NTLM-Ablösung als Projekt: Zeitplan, Rollen, Aufwand



Skizze: Phasen eines NTLM-Ablöseprojekts

WISSEN
Was der NTLM Diagnostiker erfasst, wie er arbeitet und was er kostet.
› **NTLM Diagnostiker**

BERATUNG
Projektplanung, Bestandsaufnahme und Abschaltplan mit Begleitung.
› **Beratung zur NTLM-Ablösung**

SCHULUNG
NTLM-Ereignisse lesen, sammeln und bewerten: für dein ganzes Team.
› **Schulung zum NTLM Diagnostiker**

Es gibt IT-Vorhaben, die sich mit einem Ticket erledigen lassen. Und es gibt die NTLM-Ablösung. Sie sieht auf dem Papier aus wie ein Haken in einer Gruppenrichtlinie, fühlt sich in der Praxis aber an wie der Umzug eines Archivs, in dem seit zwanzig Jahren jeder etwas abgestellt hat, das er „nur kurz“ dort lassen wollte. Niemand weiß genau, was in den Kisten ist. Aber alle sind sicher, dass es wichtig ist.

Der Termindruck ist real. Seit dem Windows-Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 Single Sign-on mit NTLMv1-abgeleiteten Anmeldedaten standardmäßig. Mit der nächsten Windows-Server-Version will Microsoft NTLM insgesamt standardmäßig abschalten. Wer jetzt noch „irgendwann mal“ plant, plant in Wahrheit einen Notfall. Die Details zum Zeitplan stehen in NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet; was bei NTLMv1 schon heute nicht mehr geht, in NTLMv1 blockiert: was seit Oktober 2026 nicht mehr geht.

Dieser Beitrag richtet sich an dich als IT-Leitung oder Projektleitung. Es geht nicht um einzelne Ereignis-IDs, sondern um das Gerüst: in welchen Phasen du vorgehst, wie lange das realistisch dauert, wen du an den Tisch holen musst und wo das Geld hinfließt. Kurz: alles, was du brauchst, um dem Management einen Plan vorzulegen, der die erste Rückfrage überlebt.

FAKTEN · Die Rahmenbedingungen für dein Projekt

NTLMv1: Seit dem Update vom 13.10.2026 auf Windows 11 ab 24H2 und Windows Server 2025 für Single Sign-on standardmäßig blockiert (Registrierungswert BlockNtlmv1SSO, Ereignisse 4024 und 4025).

Phase 1 des Microsoft-Fahrplans: erweitertes NTLM-Auditing nach KB5064479 mit den Ereignissen

4020 bis 4023 auf Clients und Servern sowie 4030 bis 4033 auf Domain Controllern. Verfügbar auf Windows 11 ab 24H2, Windows Server 2025 sowie Windows Server 2022 und 2019 mit Updates ab dem 13.10.2026.

Phase 2: IAKerb und lokales KDC schließen technische Lücken, in denen Windows bisher auf NTLM ausweichen musste.

Phase 3: Mit der nächsten Windows-Server-Version ist NTLM standardmäßig abgeschaltet und nur noch per Richtlinie wieder einschaltbar.

Ältere Systeme: Die klassische Restrict-NTLM-Überwachung mit den Ereignissen 8001 bis 8004 funktioniert auch dort, liefert aber keine Ursache.

Warum die NTLM-Ablösung ein Projekt ist und kein Wochenend-Ticket

NTLM ist kein Dienst, den du stoppst. Es ist ein Rückfallverfahren, das immer dann einspringt, wenn Kerberos nicht klappt: weil ein Laufwerk per IP-Adresse verbunden ist, weil ein SPN fehlt oder doppelt vorhanden ist, weil ein lokales Konto im Spiel ist, weil eine Anwendung NTLM direkt aufruft oder weil ein Gerät den Domain Controller schlicht nicht erreicht. Jede dieser Ursachen hat einen anderen Besitzer und einen anderen Lösungsweg. Genau deshalb wird daraus ein Projekt: viele kleine Baustellen, verteilt auf Abteilungen, Hersteller und Wartungsfenster.

