

Schulung NTLM-Ablösung: Kerberos statt NTLM in der Praxis

Kerberos gilt bei vielen Admins als schwarze Magie: Solange es läuft, fragt keiner, und wenn es nicht läuft, fällt Windows still auf NTLM zurück, und niemand merkt etwas. Genau dieser stille Rückfall ist der Grund, warum NTLM in fast jeder Domäne noch quicklebendig ist. Und genau das ändert sich jetzt: NTLMv1 wird seit Oktober 2026 blockiert, mit der nächsten Windows-Server-Version ist NTLM standardmäßig aus.

In dieser Schulung lernst du, NTLM in deiner Umgebung sichtbar zu machen, die Ursachen zu verstehen und Schritt für Schritt abzuschalten. Ohne Folienschlacht, mit echten Ereignissen, echten SPN-Problemen und einem Plan, den du am nächsten Tag anwenden kannst.

Produkt

Der NTLM Diagnostiker, mit dem wir in der Schulung arbeiten.

[Zum NTLM Diagnostiker](#)

Beratung

Lieber begleitet als allein?
Beratung zur NTLM-Ablösung.

[Zur Beratung](#)

Wissen

Kerberos, SPNs und Delegierung zum Nachlesen.

[Zum Kompetenzbereich Kerberos](#)

Für wen ist die Schulung?

- **Administratorinnen und Administratoren** in Active-Directory-Umgebungen, die die NTLM-Ablösung selbst durchziehen wollen.
- **Techniker in Systemhäusern**, die das Thema bei vielen Kunden vor sich haben und ein wiederholbares Vorgehen brauchen.
- **IT-Leitung und Informationssicherheit** im Kurzformat: Was steht an, was kostet es, worauf muss man achten?

Vorausgesetzt werden solide Grundlagen in Active Directory, Gruppenrichtlinien und PowerShell. Kerberos-Vorwissen ist hilfreich, aber nicht nötig, das holen wir im ersten Block nach.

Die Formate

Format	Dauer	Für wen	Schwerpunkt
Workshop „NTLM ablösen in der Praxis“	1 Tag, online	Admins, Systemhaus-Techniker	Vom Auditing bis zur Abschaltung, mit Übungsumgebung
Inhouse-Workshop mit eigenen Daten	1 Tag, online oder vor Ort	IT-Team eines Unternehmens	Wie der Workshop, aber mit den Befunden aus deiner eigenen Domäne
Onboarding NTLM Diagnostiker	½ Tag, online	Systemhäuser, Partner	Einrichtung, Auswertung, Berichte, wiederholbares Vorgehen bei Kunden
Kurzformat für Entscheider	2 Stunden, online	IT-Leitung, CISO	Fahrplan, Risiken, Aufwand, Entscheidungen

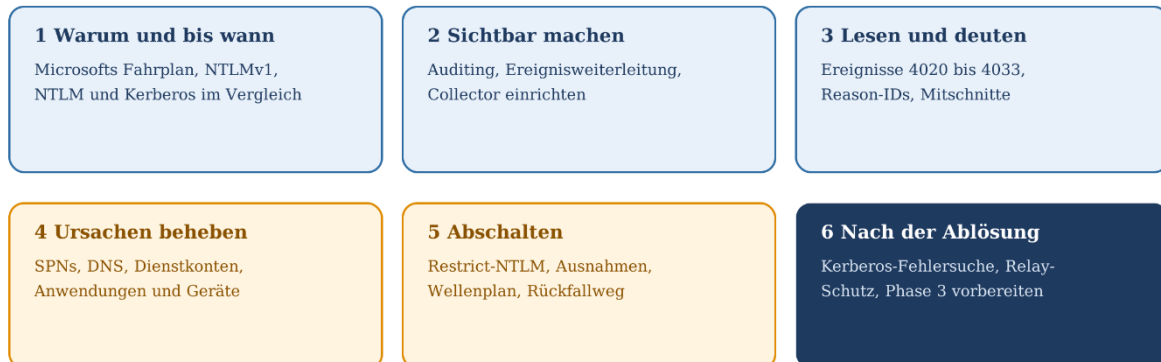
Tipp: der Inhouse-Workshop mit eigenen Daten

Am meisten bringt die Schulung, wenn du vorher den kostenlosen Express des [NTLM Diagnostikers](#) laufen lässt oder schon ein paar Wochen Erfassung hast. Dann arbeiten wir nicht an Beispielen, sondern an deinen echten Befunden, und am Ende des Tages steht ein erster Phasenplan für deine Domäne.

