CNEXT SECURITY SERVICES · BEFUNDBERICHT · EINMALIG

Befundbericht Active Directory

KUNDE
Muster AG, Bern (erfunden)

ANALYSE AM
13. Oktober 2026

UMFANG
Gesamtstruktur muster.local, 2 Domänen, 4 Domänencontroller, 184 Benutzer

WERKZEUGE
PingCastle 3.3, Purple Knight 5, BloodHound CE, Microsoft Security Baselines

3	7	11	4
kritische Funde	hohe Funde	mittlere Funde	Pfade zum Domänen-Admin

Wann Sie dieses Dokument erhalten: Nach der Analyse, vor der ersten Umsetzungswelle.

Zusammenfassung

Das Verzeichnis ist funktional in gutem Zustand, trägt aber Entscheide aus den Jahren 2014 bis 2019 weiter: Dienstkonten mit Domänen-Admin-Rechten, NTLMv1 auf zwei Servern und ein Domänencontroller auf Windows Server 2016. Vier Wege führen von einem gewöhnlichen Benutzerkonto zum Domänen-Admin; zwei davon lassen sich mit je einer Änderung schliessen.

Funde nach Schweregrad

NR.	FUND	SCHWERE GRAD	FUNDSTELLE	EMPFEHLUNG
AD-01	Dienstkonto svc_backup ist Mitglied der Domänen-Admins, Passwort ohne Ablauf seit 2014	**Kritisch**	OU Service Accounts, Gruppe Domain Admins	Group Managed Service Account, Rechte nur auf Backup-Server
AD-02	Uneingeschränkte Kerberos-Delegation auf SRV-FILE01	**Kritisch**	Computerkonto SRV-FILE01	Auf ressourcenbasierte eingeschränkte Delegation umstellen
AD-03	Domänencontroller DC02 auf Windows Server 2016, Support endet 12. Januar 2027	**Kritisch**	DC02, Standort Bern	Ersatz durch Windows Server 2025 in Welle 2
AD-04	NTLMv1 auf SRV-BACKUP01 und SRV-PRINT01 zugelassen	**Hoch**	Richtlinie LAN Manager authentication level	NTLMv2 erzwingen, Audit vorher zwei Wochen
AD-05	23 Konten mit Kennwort-nie-ablaufen ausserhalb der Dienstkonten-OU	**Mittel**	Diverse OUs	Prüfen, ablaufen lassen oder als gMSA führen

Angriffspfade

- Pfad 1: Benutzer in Gruppe Helpdesk darf Passwörter der Gruppe Server-Admins zurücksetzen, ein Server-Admin ist lokal Admin auf DC02. Schliesst mit AD-06.
- Pfad 2: svc_backup meldet sich an SRV-BACKUP01 an, dort ist NTLMv1 erlaubt und ein weiteres Konto hat lokale Adminrechte. Schliesst mit AD-01 und AD-04.
- Pfad 3 und 4: über die Delegation auf SRV-FILE01. Schliessen mit AD-02.

Bewusste Ausnahmen

- Keine. Ausnahmen, die Sie nach der Besprechung behalten, tragen wir hier mit Begründung, Verantwortung und Überprüfungsdatum ein.

So geht es weiter

Besprechung des Berichts mit IT-Leitung und Geschäftsleitung am 20. Oktober 2026; der Massnahmenplan folgt mit den dort gefällten Entscheiden.

Alle Namen, Systeme und Zahlen in diesem Dokument sind erfunden. Ihr Bericht enthält Ihre Umgebung am Tag der Prüfung.