NTLM-Relay verhindern: MIC, Kanalbindung und erweiterter Schutz



WISSEN
Wie der NTLM Diagnostiker Verbindungen ohne MIC, ohne Kanalbindung oder ohne Session Key sichtbar macht.
› NTLM Diagnostiker

BERATUNG
Signierung, Kanalbindung und erweiterten Schutz einführen, ohne dass Montag früh das Telefon glüht.
› Beratung zur NTLM-Ablösung

SCHULUNG
Sicherheitsfelder im NTLM-Audit lesen und bewerten, damit dein Team die Risiken selbst einschätzt.
› Schulung zum NTLM Diagnostiker

NTLM hat eine Eigenschaft, die man im Bewerbungsgespräch eher verschweigen würde: Es glaubt jedem, der die richtigen Antworten weiterreicht. Ein Angreifer im Netz muss dein Passwort nicht knacken, er muss es nicht einmal sehen. Es reicht, wenn sich ein Rechner bei ihm anmeldet und er diese Anmeldung frisch und warm an einen anderen Server durchreicht. Der Server sieht eine einwandfreie Anmeldung und rollt den roten Teppich aus. Das nennt sich NTLM-Relay, und es gehört seit gut zwanzig Jahren zum Standardrepertoire jedes Penetrationstests. Meistens liegt der Bericht danach in einer Schublade, gleich neben dem vom letzten Jahr.

Die eigentliche Antwort darauf ist bekannt: NTLM ablösen. Microsoft zieht das inzwischen durch. Seit dem Windows-Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 NTLMv1 für Single Sign-on standardmäßig, gesteuert über den Registrierungswert BlockNtlmv1SSO und protokolliert mit den Ereignissen 4024 und 4025. Phase 2 bringt IAKerb und ein lokales KDC, mit der nächsten Windows-Server-Version ist NTLM standardmäßig abgeschaltet. Den vollständigen Zeitplan findest du in NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet.

Nur: Bis zur letzten NTLM-Anmeldung vergehen in einem echten Mittelstandsnetz Monate, in Kliniken mit zugelassener Medizintechnik eher Jahre. Für diese Übergangszeit und für die Ausnahmen, die am Ende übrig bleiben, brauchst du Schutz gegen Relay. Dieser Beitrag erklärt, wie Relay grundsätzlich funktioniert (ohne Bastelanleitung), welche Gegenmittel Windows mitbringt, nämlich SMB-Signierung, LDAP-Signierung, Kanalbindung, Extended Protection for

Authentication und MIC, wie du prüfst, ob sie greifen, und warum all das trotzdem nur die Brücke ist und nicht das Ufer.

FAKTEN · NTLM-Relay auf einen Blick

Relay heißt: Ein Mittelsmann nimmt eine NTLM-Anmeldung entgegen und reicht sie an einen anderen Server weiter. Er kennt weder Passwort noch Hash, er leitet nur die Nachrichten durch.

Gegenmittel binden die Anmeldung an etwas, das der Mittelsmann nicht fälschen kann: an einen Sitzungsschlüssel (Signierung), an die TLS-Verbindung (Kanalbindung) oder an den Zielnamen (Dienstbindung). Der MIC schützt die Aushandlung selbst vor Manipulation.

Windows 11 24H2 verlangt SMB-Signierung standardmäßig für alle Verbindungen, Windows Server 2025 für ausgehende. Neue Active-Directory-Bereitstellungen ab Server 2025 verlangen LDAP-Signierung, die LDAP-Kanalbindung steht dort auf „When supported“.

Extended Protection for Authentication ist laut KB5021989 in allen unterstützten Windows-Versionen standardmäßig verfügbar, muss aber von der jeweiligen Anwendung genutzt werden. Für NTLMv1 gilt sie nicht.

Das erweiterte NTLM-Auditing nach KB5064479 zeigt in jedem Ereignis die Felder MIC Status, Channel Binding und Session Key Status.

