

Beratung zur NTLM-Ablösung: raus aus NTLM, ohne dass montags das Telefon klingelt

Die meisten NTLM-Projekte scheitern nicht an der Technik. Sie scheitern daran, dass niemand weiß, wo man anfangen soll, und dass der Mut fehlt, irgendwo den Schalter umzulegen. Verständlich: Wenn nach der Abschaltung der Laborrechner nicht mehr druckt oder die Buchhaltung nicht mehr auf die Fibu kommt, ist die Geschichte schneller beim Geschäftsführer als beim Admin.

Ich begleite dich von der ersten Bestandsaufnahme bis zum Tag, an dem NTLM in deiner Domäne nur noch eine Fußnote ist. Mit einem Werkzeug, das die Fleißarbeit erledigt, dem **NTLM Diagnostiker**, und mit gut 30 Jahren Erfahrung in Microsoft-Umgebungen für den Teil, den kein Werkzeug kann: die richtige Reihenfolge, die Gespräche mit Herstellern und die Entscheidung, wann man abschaltet.

Produkt

Der NTLM Diagnostiker:
Bestandsaufnahme, Ursachen,
Simulation.

[Zum NTLM Diagnostiker](#)

Schulung

Kerberos statt NTLM: Workshop
für Admins und Systemhäuser.

[Zum Schulungsangebot](#)

Wissen

SPNs, Delegierung, Fehlersuche:
das Kerberos-Fundament.

[Zum Kompetenzbereich Kerberos](#)

Kennst du eine dieser Lagen?

„Seit Mitte Oktober geht der Scanner nicht mehr“

Seit dem Windows-Update vom 13. Oktober 2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 die einfache Anmeldung mit NTLMv1 standardmäßig. Was vorher still funktioniert hat, meldet sich jetzt mit Fehlern. Hier geht es erst um schnelle, saubere Hilfe und dann darum, das Thema richtig anzugehen, statt den Registrierungswert einfach wieder zurückzudrehen.

„Wir wissen, dass wir müssen, aber nicht, wo wir anfangen sollen“

Der Klassiker. Das Thema steht seit Monaten auf der Liste, aber zwischen Tagesgeschäft und Projekten findet niemand die Zeit, sich durch Tausende Ereignisse zu wühlen. Hier bringt eine strukturierte Bestandsaufnahme mit klarer Priorisierung den Stein ins Rollen.

„Der CISO, die Versicherung oder der Prüfer will einen Nachweis“

NTLM ist ein beliebter Weg für Relay- und Pass-the-Hash-Angriffe. Wer gegenüber einer Cyberversicherung, einem Auditor oder im Rahmen von NIS2 erklären muss, wie es um die Altlasten steht, braucht belastbare Zahlen und einen Plan mit Terminen.

„Wir betreuen 40 Kunden, und alle haben dasselbe Problem“

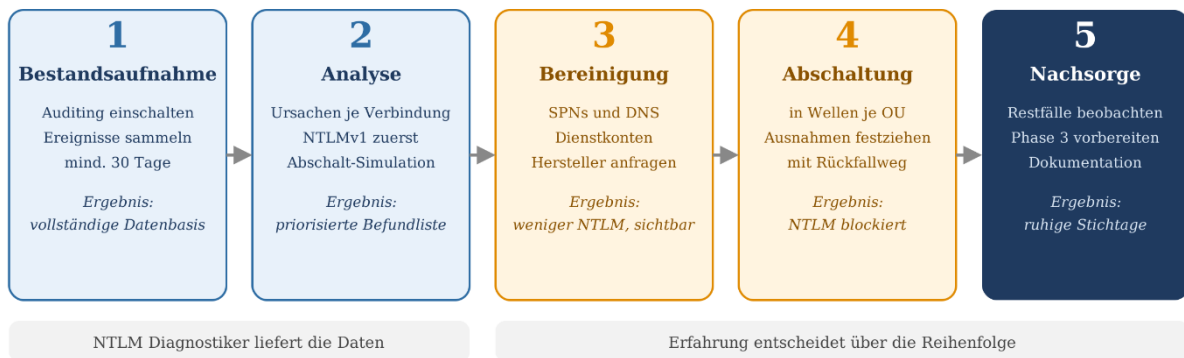
Für Systemhäuser ist die NTLM-Ablösung kein Einzelprojekt, sondern eine Serie. Hier geht es um ein wiederholbares Vorgehen, das deine Techniker selbst fahren können, und um Unterstützung bei den kniffligen Fällen.

So gehen wir vor

Jede Ablösung folgt im Kern denselben fünf Schritten. Was sich unterscheidet, sind Umfang, Tempo und die Zahl der Überraschungen auf dem Weg.

