Security & Compliance

Windows: NTLM-Signierung wird ab November 2026 standardmäßig angeboten, ab Mai 2027 erzwungen

Executive Summary

NTLM ist das Protokoll, das in jedem Windows-Netz herumgeistert wie ein Untoter im Keller: offiziell längst abgekündigt, praktisch quicklebendig und bei Angreifern beliebter als jede Zero-Day-Lücke. Laut Microsoft-Ankündigung MC1549242, zuletzt geändert am 11.11.2026, zieht Microsoft jetzt eine Schraube an, die eigentlich schon seit zwanzig Jahren fest sein sollte: Mit den Windows-Updates vom **10. November 2026** bieten Windows-Clients bei allen nicht anonymen NTLM-Verbindungen **echte Nachrichtensignierung** an. Ab **Mai 2027** verlangen Windows-Server diese Signierung standardmäßig, und Clients, die nicht signieren, fliegen raus.

Ohne dein Eingreifen passiert im November erst einmal wenig Sichtbares: Server akzeptieren weiter beides, schreiben aber Ereignisse ins Log, die unsignierte Verbindungen verraten. Im Mai knallt es dann bei allem, was du bis dahin nicht gefunden hast: alte NAS-Systeme, Multifunktionsdrucker mit Scan-to-Folder, Linux-Kisten mit Samba-Client und die eine Fachanwendung, deren Hersteller 2014 insolvent gegangen ist. Du hast also sechs Monate Zeit, um herauszufinden, wer in deinem Netz ohne Siegel spricht. Das klingt nach viel. Das dachten die Leute beim Jahr-2000-Problem auch.

Wichtig: Die Frist ist weit weg. Die Arbeit nicht.

Bis **Ende November 2026** gehören die November-Updates auf Clients und Server und das erweiterte NTLM-Auditing eingeschaltet. Von **Dezember 2026 bis März 2027** wertest du aus und räumst auf. Im **April 2027** erzwingst du die Signierung selbst, Server-Ring für Server-Ring, damit dich der Mai-Patchday nicht mit heruntergelassener Hose erwischt. Sicherheitlich ist das kein Kür-Thema: Microsoft stuft die zugehörige Lücke CVE-2026-118737 als **kritisch** ein.

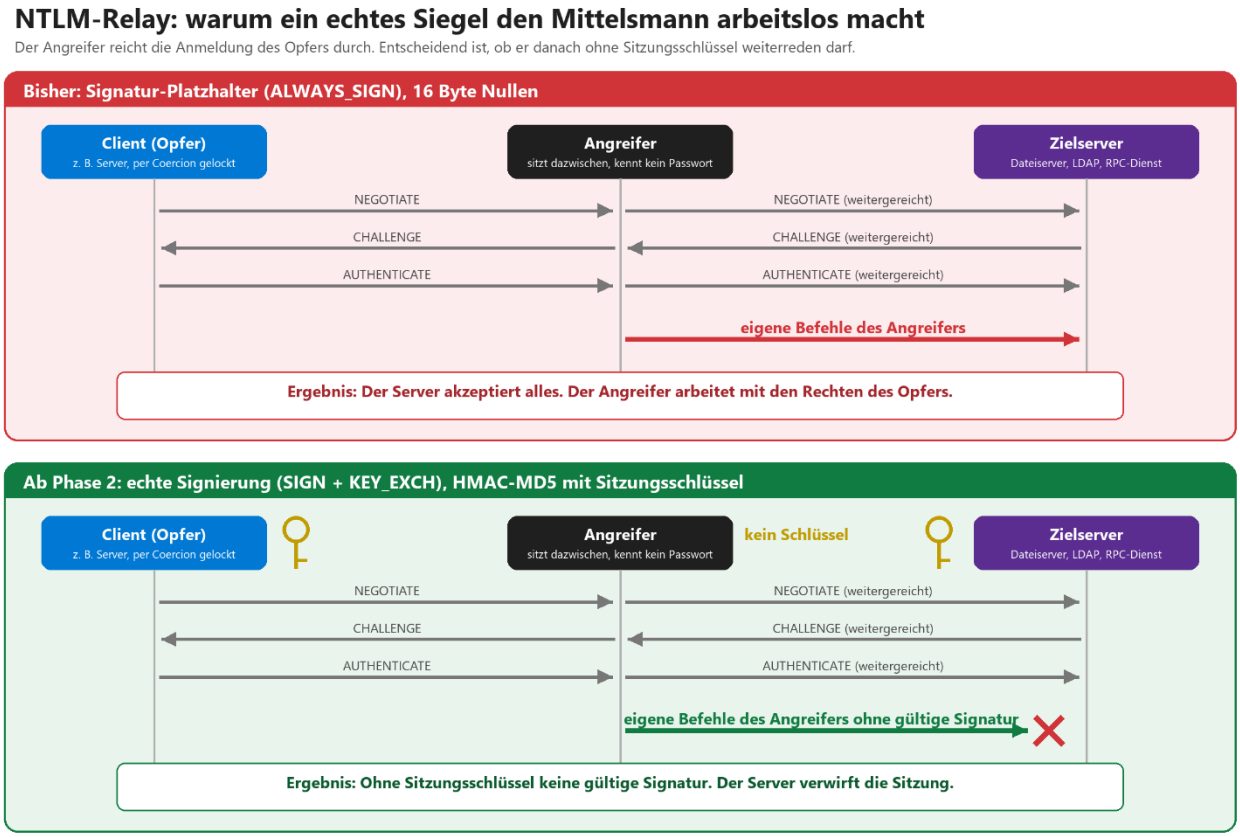
Worum geht es im Detail?