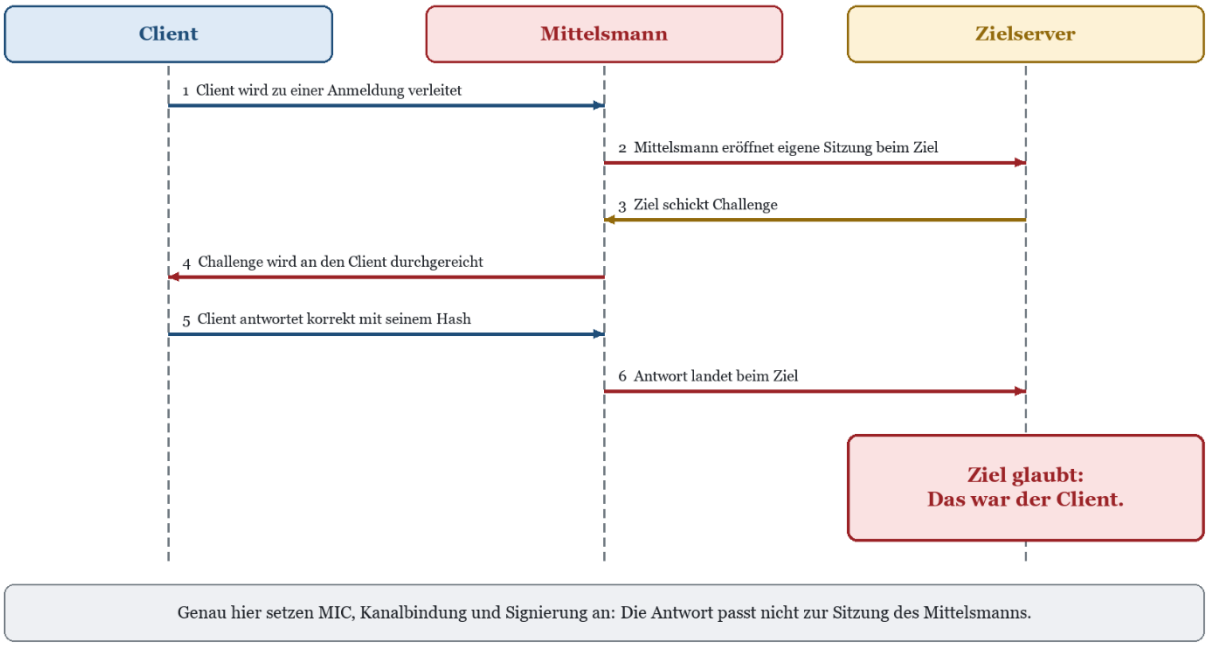
Wie NTLM-Relay funktioniert, ohne dass du es nachbauen musst

NTLM ist ein Challenge-Response-Verfahren mit drei Nachrichten. Der Client kündigt sich an (Negotiate), der Server schickt eine Zufallszahl (Challenge), der Client rechnet daraus mit dem Hash seines Passworts eine Antwort (Authenticate). Der Server prüft die Antwort, bei Domänenkonten mit Hilfe des Domänencontrollers. So weit, so ordentlich.

Das Problem: Nichts in diesem Austausch sagt, mit wem der Client eigentlich reden wollte und über welche Verbindung. Die Antwort beweist nur, dass jemand mit dem richtigen Hash die Challenge beantwortet hat. Wenn ein Mittelsmann die Challenge vom echten Ziel holt, sie dem Client vorlegt und dessen Antwort zurückreicht, ist die Antwort für das Ziel völlig korrekt. Der Mittelsmann spielt Briefträger, der deine unterschriebenen Briefe einfach an eine andere Adresse zustellt.

Wie ein Relay grundsätzlich abläuft

Der Mittelsmann muss dein Passwort nie kennen. Er braucht nur deine Bereitschaft, dich anzumelden.



Skizze: konzeptionelle Darstellung, keine Anleitung

Wie der Client überhaupt zum Mittelsmann kommt

Damit Relay funktioniert, muss sich der Client beim Mittelsmann anmelden. Dafür gibt es erschreckend viele harmlose Gründe: ein Tippfehler im Freigabepfad, eine Namensauflösung per Broadcast, weil DNS nichts gefunden hat, eine Verknüpfung auf einer Freigabe, die ein Symbol von einem fremden Server lädt, oder ein Dienst, der sich auf Zuruf irgendwohin verbindet. Windows meldet sich bei solchen Zielen bereitwillig mit NTLM an, gerade weil für sie kein Kerberos-Ticket zu bekommen ist. Wer sich mit den Reason IDs beschäftigt hat, erkennt das Muster: Zielname nicht auflösbar, IP-Adresse statt Name. Die Ursachen, die NTLM erzeugen, sind oft dieselben, die Relay ermöglichen.

WARNUNG · Auch Computerkonten sind Beute

Besonders unangenehm wird es, wenn nicht ein Benutzerkonto, sondern das Computerkonto eines Servers weitergereicht wird, im schlimmsten Fall das eines Domänencontrollers. Landet so eine Anmeldung bei einem Dienst ohne Schutz, etwa bei der Web-Registrierung einer Zertifizierungsstelle oder bei LDAP ohne Kanalbindung, ist der Weg zur Übernahme der Domäne kurz. Deshalb sind AD CS, LDAP und SMB auf Domänencontrollern die Stellen, an denen Relay-Schutz zuerst sitzen muss.

