# 09_Security-Baselines & Härtung

# Windows & AD

# Baseline – Windows Server 2019

# Baseline – Windows Server 2019

- CIS/MS Baselines als Orientierung; nur benötigte Rollen/Features
- Lokale Firewall aktiv, SMB-Signierung, NTLM-Härtung
- Protokollierung: Security, Sysmon (optional), Weiterleitung an SIEM

# Baseline – Active Directory & GPO

# Baseline – Active Directory & GPO

- Admin-Tiering, getrennte Admin-Konten, JIT/PIM (falls verfügbar)
- Basis-GPO: Passwort/MFA, Audit-Policy, BitLocker, Applocker/WDAC (optional)
- Regelmäßige Rezertifizierung von Gruppenmitgliedschaften

# Endpoints

Endpoints

# Baseline – Windows 10/11

# Baseline – Windows 10/11

- BitLocker, TPM, Secure Boot, Defender aktiv, SmartScreen
- Angriffsflächenreduktion (ASR), Gerätestatus Compliance, Patch-Zeitfenster
- Lokale Adminrechte restriktiv, Softwareinstallationen über kontrollierte Wege

# Festplattenverschlüsselung (BitLocker)

# Festplattenverschlüsselung (BitLocker)

- Richtlinien, Wiederherstellungsschlüsselablage, Nachweise

Endpoints

# Lokale Adminrechte

# Lokale Adminrechte

- Prinzip: keine lokalen Admins; Ausnahme nur genehmigt & zeitlich befristet

# Netzwerk & Firewall (Sophos XGS)

# Baseline – Sophos XGS (Deutsch)

# Baseline – Sophos XGS

**Menü (Deutsch, Beispiele):**

- *Schutz* → **Regeln und Richtlinien** → *Firewall-Regeln*: Segmentierung, nur erforderliche Ports
- *VPN* → **IPSec/SSL VPN**: Starke Verschlüsselung, MFA, Benutzergruppen
- *Protokollierung & Berichte* → **Berichte**: Regelmäßige Auswertung, Export als Nachweis
- *Konfiguration* → **Sicherung & Wiederherstellung**: Backup der Konfiguration, Versionierung

**Kontrollen:** Geo-IP (falls erforderlich), Web/IPS, Anwendungskontrolle → auf relevante Zonen beschränkt

# Netzwerksegmentierung

# Netzwerksegmentierung

- VLANs nach Rolle/Schutzbedarf (Server, Clients, Drucker, Gäste)
- East-West-Traffic minimieren, Jump-Hosts für Adminzugriffe

# M365/Exchange/Teams

# Baseline – M365 (Light)

# Baseline – M365 (Light)

- MFA/CA Policies, sichere Adminrollen, Audit-Logs
- E-Mail: Anti-Phishing/Spam, DLP/Retention (falls lizenziert)

# E-Mail Security (SPF/DKIM/DMARC)

# E-Mail Security (SPF/DKIM/DMARC)

- SPF-Record restriktiv, DKIM aktiv, DMARC „quarantine/reject“ nach Monitoring-Phase