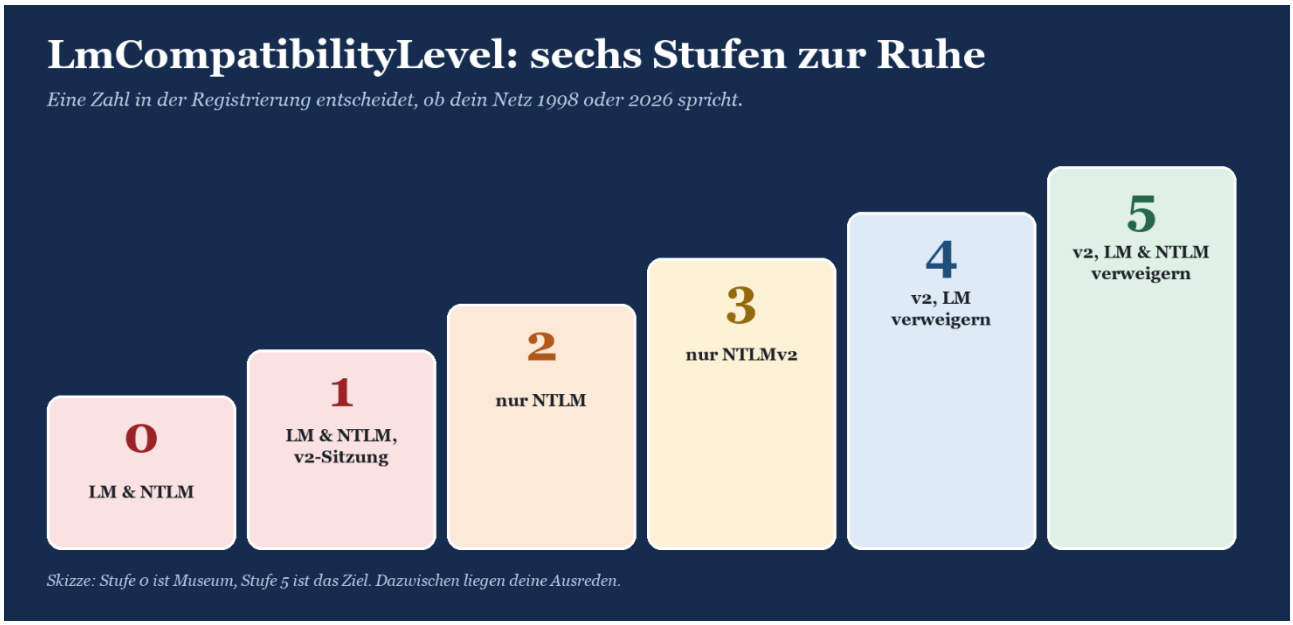
LmCompatibilityLevel richtig setzen: NTLMv2 erzwingen ohne Ausfall



WISSEN
Was der NTLM Diagnostiker erfasst, wie er arbeitet und was er dir zeigt.
› **NTLM Diagnostiker**

BERATUNG
Stufe 5 auf den DCs, aber bitte ohne Montagmorgen-Anrufe? Wir planen mit.
› **Beratung zur NTLM-Ablösung**

SCHULUNG
NTLM-Ereignisse, Richtlinien und Umstellung: praxisnah für dein Team.
› **Schulung zum NTLM Diagnostiker**

Es gibt Registrierungswerte, die niemand anfasst, weil niemand mehr weiß, warum sie so stehen, wie sie stehen. LmCompatibilityLevel ist der Klassiker unter ihnen. Irgendwann 2009 hat jemand ihn auf 1 gesetzt, weil der Kopierer im zweiten Stock sonst nicht scannen wollte. Der Kopierer ist längst verschrottet, der Kollege in Rente, die Gruppenrichtlinie lebt. Und mit ihr ein Stück Authentifizierung aus der Zeit, als Windows NT 4.0 noch als modern galt.

Jetzt wird es ernst. Seit dem Windows-Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 NTLMv1 für Single Sign-on standardmäßig (Registrierungswert BlockNtlmv1SSO, Ereignisse 4024 und 4025). Mit der nächsten Windows-Server-Version ist NTLM insgesamt ab Werk abgeschaltet. Wer da noch Stufe 0, 1 oder 2 in seinen Richtlinien hat, sitzt auf einem Stuhl, an dem schon gesägt wird.

In diesem Beitrag setzt du lmcompatibilitylevel so, dass am Ende überall Stufe 5 steht: Clients senden nur noch NTLMv2, Domain Controller nehmen nichts anderes mehr an. Du bekommst die Werte 0 bis 5 mit ihrer Wirkung auf Client und DC, den Weg über die Gruppenrichtlinie, eine Reihenfolge, die keinen Ausfall produziert, und das Zusammenspiel mit der neuen NTLMv1-Sperre. Den großen Rahmen der Ablösung findest du im Beitrag Der Fahrplan zur NTLM-Abschaltung; hier geht es um genau diesen einen Wert.

FAKTEN · LmCompatibilityLevel in 30 Sekunden

Registrierung: HKLM\SYSTEM\CurrentControlSet\Control\Lsa, Wert LmCompatibilityLevel (DWORD, 0 bis 5).

Gruppenrichtlinie: Computerkonfiguration › Richtlinien › Windows-Einstellungen › Sicherheitseinstellungen › Lokale Richtlinien › Sicherheitsoptionen › „Netzwerksicherheit: LAN Manager-Authentifizierungsebene“.

Wirkt in zwei Richtungen: Was ein Rechner als Client sendet, und was ein Domain Controller annimmt.

Effektiver Standard bei aktuellen Windows-Versionen: Stufe 3 („Nur NTLMv2-Antworten senden“). Ist der Wert nicht gesetzt, gilt dieses Verhalten.