Erst die Hintergründe, sonst versteht niemand, warum ein unscheinbares Flag so viel Lärm macht. NTLM ist ein Challenge-Response-Verfahren: Der Server schickt eine Zufallszahl, der Client beweist mit seinem Kennwort-Hash, dass er das Kennwort kennt. Das Kennwort selbst wandert nie über die Leitung. Das Problem: Der Beweis ist an nichts gebunden. Wer sich zwischen Client und Server setzt, kann die drei NTLM-Nachrichten einfach durchreichen und sitzt danach mit der Identität des Opfers am Server. Das nennt sich **NTLM-Relay**, und es funktioniert seit den Neunzigern zuverlässiger als die meisten Drucker.

Damit das Opfer sich überhaupt beim Angreifer meldet, braucht es eine Einladung. Die liefern sogenannte **Coercion-Techniken**: Ein Angreifer mit Netzwerkzugang bringt einen Server über harmlose RPC-Aufrufe dazu, sich bei ihm zu authentifizieren. Wenn dieser Server ein Domänencontroller oder ein Zertifikatsserver ist, endet der Nachmittag gern mit Domänen-

Admin-Rechten und einem Anruf bei der Cyberversicherung. Viele Ransomware-Vorfälle der letzten Jahre hatten irgendwo in der Mitte genau diesen Schritt.

Die Gegenwehr heißt **Signierung**. Nach der Anmeldung leiten Client und Server aus dem Kennwort-Hash einen **Sitzungsschlüssel** ab, den der Mittelsmann nicht kennt. Jede weitere Nachricht wird damit per HMAC-MD5 signiert. Der Angreifer kann zwar die Anmeldung durchreichen, aber danach keine einzige gültig signierte Nachricht schreiben. Laut KB5135557 gab es bisher allerdings eine fiese Lücke im Kleingedruckten: Verbindungen, bei denen die Anwendung keine Integrität angefordert hat, erhielten nur das Flag **ALWAYS_SIGN**, und das bedeutet eine Signatur aus **16 Byte Nullen**. Ein Siegel aus Luft, sozusagen. Sieht im Protokoll ordentlich aus, schützt aber genau nichts.



