NTLM schrittweise abschalten, ohne dass etwas ausfällt



WISSEN
Wie der NTLM Diagnostiker vor jeder Welle zeigt, welche Verbindungen ein Verweigern treffen würde.
› **NTLM Diagnostiker**

BERATUNG
Wellenplan, Erfolgskriterien und Rückfallweg gemeinsam aufsetzen und die Abschaltung begleiten lassen.
› **Beratung zur NTLM-Ablösung**

SCHULUNG
Dein Team lernt, Befunde zu lesen, Wellen zu planen und Ausnahmen sauber zu begründen.
› **Schulung zum NTLM Diagnostiker**

Es gibt zwei Arten, NTLM zu deaktivieren. Bei der ersten setzt du an einem Freitagnachmittag in der Default Domain Policy „Alle verweigern“, fährst ins Wochenende und erfährst am Montag, dass die Produktion steht, die Scanner schweigen, das Labor keine Befunde mehr ablegt und die Geschäftsführung dein Gesicht inzwischen sehr genau kennt. Bei der zweiten merkt fast niemand, dass überhaupt etwas passiert ist. Dieser Beitrag handelt von der zweiten Art.

Die Zeit für Variante zwei läuft. Seit dem Windows-Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 NTLMv1 für Single Sign-on standardmäßig; mit dem Registrierungswert BlockNtlmv1SSO steuerst du Überwachung und Erzwingung, die Ereignisse 4024 und 4025 zeigen, was betroffen ist. Phase 2 bringt IAKerb und ein lokales KDC, damit Kerberos auch dort funktioniert, wo es bisher keine Chance hatte. Und mit der nächsten Windows-Server-Version ist NTLM standardmäßig abgeschaltet. Den gesamten Zeitplan erklärt NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet. Die Frage lautet also nicht mehr, ob du NTLM abschaltest, sondern ob du es selbst tust oder ob ein Update es für dich erledigt, zu einem Zeitpunkt, den du nicht ausgesucht hast.

Wer „ntlm deaktivieren“ sucht, findet meist den Pfad zur Gruppenrichtlinie und einen fröhlichen Screenshot von „Alle verweigern“. Das ist ungefähr so hilfreich wie eine Anleitung zum Fallschirmspringen, die mit „Tür auf“ endet. Hier geht es um alles, was zwischen Tür auf und Landung passiert: den Wellenplan je OU, die Pilot-OU, messbare Erfolgskriterien, den Rückfallweg, die Kommunikation an die Fachabteilungen und das Änderungsfenster.

FAKTEN · Die Ausgangslage im November 2026

NTLMv1 für Single Sign-on: seit dem Update vom 13.10.2026 auf Windows 11 ab 24H2 und Windows Server 2025 standardmäßig blockiert. Steuerung über BlockNtlmv1SSO, Protokoll über die Ereignisse 4024 und 4025.

Erweitertes NTLM-Auditing nach KB5064479: Ereignisse 4020 und 4021 (ausgehend, Client), 4022 und 4023 (eingehend, Server), 4030 bis 4033 (Domänencontroller), jeweils mit Reason ID 0 bis 11. Verfügbar ab Windows 11 24H2 und Windows Server 2025, auf Windows Server 2022 und 2019 mit Updates ab dem 13.10.2026.

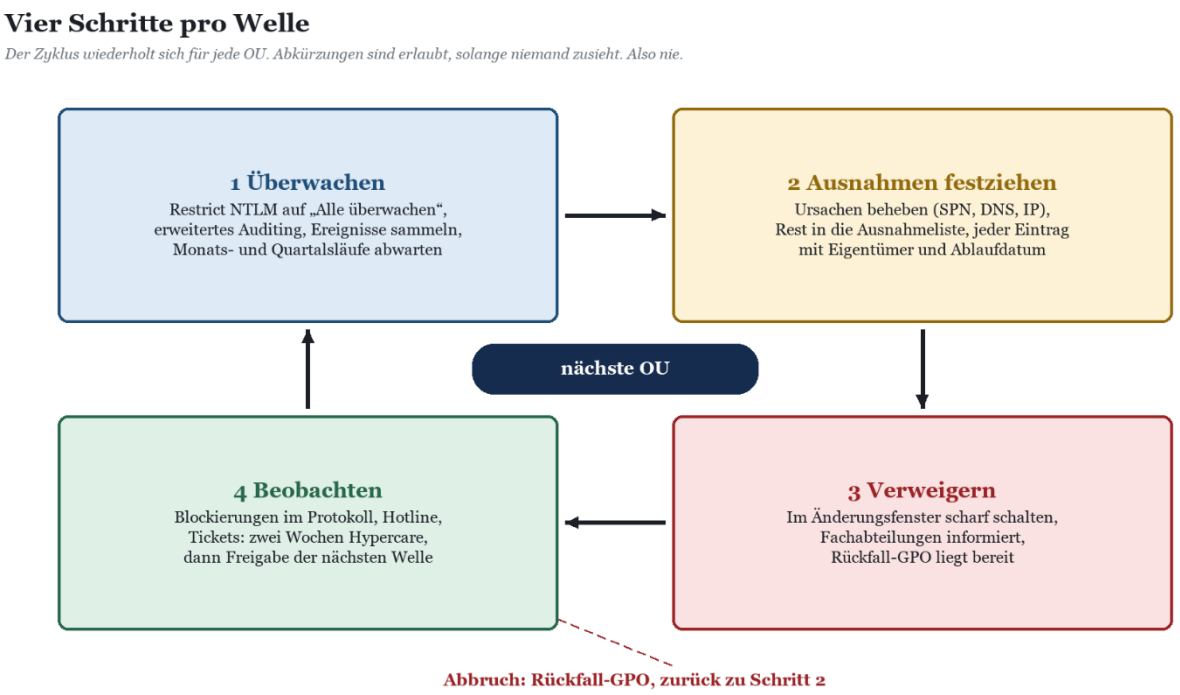
Klassische Restrict-NTLM-Überwachung mit den Ereignissen 8001 bis 8004 funktioniert auch auf älteren Systemen. Alles landet im Kanal Microsoft-Windows-NTLM/Operational.