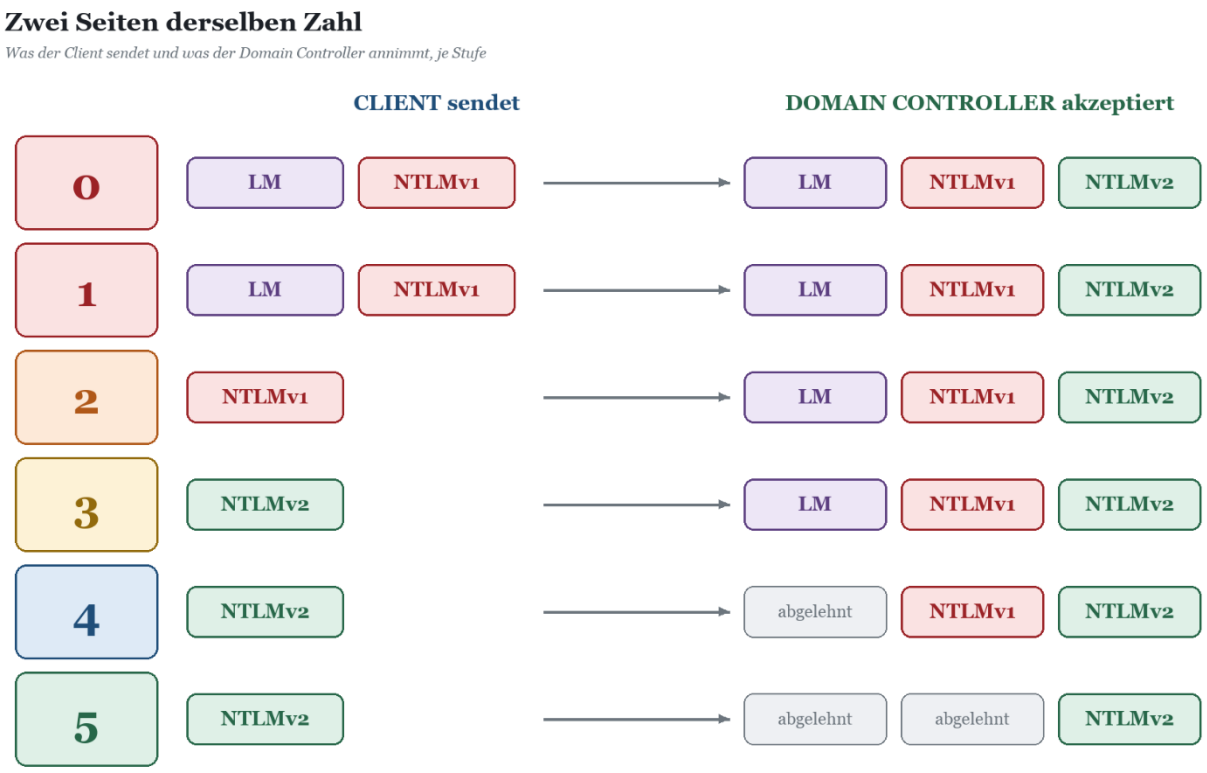
Kein Neustart nötig: Änderungen greifen, sobald die Richtlinie angewendet ist.

Zielwert für 2026: Stufe 5 auf allen Windows-Rechnern, zuletzt auf den Domain Controllern.

Die Werte 0 bis 5: was Client und Domain Controller jeweils tun

Der Name täuscht: LmCompatibilityLevel regelt nicht nur LAN Manager, sondern die ganze Challenge-Response-Familie aus LM, NTLMv1 und NTLMv2. Der Wert hat zwei Gesichter. Als Client entscheidet ein Rechner damit, welche Antwort er auf eine NTLM-Challenge schickt. Als Domain Controller entscheidet derselbe Wert, welche Antworten er bei der Prüfung von Domänenkonten überhaupt noch akzeptiert. Die Stufen 0 bis 3 ändern nur die Client-Seite, erst 4 und 5 machen den DC wählerisch.

Wert	Gruppenrichtlinie (deutsche Bezeichnung)	Client sendet	Domain Controller akzeptiert	Bewertung
0	LM- und NTLM-Antworten senden	LM und NTLMv1, nie NTLMv2-Sitzungssicherheit	LM, NTLMv1, NTLMv2	Museum. Sofort weg.
1	LM- und NTLM-Antworten senden (NTLMv2-Sitzungssicherheit verwenden, wenn ausgehandelt)	LM und NTLMv1, NTLMv2-Sitzungssicherheit, wenn der Server sie kann	LM, NTLMv1, NTLMv2	Kaum besser als 0.
2	Nur NTLM-Antworten senden	NTLMv1, NTLMv2-Sitzungssicherheit, wenn möglich	LM, NTLMv1, NTLMv2	Immer noch NTLMv1. Weg damit.
3	Nur NTLMv2-Antworten senden	NTLMv2	LM, NTLMv1, NTLMv2	Effektiver Standard. Client sauber, DC offen.
4	Nur NTLMv2-Antworten senden. LM verweigern	NTLMv2	NTLMv1, NTLMv2 (LM abgelehnt)	Zwischenschritt, selten sinnvoll.
5	Nur NTLMv2-Antworten senden. LM & NTLM verweigern	NTLMv2	nur NTLMv2	Zielwert.



Skizze nach der Microsoft-Dokumentation zur LAN Manager-Authentifizierungsebene; Sitzungssicherheit vereinfacht

Warum Stufe 3 nicht reicht

Viele Admins atmen auf, wenn sie sehen, dass ihre Windows-Clients ohnehin auf Stufe 3 stehen. Die Clients sind dann tatsächlich sauber: Sie senden nur NTLMv2. Der Domain Controller auf Stufe 3 nimmt aber weiterhin alles an, was ihm gereicht wird, auch LM und NTLMv1. Und genau das schicken die Teilnehmer, die gar keine Gruppenrichtlinie lesen: das NAS aus dem Keller, die Laborwaage mit Embedded-Windows, die Linux-Appliance mit uralter Samba-Version, das Fachverfahren mit eigenem Authentifizierungscode. Stufe 3 sperrt also die eigene Haustür ab und lässt das Garagentor offen.

Erst Stufe 5 auf dem Domain Controller schließt beides. Der DC lehnt dann jede NTLMv1- und LM-Antwort für Domänenkonten ab, egal, woher sie kommt. Darum ist 5 der empfohlene Zielwert, und darum ist er gleichzeitig der Wert, der dir das Wochenende ruinieren kann, wenn du ihn ungeprüft setzt.

Mitgliedsserver und lokale Konten

Ein Detail, das gern übersehen wird: Meldet sich jemand mit einem Domänenkonto an einem Mitgliedsserver an, reicht der Server die Prüfung an einen Domain Controller weiter, und dort zählt die Stufe des DCs. Bei lokalen Konten prüft der Server selbst, und dann zählt seine eigene Stufe. Das ist relevant für Laborrechner, Kassensysteme oder Appliances mit lokalen Dienstkonten. Für Rechner ohne Domänenmitgliedschaft gibt es einen eigenen Beitrag: Rechner ohne Domäne: Arbeitsgruppen, Laborgeräte und NTLM.