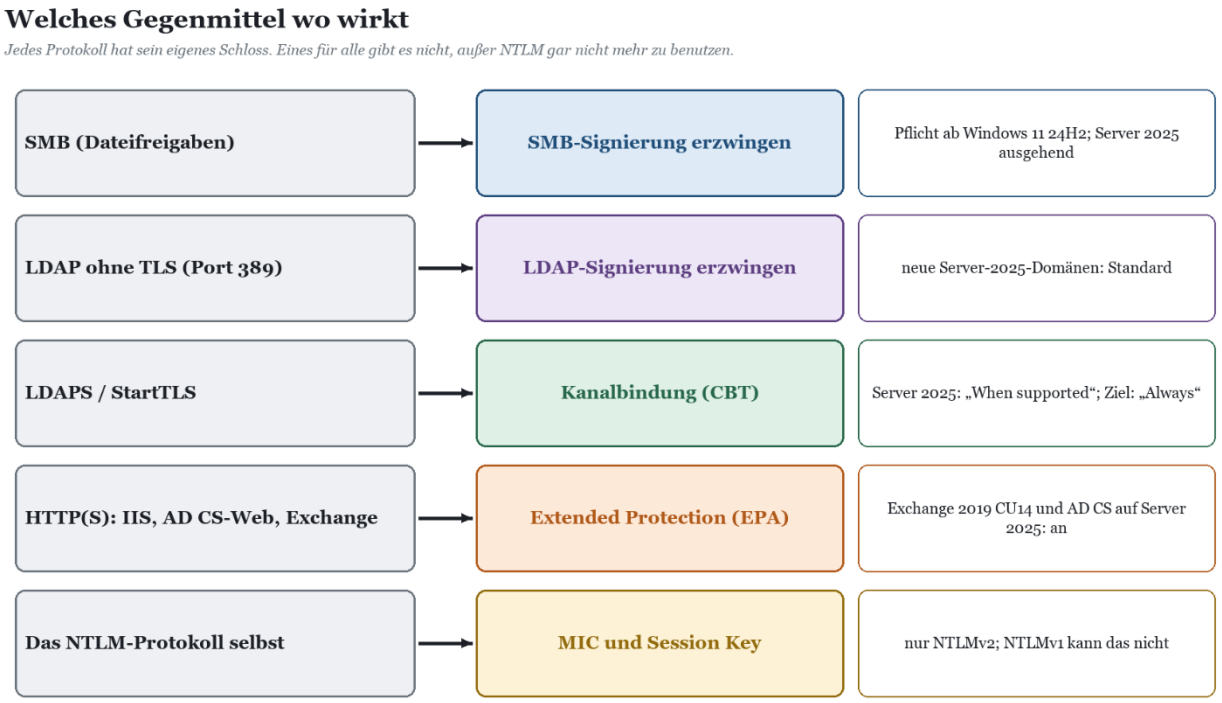
Was Relay nicht ist

Relay ist kein Passwortknacken. Wer ein starkes Passwort hat, ist trotzdem betroffen, denn der Hash wird ja nie geknackt, nur benutzt. Relay ist auch kein reines NTLMv1-Thema: NTLMv2 ist gegen Relay genauso anfällig, solange keines der Gegenmittel greift. Der Unterschied ist, dass NTLMv2 die Gegenmittel überhaupt unterstützt. NTLMv1 kennt weder MIC noch Kanalbindung, und laut KB5021989 gilt Extended Protection für NTLMv1 ausdrücklich nicht. Warum NTLMv1 deshalb zuerst gehen muss, erklärt NTLMv1 blockiert: was seit Oktober 2026 nicht mehr geht.

Die Gegenmittel: Signierung, Kanalbindung, EPA und MIC

Alle Gegenmittel folgen derselben Idee: Die Anmeldung wird an etwas geknüpft, das der Mittelsmann nicht besitzt. Bei der Signierung ist das der Sitzungsschlüssel, der aus dem Passwort-

Hash des Clients entsteht und den nur Client und Server (über den DC) kennen. Bei der Kanalbindung ist es die konkrete TLS-Verbindung. Bei der Dienstbindung ist es der Name des Ziels. Welches Mittel wo greift, hängt vom Protokoll ab.



Skizze: Gegenmittel nach Protokoll, Stand der Standardwerte laut Microsoft

SMB-Signierung

Wenn der Server signierte SMB-Pakete verlangt, muss jede Nachricht mit dem Sitzungsschlüssel unterschrieben sein. Der Mittelsmann hat die Anmeldung zwar durchgereicht, den Schlüssel aber nie gesehen. Er kann sich anmelden, aber keinen einzigen gültigen Befehl schicken. Das ist ungefähr so nützlich wie ein Hausschlüssel für ein Haus ohne Türen.