Das eigentliche Abschalten erledigen die Sicherheitsoptionen „Netzwerksicherheit: NTLM einschränken“: ausgehend auf Clients, eingehend auf Servern, „in dieser Domäne“ auf Domänencontrollern.

Warum Wellen statt Urknall

NTLM ist in einer gewachsenen Active-Directory-Umgebung kein Protokoll, sondern ein Biotop. Es lebt in Laufwerkszuordnungen auf IP-Adressen, in Diensten unter lokalen Konten, in Fachanwendungen, deren Hersteller „Kerberos“ für einen Hund aus der griechischen Sage hält, und in Multifunktionsgeräten, die seit 2014 tapfer in eine Freigabe scannen. Niemand kennt alle Bewohner. Wer das ganze Biotop auf einmal trockenlegt, findet die Bewohner anhand der Beschwerden. Wer es abschnittsweise tut, findet sie anhand der Protokolle. Das ist der ganze Trick.

Eine Welle ist eine abgegrenzte Menge Computer, meist eine OU, für die du NTLM gemeinsam einschränkst. Sie ist klein genug, dass ein Fehler überschaubar bleibt, und groß genug, dass du nicht bis 2030 beschäftigt bist. Jede Welle durchläuft denselben Zyklus aus vier Schritten.



Skizze: Ablauf je Welle; Richtlinienbezeichnungen nach Sicherheitsoptionen „Netzwerksicherheit: NTLM einschränken“

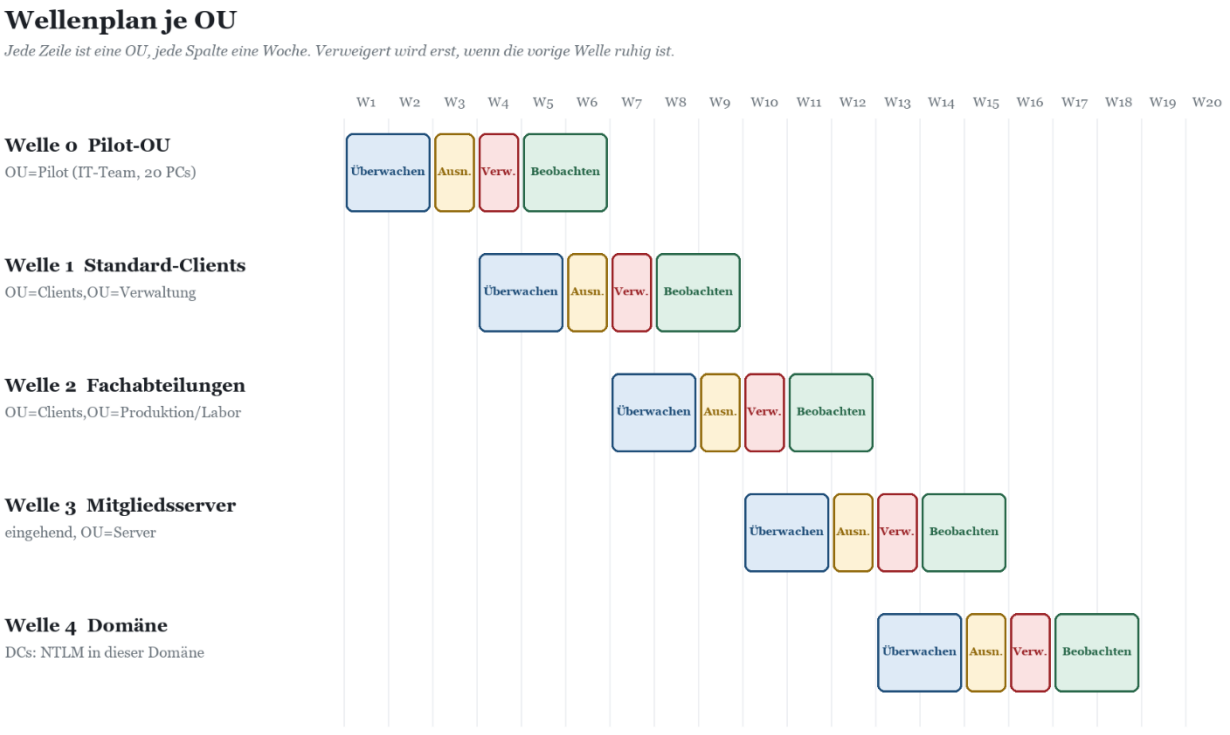
Die vier Schritte je Welle

Schritt	Was du tust	Woran du merkst, dass er fertig ist
1 Überwachen	Restrict NTLM für die OU auf „Alle	Alle Maschinen der OU liefern

	überwachen“ beziehungsweise die Überwachungsrichtlinien setzen, erweitertes Auditing nutzen, Ereignisse zentral sammeln.	Ereignisse; mindestens ein Monatswechsel liegt im Messzeitraum.
2 Ausnahmen festziehen	Ursachen beheben (SPN, DNS-Namen statt IP, Dienstkonten statt lokaler Konten), den Rest in die Remoteserverausnahmen eintragen.	Kein NTLM-Ziel mehr ohne Ursache, Eigentümer und Ablaufdatum.
3 Verweigern	Im Änderungsfenster „Alle verweigern“ für die OU aktivieren, Stichprobe testen.	Die GPO ist auf allen Maschinen angekommen, keine unerwarteten Blockierungen in der ersten Stunde.
4 Beobachten	Hypercare: Protokolle, Hotline, Tickets. Nachzügler (Quartalsläufe, Urlaubsrückkehrer) abfangen.	Zwei Wochen ohne neue Blockierung, die nicht schon bekannt war. Freigabe der nächsten Welle.