WARNUNG · Stufe 5 auf dem DC trifft auch, was du nicht siehst

Windows-Clients mit Stufe 3 merken von der Umstellung des DCs nichts. Getroffen werden Geräte, die selbst NTLMv1 senden: Multifunktionsgeräte mit Scan-to-Folder, ältere NAS-Systeme, Laborgeräte, Fremdsysteme mit eigener NTLM-Implementierung. Diese Geräte schreiben kein Windows-Ereignisprotokoll. Ohne Messung erfährst du erst durch den Anruf aus der Buchhaltung, dass der Scanner nicht mehr speichert.

Mehr dazu: NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll und Scan-to-Folder ohne NTLM: Multifunktionsgeräte richtig anbinden.

WICHTIG · MSCHAPv2 und WLAN: vor Stufe 5 prüfen

MSCHAPv2, etwa bei PEAP-WLAN-Anmeldungen über NPS oder älteren VPN-Zugängen, baut auf derselben Kryptografie wie NTLMv1 auf. Bevor du Domain Controller auf Stufe 5 setzt, prüfe in einer Testumgebung, ob deine RADIUS-Anmeldungen weiter funktionieren. Die Details stehen in MSCHAPv2, NPS und WLAN: die versteckte NTLM-Abhängigkeit; Zusammenhänge mit Credential Guard in Credential Guard und NTLM: was danach nicht mehr funktioniert.

Die Gruppenrichtlinie „Netzwerksicherheit: LAN Manager-Authentifizierungsebene“

Den Registrierungswert per Hand oder per Skript zu setzen, ist möglich, aber eine Einladung zum Wildwuchs. In einer Domäne setzt du lmcompatibilitylevel über die Gruppenrichtlinie. Sie schreibt genau den Wert in HKLM\SYSTEM\CurrentControlSet\Control\Lsa und sorgt dafür, dass ihn niemand still zurückdreht. Laut Microsoft ist in der Default Domain Policy und der Default Domain Controllers Policy nichts definiert; der effektive Standard auf Servern und aktuellen Clients ist „Nur NTLMv2-Antworten senden“, also Stufe 3. Die englische Originalbeschreibung findest du unter Network security: LAN Manager authentication level.

Wo die Richtlinie sitzt

- **Pfad:** Computerkonfiguration › Richtlinien › Windows-Einstellungen › Sicherheitseinstellungen › Lokale Richtlinien › Sicherheitsoptionen.
- **Name:** „Netzwerksicherheit: LAN Manager-Authentifizierungsebene“.
- **Wert:** „Nur NTLMv2-Antworten senden. LM & NTLM verweigern“ entspricht Stufe 5.
- **Neustart:** nicht erforderlich. Nach gpupdate oder dem nächsten Richtlinienzyklus gilt die neue Stufe.

Eigene GPOs statt Default-Policys

Lege für die Umstellung eigene Gruppenrichtlinienobjekte an, getrennt nach Clients, Servern und Domain Controllern. So kannst du jede Etappe einzeln verknüpfen und im Notfall mit einem Klick zurücknehmen. Wer alles in die Default Domain Policy schreibt, hat beim Rückbau ein Problem: Er weiß nicht mehr, welche Einstellung wann dazugekommen ist. Und die Default Domain Controllers Policy ist ohnehin der schlechteste Ort, um zu experimentieren.

GPO	Verknüpft mit	LAN Manager-Authentifizierungsebene	Etappe
LMC-Clients-Pilot	OU Pilot (Clients)	Stufe 5	2a
LMC-Clients	OU Clients, alle Standorte	Stufe 5	2b
LMC-Server	OU Server	Stufe 5	3
LMC-DC	OU Domain Controllers	Stufe 5	4

Ist-Wert prüfen: Registrierung schlägt Richtlinie

Was in der GPO steht, ist der Wunsch. Was in der Registrierung steht, ist die Wahrheit. Ältere Richtlinien mit niedrigerer Stufe, lokale Einstellungen auf Rechnern außerhalb der OU-Struktur oder Images mit eingebackenen Werten sorgen regelmäßig für Überraschungen. Den Ist-Wert prüfst du lokal so:

```
# Ist-Wert lesen (kein Eintrag = effektiver Standard, bei aktuellen Versionen Stufe 3)
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' `
  -Name LmCompatibilityLevel -ErrorAction SilentlyContinue |
  Select-Object LmCompatibilityLevel

# Welche GPO setzt den Wert? Bericht erzeugen und nach der Einstellung suchen
gpresult /h C:\Temp\gpresult.html /scope computer
```

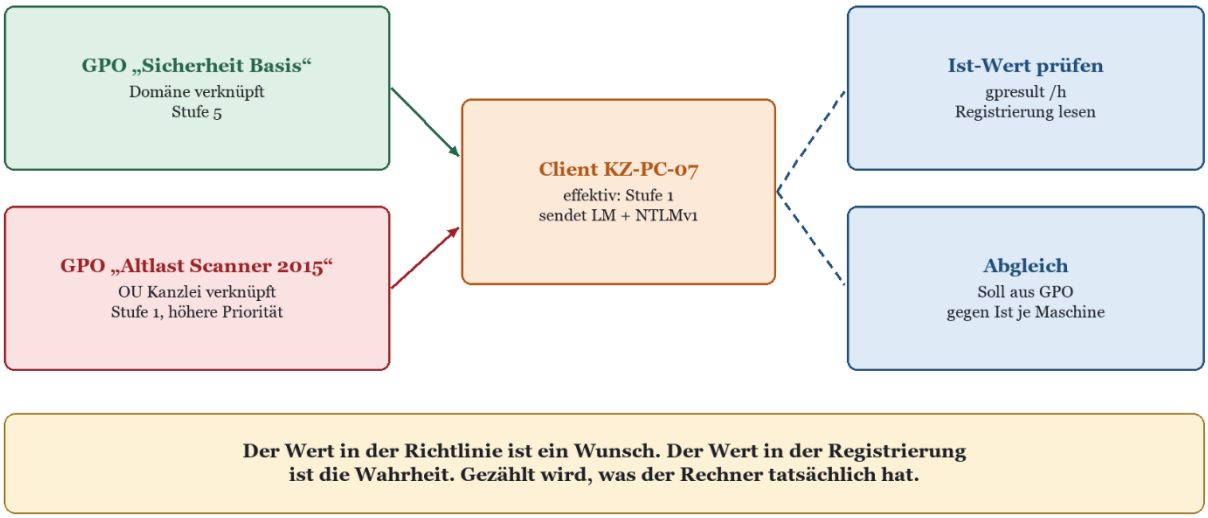
Für mehrere Rechner geht das per Invoke-Command, sofern WinRM erreichbar ist:

```
$pcs = Get-ADComputer -Filter 'Enabled -eq $true' -SearchBase
'OU=Clients,DC=musterwerk,DC=local' |
  Select-Object -ExpandProperty DNSHostName
Invoke-Command -ComputerName $pcs -ErrorAction SilentlyContinue -ScriptBlock {
  $v = (Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa').LmCompatibilityLevel
  [pscustomobject]@{ Rechner = $env:COMPUTERNAME; Stufe = if ($null -eq $v) {'nicht gesetzt'}
else {$v} }
} | Sort-Object Stufe | Format-Table Rechner, Stufe
```

Das funktioniert für die Rechner, die gerade laufen und WinRM erlauben. Die anderen fehlen einfach in der Liste, ohne dass dich jemand darauf hinweist. Ein ausgeschalteter Laptop meldet sich nicht krank, er fehlt nur.