Microsoft hat hier den Standard gedreht. Früher war Signierung nur für SYSVOL und NETLOGON sowie für Verbindungen zu Domänencontrollern Pflicht. Seit Windows 11 24H2 verlangen Home, Pro, Education und Enterprise die Signierung für alle Verbindungen, Windows Server 2025 für alle ausgehenden. Ältere Server im Bestand haben diese Standards nicht. Die Richtlinien heißen „Microsoft-Netzwerk (Server): Kommunikation digital signieren (immer)" und das Gegenstück für den Client. Den aktuellen Stand prüfst du per PowerShell:

```
# Server-Seite: verlangt dieser Rechner Signierung?
Get-SmbServerConfiguration | Select-Object RequireSecuritySignature, EnableSecuritySignature

# Client-Seite
Get-SmbClientConfiguration | Select-Object RequireSecuritySignature, EnableSecuritySignature

# Bestehende Verbindungen: wird tatsächlich signiert?
Get-SmbConnection | Select-Object ServerName, ShareName, Dialect, Signed
```

WICHTIG · Wo SMB-Signierung wehtut

Ältere NAS, Multifunktionsgeräte mit Scan-to-Folder und manche Linux-Freigaben können nicht signieren oder nur langsam. Gastzugriffe unterstützen Signierung grundsätzlich nicht. Microsoft rät ausdrücklich davon ab, die Signierung wieder abzuschalten, und empfiehlt, sie am Gerät zu aktivieren

oder das Gerät zu ersetzen. Welche Geräte das betrifft, findest du am besten heraus, bevor du die Richtlinie flächig ausrollst. Mehr dazu in NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll.

LDAP-Signierung und LDAP-Kanalbindung

Bei LDAP gibt es zwei Wege und darum zwei Schlösser. Über Port 389 ohne TLS schützt die LDAP-Signierung die Sitzung mit dem Sitzungsschlüssel, ähnlich wie bei SMB. Über LDAPS oder StartTLS übernimmt TLS die Verschlüsselung, aber TLS allein verhindert kein Relay: Der Mittelsmann baut einfach seine eigene TLS-Verbindung zum DC auf und reicht die Anmeldung hinein. Dagegen hilft die Kanalbindung. Client und Server leiten aus der TLS-Sitzung ein Channel Binding Token ab, der Client legt es in die Anmeldung, und der DC vergleicht. Die TLS-Sitzung des Mittelsmanns hat ein anderes Token, die Anmeldung fällt durch.

Einstellung	Wo	Werte und Standard
Domain controller: LDAP server signing requirements	DC	neue Domänen ab Server 2025: Signierung verlangt; aktualisierte Server behalten ihre Einstellung
Network security: LDAP client signing requirements	Clients	Signierung aushandeln oder verlangen
Domain controller: LDAP server channel binding token requirements	DC	Never, When supported, Always; Server 2025: When supported, Server 2022 und älter: Never

Die Richtliniennamen stehen hier im englischen Original; in deutschen Konsolen findest du sie unter den Sicherheitsoptionen mit der Vorsilbe „Domänencontroller:“ beziehungsweise „Netzwerksicherheit:“. Bevor du „Always“ setzt, schau in die Protokolle. Der DC schreibt im Protokoll Directory Service Ereignis 2887 als Tageszusammenfassung unsignierter Bindungen und 3040 als Tageszusammenfassung ungeschützter LDAPS-Bindungen. Wer genau die Übeltäter sind, zeigen 2889 (unsigniert) und 3039, 3074, 3075 (Kanalbindung) pro Client, sobald die Diagnose für „16 LDAP Interface Events“ auf 2 steht.

```
# LDAP-Diagnose auf einem DC hochdrehen (nach der Auswertung wieder auf 0)
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics' `
    -Name '16 LDAP Interface Events' -Value 2 -Type DWord

# Unsignierte Bindungen und Kanalbindungsprobleme der letzten 24 Stunden
Get-WinEvent -FilterHashtable @{LogName='Directory Service'; Id=2889,3039,3074,3075;
    StartTime=(Get-Date).AddDays(-1)} | Group-Object Id | Select-Object Name, Count
```

Extended Protection for Authentication (EPA)

EPA ist der Oberbegriff für Kanal- und Dienstbindung bei Windows-integrierter Authentifizierung, also überall dort, wo NTLM oder Negotiate über HTTP läuft: IIS, die Web-Registrierung von AD CS, Exchange, Reporting Services und Fachanwendungen. KB5021989: Extended Protection for Authentication beschreibt die Grundlage: Die Anmeldung wird an den SPN des Zielservers und an den äußeren TLS-Kanal gebunden. Das Update selbst verhindert noch kein Relay, es ermöglicht Anwendungen, EPA zu nutzen. Wo die Anwendung es nicht einschaltet, passiert nichts.

Für TLS-terminierende Load Balancer gibt es die Dienstbindung als Rückfallebene: Der Server prüft dann nicht die TLS-Sitzung, sondern ob der Client sich bei einem Namen angemeldet hat, der zum Zertifikat passt. Bei Exchange 2019 ist EPA seit CU14 standardmäßig aktiv, bei AD CS auf Windows Server 2025 steht es auf „When Supported“. Auf Server 2022 und 2019 musst du es selbst einschalten. Clientseitig steuert laut KB5021989 der Registrierungswert

SuppressExtendedProtection, ob Windows die Bindungsinformationen mitsendet; 0 heißt eingeschaltet, und das ist der Standard. Wenn du in einem Altbestand auf einen anderen Wert stößt, hat jemand vor Jahren ein Problem auf die bequeme Art gelöst.