In fünf Schritten raus aus NTLM

Jeder Schritt hat ein Ergebnis, mit dem du weiterarbeiten kannst



Skizze 1: Die fünf Schritte der NTLM-Ablösung

1 Bestandsaufnahme

Wir schalten das NTLM-Auditing ein, richten bei Bedarf einen Windows Event Collector ein und sammeln mindestens 30 Tage lang. Dafür gibt es das kostenlose [Audit-GPO-Skript](#), und der [NTLM Diagnostiker](#) prüft, ob die Daten wirklich von allen Maschinen kommen. Wo Geräte kein Windows-Protokoll schreiben, ergänzen wir gezielte Netzwerkmitschnitte.

2 Analyse

Der Diagnostiker ordnet jeder Verbindung eine Ursache zu. Ich bewerte die Befunde, sortiere nach Risiko und Aufwand und mache daraus eine Liste, die man abarbeiten kann. NTLMv1 kommt immer zuerst. Mit der Abschalt-Simulation sehen wir außerdem früh, welche Bereiche der Domäne schon heute ohne NTLM auskämen.

3 Bereinigung

Fehlende oder doppelte SPNs, Zugriffe per IP-Adresse, Dienste unter lokalen Konten, Anwendungen mit fest eingebautem NTLM: Für jede Ursachengruppe gibt es einen Lösungsweg. Ich liefere Skripte und Anleitungen und formuliere die Anfragen an Hersteller so, dass sie eine brauchbare Antwort bekommen.

4 Abschaltung in Wellen

Abgeschaltet wird nicht auf einen Schlag, sondern OU für OU: erst überwachen, dann Ausnahmen festziehen, dann blockieren. Jede Welle hat ein Erfolgskriterium und einen Rückfallweg, den wir vorher getestet haben.

5 Nachsorge

Nach der Abschaltung beobachten wir die Restfälle, dokumentieren die bewusst verbliebenen Ausnahmen und bereiten dich auf Phase 3 vor, in der Microsoft NTLM mit der nächsten Windows-Server-Version standardmäßig abschaltet.

Wer macht was?

Wer macht was?

Du behältst die Hand am Schalter, ich bringe Plan und Erfahrung



Skizze 2: Aufgabenverteilung zwischen boddenberg.de und deiner IT

Ich ändere nichts in deiner Umgebung, ohne dass du es freigegeben hast. Der NTLM Diagnostiker arbeitet ohnehin nur lesend. Ob deine IT die Änderungen selbst umsetzt oder wir sie gemeinsam in einer Sitzung durchziehen, entscheidest du.

Beratungspakete

Paket	Was drin ist	Ergebnis	Preis (netto)
NTLMv1-Soforthilfe	Remote-Sitzung, Analyse der blockierten Anmeldungen, saubere Übergangslösung statt Rolle rückwärts	Betrieb läuft wieder, Plan für die dauerhafte Lösung	Preis folgt
Bestandsaufnahme mit Servicepaket	Lizenz des NTLM Diagnostikers, Initial-Beratung, Einrichtung der Erfassung, Premium-Report, Ergebnis-Workshop	Vollständiges Lagebild, priorisierte Befundliste, Empfehlung	Lizenz plus Preis folgt
Ablösekonzept	Auf Basis der Bestandsaufnahme: Phasenplan je OU, Ausnahmeliste, Herstellerliste, Rückfallwege, Kommunikationsplan	Konzept, mit dem die IT selbst abschalten kann	Festpreis folgt
Begleitung der Abschaltung	Gemeinsame Umsetzung der Wellen, Fehlersuche, Herstellerkontakte, Nachsorge	NTLM blockiert, Restfälle dokumentiert	nach Aufwand, Tagessatz Preis folgt

Ganz ohne Gespräch anfangen?

Geht. Lad dir den kostenlosen Express des [NTLM Diagnostikers](#) herunter und lass ihn fünf Minuten gegen deine Domain Controller laufen. Der Kurzbefund zeigt dir, wie viel NTLM in deiner Domäne steckt und wie es um NTLMv1 steht. Schick ihn mir, und wir reden über konkrete Zahlen statt über Vermutungen.

Ein Beispiel aus der Praxis

Musterwerk GmbH: 1.800 Rechner, zwei Domänen, ein Scanner zu viel

Die Musterwerk GmbH ist unsere fiktive, aber typische Beispielfirma. Der erste Express-Befund zeigte rund 40.000 NTLM-Anmeldungen am Tag, davon gut 300 mit NTLMv1. Nach 30 Tagen Erfassung lag das Bild klar auf dem Tisch: Drei Viertel der Verbindungen gingen auf Laufwerkszuordnungen und Skripte mit IP-Adressen zurück, ein großer Teil des Rests auf zwei fehlende SPNs und ein falsch konfiguriertes Dienstkonto.