Genau hier setzt die Lücke **CVE-2026-118737** an. Microsoft führt sie im Security Update Guide als Remotecodeausführung in der RPC-Laufzeit mit einem CVSS-Basiswert von **8,1** und der Einstufung **kritisch**. Die Ursache ist eine unzureichende Prüfung kryptografischer Signaturen: Ein Angreifer ohne Anmeldedaten, aber mit Netzwerkzugang, könnte über eine zeitkritische Schwäche im Authentifizierungsablauf Code auf einem Server ausführen. Er muss dafür eine Race Condition gewinnen, deshalb bewertet Microsoft die Ausnutzung als „weniger wahrscheinlich“. Bekannt geworden oder ausgenutzt ist die Lücke laut Microsoft bislang nicht. Wer daraus „kann warten“ liest, liest auch Beipackzettel nur bis zur Dosierung.

Die Korrektur kommt in zwei Phasen und wird über zwei Registrierungswerte gesteuert, beide als DWORD unter **HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0**. Gruppenrichtlinien-Einstellungen dafür dokumentiert Microsoft nicht, du verteilst die Werte also per Gruppenrichtlinien-Einstellung vom Typ Registrierung, per Intune-Plattformskript oder per PowerShell.

	Phase 1 (ab 10.11.2026)	Phase 2 (ab Mai 2027)
Windows-Client	bietet **SIGN** auf allen nicht anonymen Verbindungen an	unverändert, bietet SIGN an
Windows-Server	akzeptiert signierte und unsignierte Clients	**verlangt** Signierung, weist unsignierte Clients ab
Fehlerbild	keins, nur Warnereignisse im Log	Client erhält **SEC_E_UNSUPPORTED_FUNCTION (0x80090302)**
Auditing	Ereignisse 4022/4023 im Log NTLM/Operational	Ereignis 4023 mit dem Abweisungsstatus
Ausnahmen	anonyme Verbindungen (Null Session) und Gastkonto	anonyme Verbindungen und Gastkonto

Registrierungswert	Standard (0)	Wert 1
ClientAllowUnsignedNtlm	Client bietet SIGN auf allen nicht anonymen Verbindungen an	Client bietet SIGN nicht an, laut Microsoft nur als vorübergehende Kompatibilitätskrücke gedacht
ServerRequireNtlmSign	Server akzeptiert signierte und unsignierte Clients	Server weist unsignierte Clients ab, kein Neustart nötig, empfohlen sobald das Audit sauber ist

Fakten: Wer die Änderung bekommt

Laut KB5135557 betroffen sind **Windows 11** in den Versionen 23H2, 24H2, 25H2, 26H1 und 26H2, **Windows 10 Enterprise LTSC 2021** sowie **Windows Server 2016, 2019, 2022 und 2025**. Kerberos bleibt unberührt. Spricht ein Client mit einem alten Server, der SIGN nicht zurückmeldet, fällt er ohne Fehler auf das alte Verhalten zurück. Alle unterstützten Windows-Server können laut Microsoft ohnehin signieren. Und: Microsoft behält sich vor, die beiden Registrierungswerte später wieder zu entfernen.

Alle Details samt Prüfskript beschreibt Microsoft im Support-Artikel NTLM signing security improvements in Windows (KB5135557).

Einordnen sollte man das Ganze in Microsofts größeren Plan. Im Januar 2026 hat Microsoft im Windows IT Pro Blog angekündigt, Netzwerk-NTLM mit der nächsten großen Windows-Version standardmäßig abzuschalten, vorbereitet durch erweitertes Auditing und Ersatztechniken wie IAKerb und einen lokalen KDC. Die Signierungspflicht ist der Zwischenschritt: NTLM darf noch leben, aber nur noch mit Siegel. Wer jetzt aufräumt, räumt also zweimal auf einmal auf.

Was sind Chancen? Was sind Risiken?

Die Chance ist schlicht: Eine der ältesten und zuverlässigsten Angriffstechniken im Active Directory verliert einen großen Teil ihres Werkzeugkastens, und zwar ohne Lizenzkosten, ohne neues Produkt und ohne Beraterprojekt mit siebenstelligem Budget. Nebenbei bekommst du über das Auditing zum ersten Mal ein ehrliches Bild davon, wer in deinem Netz noch NTLM spricht. Das ist für die geplante NTLM-Abschaltung ohnehin Pflichtlektüre.