TIPP · IIS: erst Negotiate, dann EPA

In IIS heißt EPA „Erweiterter Schutz“ in den erweiterten Einstellungen der Windows-Authentifizierung, mit den Stufen Aus, Akzeptieren und Erforderlich. Fang mit Akzeptieren an, beobachte, und geh dann auf Erforderlich. Und wenn du schon dort bist: Steht NTLM als einziger Anbieter drin, ist das die eigentliche Baustelle. Wie du auf Negotiate umstellst, zeigt NTLM in IIS und Webanwendungen: Negotiate statt NTLM.

MIC: das Siegel auf der Aushandlung

Der Message Integrity Code ist das unauffälligste und zugleich wichtigste Gegenmittel, weil die anderen auf ihm aufbauen. Beim NTLM-Handschlag handeln Client und Server per Flags aus, ob signiert wird, welche Verschlüsselung gilt und so weiter. Der MIC ist eine Prüfsumme über alle drei NTLM-Nachrichten, berechnet mit dem Sitzungsschlüssel. Ändert der Mittelsmann unterwegs ein Flag, etwa um die Signierung abzuwählen, passt der MIC nicht mehr, und der Server verwirft die Anmeldung.

Ohne MIC kann der Mittelsmann genau das tun: die Signierung herausverhandeln und damit das schönste SMB- oder LDAP-Schloss aushebeln. Den MIC gibt es nur bei NTLMv2. Moderne Windows-Clients senden ihn von sich aus; fehlen tut er bei alten Betriebssystemen, bei manchen Fremdimplementierungen auf Geräten und bei Bibliotheken in Fachanwendungen, die NTLM selbst nachbauen.

Gegenmittel	Bindet an	Wirkt bei	Schwachstelle
SMB-Signierung	Sitzungsschlüssel	SMB	Geräte ohne Signierung, Gastzugriff
LDAP-Signierung	Sitzungsschlüssel	LDAP über Port 389	einfache Bindungen, Altclients
LDAP-Kanalbindung	TLS-Sitzung	LDAPS, StartTLS	Standard „Never“ bis Server 2022
EPA (Kanalbindung)	TLS-Sitzung	HTTP(S) mit Windows-Anmeldung	muss pro Anwendung aktiv sein
EPA (Dienstbindung)	Zielname (SPN)	HTTP(S) hinter Load Balancern	schwächer als Kanalbindung
MIC	alle drei NTLM-Nachrichten	jedes NTLMv2	fehlt bei NTLMv1 und Fremdimplementierungen

AUS DER PRAXIS · Musterwerk GmbH: das NAS, das alles erklärte

Bei der Musterwerk GmbH (musterwerk.local) hatte der Pentest-Bericht wieder einmal „SMB-Signierung nicht erzwungen“ in Rot. Die IT wollte die GPO ausrollen und testete vorher mit zwei Abteilungen. Ergebnis: Die Konstruktion konnte nicht mehr auf das Zeichnungsarchiv zugreifen, ein zehn Jahre altes NAS, das weder signieren konnte noch einen MIC schickte. Statt die Signierung für alle wieder auszuschalten, bekam das NAS ein Ablösedatum, eine befristete Ausnahme für genau die zwölf Konstruktionsrechner und einen Eintrag im Risikoregister. Vier Monate später war es weg, und der rote Punkt im nächsten Bericht auch.

Prüfen, ob die Schlösser wirklich zu sind

Eine GPO, die Signierung verlangt, sagt dir, was gelten soll. Was tatsächlich passiert, sagen die Protokolle. Und da hat das erweiterte NTLM-Auditing nach Microsoft KB5064479 einen echten Fortschritt gebracht: Jede protokollierte NTLM-Anmeldung enthält jetzt die Sicherheitsmerkmale, mit denen sie stattgefunden hat.



Skizze: Feldnamen wie im Meldungstext nach Microsoft KB5064479

Die Sicherheitsfelder im erweiterten Auditing

Das erweiterte Auditing läuft ab Windows 11 24H2 und Windows Server 2025 sowie auf Windows Server 2022 und 2019 mit den Updates ab 13.10.2026. Es schreibt die Ereignisse 4020 und 4021 auf dem Client, 4022 und 4023 auf dem Server und 4030 bis 4033 auf dem DC. Die Informationsereignisse 4020, 4022, 4030 und 4032 stehen für normale Sicherheit, die Warnungen 4021, 4023, 4031 und 4033 für herabgesetzte Sicherheit: NTLMv1, fehlender oder unsicherer erweiterter Schutz oder fehlende Merkmale wie der MIC. Wie du das Auditing einschaltest, steht in Erweitertes NTLM-Auditing einschalten: Schritt für Schritt; das NTLM-Audit-GPO-Skript nimmt dir die Klickarbeit in der Gruppenrichtlinienverwaltung ab.