Was ein Abschalten ohne Projekt kostet

Natürlich kannst du die Richtlinie „Netzwerksicherheit: NTLM einschränken“ morgen früh auf Verweigern stellen. Das ist die schnellste Form der Bestandsaufnahme: Du erfährst innerhalb von Minuten, wer NTLM benutzt, nämlich über das Telefon. Der Scanner im Erdgeschoss scannt nicht mehr, die Lohnbuchhaltung kommt nicht mehr an ihre Fachanwendung, und der Server, der jede Nacht die Sicherung anstößt, macht ab sofort Urlaub. Die Rücknahme dauert fünf Minuten, das Vertrauen der Fachabteilungen in dein nächstes Vorhaben deutlich länger.

WARNUNG · Der Monatsabschluss ist kein Testfall

Viele NTLM-Anmeldungen passieren selten: Jahresabschluss, Quartalsberichte, Zeugnisdruck, Inventur, das Notfallskript, das nur nach einem Stromausfall läuft. Wer nur eine Woche misst und dann abschaltet, findet diese Fälle garantiert, nur eben zum ungünstigsten Zeitpunkt.

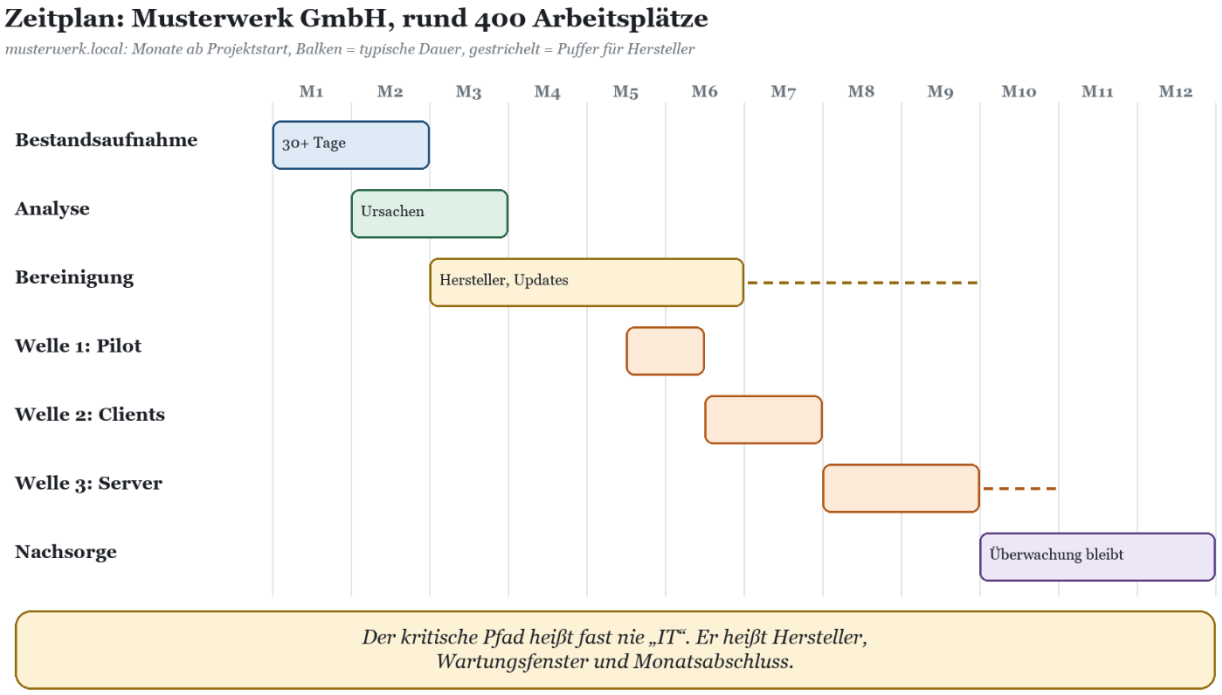
Der Projektauftrag auf einer Seite

Bevor jemand das erste Ereignis sammelt, schreibst du den Auftrag auf. Eine Seite reicht. Sie verhindert, dass das Projekt still zur Daueraufgabe verkommt, die irgendwann niemand mehr verantworten will.