Die Reihenfolge der Wellen

Bewährt hat sich, von außen nach innen zu arbeiten: zuerst die ausgehende Richtlinie auf Clients, weil es dort mit den Remoteserverausnahmen ein Ventil gibt. Dann eingehend auf Mitgliedsservern, wo es keine Ausnahmeliste gibt und du dir deshalb sehr sicher sein musst. Ganz zum Schluss die Richtlinie „NTLM-Authentifizierung in dieser Domäne“ auf den Domänencontrollern, die den Deckel draufsetzt. Wie die einzelnen Optionen wirken und warum jede Station für sich prüft, steht ausführlich in Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern.



Skizze: Beispiel Musterwerk GmbH, Zeiträume als Richtwert; Überwachungsphase vereinfacht dargestellt

Welle	Zielgruppe	Richtlinie	Typisches Risiko
0 Pilot	IT-Abteilung, 15 bis 30 Geräte, freiwillige Kolleginnen und Kollegen aus Fachbereichen	Ausgehend: Alle verweigern, mit Ausnahmeliste	gering, die Betroffenen sitzen neben dir

1 Standard-Clients	Verwaltung, Vertrieb, Büroarbeitsplätze	Ausgehend: Alle verweigern	Laufwerke auf IP-Adressen, alte Drucker-Freigaben
2 Fachabteilungen	Produktion, Labor, Lager, Leitstände	Ausgehend: Alle verweigern, längere Ausnahmeliste	Fachanwendungen, Geräte mit Uralt-Firmware
3 Mitgliedsserver	Datei-, Anwendungs- und Druckserver	Eingehend: Alle Domänenkonten verweigern	keine Ausnahmeliste, Geräte ohne Ereignisprotokoll
4 Domäne	Domänencontroller	NTLM-Authentifizierung in dieser Domäne, stufenweise	alles, was die Wellen 0 bis 3 übersehen haben

WICHTIG · Überwachen ist kein Schritt, den du einmal machst

Die Überwachung bleibt während des gesamten Projekts überall aktiv, auch in OUs, die schon verweigern. Nur so siehst du Nachzügler, neue Anwendungen und den Kollegen, der „nur kurz“ einen Testserver per IP anbindet.

Wie du das erweiterte Auditing per Gruppenrichtlinie ausrollst, zeigt Erweitertes NTLM-Auditing einschalten: Schritt für Schritt; eine fertige Vorlage dafür liefert das NTLM-Audit-GPO-Skript.

Die Pilot-OU: dein Labor mit echten Menschen

Die Pilot-OU ist die einzige Welle, bei der Ausfälle ausdrücklich erwünscht sind. Nicht, weil du gern Tickets bearbeitest, sondern weil jeder Ausfall im Pilot einer ist, den du in Welle 1 nicht vor 400 Leuten erlebst. Ein guter Pilot ist deshalb kein Sammelbecken für die drei neuesten Laptops, sondern ein Querschnitt.

Wen du in den Pilot holst

- **Das IT-Team selbst.** Ihr seid die Ersten, die es merken, und die Letzten, die sich beschweren dürfen.
- **Je eine Person aus jeder größeren Fachabteilung.** Freiwillig, technisch neugierig, mit kurzem Draht zu dir. Die Buchhaltung bringt den Lohnlauf mit, die Konstruktion das PDM-System, der Einkauf den alten Lieferantenzugang.
- **Mindestens ein Gerät pro Betriebssystemstand.** Windows 11 24H2 verhält sich bei NTLMv1 anders als ein vergessener Rechner mit Windows 10 im Lager.
- **Ein Standort ohne direkte Sichtverbindung zum DC, falls vorhanden.** Dort wartet Reason ID 9 auf dich.

Die Pilot-OU technisch aufsetzen

Lege eine eigene OU an, verschiebe die Pilotgeräte dorthin und verknüpfe eine eigene GPO, zum Beispiel „NTLM-Restrict-Welleo“. Sie setzt nur eine einzige Sicherheitsoption: „Netzwerksicherheit: NTLM einschränken: Ausgehender NTLM-Datenverkehr zu Remoteservern“, zuerst auf „Alle überwachen“, später auf „Alle verweigern“, dazu die Remoteserverausnahmen. Alles andere erbst du weiter aus den bestehenden GPOs. Prüfe vorher mit gpresult, ob die OU die Vererbung blockiert oder eine erzwungene GPO weiter oben deinen Wert überschreibt; Sicherheitsoptionen werden nicht zusammengeführt, es gilt der Wert mit der höchsten Priorität.

```
# Pilotgeräte in die OU verschieben (Beispiel musterwerk.local)
$ziel = 'OU=Pilot,OU=NTLM-Wellen,DC=musterwerk,DC=local'
'PC-IT-01','PC-IT-02','PC-BUHA-07','PC-KONS-12' | ForEach-Object {
    Get-ADComputer $_ | Move-ADObject -TargetPath $ziel
}
```

```
# Wirksamen Wert auf einem Pilotgerät prüfen (0 = zulassen, 1 = überwachen, 2 = verweigern)
reg query HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0 /v RestrictSendingNTLMTraffic
reg query HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0 /v ClientAllowedNTLMServers
```

Was der Pilot dir verraten soll

Nach zwei bis vier Wochen Überwachung kennst du die NTLM-Ziele der Pilotgeräte. Wichtiger als die Liste selbst ist die Frage nach dem Warum. Die Reason ID in den Ereignissen 4020 und 4021 sagt es dir: 6 für einen Zielnamen, den Kerberos nicht auflösen konnte, 7 für eine IP-Adresse als Ziel, 8 für einen doppelten Zielnamen im Active Directory, 2 für ein lokales Konto, 9 für fehlende Sichtverbindung zum DC. Jede dieser Ursachen hat eine eigene Lösung; die Übersicht steht in NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat. Was sich im Pilot zeigt, zeigt sich später hundertfach. Deshalb lohnt es sich, jede Ursache hier gründlich zu verstehen, statt sie mit einer Ausnahme zuzukleben.