Feld im Meldungstext	Gut	Bedenklich	Was es für Relay bedeutet
NTLM Version	NTLMv2	NTLMv1	NTLMv1 kennt weder MIC noch Kanalbindung
MIC Status	Protected	Unprotected	Aushandlung manipulierbar, Signierung abwählbar
Channel Binding	Supported	Not Supported	Anmeldung passt in fremde TLS-Sitzungen
Session Key Status	Present	Missing	keine Signierung, keine Versiegelung möglich
Service Binding	SPN des Ziels	leer oder unpassend	Dienstbindung kann nicht greifen

Die klassischen Restrict-NTLM-Ereignisse 8001 bis 8004 laufen auch auf älteren Systemen, enthalten diese Sicherheitsfelder aber nicht. Für die Frage „Wo ist Relay möglich?“ brauchst du deshalb das erweiterte Auditing. Die Details zu den einzelnen Ereignissen findest du in Ereignis

4020 und 4021: ausgehende NTLM-Anmeldungen lesen, Ereignis 4022 und 4023: eingehende NTLM-Anmeldungen auf Servern und NTLM auf dem Domain Controller: Ereignisse 4030 bis 4033 und 8004.

Mit Bordmitteln auswerten

Auf einem einzelnen Server kommst du mit PowerShell schnell zu einem ersten Bild. Das folgende Beispiel holt die Warnungen 4023 aus dem NTLM-Betriebsprotokoll und durchsucht den Meldungstext nach den drei kritischen Werten. Bewusst über den Meldungstext, damit wir keine Feldnamen im XML erraten müssen.

```
$ev = Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-NTLM/Operational'; Id=4023} `
      -MaxEvents 5000 -ErrorAction SilentlyContinue
$ev | ForEach-Object {
    [pscustomobject]@{
        Zeit       = $_.TimeCreated
        OhneMIC    = $_.Message -match 'MIC Status:\s*Unprotected'
        OhneCBT    = $_.Message -match 'Channel Binding:\s*Not Supported'
        OhneKey    = $_.Message -match 'Session Key Status:\s*Missing'
        NTLMv1     = $_.Message -match 'NTLM Version:\s*NTLMv1'
    }
} | Group-Object OhneMIC, OhneCBT, OhneKey, NTLMv1 | Select-Object Count, Name
```

Das funktioniert, und für den Dateiserver der Sparfuchs & Partner Steuerberatungs GmbH mit 40 Arbeitsplätzen reicht es auch. Dann kommt die Realität. Du willst nicht wissen, dass es 1.800 Anmeldungen ohne MIC gab, sondern von welchem Client zu welchem Ziel, mit welchem Konto und warum. Dafür musst du die Ereignisse von Clients, Servern und DCs zusammenführen, nach Quelle und Ziel gruppieren, Duplikate entfernen und die Geräte ergänzen, die gar kein Windows-Protokoll schreiben. Bei 300 Servern und 2.000 Clients ist das kein Skript mehr, das ist ein Nebenjob.

WARNUNG · Das stille Gerät ist das gefährlichste

Ein Scanner, der sich per NTLMv1 ohne MIC an einer Freigabe anmeldet, schreibt kein Ereignis. Du siehst ihn nur auf der Serverseite oder im Netzwerkmitschnitt. Wenn du ausschließlich Client-Ereignisse sammelst, fehlt dir genau die Gruppe, die am schlechtesten geschützt ist. Wie du solche Geräte im Mitschnitt findest, zeigt NTLM im Netzwerkmitschnitt finden: Wireshark richtig einsetzen.

Wenn die Ereignisse nicht mehr in eine Tabelle passen

Genau für diese Stelle haben wir den NTLM Diagnostiker gebaut. Er sammelt die NTLM-Ereignisse direkt vom DC, über einen Windows Event Collector oder per Direktabfrage, führt sie zu einer Kommunikationsmatrix zusammen und markiert jede Verbindung, die ohne MIC, ohne Kanalbindung oder ohne Session Key läuft. Er arbeitet ausschließlich lesend: keine Agenten, keine Änderungen an Richtlinien, keine Schreibzugriffe im Active Directory.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Relay-Risiken in der Übergangszeit sichtbar machen

Sicherheitsflaggen: Jede Verbindung ohne MIC, ohne Kanalbindung oder ohne Session Key wird markiert, mit Quelle, Ziel und Konto. So siehst du, welche Ausnahmen echte Relay-Risiken sind und welche nur unschön.

Kommunikationsmatrix und Konten-Sicht: Wer spricht mit wem per NTLM, und welche Konten sind dabei, insbesondere Computerkonten von Servern und DCs.

NTLMv1-Hitliste: die Quellen, die gar keine Gegenmittel unterstützen und deshalb zuerst gehen

müssen.

Ursachen-Engine mit SPN- und DNS-Prüfung: zeigt, warum eine Verbindung überhaupt NTLM nutzt, denn die beste Relay-Abwehr ist die NTLM-Anmeldung, die gar nicht erst stattfindet.