Baustein	Inhalt	Beispiel Musterwerk GmbH
Ziel	Was ist am Ende erreicht?	Kein NTLMv1 mehr, NTLM auf Domänenebene verweigert, dokumentierte Ausnahmen
Umfang	Welche Domänen, Standorte, Systeme?	musterwerk.local, zwei Werke, Produktionsnetz zunächst ausgenommen
Termine	Meilensteine pro Phase	Bestandsaufnahme bis Ende Januar, erste Welle im März
Rollen	Wer entscheidet, wer liefert zu?	IT-Leitung entscheidet, Fachabteilungen testen
Abbruchkriterien	Wann wird eine Welle zurückgenommen?	Ausfall einer kritischen Anwendung länger als 30 Minuten
Nachweis	Woran wird Erfolg gemessen?	Ereigniszahlen, Ausnahmeliste, Abschlussbericht

Die fünf Phasen und ihr realistischer Zeitplan

Das Vorgehen folgt einer einfachen Logik: erst sehen, dann verstehen, dann reparieren, dann abschalten, dann aufpassen. Die Phasen überlappen sich bewusst. Während die Analyse läuft, sammelt die Bestandsaufnahme weiter, und während die ersten Ursachen bereinigt sind, wartest du bei anderen noch auf den Hersteller.



Skizze: Beispielplanung, Firmenname frei erfunden; Phasen überlappen bewusst

Phase 1: Bestandsaufnahme

Ziel der Bestandsaufnahme ist eine vollständige Liste aller NTLM-Anmeldungen: wer, wohin, mit welcher Version und, wo verfügbar, warum. Dazu schaltest du das Auditing ein, sammelst die Ereignisse zentral und gleichst sie mit dem Bestand an Rechnern ab. Wie das technisch geht, steht in Erweitertes NTLM-Auditing einschalten: Schritt für Schritt; ein fertiges Gruppenrichtlinienskript liefert das NTLM-Audit-GPO-Skript.

Die wichtigste Zahl dieser Phase lautet: **mindestens 30 Tage Erfassung**. Besser ist ein voller Monatszyklus inklusive Monatsabschluss, in Branchen mit Quartalsgeschäft auch ein Quartal. Kürzere Messungen liefern eine schöne Statistik über den Normalbetrieb und verpassen genau die Fälle, die später wehtun.

Mit Bordmitteln prüfst du zuerst, ob das NTLM-Protokoll auf einem System groß genug ist und was überhaupt ankommt:

```
# Größe und Zustand des NTLM-Protokolls anzeigen
wevtutil gl Microsoft-Windows-NTLM/Operational

# NTLM-Ereignisse der letzten 30 Tage pro Ereignis-ID zählen
Get-WinEvent -FilterHashtable @{
    LogName   = 'Microsoft-Windows-NTLM/Operational'
    StartTime = (Get-Date).AddDays(-30)
} | Group-Object Id | Sort-Object Count -Descending |
    Select-Object Name, Count
```

Für einen Server funktioniert das gut. Für 400 Arbeitsplätze, 60 Server und vier Domain Controller wird es zur Fleißarbeit: Protokolle rotieren, bevor du sie abholst, manche Rechner sind im Urlaub ausgeschaltet, und die spannendste Frage beantwortet kein Zähler, nämlich welche Systeme gar nichts melden. Wie du die Ereignisse zentral einsammelst, beschreibt NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding; den kompletten Weg durch alle Quellen zeigt NTLM-Nutzung ermitteln: der komplette Leitfaden.

> **WICHTIG · Vor dem Einschalten: Datenschutz und Betriebs- oder Personalrat**
>
> NTLM-Ereignisse enthalten Benutzer- und Rechnernamen, Zeitpunkte und Zielsysteme. Damit lässt sich nachvollziehen, wer wann wo gearbeitet hat. Das ist eine technische Einrichtung, die grundsätzlich geeignet ist, Verhalten oder Leistung zu überwachen. Kläre Zweck, Speicherdauer und Zugriff vorher mit dem Datenschutz und hole den Betriebs- oder Personalrat rechtzeitig ins Boot.
>
> Was dabei konkret zu beachten ist, steht in NTLM-Audit, Datenschutz und Betriebsrat: was du beachten musst.