AUS DER PRAXIS · Musterwerk GmbH: der Pilot, der nur aus Laptops bestand

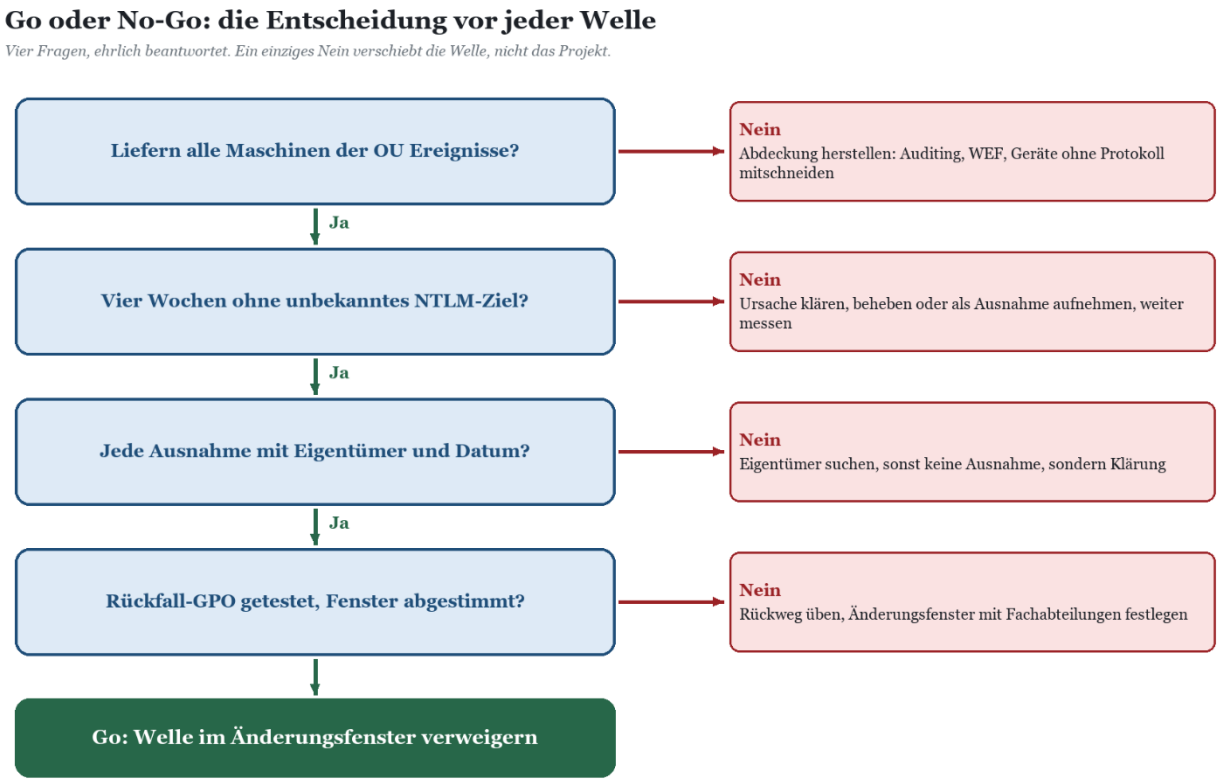
Die Musterwerk GmbH startete mit 25 Geräten aus der IT-Abteilung. Überwachung vier Wochen, Verweigern ohne Zwischenfall, alle zufrieden. In Welle 1 fielen dann am ersten Tag die Netzlaufwerke in der Buchhaltung aus: Ein Anmeldeskript aus dem Jahr 2016 verband Laufwerk K: mit \\10.20.1.15\buha. Die IT-Laptops hatten ein anderes Skript.

Die Lehre: Ein Pilot ohne Fachabteilung testet vor allem, ob die IT-Abteilung ihre eigenen Geräte im Griff hat. Seitdem sitzt in jedem Pilot mindestens ein Gerät pro Anmeldeskript und pro Fachanwendung.

Erfolgskriterien und Rückfallweg festlegen, bevor du schaltest

„Wir schauen mal, ob es klappt“ ist kein Erfolgskriterium, sondern eine Prognose für die Nachbesprechung. Lege vor jeder Welle schriftlich fest, wann du verweigerst, wann du die Welle als erfolgreich abschließt und wann du zurückrollst. Der Charme daran: Du entscheidest im ruhigen Moment, nicht um 7:40 Uhr mit drei Anrufen in der Warteschleife.