Wenn zwei GPOs sich streiten

Sparfuchs & Partner Steuerberatungs GmbH: Soll und Ist laufen auseinander



Skizze: Namen fiktiv

TIPP · Begleitende Einstellungen gleich mit erledigen

„Netzwerksicherheit: Keine LAN Manager-Hashwerte für nächste Kennwortänderung speichern“ sollte aktiviert sein; das ist seit Langem der Standard, aber prüfe es in alten GPOs.

„Netzwerksicherheit: Minimale Sitzungssicherheit für NTLM-SSP-basierte Clients“ und das Gegenstück für Server verlangen NTLMv2-Sitzungssicherheit und 128-Bit-Verschlüsselung. Auch sie liegen unter den Sicherheitsoptionen und sind ein sinnvoller Begleiter von Stufe 5.

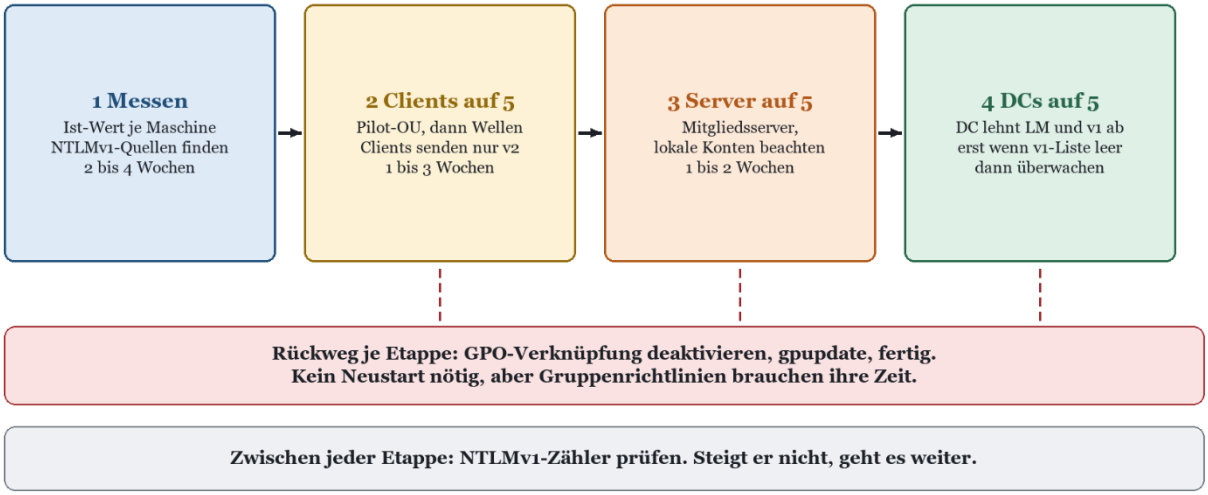
Die Reihenfolge: erst messen, dann Clients, dann Domain Controller

Die goldene Regel ist simpel und wird trotzdem ständig gebrochen: Der Domain Controller kommt zuletzt. Clients auf Stufe 5 zu setzen, ist risikoarm, weil aktuelle Windows-Versionen ohnehin

NTLMv2 senden. Den DC auf Stufe 5 zu setzen, betrifft dagegen jedes Gerät im Netz, auch die, von denen du nichts weißt. Wer mit dem DC anfängt, testet in Produktion. Mit Publikum.

Die Reihenfolge, die dir das Wochenende rettet

Musterwerk GmbH, musterwerk.local: vier Etappen, jede mit Rückweg



Skizze: Zeiträume beispielhaft, abhängig von Größe und Mut deiner Umgebung

Etappe 1: messen, wer heute noch NTLMv1 spricht

Bevor du irgendetwas umstellst, brauchst du zwei Listen: den Ist-Wert von lmcompatibilitylevel je Maschine und alle Verbindungen, die heute noch mit NTLMv1 oder LM ankommen. Für die zweite Liste gibt es mehrere Quellen. Das Sicherheitsprotokoll zeigt in Ereignis 4624 das Feld „Paketname (nur NTLM)“ (siehe Ereignis 4624: NTLM V1 und V2 im Anmeldeprotokoll erkennen). Aussagekräftiger ist das erweiterte NTLM-Auditing ab Windows 11 24H2, Windows Server 2025 sowie Server 2022 und 2019 mit den Updates ab 13.10.2026: Die Ereignisse 4020/4021 (ausgehend, Client), 4022/4023 (eingehend, Server) und 4030 bis 4033 (Domain Controller) enthalten das Feld NtlmVersion. Bei den ausgehenden Ereignissen steht zusätzlich ProcessName, also der Prozess, der NTLM ausgelöst hat; bei den eingehenden RemoteClientMachine und ClientIP.

Wie du das Auditing einschaltest, steht in Erweitertes NTLM-Auditing einschalten; eine fertige Gruppenrichtlinie liefert das NTLM-Audit-GPO-Skript. Damit die Ereignisse nicht auf jedem Rechner einzeln liegen bleiben, sammelst du sie zentral, siehe NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding.

```
# Eingehende NTLMv1-Anmeldungen auf einem Server (erweitertes Auditing)
Get-WinEvent -LogName 'Microsoft-Windows-NTLM/Operational' -FilterXPath `
  "*[System[(EventID=4022 or EventID=4023)]]" -MaxEvents 20000 |
  ForEach-Object {
    $x = [xml]$_.ToXml()
    $f = @{}; $x.Event.EventData.Data | ForEach-Object { $f[$_.Name] = $_.'#text' }
    [pscustomobject]@{ Client = $f['RemoteClientMachine']; IP = $f['ClientIP'];
                       Version = $f['NtlmVersion'] }
  } | Where-Object { $_.Version -match '1' } |
  Group-Object Client, IP | Sort-Object Count -Descending | Select-Object -First 20 Count, Name
```

Prüfe vorher an einem echten Ereignis, wie das Feld NtlmVersion bei dir befüllt ist, und passe den Filter an. Werte immer über die EventData-Felder aus, nie über den Meldungstext: Über Windows Event Forwarding weitergeleitete Ereignisse kommen gelegentlich mit leerem Meldungstext an, die

Felder bleiben aber erhalten. Leere Felder stehen als „Null“ oder „(NULL)“ drin. Mehr Rezepte gibt es in NTLM-Ereignisse mit PowerShell auswerten: Get-WinEvent-Rezepte.