Chance	Risiko
Relay-Angriffe auf Windows-Server werden deutlich schwerer	Geräte ohne Signierung verlieren im Mai 2027 den Zugriff
Keine Zusatzlizenz, kommt mit dem regulären Patch	Altgeräte und Fremdsysteme tauchen in keiner Microsoft-Liste auf
Auditing liefert erstmals belastbare NTLM-Inventur	Audit-Ereignisse enthalten Benutzernamen, IPs, Prozesse: Datenschutzthema
Früh selbst erzwingen schafft planbare Umstellung	Ausnahmen per ClientAllowUnsignedNtlm werden zum Dauerprovisorium
Vorarbeit für die NTLM-Abschaltung der nächsten Windows-Version	Zweistufige Logik verführt zum Abwarten bis April 2027

Warnung: Der Scanner im zweiten Stock

Ein Fall, den wir in ähnlicher Form schon bei der SMB- und LDAP-Härtung erlebt haben: Ein Steuerbüro mit 40 Leuten, Montagmorgen, Patchday-Woche. Der Multifunktionsdrucker im zweiten Stock scannt seit 2017 zuverlässig in eine Freigabe auf dem Dateiserver, mit einem Dienstkonto, dessen Kennwort auf einem Post-it im Druckerschrank klebt. Nach dem Update: „Zugriff verweigert“. Der Drucker zeigt keine Fehlernummer, sondern ein trauriges Symbol, der Hersteller-Support verweist auf ein Firmware-Update für ein Modell, das er nicht mehr unterstützt, und die Mandantenbelege stapeln sich auf Papier. **Die Firmware des Druckers hat nie signiert. Gemerkt hat es nur keiner, weil niemand gefragt hat.** Ab Mai 2027 fragt Windows.

Sicherheitsfolgen und Prioritäten: Ganz oben stehen Domänencontroller, Zertifikatsdienste und Server mit hohen Rechten, denn dort lohnt sich Relay für Angreifer am meisten. Dann Dateiserver mit sensiblen Daten. Ganz unten stehen isolierte Systeme ohne Domänenanbindung. Die November-Updates sind dabei nicht verhandelbar, schon wegen der kritischen Einstufung der Lücke. Die eigentliche Arbeit ist aber nicht das Patchen, sondern die Inventur der Gegenstellen.