Go-Kriterien vor dem Verweigern



Skizze: Entscheidungsweg vor jeder Welle

Kriterium	Messung mit Bordmitteln	Schwelle (Vorschlag)
Abdeckung	Pro Computer der OU: liegt mindestens ein Ereignis im Kanal NTLM/Operational vor, oder ist das Gerät nachweislich NTLM-frei?	100 Prozent der aktiven Computerkonten bewertet
Unbekannte Ziele	Ereignisse 8001 beziehungsweise 4020/4021 der OU, gruppiert nach Zielname	vier Wochen kein neues Ziel ohne Klärung
Ausnahmen	Remoteserverausnahmen gegen die Liste der offenen NTLM-Ziele abgleichen	jeder Eintrag mit Eigentümer, Grund, Ablaufdatum
Zeitraum	Kalender der Fachabteilungen	Monatswechsel und, wo relevant, Quartalsende enthalten
NTLMv1	Ereignisse 4024/4025 und Warnungen 4021/4023	kein offener NTLMv1-Fall in der OU
Rückweg	Rückfall-GPO auf einem Testgerät angewendet	in unter 15 Minuten wirksam

Abbruchkriterien während der Welle

- Ein geschäftskritischer Prozess steht und lässt sich nicht innerhalb von 30 Minuten über eine Ausnahme wiederherstellen.
- Mehr Blockierungen als vorher festgelegt, zum Beispiel mehr als fünf unterschiedliche, bisher unbekannte Ziele am ersten Tag. Dann war die Messung lückenhaft, und das ist eine Aussage über die Messung, nicht über die Anwenderinnen und Anwender.
- Patientenversorgung, Produktion oder Zahlungsverkehr betroffen. In Kliniken gilt das ohne Diskussion; die Besonderheiten dort beschreibt NTLM in der Klinik: Medizintechnik, Labor und Fachanwendungen.

Der Rückfallweg: vorbereitet, getestet, langweilig

Der Rückweg muss so langweilig sein, dass ihn auch die Rufbereitschaft um 6 Uhr morgens ohne Nachdenken gehen kann. Ein Detail entscheidet dabei über Erfolg oder Frust: Sicherheitsoptionen aus Gruppenrichtlinien bleiben in der Registrierung stehen, wenn du die GPO einfach entfernst oder auf „Nicht definiert“ setzt. Das Gerät verweigert dann munter weiter, obwohl die GPO-Verwaltung unschuldig aussieht. Der saubere Rückweg setzt deshalb den Wert ausdrücklich zurück.

Rückweg	So geht's	Wann
Einzelnes Ziel freigeben	Servernamen in die Remoteserverausnahmen der Wellen-GPO eintragen, gpupdate auf den betroffenen Geräten	ein Ziel fällt aus, der Rest läuft
Welle zurückrollen	Vorbereitete Rückfall-GPO mit „Alle überwachen“ an die OU verknüpfen und auf Rang 1 setzen, dann Invoke-GPUpdate oder gpupdate /force	mehrere Ziele oder ein kritischer Prozess betroffen
Einzelgerät herausnehmen	Computerkonto in eine Warte-OU verschieben, in der die Rückfall-GPO gilt	ein Sonderling, etwa ein Messplatz mit Altsoftware

```
# Rückfall-GPO vorbereiten (einmalig, noch NICHT verknüpfen)
New-GPO -Name 'NTLM-Rückfall-Überwachen' -Comment 'Setzt Restrict NTLM ausgehend auf Alle
überwachen'
# Wert in der GPMC setzen: Sicherheitsoptionen > NTLM einschränken: Ausgehender
# NTLM-Datenverkehr zu Remoteservern = Alle überwachen

# Im Ernstfall: an die Wellen-OU verknüpfen, auf Rang 1, Clients aktualisieren
$ou = 'OU=Clients,OU=Verwaltung,DC=musterwerk,DC=local'
New-GPLink -Name 'NTLM-Rückfall-Überwachen' -Target $ou -Order 1
Get-ADComputer -SearchBase $ou -Filter * | ForEach-Object {
    Invoke-GPUpdate -Computer $_.Name -Force -RandomDelayInMinutes 0 -ErrorAction
SilentlyContinue
}
```

Ein Neustart ist für die Restrict-NTLM-Optionen nicht nötig, sie greifen nach der Gruppenrichtlinien-Aktualisierung. Invoke-GPUpdate setzt voraus, dass die Clients Remote-Aufgaben zulassen; teste das im Pilot, nicht im Ernstfall. Und schreib den Rückweg auf eine Seite, mit Namen der GPO, Ziel-OU und Telefonnummer der zuständigen Person.

WARNUNG · „Nicht definiert“ ist kein Rückweg

Wer im Ernstfall die Wellen-GPO löscht oder die Option auf „Nicht definiert“ zurücksetzt, ändert nichts an den Geräten: Der zuletzt geschriebene Wert bleibt in der Registrierung stehen. Der Rückweg setzt den Wert ausdrücklich auf „Alle überwachen“ oder „Alle zulassen“. Erst wenn das überall angekommen ist, darfst du aufräumen.

BEGLEITUNG · Abschaltung mit Begleitung

Den Wellenplan, die Erfolgskriterien und den Rückfallweg kannst du selbst bauen, dieser Beitrag liefert das Gerüst. Wenn du für die kritischen Wellen lieber jemanden an der Seite hast, der das schon einige Male gemacht hat, begleitet dich die Beratung zur NTLM-Ablösung: von der Pilot-OU über die Go/No-Go-Entscheidung bis zur Hypercare nach dem Verweigern, mit klaren Befunden statt Bauchgefühl.

Kommunikation und Änderungsfenster

Technisch ist eine Welle ein einziger Registrierungswert. Organisatorisch ist sie ein Eingriff in die Arbeit von Menschen, die NTLM nicht kennen und nicht kennen müssen. Sie kennen ihr Laufwerk K:, ihren Scanner und ihre Fachanwendung. Wenn eines davon ausfällt, ist das für sie kein Authentifizierungsproblem, sondern „die IT hat wieder was kaputt gemacht“. Gute Kommunikation macht aus diesem Satz ein „ah, das war angekündigt, ich rufe die Nummer an“.