Phase 2: Analyse

Aus Zehntausenden Ereignissen werden in der Analyse wenige Dutzend Ursachen. Das wichtigste Werkzeug ist die Reason-ID aus den Client-Ereignissen 4020 und 4021, die Windows mit Werten von 0 bis 11 befüllt: von „Anwendung ruft NTLM direkt auf“ über „Ziel enthält eine IP-Adresse“ bis „keine Sichtverbindung zum Domain Controller“. Was die einzelnen Werte bedeuten, erklärt NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat. Microsoft beschreibt die Ereignisse im Supportartikel Overview of NTLM auditing enhancements in Windows 11 and Windows Server 2025.

Ergebnis der Analyse ist eine Ursachenliste mit Besitzern. Jede Zeile hat eine Quelle, ein Ziel, eine Ursache, eine verantwortliche Person und eine geschätzte Lösung. Ohne Besitzer bleibt jede Zeile ewig offen. Mit Bordmitteln heißt das: Ereignisse exportieren, nach Quelle und Ziel gruppieren, Ursachen per setspn und nslookup prüfen und in einer Tabelle sammeln. Bei elf Ursachen ist das ein Nachmittag, bei 1.600 Paaren aus Quelle und Ziel ein Quartal.

```
# Doppelte SPNs in der Gesamtstruktur suchen (Reason-ID 8)
setspn -X -F

# SPNs eines Dienstkontos anzeigen
setspn -L MUSTERWERK\svc-erp
```

Phase 3: Bereinigung

Die Bereinigung ist der größte Block und der am schwersten planbare. Ein fehlender DNS-Eintrag ist in fünf Minuten angelegt, ein Laufwerksskript mit IP-Adressen an einem Vormittag umgestellt. Eine Fachanwendung, die NTLM fest eingebaut hat, braucht dagegen ein Update des Herstellers, und dessen Zeitplan richtet sich nicht nach deinem. Wie du die richtigen Fragen stellst, damit nicht nur „Wir prüfen das“ zurückkommt, zeigt Wenn die Anwendung NTLM fest eingebaut hat: Hersteller richtig fragen. Typische weitere Baustellen sind Dienstkonten als NTLM-Quelle: finden, prüfen, umstellen und NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll.

Ursache	Typische Lösung	Aufwand	Abhängig von
Zugriff per IP-Adresse	Pfade, Skripte, Laufwerke auf DNS-Namen umstellen	gering	IT
Fehlender oder doppelter SPN	SPN setzen oder bereinigen	gering	IT, ggf. Hersteller

Lokale Konten	Domänenkonto oder verwaltetes Dienstkonto	mittel	IT, Fachabteilung
Anwendung ruft NTLM direkt	Update, Konfiguration, Austausch	hoch	Hersteller
Keine Sichtverbindung zum DC	Netz, Firewall, später IAKerb	mittel	Netzwerk, Phase 2
Geräte ohne Kerberos	Firmware, Austausch, Ausnahme	mittel bis hoch	Hersteller, Budget