WICHTIG · Geräte ohne Ereignisprotokoll fallen durchs Raster

Ein NAS oder Scanner schreibt keine Windows-Ereignisse. Seine NTLMv1-Anmeldungen siehst du nur auf der Gegenseite: im eingehenden Ereignis des Zielservers oder auf dem Domain Controller. Fehlt dort das Auditing, fehlt das Gerät in deiner Liste. Dann hilft nur ein Netzwerkmitschnitt am Zielserver.

Etappe 2: Clients auf Stufe 5

Starte mit einer Pilot-OU aus 20 bis 50 Rechnern quer durch die Abteilungen, nicht nur aus der IT. Die IT hat die modernsten Geräte und die wenigsten Fachverfahren. Die Lohnbuchhaltung mit dem Kartenleser von 2016 ist der bessere Testfall. Nach einer Woche ohne Auffälligkeiten folgt die nächste Welle, Standort für Standort.

Was kann auf Client-Seite brechen? Wenig, aber nicht nichts. Ein Windows-Client auf Stufe 5 sendet nur NTLMv2. Spricht er mit einem Gerät, das nur NTLMv1 versteht, etwa einem sehr alten NAS mit lokaler Benutzerverwaltung, scheitert die Anmeldung dort. Das ist selten, aber genau der Fall, den du in Etappe 1 gefunden haben solltest.

Etappe 3: Mitgliedsserver

Server auf Stufe 5 ändern ihr Verhalten als Client, etwa wenn ein Applikationsserver auf eine Freigabe zugreift oder ein Dienst sich an einem Fremdsystem anmeldet. Bei lokalen Konten auf dem Server greift zusätzlich die Prüfung auf eigener Seite. Gehe auch hier in Wellen vor: erst Datei- und Druckserver, dann Anwendungsserver mit Fachverfahren, deren Hersteller du vorher fragst.

Etappe 4: Domain Controller

Die DCs stellst du erst um, wenn deine NTLMv1-Liste leer ist oder jeder verbliebene Eintrag einen Plan hat: Gerät ersetzt, Firmware aktualisiert, Hersteller angeschrieben, Ausnahme bewusst akzeptiert. Stelle alle DCs einer Domäne zeitnah um. Ein Gemisch aus DCs mit Stufe 3 und Stufe 5 erzeugt das Lieblingsphänomen jedes Supports: Es geht mal und mal nicht, je nachdem, welchen DC das Gerät gerade erwischt. Danach beobachtest du die Ereignisse 4030 bis 4033 auf den DCs und die fehlgeschlagenen Anmeldungen; abgelehnte Antworten tauchen dort mit Status wie 0xC000006D auf, siehe Fehlercodes 0xC000006D und Co.: fehlgeschlagene NTLM-Anmeldungen deuten.

Etappe	Was sich ändert	Typisches Risiko	Rückweg
1 Messen	nichts	keins, außer Zeitverlust	nicht nötig
2 Clients	Clients senden nur noch NTLMv2	sehr altes Gerät mit lokaler Anmeldung	GPO-Verknüpfung deaktivieren, gpupdate
3 Server	Server senden nur noch NTLMv2, lokale Konten nur v2	Fachverfahren, Appliance	GPO-Verknüpfung deaktivieren, gpupdate
4 DCs	DCs lehnen LM und NTLMv1 ab	Scanner, NAS, Fremdsysteme, MSCHAPv2	GPO-Verknüpfung deaktivieren, Replikation abwarten, gpupdate

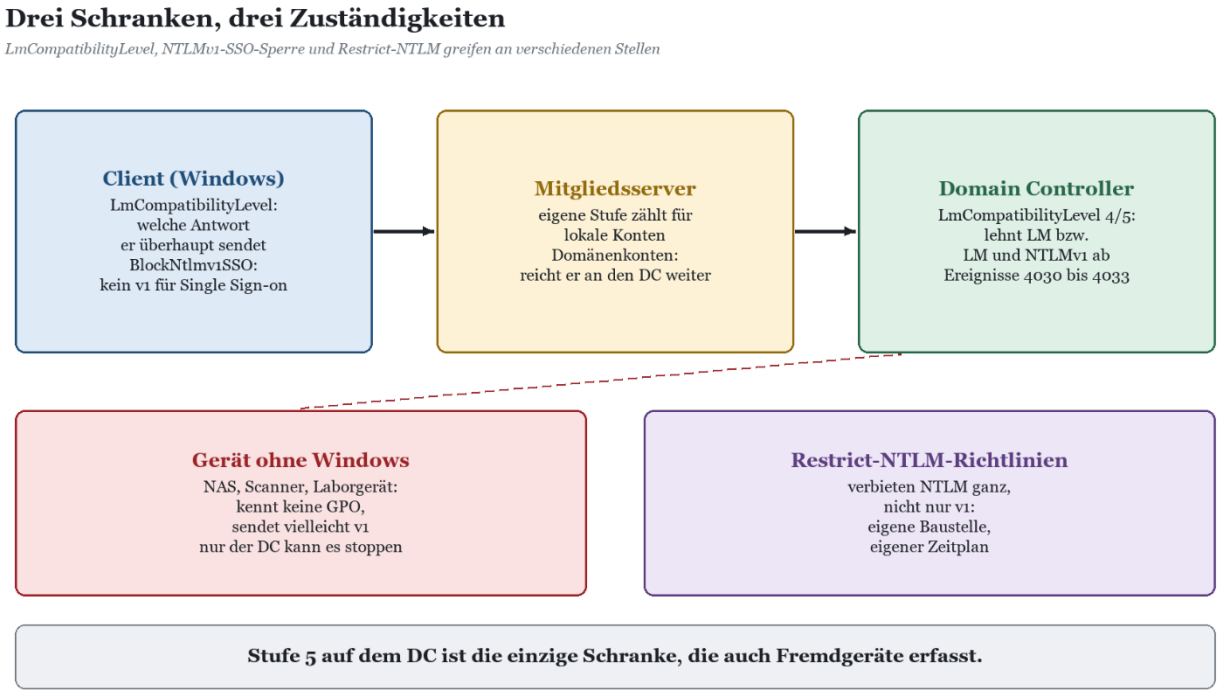
AUS DER PRAXIS · Die Trendforge Digital GmbH und der Plotter

Bei der Trendforge Digital GmbH (trendforge.local) standen alle Clients seit Jahren auf Stufe 3, die DCs ebenso. Das Team wollte die DCs am Freitagnachmittag auf 5 stellen, „ist doch nur eine Zahl“.