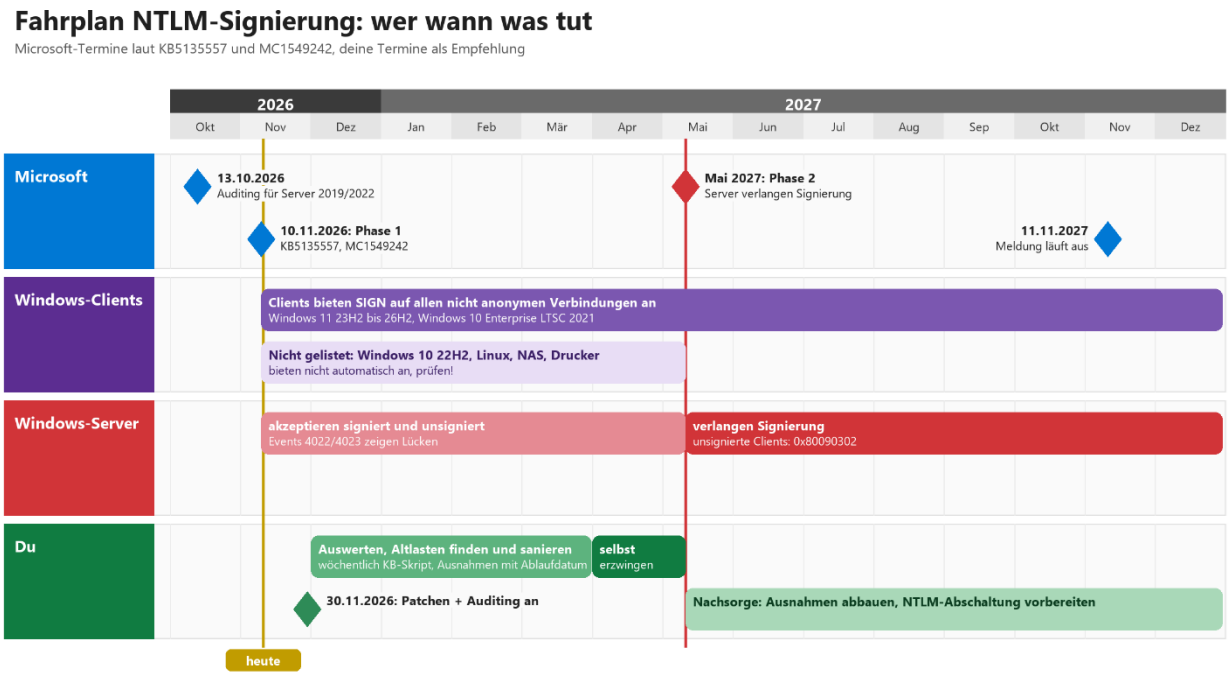
Mittelstand und öffentliche Auftraggeber: Im Mittelstand sind die Verdächtigen fast immer dieselben: NAS-Systeme, Drucker, ältere ERP- und Warenwirtschaftsclients, Zeiterfassungsterminals und Maschinensteuerungen, die in die Windows-Freigabe schreiben. In der öffentlichen Verwaltung kommen Fachverfahren hinzu, deren Weiterentwicklung über Vergabeverfahren läuft, und die sind selten schneller als sechs Monate. Wer dort ein Fachverfahren als Risiko identifiziert, sollte den Hersteller noch **im Dezember 2026** schriftlich anfragen. Für Organisationen unter dem NIS2-Umsetzungsgesetz gilt zudem: Wer Maßnahmen nach dem Stand der Technik umsetzen muss, wird erklären müssen, warum er eine von Microsoft angebotene Härtung gegen eine kritische Lücke ein halbes Jahr liegen lässt.

Datenschutz und Mitbestimmung: Das erweiterte NTLM-Auditing protokolliert pro Anmeldung Benutzername, Client-IP, Rechnername und den aufrufenden Prozess. Das sind personenbezogene Daten, und sie sind technisch geeignet, Verhalten nachzuvollziehen. Damit ist der Betriebsrat nach § 87 Abs. 1 Nr. 6 BetrVG im Boot, in Behörden der Personalrat nach dem jeweiligen Personalvertretungsrecht. In der Praxis reicht oft eine kurze Ergänzung der IT-Rahmenvereinbarung: Zweck ausschließlich Sicherheitshärtung, keine Leistungs- und Verhaltenskontrolle, Auswertung nur durch die IT-Sicherheit, Löschung nach Abschluss des Projekts. Schreib das vor dem Einschalten auf, nicht danach. **Lizenzen:** Für die Änderung selbst

brauchst du nichts. Wer aber noch Windows 10 22H2 betreibt, findet diese Version nicht in der Liste der betroffenen Systeme und sollte sich schon deshalb mit der Migration beeilen.

Was müssen wir jetzt schon vorbereiten?

Ohne Eingreifen sieht dein Jahr so aus: November-Patch installiert sich, Clients signieren brav, Server akzeptieren alles, das Log füllt sich unbemerkt mit Warnungen. Im Mai kommt der nächste Patch, Server verlangen Signierung, und das Helpdesk lernt neue Fehlermeldungen kennen. Steuern kannst du das in beide Richtungen: früher erzwingen über **ServerRequireNtlmSign = 1** oder einzelne Clients vorübergehend herausnehmen über **ClientAllowUnsignedNtlm = 1**. Ob ein explizit gesetzter Serverwert 0 auch nach Mai 2027 noch als Rückweg funktioniert, lässt Microsoft offen. Plane nicht damit.