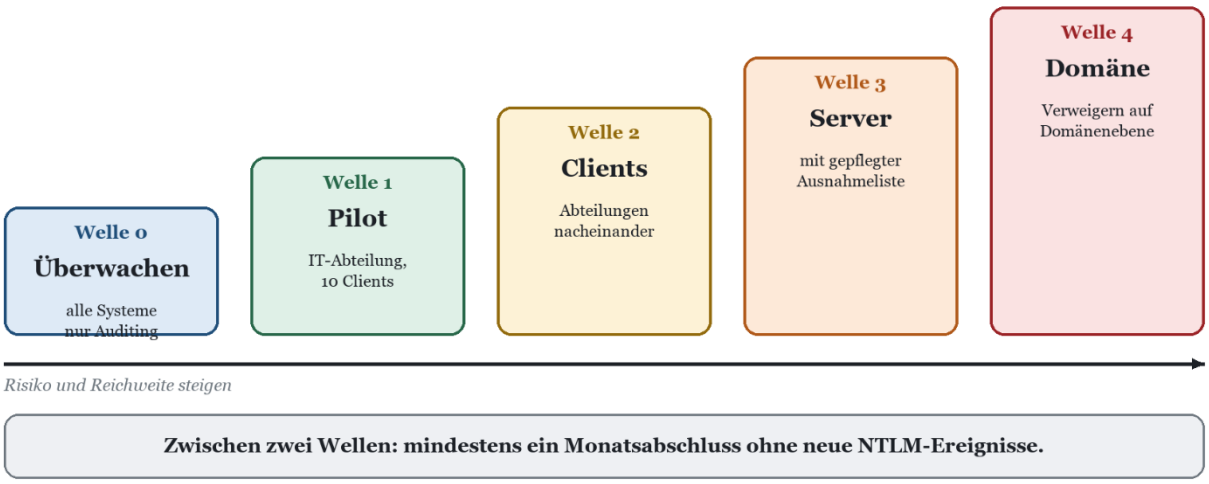
Manches erledigt Microsoft für dich, aber nicht alles: IAKerb und das lokale KDC aus Phase 2 helfen bei fehlender Sichtverbindung zum Domain Controller und bei lokalen Konten, nicht bei deinen Altlasten. Mehr dazu in Keine Sichtverbindung zum DC: Reason-ID 9, IAKerb und lokales KDC. Wer bei der Bereinigung tiefer in Kerberos einsteigen muss, findet das Fundament im Kompetenzbereich Microsoft Kerberos.

Phase 4: Abschaltung in Wellen

Abgeschaltet wird nicht auf einen Schlag, sondern in Wellen: erst ein Pilot, dann Gruppen von Clients, dann Server mit gepflegter Ausnahmeliste, zuletzt die Domäne. Jede Welle hat ein Ziel, ein Wartungsfenster, einen Ansprechpartner in der Fachabteilung und einen dokumentierten Rückweg. Das klingt bürokratisch, ist aber der Unterschied zwischen „kurz zurückgenommen“ und „ganzer Tag Krisenstab“.

Abschaltung in Wellen

Trendforge Digital GmbH, trendforge.local: jede Welle hat ein Ziel, ein Fenster und einen Rückweg



Skizze: Wellenplan nach Restrict-NTLM-Richtlinien; Firmenname frei erfunden

Technisch arbeitest du dabei mit den Restrict-NTLM-Richtlinien und deren Ausnahmelisten. Wie du die Wellen konkret schneidest, beschreibt NTLM schrittweise abschalten, ohne dass etwas ausfällt; wie Ausnahmen gepflegt bleiben, statt zu wuchern, steht in Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren.

TIPP · Rückweg vorher testen

Leg für jede Welle fest, wer die Richtlinie zurücknehmen darf, wie lange das bis zur Wirkung dauert und wie du das prüfst. Ein Rückweg, den niemand ausprobiert hat, ist eine Hoffnung, kein Plan.

Phase 5: Nachsorge

Nach der letzten Welle ist das Projekt vorbei, das Thema nicht. Neue Software, neue Geräte und neue Dienstleister bringen NTLM gern wieder mit, als Gastgeschenk. Das Auditing bleibt deshalb an, neue Ereignisse landen in einem festen Prüfprozess, und die Ausnahmeliste bekommt ein Ablaufdatum pro Eintrag. Wer das nicht tut, steht in zwei Jahren wieder am Anfang, nur mit weniger Geduld der Geschäftsführung.