Wireshark-Import: Mitschnitte von stillen Geräten wie NAS, Scannern oder Medizintechnik fließen in dieselbe Auswertung ein.

Abschalt-Simulation, Readiness-Ampel und Word-Bericht: zeigen, was beim Verweigern von NTLM ausfallen würde, und liefern das Ergebnis für IT-Leitung und Pentest-Nachbereitung, dazu Excel/CSV-Export.

Einstieg: Die Edition Express ist kostenlos und liefert einen Fünf-Minuten-Befund; die Vollversion kannst du 7 Tage testen, lizenziert wird pro aktivem Computerkonto.

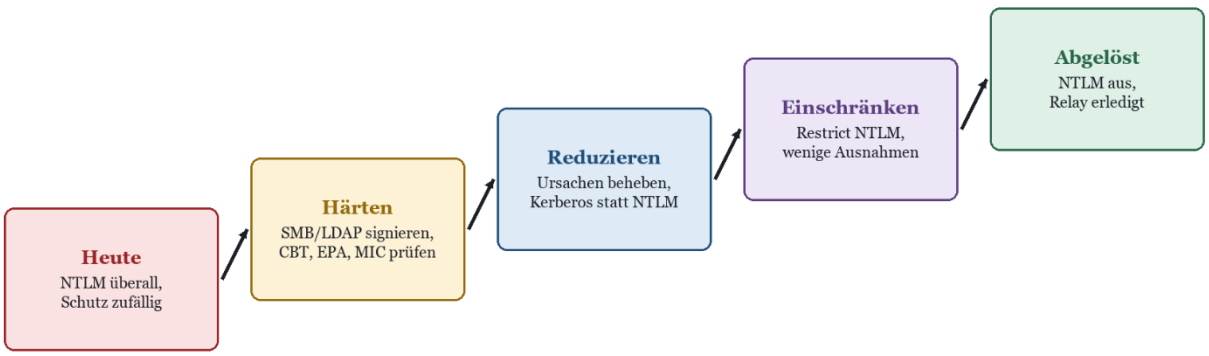
Ein Kerberos-Gegencheck, der prüft, ob nach dem Abschalten tatsächlich Kerberos übernimmt, ist als Ausbaustufe geplant, ebenso ein Ausnahmelisten-Generator. Heute vorhanden sind die oben genannten Funktionen.

Warum die Ablösung trotzdem das Ziel bleibt

Nach all den Schlössern könnte man meinen: Signierung überall, Kanalbindung auf „Always“, EPA an, MIC geprüft, fertig. Leider nicht. Relay-Schutz ist eine Sammlung von Einzellösungen, eine pro Protokoll und eine pro Anwendung. Jede neue Fachanwendung, jedes neue Gerät und jedes vergessene Altsystem kann eine Lücke sein. Und Relay ist nur einer von mehreren Angriffen auf NTLM: Hashes lassen sich offline angreifen, Pass-the-Hash funktioniert unabhängig von Kanalbindung, und NTLM kennt keine gegenseitige Authentifizierung.

Härten ist die Brücke, Ablösen ist das Ufer

Relay-Schutz kauft dir Zeit. Er macht NTLM nicht zu Kerberos.



Phase 3 laut Microsoft: NTLM in der nächsten Windows-Server-Version standardmäßig aus.

Skizze: Reihenfolge der Maßnahmen, Zeitbedarf je nach Umgebung

Kerberos löst das Problem an der Wurzel. Das Ticket ist an einen Dienst gebunden, der Server weist sich gegenüber dem Client aus, und eine weitergereichte Anmeldung nützt nichts. Hintergründe findest du im Kompetenzbereich Microsoft Kerberos. Deshalb gehört Relay-Schutz in die Übergangszeit und an die verbliebenen Ausnahmen, nicht an die Stelle der Ablösung.

Situation	Kurzfristig	Ziel
Clients und Server mit aktuellem Windows	Signierung prüfen, Auditing auswerten	Ursachen beheben, NTLM einschränken
DCs mit LDAP und	Signierung und Kanalbindung auf	Kerberos-SASL mit Kanalbindung

LDAPS	Always	
AD CS Web-Registrierung	EPA Erforderlich, nur HTTPS	Web-Registrierung abschaffen, wo möglich
Fachanwendung mit eingebautem NTLM	EPA, wenn die Anwendung es kann; Ausnahme befristen	Herstellerupdate mit Kerberos
Gerät ohne MIC und ohne Signierung	eng gefasste Ausnahme, Netzsegment	Gerät ersetzen

Für die Ausnahmen, die am Ende stehen bleiben, gilt: Eine Ausnahme mit Signierung und MIC ist ein vertretbares Restrisiko, eine Ausnahme ohne beides ist ein offenes Fenster im Erdgeschoss. Wie du Ausnahmen eng fasst und befristest, zeigt Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren. Die Reihenfolge der Abschaltschritte beschreibt NTLM schrittweise abschalten, ohne dass etwas ausfällt.

