IT-DOKUMENTATION Security Konfiguration/Hardening

Windows Clients

Security – NTLMv2 Enforcement

Security – NTLMv2 Enforcement

GPO-Dokumentation / ISMS-Nachweis

□□ Zweck der Richtlinie

Diese Gruppenrichtlinie erzwingt die Verwendung von **NTLMv2** und verhindert die Nutzung der unsicheren Authentifizierungsverfahren **LM** und **NTLMv1**.
Ziel ist die Erhöhung der Authentifizierungssicherheit und die Erfüllung von Compliance-Anforderungen (ISO 27001 / BSI).

□□ GPO-Informationen

Name der GPO:
Security – NTLMv2 Enforcement

Geltungsbereich:
Alle Windows-Clients und -Server (DCs bei Bedarf separat)

Verantwortlich:
IT-Security / Domain-Administratoren

□□ Enthaltene Richtlinien & Einstellungen

1. LAN-Manager / NTLM-Einstellungen

Pfad:
Computerkonfiguration → Windows-Einstellungen → Sicherheitseinstellungen → Lokale Richtlinien → Sicherheitsoptionen

Richtlinie	Wert	Zweck
Netzwerksicherheit: LAN Manager-Authentifizierungsebene	Nur NTLMv2-Antworten senden. LM- und NTLM verweigern.	Erzwingt NTLMv2
Speichern von LAN Manager-Hashwerten verhindern	Aktiviert	Entfernt unsichere LM-Hashes
RestrictSendingNTLMTraffic (Registry)	2	NTLM-Ausgehend blockieren
NTLMMinClientSec	0x20000000	128-Bit Session Security
NTLMMinServerSec	0x20000000	128-Bit Session Security

□□ Sicherheit & Risikoanalyse

Risiko	Beschreibung	Bewertung	Maßnahme
Unsichere Authentifizierung	LM & NTLM1 leicht kompromittierbar	Hoch	NTLMv2 erzwingen
Pass-the-Hash / Relay	Alte Protokolle erleichtern Angriffe	Mittel	NTLMv1/LM blockieren
Legacy-Geräte inkompatibel	Alte Drucker/NAS benötigen NTLM1	Niedrig–Mittel	Monitoring & Ausnahmen
Compliance-Verstoß	Unsichere Protokolle verletzen BSI/ISO	Hoch	Hardening-GPO

□□ Rollout-Plan

Phase 1 – Monitoring

NTLM-Restriktion auf „Überwachen“ setzen, Logs prüfen.

Phase 2 – Analyse

Betroffene Geräte identifizieren (Eventlog → NTLM Operational Log).

Phase 3 – Anpassung

Legacy-Geräte ersetzen oder NTLMv2 aktivieren.

Phase 4 – Rollout

GPO produktiv aktivieren (NTLMv2 only).

Phase 5 – Review

Nach 7–14 Tagen Logs prüfen, ISMS-Dokumentation aktualisieren.

□□ Änderungsprotokoll

Datum	Änderung	Verantwortlich
TT.MM.JJJJ	GPO erstellt	IT-Security
TT.MM.JJJJ	Testphase durchgeführt	Systemadmin
TT.MM.JJJJ	Produktiver Rollout	Domain Admin
TT.MM.JJJJ	Abnahme durch ISMS	ISMS-Beauftragter

□□ Anhänge

- Importierbare GPO-Vorlage (.txt)
- NTLM-Monitoring-Logs #todo
- Audit-Report ISO/BSI

Diese Vorlage wurde automatisch für die Verwendung in BookStack optimiert.