Wie lange das wirklich dauert

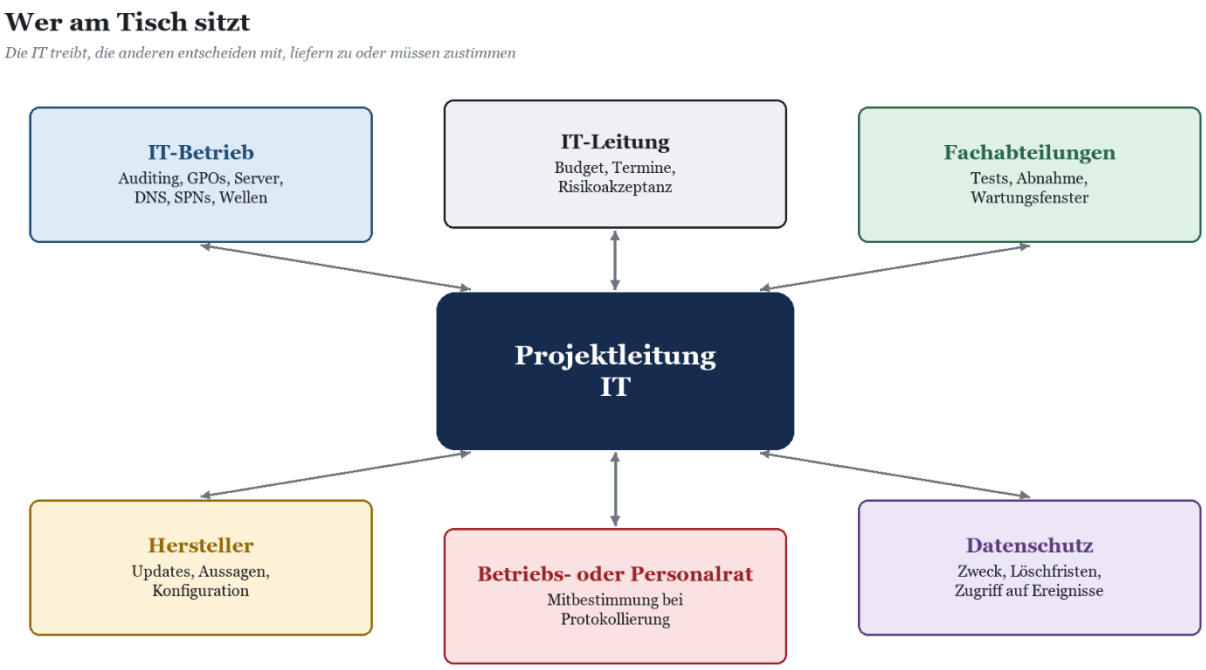
Die ehrliche Antwort lautet: Es hängt weniger an der Größe der Umgebung als an der Zahl der Hersteller, die etwas liefern müssen. Die folgenden Werte sind Erfahrungswerte für Umgebungen ohne größere Überraschungen. Überraschungen gibt es trotzdem.

Phase	Kleine Umgebung (bis 100 PCs)	Mittelstand (100 bis 1.000)	Klinik oder Verwaltung
Bestandsaufnahme	30 Tage	30 bis 60 Tage	60 bis 90 Tage
Analyse	1 bis 2 Wochen	4 bis 8 Wochen	2 bis 4 Monate
Bereinigung	1 bis 2 Monate	2 bis 6 Monate	6 bis 12 Monate
Abschaltung in Wellen	2 bis 4 Wochen	2 bis 3 Monate	3 bis 6 Monate
Nachsorge	dauerhaft	dauerhaft	dauerhaft
Gesamt bis Domäne	rund 3 bis 4 Monate	rund 6 bis 12 Monate	rund 12 bis 18 Monate

Kliniken und Verwaltungen liegen nicht deshalb hinten, weil dort langsamer gearbeitet wird, sondern wegen Medizintechnik mit Zulassung, Fachverfahren mit Landeslizenz und Wartungsfenstern, die es im 24-Stunden-Betrieb kaum gibt. Die Besonderheiten im Krankenhaus behandelt NTLM in der Klinik: Medizintechnik, Labor und Fachanwendungen.

Rollen: wer was tut und wer es nur glaubt

Ein NTLM-Projekt, das nur in der IT stattfindet, scheitert nicht an der Technik, sondern am Kalender der anderen. Die Fachabteilung hat gerade Inventur, der Hersteller einen neuen Ansprechpartner, und der Betriebsrat erfährt aus dem Flurfunk, dass „die IT jetzt alle Anmeldungen mitschreibt“. Das lässt sich vermeiden, wenn alle Beteiligten von Anfang an wissen, was von ihnen erwartet wird.



