CNEXT SECURITY SERVICES · PLAN OF MEASURES · ONE-OFF

Hardening plan of measures

CUSTOMER
Muster AG, Bern (fictional)

STATUS
27 October 2026, after wave 1

WAVES
3 waves, one maintenance window each, Saturday 06:00 to 10:00

APPROVAL
IT lead Muster AG, per wave

14	6	2	2
measures	implemented	waves open	paths closed

When you receive this document: After the review of the findings, updated after every wave.

Summary

Wave 1 closed the two paths with the smallest effort for an attacker. Wave 2 replaces DC02 and enforces NTLMv2, wave 3 brings the baselines and Defender for Identity. Every measure carries an owner, a deadline, the implementation risk and the re-test that marks it done.

Measures

NO.	MEASURE	WAVE	OWNER	DEADLINE	STATUS
M-01	Replace svc_backup with a gMSA, remove from Domain Admins (AD-01)	1	CNEXT with Muster AG IT	18 Oct 2026	Done, re-test passed
M-02	Switch delegation on SRV-FILE01 to RBCD (AD-02)	1	CNEXT	18 Oct 2026	Done, re-test passed
M-03	Limit Helpdesk delegation to the user OU (AD-06)	1	Muster AG IT	18 Oct 2026	Done
M-05	Replace DC02 with Windows Server 2025, transfer roles (AD-03)	2	CNEXT	15 Nov 2026	Planned
M-06	Enforce NTLMv2 after two weeks of auditing (AD-04)	2	CNEXT	15 Nov 2026	Audit running
M-10	Defender for Identity sensor on all domain controllers	3	CNEXT	6 Dec 2026	Open

Risks and rollback

- M-06: applications that still speak NTLMv1 would refuse sign-in after the switch. The two-week audit shows which they are; the rollback is resetting the policy, effective after the next policy cycle.
- M-05: no account changes during the role transfer. System state backup of DC01 and DC02 before the maintenance window, restore rehearsed on 8 November.

Next steps

Wave 2 on 15 November 2026. The plan is then updated and sent to the IT lead with the re-test.

Every name, system and number in this document is invented. Your report contains your environment on the day of the check.