Was die Fachabteilungen wissen müssen

Zeitpunkt	An wen	Inhalt
Projektstart	Abteilungsleitungen, Betriebsrat, Datenschutz	Warum NTLM abgelöst wird, dass Anmeldeereignisse ausgewertet werden, wofür und wie lange
T minus 14 Tage	Alle Betroffenen der Welle	Datum, Zeitfenster, was sich ändern kann, wer anzurufen ist
T minus 3 Tage	Schlüsselpersonen der Fachbereiche	Go/No-Go-Ergebnis, Testauftrag am Morgen danach
Tag T	Alle Betroffenen	Kurze Info: Änderung aktiv, Hotline verstärkt
T plus 14 Tage	Abteilungsleitungen, IT-Leitung	Ergebnis, offene Ausnahmen, nächste Welle

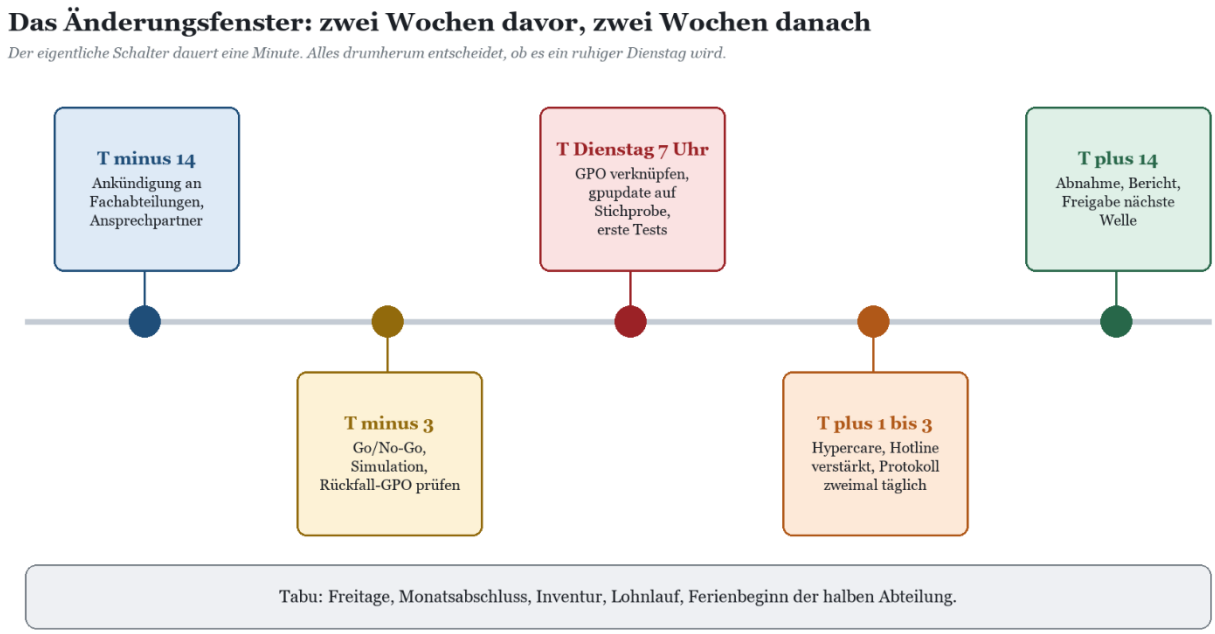
Der erste Punkt wird gern übersehen. NTLM-Ereignisse enthalten Kontonamen und Gerätenamen, also personenbezogene Daten, und eine zentrale Sammlung über Wochen ist für viele Betriebsräte kein Detail. Was du dort klären solltest, steht in NTLM-Audit, Datenschutz und Betriebsrat: was du beachten musst.

TIPP · Eine Mail, die gelesen wird

Betreff: „Dienstag, 7 Uhr: Umstellung der Anmeldung an Netzlaufwerken (Verwaltung)“. Kein „NTLM“, kein „Authentifizierungsprotokoll“, kein „Härtung“. Im Text drei Sätze: was passiert, was du bemerken könntest (ein Laufwerk oder ein Drucker fragt nach Kennwort oder ist nicht erreichbar), wen du anrufst. Dazu die Bitte, am Dienstag die eigenen wichtigsten Abläufe einmal anzustoßen.

Wer so ankündigt, bekommt Störungen in der ersten Stunde gemeldet statt am Monatsende.

Das Änderungsfenster wählen



Skizze: Änderungsfenster einer Welle, Zeitpunkte als Beispiel

Ein gutes Fenster liegt früh in der Woche und früh am Tag: Dienstag oder Mittwoch, kurz vor Arbeitsbeginn, wenn das Team vollständig da ist und Hersteller erreichbar sind. Montag ist ungünstig, weil am Montag ohnehin alles kaputt ist und niemand die Ursache sauber zuordnen kann. Freitag ist aus Gründen tabu, die jeder kennt, der einmal ein Wochenende im Serverraum verbracht hat. Prüfe außerdem den Kalender der Fachbereiche: Lohnlauf, Monatsabschluss, Inventur und Jahresabschluss sind schlechte Begleiter, weil dort Prozesse laufen, die man sonst nie sieht.

AUS DER PRAXIS · Sparfuchs & Partner: die Steuerkanzlei und der 10. des Monats

Bei der Sparfuchs & Partner Steuerberatungs GmbH lief die Überwachung der Welle 1 vier Wochen ohne Auffälligkeit. Geplantes Verweigern: der 10. des Folgemonats. Im Go/No-Go fiel auf, dass der Messzeitraum genau zwischen zwei Umsatzsteuer-Voranmeldungsterminen lag. Die Welle wurde um eine Woche verschoben, der Messzeitraum verlängert, und siehe da: Eine Exportfunktion der Kanzleisoftware schrieb zum Stichtag per IP-Adresse auf einen Dateiserver.