Skizze: Rollen im NTLM-Ablöseprojekt; Betriebs- oder Personalrat vor dem Einschalten der Protokollierung

Rolle	Aufgabe im Projekt	Wann gebraucht	Typischer Stolperstein
IT-Leitung	Auftrag, Budget, Risikoakzeptanz für Ausnahmen	Start, jede Welle	Ausnahmen ohne Ablaufdatum abnicken
Projektleitung IT	Plan, Ursachenliste, Kommunikation	durchgehend	Projekt nebenbei führen
IT-Betrieb	Auditing, Sammeln, SPN, DNS, Richtlinien	durchgehend	Ereignisse sammeln, aber nicht auswerten
Fachabteilungen	Anwendungen benennen, testen, abnehmen	Analyse, Wellen	„Bei uns läuft nichts Besonderes“
Hersteller	Aussagen zu NTLM, Updates, Konfiguration	Bereinigung	Antwort erst nach dem Stichtag
Datenschutz	Zweck, Speicherdauer, Zugriffsrechte	vor Phase 1	zu spät gefragt
Betriebs- oder Personalrat	Mitbestimmung bei der Protokollierung	vor Phase 1	aus dem Flurfunk informiert

Die Fachabteilungen: Kronzeugen wider Willen

Fachabteilungen wissen selten, dass sie NTLM benutzen, aber sie wissen sehr genau, welche Anwendung wann laufen muss. Diesen Schatz hebst du nicht mit einer Rundmail, sondern mit einer Liste aus der Bestandsaufnahme: „Euer Rechner in der Lohnbuchhaltung meldet sich jeden Monat am Dritten per NTLM an einem Server an, was passiert da?“ Konkrete Fragen bekommen konkrete Antworten. Allgemeine Fragen bekommen „Das muss so“.

Hersteller: der kritische Pfad

Plane die Herstelleranfragen so früh wie möglich, idealerweise direkt nach den ersten Analyseergebnissen. Frag schriftlich, frag konkret nach Kerberos-Unterstützung und frag nach

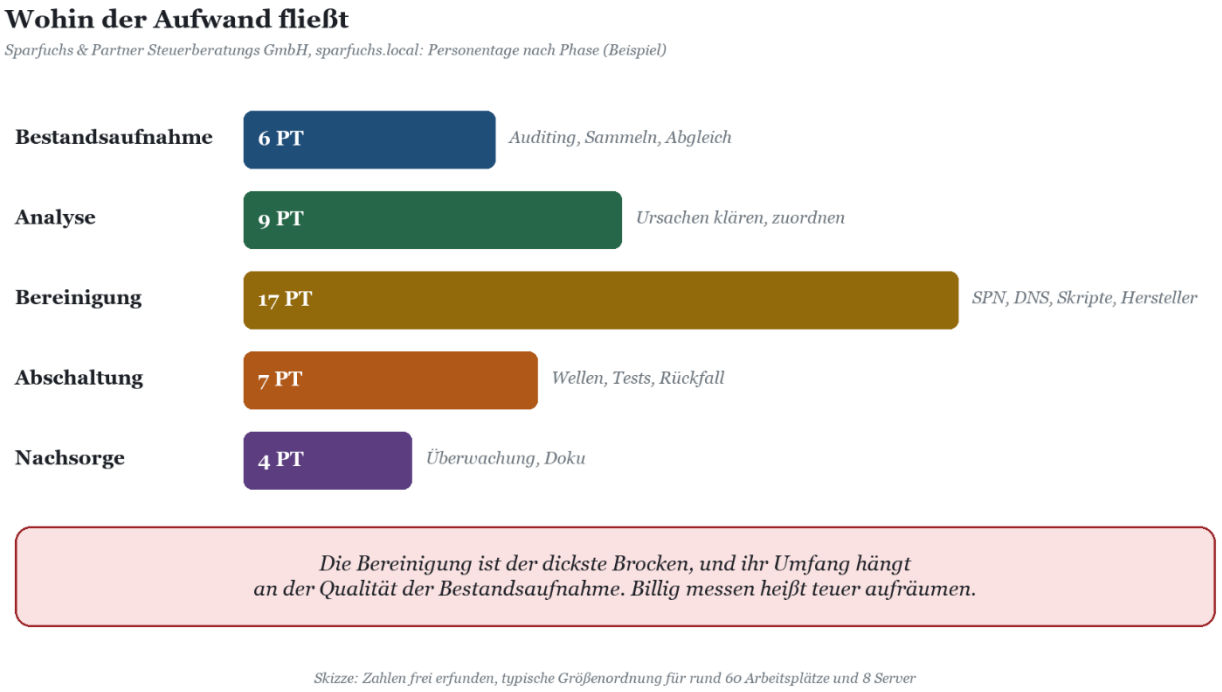
einem Termin. Erfahrungsgemäß liegen zwischen Anfrage und brauchbarer Antwort Wochen, zwischen Antwort und eingespieltem Update oft Monate. Das ist kein Grund zur Verzweiflung, sondern ein Grund, die Bereinigung mit Puffer zu planen.