Schritt 1, bis 30.11.2026 – Patchen und Auditing einschalten: Die November-Updates auf alle Clients und Server. Das erweiterte Auditing ist auf Windows 11 24H2 und Windows Server 2025 eingebaut, auf Server 2019 und 2022 seit den Updates vom 13.10.2026. Per Gruppenrichtlinie aktivierst du es unter **Computerkonfiguration › Administrative Vorlagen › System › NTLM › NTLM Enhanced Logging**, auf Domänencontrollern zusätzlich unter **System › Netlogon › Log Enhanced Domain-wide NTLM Logs**. Die Ereignisse landen im Ereignisprotokoll unter **Anwendungs- und Dienstprotokolle › Microsoft › Windows › NTLM › Operational**.

Hintergrund und alle Ereignis-IDs beschreibt Microsoft unter Overview of NTLM auditing enhancements in Windows 11, version 24H2 and Windows Server 2025.

Schritt 2, Dezember 2026 bis Februar 2027 – Auswerten: Achtung, Falle: Microsoft protokolliert signierte und unsignierte Verbindungen gleichermaßen als **Warnung**. Wer nach Ereignisstufe filtert, sieht nur Rauschen. Entscheidend sind die **Negotiated Flags**: Fehlt das Bit 0x00000010 (SIGN), ist die Verbindung ungeschützt. Ein sauberer Wert sieht etwa so aus: 0xE0888215 mit Sitzungsschlüssel „Present“. Ein Problemfall: 0xA0888205 mit „Missing“. KB5135557 liefert dafür ein PowerShell-Skript. Das Prinzip sieht so aus:

PowerShell: unsignierte NTLM-Verbindungen finden (Prinzip, vollständiges Skript in KB5135557)

```
Get-WinEvent -LogName 'Microsoft-Windows-NTLM/Operational' |
  Where-Object { $_.Id -in 4022, 4023 } |
  ForEach-Object {
    $x = [xml]$_.ToXml()
    $f = ($x.Event.EventData.Data | Where-Object Name -match 'Flags').'#text'
    if ($f -and (([Convert]::ToUInt32($f, 16) -band 0x10) -eq 0)) { $_ }
  } | Select-Object TimeCreated, Id, MachineName, Message
```

Die Feldnamen in den Ereignisdaten können je nach Version leicht abweichen, deshalb im Zweifel das Original aus der KB nehmen. Das Skript läuft am besten wöchentlich auf allen Servern und schreibt nach Client-IP gruppiert in eine Tabelle. Jede IP bekommt einen Besitzer, jeder Besitzer eine Frist.

Schritt 3, bis 31.03.2027 – Sanieren: Firmware aktualisieren, Samba-Clients auf Signierung konfigurieren, Fachanwendungen auf Kerberos umstellen, wo es geht. Wo nichts geht, setzt du auf dem betroffenen Windows-Client **ClientAllowUnsignedNtlm = 1**, mit Ticketnummer und Ablaufdatum. Für Fremdgeräte gibt es diesen Schalter nicht, dort hilft nur Ersatz oder ein eigener, isolierter Server ohne Erzwingung, und das ist eine bewusste Risikoentscheidung der Leitung, nicht der Administration.

Schritt 4, April 2027 – Selbst erzwingen: Sobald das Skript auf einem Server nichts mehr findet, setzt du dort **ServerRequireNtlmSign = 1**. Ein Neustart ist laut Microsoft nicht nötig. Reihenfolge: zuerst ein Pilot-Dateiserver, dann die übrigen Mitgliedsserver, zum Schluss die kritischen Systeme mit der größten Angriffsfläche, aber mit dem saubersten Audit. So kommt der Mai-Patchday als Nicht-Ereignis.

PowerShell: Signierung auf einem Server vorzeitig erzwingen

```
$p = 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0'
New-ItemProperty -Path $p -Name 'ServerRequireNtlmSign' -PropertyType DWord -Value 1 -Force
# Rückweg vor Phase 2: Wert auf 0 setzen
```