Die Lösung war eine Zeile im Konfigurationsdialog, DNS-Name statt IP. Wie du solche Fälle systematisch findest, beschreibt NTLM wegen IP-Adresse: Laufwerke und Skripte auf DNS-Namen umstellen.

Vor jeder Welle wissen, was ausfallen würde

Mit Bordmitteln kommst du erstaunlich weit. Für eine einzelne OU sammelst du die Ereignisse der letzten Wochen ein und gruppierst sie nach Ziel. Das Skript unten ist bewusst einfach gehalten und fragt jedes Gerät direkt ab; wenn du Windows Event Forwarding nutzt, fragst du stattdessen den Collector. Wie du das aufbaust, steht in NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding.

```
$ou   = 'OU=Clients,OU=Verwaltung,DC=musterwerk,DC=local'
$seit = (Get-Date).AddDays(-28)
$pcs  = Get-ADComputer -SearchBase $ou -Filter 'Enabled -eq $true' | Select-Object -Expand Name
$ergebnis = foreach ($pc in $pcs) {
    try {
        Get-WinEvent -ComputerName $pc -ErrorAction Stop -FilterHashtable @{
```

```
            LogName = 'Microsoft-Windows-NTLM/Operational'; Id = 8001,4020,4021; StartTime =
$seit } |
        Select-Object @{n='Computer';e={$pc}}, Id, TimeCreated, Message
    } catch { [pscustomobject]@{ Computer = $pc; Id = 'keine Daten'; TimeCreated = $null;
Message = $_.Exception.Message } }
}
$ergebnis | Export-Csv C:\Temp\welle1-ntlm.csv -NoTypeInformation -Encoding UTF8
```

Damit hast du eine CSV-Datei, eine Tasse Kaffee und ein Problem. Die Zielnamen und die Reason ID stecken im Meldungstext und wollen herausgeschnitten werden, ältere Systeme liefern nur 8001 ohne Reason ID, ein Teil der Geräte antwortet nicht, weil er ausgeschaltet, im Homeoffice oder durch die Firewall abgeschirmt ist, und die Zeile „keine Daten“ kann bedeuten, dass das Gerät NTLM-frei ist oder dass du schlicht nichts weißt. Drucker, NAS-Systeme und Scanner tauchen gar nicht auf, weil sie kein Ereignisprotokoll haben; für sie hilft nur der Blick auf den Server oder ein Mitschnitt, siehe NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll. Bei einer OU mit 40 Geräten ist das ein Nachmittag. Bei fünf Wellen mit zusammen 1.200 Maschinen, mehreren Standorten und einer Ursachenanalyse pro Ziel ist es ein Nebenjob.

Genau hier setzt der NTLM Diagnostiker an. Er sammelt die Ereignisse, ordnet sie den Maschinen und Konten zu, erklärt die Ursache und beantwortet vor jeder Welle die eine Frage, die zählt: Was würde ausfallen, wenn du jetzt verweigerst?

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Abschalt-Simulation vor jeder Welle

Der NTLM Diagnostiker arbeitet ausschließlich lesend. Er setzt keine Gruppenrichtlinie, verschiebt keine OU und schaltet nichts scharf. Er zeigt dir, was passieren würde, bevor du es tust.

Die Abschalt-Simulation spielt ein Verweigern gegen den tatsächlich beobachteten Verkehr durch und listet die Verbindungen, die betroffen wären, mit Quelle, Ziel, Konto und Ursache. Das ist dein Go/No-Go auf einer Seite.

Die Readiness-Ampel fasst den Stand zusammen, Abdeckungsmonitor und OS-Landkarte zeigen, welche Maschinen Ereignisse liefern, welche schweigen und wo das erweiterte Auditing überhaupt verfügbar ist. Damit wird aus „keine Daten“ eine klare Lücke, die du schließen kannst.

Ereignisse kommen direkt vom DC, über einen vorhandenen Windows Event Collector oder per Direktabfrage. Die Ursachen-Engine mit SPN- und DNS-Prüfung erklärt, warum eine Anmeldung bei NTLM gelandet ist; Kommunikationsmatrix und Konten-Sicht zeigen, wer mit wem spricht. Dazu kommen die NTLMv1-Hitliste, Sicherheitsflaggen und der Wireshark-Import für Geräte ohne Ereignisprotokoll.

Für die Kommunikation: Word-Bericht an IT-Leitung und Abteilungsleitungen, Excel/CSV-Export als Arbeitsliste für die Fachbereiche.

Ein Phasenplan sowie ein Ausnahmelisten- und Skript-Generator sind geplant, aber noch nicht vorhanden. Heute baust du Wellen und Ausnahmelisten selbst, auf Basis der Befunde.

Zum Einstieg liefert die kostenlose Edition Express einen Fünf-Minuten-Befund; den vollen Umfang kannst du sieben Tage testen. Lizenziert wird pro aktivem Computerkonto.

AUS DER PRAXIS · Trendforge Digital: Welle 3, die fast keine war

Die Trendforge Digital GmbH wollte auf den Mitgliedsservern eingehend „Alle Domänenkonten verweigern“. Die Bordmittel-Auswertung der Server sah sauber aus. Die Abschalt-Simulation zeigte trotzdem zwei betroffene Verbindungen: ein Build-Dienst unter einem lokalen Konto, der nachts einen Dateiserver ansprach, und ein Netzwerkspeicher, der Sicherungen per NTLM auf einen Anwendungsserver schob. Beide Quellen hatten in der Client-Auswertung gefehlt, weil sie keine Clients im Sinne der OU waren.