Die NTLMv1-Quellen waren genau zwei: ein alter Dokumentenscanner in der Poststelle und eine Fachanwendung, die per Herstellerupdate umgestellt werden konnte. Nach drei Abschaltwellen blieben elf bewusst dokumentierte Ausnahmen übrig. Keine davon für NTLMv1.

Warum mit mir?

- **Ich kenne beide Seiten.** Rund 30 Jahre Microsoft-Infrastruktur, viele davon mit Kerberos, Delegierung und genau den Altlasten, die heute NTLM erzwingen.
- **Werkzeug und Erfahrung aus einer Hand.** Den NTLM Diagnostiker habe ich für genau diese Projekte gebaut. Ich weiß also, was die Befunde bedeuten und wo das Werkzeug aufhört.
- **Kein Rundum-Sorglos-Paket, das niemand braucht.** Wenn deine IT nach der Bestandsaufnahme allein weitermachen kann, sage ich dir das.
- **Datenschutz mitgedacht.** NTLM-Protokolle enthalten Benutzernamen. Für Datenschutz sowie Betriebs- oder Personalrat gibt es eine klare Zweckbeschreibung, und alle Daten bleiben bei dir.

Für Systemhäuser

Du hast die NTLM-Ablösung gleich bei mehreren Kunden vor dir? Dann lohnt sich ein gemeinsamer Start: ein Onboarding für deine Techniker mit dem NTLM Diagnostiker, ein Vorgehen, das ihr bei jedem Kunden gleich fahrt, und ich als Rückfallebene für die harten Fälle. Den Diagnostiker bekommst du für die eigene Domäne und zum Kennenlernen kostenlos, in den Kundenlizenzen bist du als betreuender Partner vermerkt.

Die nächsten Schritte

- **Express laufen lassen** und den Kurzbefund ansehen.
- **Kurzes Gespräch:** Wo stehst du, was drängt, welche Systeme machen dir Sorgen?
- **Angebot:** passend zu deiner Lage, mit festen Preisen für die Pakete.

Am schnellsten erreichst du mich über das Feld „Frag Uli“ unten auf dieser Seite. Die Antwort kommt innerhalb von 24 Stunden.

Häufige Fragen

Wie lange dauert eine NTLM-Ablösung?

Die Bestandsaufnahme braucht mindestens 30 Tage Erfassung, die Analyse danach wenige Tage. Wie lange Bereinigung und Abschaltung dauern, hängt vor allem an den Anwendungen und Geräten, für die Hersteller nachliefern müssen. Realistisch sind einige Monate, nicht einige Jahre.

Können wir NTLM nicht einfach abschalten und schauen, was passiert?

Kann man, macht man aber genau einmal. Mit der Abschalt-Simulation siehst du vorher, was betroffen wäre. Das ist billiger als ein Wochenende mit Notfallrücknahme.

Brauchen wir dafür den NTLM Diagnostiker?

Technisch geht es auch mit Bordmitteln und viel Geduld. Der Diagnostiker spart dir die Wochen, die sonst in Ereignisanzeige, Excel und SPN-Abfragen fließen, und er macht die Ergebnisse für alle Beteiligten nachvollziehbar.

Was ist mit NTLMv1, das seit Oktober blockiert wird?

Das gehört an den Anfang. Den Registrierungswert BlockNtlmv1SSO auf Überwachung zurückzusetzen ist eine Notlösung, keine Antwort. Wir suchen die Quellen und stellen sie um, und wo das nicht sofort geht, begrenzen wir die Ausnahme.

Arbeitest du remote oder vor Ort?

Das meiste geht remote. Vor Ort komme ich gern, wenn es um Workshops oder kritische Abschaltwellen geht.

Was, wenn eine Anwendung wirklich nur NTLM kann?

Dann dokumentieren wir sie als bewusste Ausnahme, begrenzen sie auf die nötigen Server und machen mit dem Hersteller einen Plan. Wichtig ist, dass die Ausnahme eine Entscheidung ist und kein Zufall.

Lass uns anfangen

Fang mit dem kostenlosen Express des [NTLM Diagnostikers](#) an, oder schreib mir direkt über „Frag Uli“ unten auf der Seite. Wenn dein Team erst einmal das Handwerkszeug braucht, schau dir das [Schulungsangebot zur NTLM-Ablösung](#) an.