CNEXT SECURITY SERVICES · MONATSBERICHT · MONATLICH

Monatsbericht Active Directory

KUNDE
Muster AG, Bern (erfunden)

BERICHTSMONAT
Oktober 2026

PATCHDAY
14. Oktober 2026, eingespielt am 18. Oktober

ANSPRECHPERSON CNEXT
Namentlich im echten Bericht

4/4	2	5	1
Domänencontroller aktuell	Alarme, beide geklärt	Änderungen an privilegierten Gruppen	offene Ausnahme

Wann Sie dieses Dokument erhalten: In der ersten Woche jedes Monats, im monatlichen Dienst.

Zusammenfassung

Alle vier Domänencontroller tragen die Updates vom Oktober-Patchday. Defender for Identity meldete zwei Ereignisse: eine Abfrage aller Dienstkonten von einer Admin-Workstation (geklärt: Inventur der IT) und einen Anmeldeversuch mit einem deaktivierten Konto (geklärt: alter geplanter Task, entfernt). Die Baselines sind unverändert; die eine Ausnahme bleibt bis zur Ablösung der Zeiterfassung bestehen.

Änderungen des Monats

DATUM	ÄNDERUNG	WER	NACHTEST
18. Okt.	Updates Oktober auf DC01 bis DC04, Neustart im Wartungsfenster	CNEXT	Bestanden
18. Okt.	svc_backup durch gMSA ersetzt, aus Domänen-Admins entfernt	CNEXT	Bestanden
22. Okt.	Neues Admin-Konto Tier 1 für eine neue Mitarbeiterin der IT	IT Muster AG	Geprüft
29. Okt.	Geplanter Task mit deaktiviertem Konto auf SRV-APP03 entfernt	IT Muster AG	Bestanden

Offene Punkte

- Ausnahme A-01: Zeiterfassung Terminal braucht NTLMv2 ohne Signierung; Überprüfung am 31. März 2027, Verantwortung IT-Leitung.
- Welle 2 des Massnahmenplans am 15. November 2026, Vorbereitung läuft.

So geht es weiter

Nächster Bericht in der ersten Novemberwoche. Zwischen den Berichten erreichen Sie Ihre Ansprechperson für Fragen zu Änderungen am Verzeichnis.

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