Eine Woche Messung vorher förderte genau einen NTLMv1-Kandidaten zutage: einen Großformatplotter, der Druckaufträge per SMB aus einer Freigabe abholt. Firmware aktualisiert, Option „NTLMv2“ im Webinterface gesetzt, Messung bestätigt. Erst dann die DCs. Der Montag war langweilig. So soll das sein.

Zusammenspiel mit der NTLMv1-Blockierung seit Oktober 2026

Seit dem Update vom 13.10.2026 gibt es eine zweite Schranke: Windows 11 ab 24H2 und Windows Server 2025 blockieren NTLMv1 für Single Sign-on standardmäßig. Gesteuert wird das über den Registrierungswert BlockNtlmv1SSO, Spuren hinterlässt es in den Ereignissen 4024 und 4025. Viele fragen sich nun, ob lmcompatibilitylevel damit überflüssig wird. Nein. Die beiden Mechanismen ergänzen sich, decken aber unterschiedliche Fälle ab.



Skizze: vereinfacht, Rechnernamen fiktiv

Mechanismus	Wo er wirkt	Was er verhindert	Was er nicht erfasst
LmCompatibilityLevel (Client)	auf jedem Windows-Rechner	dass dieser Rechner LM oder NTLMv1 sendet	Geräte ohne Windows und ohne GPO
LmCompatibilityLevel 5 (DC)	auf dem Domain Controller	dass LM- oder NTLMv1-Antworten für Domänenkonten akzeptiert werden	lokale Konten auf Mitgliedsservern
BlockNtlmv1SSO	Windows 11 ab 24H2, Server 2025	NTLMv1 bei Single Sign-on mit den Anmeldedaten der Sitzung	ältere Windows-Versionen, Fremdgeräte
Restrict-NTLM-Richtlinien	Client, Server, DC	NTLM generell, auch NTLMv2	nichts, aber mit viel größerer Wirkung

In der Praxis heißt das: Ereignisse 4024/4025 auf einem neuen Client zeigen dir, dass dort jemand versucht hat, NTLMv1 per Single Sign-on zu nutzen. Das passiert nur, wenn der Client selbst eine Stufe unter 3 hat, also typischerweise durch eine alte GPO. Diese Ereignisse sind damit ein

hervorragender Detektor für vergessene LmCompatibilityLevel-Altlasten. Stufe 5 auf den DCs dagegen fängt alles ab, was nicht über einen Windows-Client läuft. Und die Restrict-NTLM-Richtlinien sind der nächste Schritt, der NTLM ganz verbietet, beschrieben in Die Restrict-NTLM-Richtlinien richtig einsetzen und in NTLM schrittweise abschalten.

FAKTEN · Was die Phasen der NTLM-Abschaltung für lmcompatibilitylevel bedeuten

Phase 1 (heute): erweitertes Auditing, NTLMv1-SSO standardmäßig blockiert. Stufe 5 ist jetzt fällig, nicht irgendwann.

Phase 2: IAKerb und lokales KDC sollen Kerberos dort ermöglichen, wo heute nur NTLM geht, etwa ohne Sichtverbindung zum DC oder bei lokalen Konten.

Phase 3 (nächste Windows-Server-Version): NTLM ab Werk abgeschaltet. Wer dann noch über NTLMv1 diskutiert, diskutiert über ein Protokoll, das gar nicht mehr läuft.

Kerberos-Grundlagen findest du unter Microsoft Kerberos.

Wo es mühsam wird und wie die Readiness-Ampel hilft

Mit Bordmitteln kommst du weit, solange deine Umgebung überschaubar ist. Bei 30 Rechnern liest du die Registrierung per Skript aus, schaust in die Ereignisse und bist an einem Nachmittag fertig. Bei 1.800 Computerkonten, drei Standorten und einer Klinik mit Medizingeräten sieht es anders aus. Dann stapeln sich die Fragen: Welche Maschinen haben gar nicht geantwortet? Wo widerspricht der Ist-Wert der Richtlinie? Welche NTLMv1-Anmeldungen gehören zu welchem Gerät, und sind es zehn Verbindungen oder zehntausend, die alle aus demselben Prozess kommen? Und schweigt ein Rechner, weil er sauber ist, oder weil bei ihm das Auditing nie angekommen ist?

Aufgabe	Mit Bordmitteln	Wo es hakt
Ist-Wert je Maschine	Invoke-Command, gpresult	ausgeschaltete und nicht erreichbare Rechner fehlen still
Soll-Ist-Abgleich	GPO-Bericht gegen Registrierung	manuelle Arbeit je OU, fehleranfällig
NTLMv1-Quellen	4624, 4022/4023, Get-WinEvent	Tausende Ereignisse, verteilt auf viele Server
Geräte ohne Windows	Netzwerkmitschnitt, Wireshark	Auswertung von Hand, Zuordnung zum Gerät
Fortschritt zeigen	Excel und Geduld	keine Verlaufskurve für die Geschäftsführung

Für genau diese Lücke gibt es den NTLM Diagnostiker. Er sammelt NTLM-Ereignisse direkt vom Domain Controller, über einen Windows Event Collector, per Direktabfrage oder per Datei-Import, und arbeitet dabei ausschließlich lesend: Er ändert keine Richtlinie, keinen Registrierungswert und kein Konto. Was er vorschlägt, setzt du selbst um.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Readiness-Ampel und NTLMv1-Hitliste vor der Stufe 5

Die Übersicht zeigt dir die Readiness-Ampel, die Zahl der Verbindungen mit NTLMv1 und die Top-10-Verursacher, also gleichartige Verbindungen zusammengefasst nach Ursache, Prozess und Ziel. Aus 4.000 Einzelereignissen werden so eine Handvoll Zeilen, die du abarbeiten kannst.