Beide Fälle wurden vor der Welle gelöst, der Dienst mit einem Domänenkonto, der Speicher mit aktualisierter Firmware. Hintergrund zu lokalen Konten: Lokale Konten und NTLM: Dienste, Aufgaben und Altlasten finden.

Wenn eine Ausnahme bleiben muss

Nicht jede Ursache lässt sich vor der Welle beheben. Manche Fachanwendung bekommt Kerberos erst mit dem nächsten Release, manches Gerät nie. Dann ist die Ausnahme kein Versagen, sondern ein dokumentiertes Restrisiko: Eintrag in der Remoteserverausnahme, Eigentümer, Ablaufdatum, Ticket beim Hersteller. Wie du die Fragen an den Hersteller stellst, sodass eine brauchbare Antwort zurückkommt, zeigt Wenn die Anwendung NTLM fest eingebaut hat: Hersteller richtig fragen; wie du serverseitige Ausnahmen pflegst, ohne dass sie zum Scheunentor werden, Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren. Und weil jede verweigerte NTLM-Anmeldung danach per Kerberos funktionieren muss, lohnt sich ein Blick in den Kompetenzbereich Microsoft Kerberos.

FAQ: NTLM schrittweise deaktivieren

Kann ich NTLM nicht einfach in der Default Domain Policy deaktivieren?

Technisch ja, praktisch ist das die Variante mit dem Montag. Die Default Domain Policy wirkt auf alle Computer gleichzeitig, und du hast keinen Pilot, keinen gestaffelten Rückweg und keine Möglichkeit, eine Abteilung früher oder später umzustellen. Eigene GPOs je Welle sind der saubere Weg.

Wie lange sollte ich vor dem Verweigern überwachen?

Mindestens vier Wochen, und der Zeitraum sollte einen Monatswechsel enthalten. In Bereichen mit Quartals- oder Jahresprozessen, etwa Buchhaltung oder Controlling, entsprechend länger oder mit gezielten Tests der Sonderläufe.

Muss ich nach dem Verweigern neu starten?

Nein. Die Restrict-NTLM-Optionen greifen nach der Gruppenrichtlinien-Aktualisierung. Für den Test im Änderungsfenster beschleunigst du das mit gpupdate /force auf einer Stichprobe.

In welcher Reihenfolge schalte ich Clients, Server und Domänencontroller?

Erst ausgehend auf Clients, OU für OU, weil es dort Remoteserverausnahmen gibt. Dann eingehend auf Mitgliedsservern. Zum Schluss die Richtlinie „NTLM-Authentifizierung in dieser Domäne“ auf den Domänencontrollern. Die Überwachung läuft von Anfang an überall.

Was hat die NTLMv1-Blockade vom Oktober 2026 mit meinen Wellen zu tun?

Sie ist die erste Welle, die du nicht selbst geplant hast. Seit dem Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 NTLMv1 für Single Sign-on standardmäßig. Was betroffen ist, beschreibt NTLMv1 blockiert: was seit Oktober 2026 nicht mehr geht; die Steuerung über BlockNtlmv1SSO erklärt BlockNtlmv1SSO erklärt: Überwachung, Erzwingung, Ausnahme.

Was mache ich mit Geräten, die nie Ereignisse liefern?

Unterscheide zwischen Windows-Geräten, deren Auditing nicht greift, und Geräten ohne Ereignisprotokoll wie Druckern oder NAS-Systemen. Bei Ersteren hilft eine Abdeckungsprüfung, bei Letzteren der Blick auf die Ereignisse der Server, die sie ansprechen, oder ein Netzwerkmitschnitt.

Verändert der NTLM Diagnostiker meine Umgebung?

Nein. Er arbeitet ausschließlich lesend und zeigt mit der Abschalt-Simulation, welche Verbindungen ein Verweigern treffen würde. Das Umschalten der Gruppenrichtlinien bleibt bei dir.

Wie plane ich die Wellen in ein Gesamtprojekt ein?

Die Wellen sind der operative Kern, drumherum stehen Bestandsaufnahme, Ursachenbehebung, Kommunikation und Abnahme. Zeitplan, Rollen und Aufwand beschreibt NTLM-Ablösung als Projekt: Zeitplan, Rollen, Aufwand; wie du überhaupt erst herausfindest, wo NTLM genutzt wird, zeigt NTLM-Nutzung ermitteln: der komplette Leitfaden.

Fazit: Langweilig ist das Ziel

NTLM schrittweise abzuschalten ist kein technisches Kunststück. Der Schalter ist seit Windows 7 derselbe. Was den Unterschied macht, ist das Handwerk drumherum: ein Wellenplan je OU, ein Pilot mit echten Fachabteilungen, Erfolgskriterien, die vor dem Schalten feststehen, ein Rückweg, der geübt ist, eine Ankündigung, die gelesen wird, und ein Änderungsfenster, das nicht auf den Lohnlauf fällt. Wenn du das sauber machst, wird jede Welle ein ereignisloser Dienstag. Das klingt unspektakulär, und genau das ist der Plan.

Den Takt gibt Microsoft vor, das Tempo bestimmst du. Je früher die erste Welle läuft, desto weniger überrascht dich die nächste Windows-Server-Version. Wenn du die Abschaltung nicht allein stemmen willst, unterstützt dich die Beratung zur NTLM-Ablösung; damit dein Team die Befunde selbst sicher liest, gibt es die Schulung zum NTLM Diagnostiker.

WEITERLESEN · Weiter in dieser Serie

› Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern
› Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren
› Erweitertes NTLM-Auditing einschalten: Schritt für Schritt
› NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat
› NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding
› NTLM-Ablösung als Projekt: Zeitplan, Rollen, Aufwand
› NTLM auf dem Domain Controller: Ereignisse 4030 bis 4033 und 8004
› NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet