CNEXT SECURITY SERVICES · MASSNAHMENPLAN · EINMALIG

Massnahmenplan Hardening

KUNDE
Muster AG, Bern (erfunden)

STAND
27. Oktober 2026, nach Welle 1

WELLEN
3 Wellen, je ein Wartungsfenster Samstag 06:00 bis 10:00

FREIGABE
IT-Leitung Muster AG, pro Welle

14	6	2	2
Massnahmen	umgesetzt	Wellen offen	Pfade geschlossen

Wann Sie dieses Dokument erhalten: Nach der Besprechung des Befunds, nachgeführt nach jeder Welle.

Zusammenfassung

Welle 1 hat die beiden Pfade mit dem kleinsten Aufwand für einen Angreifer geschlossen. Welle 2 ersetzt DC02 und erzwingt NTLMv2, Welle 3 bringt die Baselines und Defender for Identity. Jede Massnahme trägt eine verantwortliche Person, eine Frist, das Risiko der Umsetzung und den Nachtest, mit dem sie als erledigt gilt.

Massnahmen

NR.	MASSNAHME	WELLE	VERANTWORTLICH	FRIST	STAND
M-01	svc_backup durch gMSA ersetzen, aus Domänen-Admins entfernen (AD-01)	1	CNEXT mit IT Muster AG	18. Okt. 2026	Erledigt, Nachtest bestanden
M-02	Delegation auf SRV-FILE01 auf RBCD umstellen (AD-02)	1	CNEXT	18. Okt. 2026	Erledigt, Nachtest bestanden
M-03	Helpdesk-Delegation auf Benutzer-OU begrenzen (AD-06)	1	IT Muster AG	18. Okt. 2026	Erledigt
M-05	DC02 durch Windows Server 2025 ersetzen, Rollen übertragen (AD-03)	2	CNEXT	15. Nov. 2026	Geplant
M-06	NTLMv2 erzwingen nach zwei Wochen Audit (AD-04)	2	CNEXT	15. Nov. 2026	Audit läuft
M-10	Defender for Identity Sensor auf allen Domänencontrollern	3	CNEXT	6. Dez. 2026	Offen

Risiken und Rückfall

- M-06: Anwendungen, die noch NTLMv1 sprechen, würden nach der Umstellung die Anmeldung verweigern. Das Audit der zwei Wochen zeigt, welche das sind; der Rückfall ist das Zurücksetzen der Richtlinie, wirksam nach dem nächsten Richtlinienzyklus.
- M-05: Während der Rollenübertragung keine Änderungen an Konten. Systemstatus-Sicherung von DC01 und DC02 vor dem Wartungsfenster, Wiederherstellung am 8. November geprobt.

So geht es weiter

Welle 2 am 15. November 2026. Der Plan wird danach nachgeführt und mit dem Nachtest an die IT-Leitung geschickt.

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