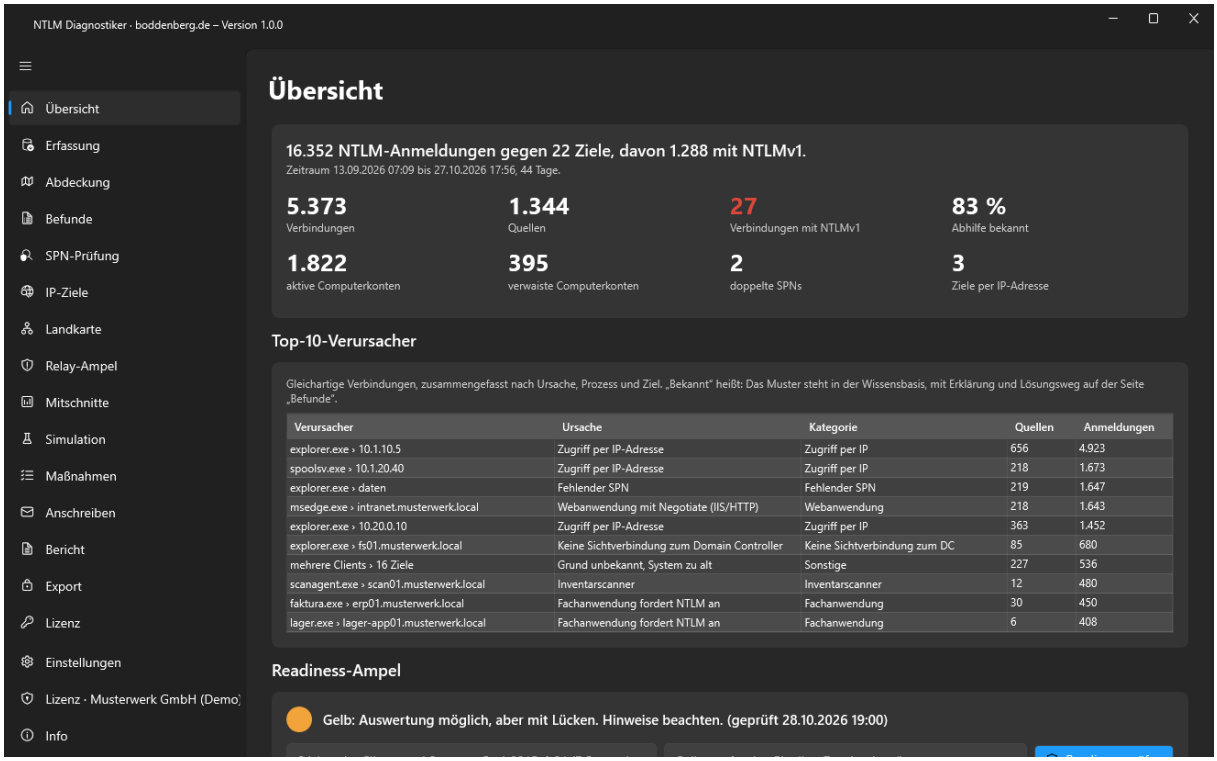
Die Readiness-Ampel berücksichtigt den LmCompatibilityLevel je Maschine und zeigt Widersprüche: Rechner, deren Ist-Wert unter dem Soll liegt, und Rechner, die trotz Stufe 3 oder höher als Quelle von NTLMv1-Verbindungen auftauchen. Das ist der Moment, in dem die vergessene Altlast-GPO auffliegt.

Die NTLMv1-Hitliste sortiert die verbliebenen v1-Quellen, die Abdeckungskarte verrät, welche

Maschinen gar keine Ereignisse liefern. Für Geräte ohne Ereignisprotokoll importierst du einen Mitschnitt (pcap oder pcapng). Die Wissensbasis erklärt bekannte Verursacher samt Lösungsweg.

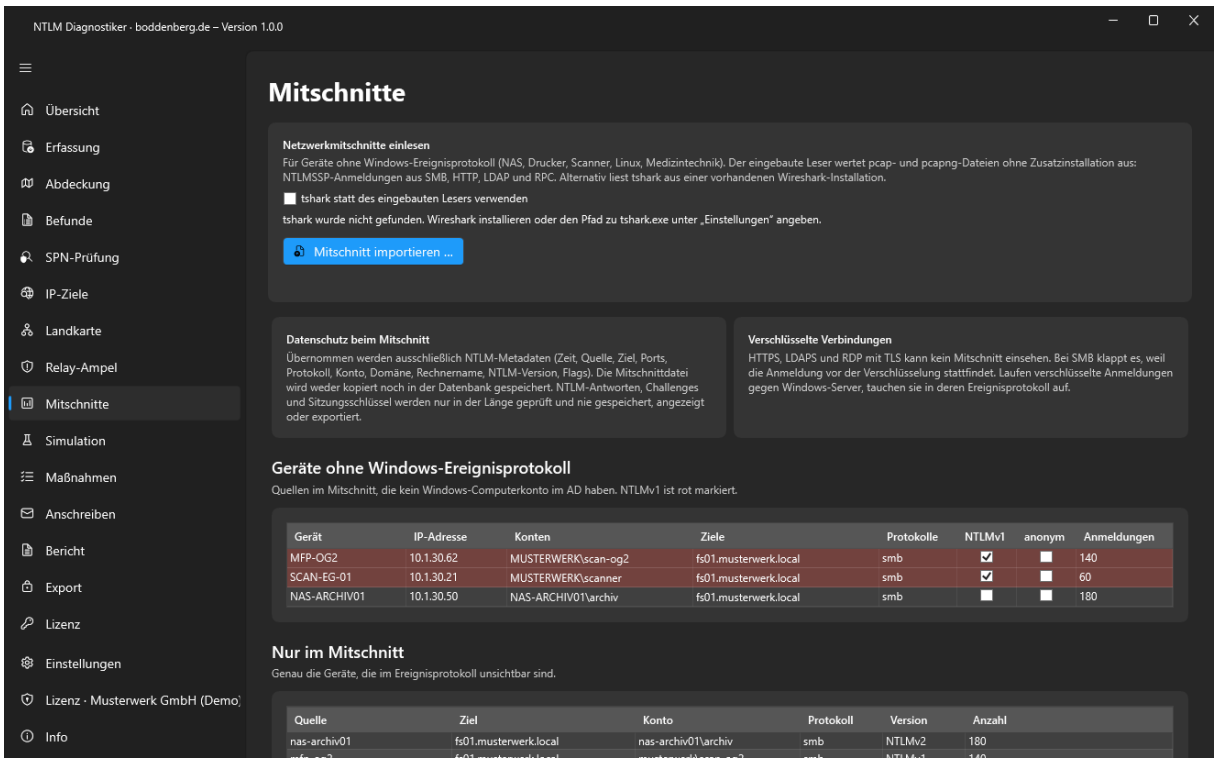
Bevor du die DCs umstellst, beantwortet der Abschalt-Simulator die Frage „Was bricht, wenn ich NTLM jetzt abdrehe?“ mit einem Vertrauenswert aus der Abdeckung. Das Maßnahmen-Board hält fest, was erledigt ist, und zeigt den Verlauf.

