM ja/nein?
- Wenn ja, wie lange aktiv?

Szenario 2 – Externer Dienstleister

- **Identität**: Gast
- **Aufgabe**: Exchange-Einstellungen prüfen
- **Dauer**: 2 Tage

Fragen:

- Rolle?
- Wie hoch ist das Risiko?
- Wer beantragt?
- Wer genehmigt?
- Wie lange sollte der Zugriff erlaubt werden?

Szenario 3 – Technischer Dienst

- Identität: Service Principal
- Aufgabe: Automatisiertes Reporting
- Zugriff: API-basiert

Fragen:

- Adminrolle nötig?
- Wie hoch ist das Risiko?
- PIM sinnvoll?
- Wer genehmigt?