Wann	Was	Wer
bis 30.11.2026	November-Updates überall, erweitertes NTLM-Auditing per Gruppenrichtlinie einschalten	Administration
bis 30.11.2026	Ergänzung der IT-Rahmenvereinbarung zum Auditing, Löschfrist festlegen	IT-Leitung, Datenschutz, Betriebs- oder Personalrat
ab 01.12.2026	Wöchentliche Auswertung nach SIGN-Bit, Liste nach Client-IP mit Besitzer	Administration, IT-Sicherheit
bis 18.12.2026	Hersteller von Fachverfahren, Druckern und NAS schriftlich anfragen	IT-Leitung, Einkauf
bis 31.03.2027	Sanierung abschließen, Ausnahmen nur mit Ablaufdatum	Administration
April 2027	ServerRequireNtlmSign = 1 ringweise, Helpdesk vorab informieren	Administration, Helpdesk
Mai 2027	Phase 2 durch Microsoft, Fehlerbild 0x80090302 beobachten	Helpdesk, IT-Sicherheit
bis 11.11.2027	Ausnahmen abbauen, Übergang zur NTLM-Abschaltung planen	IT-Leitung

Tipp: Ausnahmen bekommen ein Verfallsdatum, sonst werden sie Denkmäler

Jede Ausnahme, die ohne Ablaufdatum gesetzt wird, steht in fünf Jahren noch da, und niemand weiß mehr, warum. Trag jede ClientAllowUnsignedNtlm-Ausnahme in dein Risikoregister ein, mit Besitzer, Grund und Datum, an dem sie fällt. Der Wert ist laut Microsoft ausdrücklich nur als Übergangslösung gedacht, und Microsoft kann die Schlüssel jederzeit entfernen. Dann ist die Ausnahme ohnehin weg, nur eben ungeplant an einem Patchday.

Wichtig: Was die Belegschaft wissen muss

Für die meisten Kolleginnen und Kollegen ändert sich nichts, solange du die Hausaufgaben machst. Informiere vor April 2027 trotzdem das Helpdesk: Meldungen wie „Zugriff verweigert“ beim Scannen, bei Netzlaufwerken auf NAS-Systemen oder in alten Fachanwendungen sind ab dann sehr wahrscheinlich NTLM-Signierung, nicht Benutzerfehler. Eine kurze Meldung im Intranet an die betroffenen Abteilungen spart Tickets und die übliche Theorie, die IT habe wieder irgendwas kaputtgemacht. Diesmal hätte sie es ja auch.

Häufig gestellte Fragen

Was ändert sich bei der NTLM-Signierung in Windows ab November 2026?

Mit den Windows-Updates ab dem 10. November 2026 bieten Windows-Clients bei allen nicht anonymen NTLM-Verbindungen echte Nachrichtensignierung an, Server akzeptieren aber weiterhin auch unsignierte Clients. Ab Mai 2027 verlangen Windows-Server die Signierung standardmäßig und weisen Clients ohne Signierung ab.

Wie finde ich Geräte, die keine NTLM-Signierung verwenden?

Aktiviere das erweiterte NTLM-Auditing und werte die Ereignisse 4022 und 4023 im Protokoll Microsoft-Windows-NTLM/Operational aus. Maßgeblich ist, ob in den Negotiated Flags das Bit 0x00000010 (SIGN) gesetzt ist; die Ereignisstufe hilft nicht, weil Microsoft beide Fälle als Warnung protokolliert.

Wie kann ich die NTLM-Signierung vor Mai 2027 erzwingen?

Setze auf dem Server den DWORD-Wert ServerRequireNtlmSign unter HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0 auf 1, ein Neustart ist laut Microsoft nicht nötig. Tu das erst, wenn das Auditing auf diesem Server keine unsignierten Verbindungen mehr zeigt.

Kann ich die NTLM-Signierung für einzelne Clients deaktivieren?

Ja, der Registrierungswert ClientAllowUnsignedNtlm = 1 sorgt dafür, dass ein Windows-Client keine Signierung anbietet. Microsoft beschreibt das nur als vorübergehende Kompatibilitätslösung und behält sich vor, die Schlüssel künftig zu entfernen.

Ist Kerberos von der NTLM-Signierungspflicht betroffen?

Nein, die Änderung betrifft ausschließlich NTLM. Anonyme Verbindungen und Anmeldungen mit dem Gastkonto sind in beiden Phasen ausgenommen.