› NTLM Diagnostiker



Hier siehst du in der Übersicht die Readiness-Ampel, die Zahl der NTLMv1-Verbindungen und die Top-10-Verursacher (Demodaten der Musterwerk GmbH).

Besonders vor Etappe 4 hilft die Sicht auf Geräte, die nur im Netzwerkmitschnitt auftauchen. Sie sind die üblichen Verdächtigen für den Anruf nach der DC-Umstellung.



So findest du Geräte ohne Windows-Ereignisprotokoll, die NTLMv1 senden; die kritischen Zeilen sind rot markiert (Demodaten).

Zum Einstieg reicht die kostenlose Edition Express: Sie liefert unbegrenzt einen Fünf-Minuten-Befund direkt vom DC mit Readiness-Ampel, Abdeckungskarte, Top-10-Verursachern, Hinweisen aus der Wissensbasis und einem NTLMv1-Alarm mit Anzahl und Top 5, dazu einen Kurzbefund als PDF. Für die komplette Analyse gibt es einen Testzeitraum von sieben Tagen je Domäne und eine Lizenz pro aktivem Computerkonto für 18 Monate. Wenn du die Umstellung lieber mit jemandem planst, der schon einige Plotter, NAS-Systeme und Fachverfahren auf NTLMv2 gebracht hat, schau bei der Beratung zur NTLM-Ablösung vorbei.

FAQ zu LmCompatibilityLevel

Welchen Wert sollte LmCompatibilityLevel 2026 haben?

Stufe 5, „Nur NTLMv2-Antworten senden. LM & NTLM verweigern", auf allen Windows-Rechnern. Die Domain Controller stellst du zuletzt um, nachdem du alle NTLMv1-Quellen gefunden und behoben hast.

Was passiert, wenn der Wert in der Registrierung fehlt?

Dann gilt der effektive Standard. Bei aktuellen Windows-Versionen ist das das Verhalten von Stufe 3: Der Rechner sendet nur NTLMv2, akzeptiert als DC aber noch LM und NTLMv1.

Brauche ich nach der Änderung einen Neustart?

Nein. Laut Microsoft greift die Änderung, sobald die Richtlinie angewendet ist. Plane trotzdem die Zeit für die Gruppenrichtlinienverarbeitung und bei DCs für die Replikation ein.

Reicht es, nur die Domain Controller auf 5 zu setzen?

Technisch blockiert der DC dann NTLMv1 für Domänenkonten. Clients mit niedriger Stufe würden aber weiter NTLMv1 senden und dann scheitern. Deshalb kommen die Clients zuerst: Sie sollen gar nicht erst v1 versuchen.

Ich sehe trotz Stufe 5 auf den Clients noch NTLMv1. Wie kann das sein?

Dann kommt die Anmeldung nicht von einem Client mit Stufe 5. Typische Quellen sind Geräte ohne Windows, Rechner außerhalb der verknüpften OU, eine konkurrierende GPO mit höherer Priorität oder MSCHAPv2-basierte Anmeldungen. Prüfe den Ist-Wert auf dem Quellrechner. Mehr in Ereignis 4776 auf dem Domain Controller: NTLM-Anmeldungen im Sicherheitsprotokoll.

Ersetzt BlockNtlmv1SSO die Einstellung LmCompatibilityLevel?

Nein. BlockNtlmv1SSO verhindert auf Windows 11 ab 24H2 und Server 2025 NTLMv1 bei Single Sign-on. LmCompatibilityLevel 5 auf dem DC lehnt NTLMv1 für Domänenkonten ab, egal, welches Gerät es schickt.

Ist NTLMv2 sicher genug, um dabei zu bleiben?

Nein, nur deutlich weniger schlecht als NTLMv1. NTLMv2 bleibt anfällig für Relay-Angriffe, und mit der nächsten Windows-Server-Version ist NTLM ohnehin ab Werk abgeschaltet. Stufe 5 ist ein Zwischenziel auf dem Weg zu Kerberos.

Was ist mit Vertrauensstellungen zu anderen Domänen?

Bei NTLM über Vertrauensstellungen prüft am Ende ein DC der Kontodomäne. Dessen Stufe entscheidet. Stimme die Umstellung mit den Verantwortlichen der anderen Domäne ab, siehe NTLM über Vertrauensstellungen: Gesamtstrukturen, Domänen und Kerberos.

Wie belege ich der Geschäftsführung, dass die Umstellung sicher ist?

Mit Zahlen: NTLMv1-Verbindungen vor und nach jeder Etappe, Liste der behobenen Verursacher, verbliebene Ausnahmen mit Begründung. Eine Checkliste für den Stichtag findest du in Checkliste vor dem NTLM-Stichtag: 25 Prüfpunkte.

Fazit: Eine Zahl, vier Etappen, kein Drama

LmCompatibilityLevel ist keine Raketenwissenschaft. Sechs Stufen, eine Gruppenrichtlinie, kein Neustart. Das Risiko steckt nicht im Wert, sondern in den Geräten, die du nicht kennst. Wer zuerst misst, dann die Clients, dann die Server und zuletzt die Domain Controller auf Stufe 5 setzt, erlebt die Umstellung als ruhigen Dienstag. Wer mit den DCs anfängt, erlebt sie als Ticketflut.

Mit der NTLMv1-SSO-Sperre seit Oktober 2026 hast du einen zusätzlichen Melder für vergessene Altlasten, und mit Stufe 5 auf den DCs die Schranke, die auch Fremdgeräte erfasst. Danach ist NTLMv1 Geschichte. NTLMv2 bleibt dann noch ein paar Monate, bis Phase 3 auch ihm die Tür zeigt. Bis dahin gilt: Messen schlägt Mut.

WEITERLESEN · Weiter in dieser Serie

› Ereignis 4624: NTLM V1 und V2 im Anmeldeprotokoll erkennen
› Ereignis 4776 auf dem Domain Controller: NTLM-Anmeldungen im Sicherheitsprotokoll
› MSCHAPv2, NPS und WLAN: die versteckte NTLM-Abhängigkeit
› Credential Guard und NTLM: was danach nicht mehr funktioniert
› NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll
› Die Restrict-NTLM-Richtlinien richtig einsetzen
› NTLM schrittweise abschalten
› Nach der Abschaltung: Rückfälle erkennen und NTLM-frei bleiben