Der Tagesablauf

Ein Tag, sechs Blöcke

Vom „Warum“ bis zum Abschalten ohne Anruf am Montag



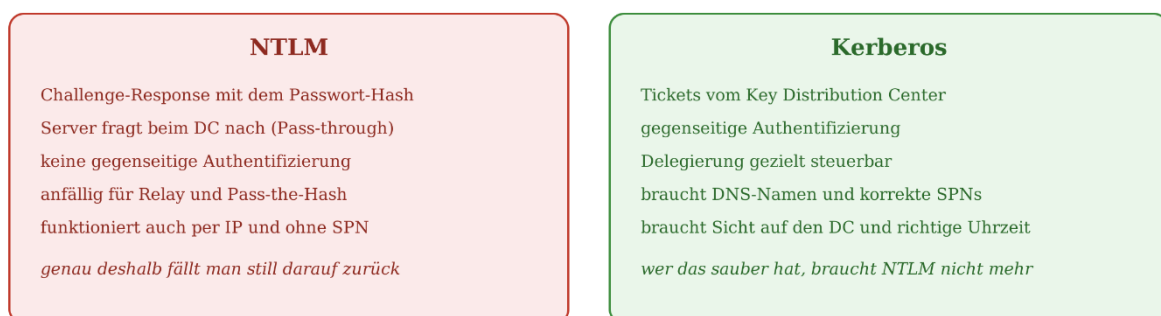
Skizze 1: Die sechs Blöcke des Workshops

Block 1: Warum und bis wann

Microsofts Fahrplan mit den drei Phasen, die NTLMv1-Blockierung seit Oktober 2026 und was das für deine Umgebung heißt. Dazu der Vergleich von NTLM und Kerberos, damit klar ist, warum Windows überhaupt auf NTLM zurückfällt.

NTLM und Kerberos im Vergleich

Warum der Wechsel mehr ist als ein Häkchen



Skizze 2: NTLM und Kerberos im Vergleich

Block 2: Sichtbar machen

Erweitertes NTLM-Auditing auf Clients, Servern und Domain Controllern einschalten, Ereignisweiterleitung zu einem Windows Event Collector einrichten, typische Stolperfallen wie fehlende Leserechte auf das Protokoll. Mit dabei: das kostenlose [Audit-GPO-Skript](#).

Block 3: Lesen und deuten

Die Ereignisse 4020 bis 4025, 4030 bis 4033 und 8001 bis 8004 im Detail, die Reason-IDs und was sie verraten. Dazu Netzwerkmitschnitte mit Wireshark für die Geräte, die kein Windows-Protokoll schreiben, und die Auswertung im NTLM Diagnostiker.

Block 4: Ursachen beheben

Fehlende und doppelte SPNs, Zugriffe per IP-Adresse, Dienste unter lokalen Konten, Dienstkonten mit falscher Konfiguration, Anwendungen mit fest eingebautem NTLM, NAS und Drucker. Für jede Gruppe der Lösungsweg und die passenden Befehle.

Block 5: Abschalten

Die Restrict-NTLM-Richtlinien im Detail, Server-Ausnahmen, Abschaltung in Wellen je OU, Abschalt-Simulation und Rückfallweg. Und die Frage, wie man das Ganze so kommuniziert, dass die Fachabteilungen mitziehen.

Block 6: Nach der Ablösung

Kerberos-Fehlersuche, wenn nach der Abschaltung etwas klemmt, Schutz vor NTLM-Relay für die verbliebenen Ausnahmen und ein Ausblick auf IAKerb und das lokale KDC aus Microsofts Phase 2.

Was du mitnimmst

- Ein klares Bild, wie NTLM in einer Domäne entsteht und wie man es wieder loswird.
- Die Fähigkeit, NTLM-Ereignisse selbst zu lesen und Ursachen zuzuordnen.
- Skripte und Checklisten für Auditing, SPN-Prüfung und Abschaltwellen.
- Beim Inhouse-Workshop: einen ersten Phasenplan für deine eigene Domäne.
- Die Schulungsunterlagen als PDF.

Rahmen und Konditionen

Auf einen Blick	
Durchführung	online mit Übungsumgebung, Inhouse auch vor Ort
Sprache	Deutsch
Teilnehmerzahl	folgt
Preise	Workshop Preis folgt , Inhouse-Workshop Preis folgt , Onboarding Preis folgt , Kurzformat Preis folgt , jeweils netto
Termine	nach Vereinbarung
Trainer	Ulrich B. Boddenberg, IT-Consultant und Fachautor, rund 30 Jahre Microsoft-Infrastruktur

Häufige Fragen

Brauche ich Kerberos-Vorwissen?

Nein. Der erste Block holt alle auf denselben Stand. Grundlagen in Active Directory und Gruppenrichtlinien solltest du aber mitbringen.

Muss ich den NTLM Diagnostiker kaufen, um teilzunehmen?

Nein. In der Übungsumgebung arbeiten wir mit dem Diagnostiker, ein eigener Kauf ist dafür nicht nötig. Für den Inhouse-Workshop mit eigenen Daten reicht der kostenlose Express oder der Testzeitraum.

Geht es nur um das Werkzeug?

Nein. Der größte Teil des Tages dreht sich um Kerberos, Ereignisse, Ursachen und Abschaltung, also um Wissen, das du auch ohne Werkzeug brauchst. Der Diagnostiker spart dir dabei nur die Fleißarbeit.

Können wir die Schulung mit einer Beratung kombinieren?

Ja, gerade der Inhouse-Workshop ist ein guter Start in die Ablösung. Mehr dazu auf der Seite [Beratung zur NTLM-Ablösung](#).

Gibt es feste Termine?

Die Termine stimmen wir individuell ab. Schreib mir über „Frag Uli“ unten auf der Seite, wann es bei euch passt.

Termin anfragen

Sag mir, welches Format dich interessiert, wie viele Personen teilnehmen und ob ihr schon NTLM-Daten gesammelt habt. Am schnellsten geht es über das Feld „Frag Uli“ unten auf dieser Seite.