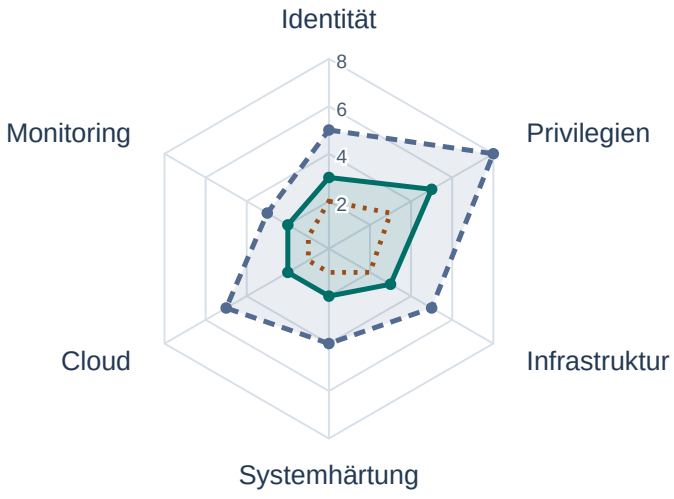
Musterwerk GmbH

Managementbericht

Scan-Vergleich / 15.05.2026 → 15.11.2026 / AD-Prüfung · musterwerk.example / Berichtsreferenz TS-D7251F28161C941D

Im ausgewählten Prüfbereich wurden in Stand A 30 und in Stand B 17 Befunde erfasst. 3 sind in B neu hinzugekommen, 8 sind nachweislich behoben, weil Stand B die Prüfung als bestanden meldet, 8 werden dort nicht mehr gemeldet.

Offene Befunde nach Sicherheitsbereich



Bereich	A	B	Δ	Ziel
Identität & Authentifizierung	5	3	-2	2
Privilegierter Zugriff & Delegation	8	5	-3	3
AD-Infrastruktur & PKI	5	3	-2	2
Systemhärtung (Server & Clients)	4	2	-2	1
Cloud · Entra ID & Microsoft 365	5	2	-3	1
Überwachung & Wiederherstellung	3	2	-1	1

Gezählt werden gemeldete Befunde pro Bereich. Null bedeutet, dass der Scan dort keinen Befund meldet. Die Prüfabdeckung kann je Quelle variieren. In B sind 0 Befunde keinem Bereich zugeordnet und 0 ohne Schweregrad.

Prioritäten für Stand B

P1 · Kennwortrichtlinie & Kontosperre

Domänen-Kennwortrichtlinie anheben (≥ 14 Zeichen) bzw. FGPP für Admins/Dienstkonten (3 Befunde · In Arbeit · Verantwortlich: Identity-Team · Zieltermin: 2026-12-15)

P1 · Privilegierte AD-Konten

DCSync-Rechte (Replicating Directory Changes All) auf Standardprinzipale beschränken – unbekannte Inhaber sofort untersuchen (5 Befunde · Geplant · Verantwortlich: Verzeichnisdienst · Zieltermin: 2026-12-20)

P1 · Zertifikatsdienste (AD CS)

Vorlagen mit ‚Supply in request' (ESC1) deaktivieren oder Genehmigungspflicht aktivieren (1 Befunde · Prüfung · Verantwortlich: Netzbetrieb · Zieltermin: 2027-01-15)

Maßnahmenstatus

Problemfeld	Status	Verantwortlich	Zieltermin
Aktualisierung & Konfigurationsstand	Offen	Plattformteam	2027-01-31
Kennwortrichtlinie & Kontosperre	In Arbeit	Identity-Team	2026-12-15
Privilegierte AD-Konten	Geplant	Verzeichnisdienst	2026-12-20
Protokollierung & Erkennung	Geplant	SOC	2027-02-15
Schutz der Cloud-Anmeldung	In Arbeit	Cloud Operations	2026-12-31
Weiterleitung von Anmeldungen	In Arbeit	Netzbetrieb	2027-01-31
Zertifikatsdienste (AD CS)	Prüfung	Netzbetrieb	2027-01-15

Datengrundlage

Stand	Scan-Datum	Quelldatei	Befunde
A	15.05.2026	Synthetische Beispieldaten	30
B	15.11.2026	Synthetische Beispieldaten	17

Verglichen werden Befundkennungen innerhalb derselben Scanreihe. „Behoben" heißt: Stand B meldet genau diese Prüfung ausdrücklich als bestanden. „Nicht mehr gemeldet" heißt: Der Befund fehlt in Stand B, ein Bestanden-Nachweis liegt aber nicht vor. Die Behebung lässt sich dann mit einem gezielten Nachtest bestätigen. Bei mehrfach belegten Kennungen bleibt die Zuordnung offen.

Berichtsreferenz TS-D7251F28161C941D · Erstellt von Matthias Totzauer · IT Consulting Totzauer