AUS DER PRAXIS · Trendforge Digital GmbH: zwei Pentests, eine Erkenntnis

Die Trendforge Digital GmbH hatte nach dem ersten Pentest SMB- und LDAP-Signierung erzwungen und die Kanalbindung eingeschaltet. Im zweiten Pentest gelang trotzdem ein Relay, diesmal auf die Web-Oberfläche einer Zeiterfassung, die NTLM ohne EPA anbot. Die Konsequenz war nicht das nächste Schloss, sondern die Frage an den Hersteller nach Kerberos-Unterstützung und ein Termin für die Umstellung. Im Projektplan heißt der Punkt seitdem „Relay-Schutz bis zur Ablösung“, nicht „Relay-Schutz erledigt“.

FAQ: NTLM-Relay-Schutz

Reicht es, SMB-Signierung zu erzwingen?

Für SMB ja, für alles andere nein. Relay funktioniert auch gegen LDAP, HTTP und andere Dienste. Jedes Protokoll braucht sein eigenes Gegenmittel, und ohne MIC lässt sich die Signierung unter Umständen schon in der Aushandlung abwählen.

Kostet SMB-Signierung spürbar Leistung?

Auf aktueller Hardware mit SMB 3.x meist kaum. Bei großen Dateiübertragungen über schnelle Netze und bei schwacher Hardware auf Gerätseite kann es messbar sein. Miss es in deiner Umgebung, statt dich auf Faustregeln zu verlassen.

Kann ich die LDAP-Kanalbindung sofort auf „Always“ stellen?

Nur wenn die Ereignisse 3039, 3074 und 3075 ruhig sind. Stell zuerst auf „When supported“, dreh die Diagnose hoch und werte ein paar Wochen aus. Clients, die keine Kanalbindung beherrschen, fallen bei „Always“ mit LDAPS-Anmeldungen durch.

Was heißt „MIC Status: Unprotected“ im Ereignis?

Die NTLM-Anmeldung lief ohne Message Integrity Code. Die Aushandlung hätte unterwegs verändert werden können. Typische Quellen sind NTLMv1, alte Betriebssysteme und Geräte oder Anwendungen mit eigener NTLM-Implementierung.

Hilft die NTLMv1-Blockade seit Oktober 2026 gegen Relay?

Sie hilft indirekt: Sie entfernt die Variante, die gar keine Gegenmittel kennt. Gegen Relay mit NTLMv2 tut sie nichts. Dafür brauchst du Signierung, Kanalbindung, EPA und am Ende Kerberos.

Ändert der NTLM Diagnostiker Einstellungen, um Relay zu verhindern?

Nein. Er arbeitet ausschließlich lesend und zeigt, wo Verbindungen ohne MIC, ohne Kanalbindung oder ohne Session Key laufen. Die Entscheidung und die Umsetzung bleiben bei dir. Wenn du dabei Unterstützung willst, gibt es die Beratung zur NTLM-Ablösung.

Was mache ich in der Klinik mit Medizintechnik, die nichts davon kann?

Netz segmentieren, Ausnahmen so eng wie möglich fassen, Konten mit minimalen Rechten verwenden und den Ablösetermin mit dem Hersteller festhalten. Die Besonderheiten zugelassener Geräte behandelt NTLM in der Klinik: Medizintechnik, Labor und Fachanwendungen.

Fazit: Schlösser einbauen, Umzug trotzdem planen

NTLM-Relay ist kein exotischer Angriff, sondern das, was in fast jedem Pentest-Bericht steht. Die Gegenmittel sind seit Jahren vorhanden und werden mit Windows 11 24H2 und Windows Server 2025 endlich zum Standard: SMB-Signierung, LDAP-Signierung, Kanalbindung, Extended Protection und der MIC. Sie wirken aber nur dort, wo beide Seiten mitspielen, und genau die Seiten, die nicht mitspielen, sind in deinem Netz die interessantesten.

Nutz die Übergangszeit also doppelt. Härte, was sich härten lässt, und schau mit dem erweiterten Auditing nach, wo MIC, Kanalbindung oder Session Key fehlen. Diese Liste ist gleichzeitig deine Prioritätenliste für die Ablösung. Denn das einzige NTLM, das garantiert nicht weitergereicht wird, ist das, das nicht mehr stattfindet. Bis dahin gilt: Lieber drei Schlösser an der Tür als ein Schild „Bitte nicht relayen“.

WEITERLESEN · Weiter in dieser Serie

› NTLMv1 blockiert: was seit Oktober 2026 nicht mehr geht
› Erweitertes NTLM-Auditing einschalten: Schritt für Schritt
› Ereignis 4022 und 4023: eingehende NTLM-Anmeldungen auf Servern
› NTLM in IIS und Webanwendungen: Negotiate statt NTLM
› Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren
› Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern
› NTLM schrittweise abschalten, ohne dass etwas ausfällt
› NTLM im Netzwerkmitschnitt finden: Wireshark richtig einsetzen