AUS DER PRAXIS · Sparfuchs & Partner Steuerberatungs GmbH

Die Bestandsaufnahme bei sparfuchs.local war nach 30 Tagen fertig, die Analyse nach zwei weiteren Wochen. 80 Prozent der Ursachen waren nach einem Monat bereinigt: IP-Adressen in Anmeldeskripten, zwei doppelte SPNs, ein vergessenes lokales Konto auf dem Scan-Server. Die restlichen 20 Prozent hingen an einer einzigen Fachanwendung. Deren Hersteller brauchte vier Monate. Das Projekt dauerte deshalb nicht sechs Wochen, sondern sechs Monate.

Aufwand und Kostentreiber

Die Frage „Was kostet das?“ beantwortest du am besten mit Personentagen statt mit Lizenzpreisen. Der größte Posten ist Arbeitszeit: die eigene, die der Fachabteilungen und gegebenenfalls die externer Unterstützung. Werkzeuge sind im Vergleich dazu ein kleiner Posten, können aber den großen Posten deutlich verkleinern.



Skizze: Zahlen frei erfunden, typische Größenordnung für rund 60 Arbeitsplätze und 8 Server

Die typischen Kostentreiber

Kostentreiber	Warum er teuer wird	Was dagegen hilft
Zahl der Anwendungen und Hersteller	Jeder Hersteller ist ein eigenes Teilprojekt	früh fragen, schriftlich, mit Termin
Unvollständige Bestandsaufnahme	Fehlende Fälle tauchen erst bei der Abschaltung auf	mindestens 30 Tage, Abgleich mit dem Bestand
Alte Betriebssysteme	Kein erweitertes Auditing, keine Reason-ID	Updates einspielen oder 8001 bis 8004 nutzen
Geräte ohne Ereignisprotokoll	NAS, Drucker, Scanner sieht man nur indirekt	Serverseite auswerten, Netzwerkmitschnitt
Manuelle Auswertung	Tausende Ereignisse, Hunderte	zentral sammeln und automatisch

	Maschinen	verdichten
Fehlende Rollenklärung	Ursachen ohne Besitzer bleiben offen	Ursachenliste mit Verantwortlichen
Ausfälle bei der Abschaltung	Krisenstab statt Wartungsfenster	Wellen mit getestetem Rückweg

Wo Bordmittel aufhören, Spaß zu machen

Alles, was du für die Bestandsaufnahme brauchst, steckt in Windows: Ereignisanzeige, PowerShell, wevtutil, setspn, Gruppenrichtlinien. Das reicht für eine kleine Umgebung und für die Einzelfallanalyse. Mühsam wird es bei vier Dingen: der Menge der Ereignisse, der Zahl der Maschinen, den stillen Geräten, die gar nichts melden, und der Ursache, die du für jedes Paar aus Quelle und Ziel einzeln nachprüfen musst. Dann sitzt der IT-Betrieb wochenlang vor Excel-Tabellen, und genau das ist der teuerste Teil der Rechnung. Einen sachlichen Vergleich der Möglichkeiten findest du in NTLM-Analyse im Vergleich: Bordmittel, Skripte und NTLM Diagnostiker.

Für diesen Teil haben wir den NTLM Diagnostiker gebaut. Er sammelt die NTLM-Ereignisse wahlweise direkt vom Domain Controller, über einen Windows Event Collector oder per Direktabfrage, verdichtet sie und ordnet jeder Verbindung eine Ursache zu. Für das Projekt ist vor allem wichtig, dass er ausschließlich lesend arbeitet: Er ändert keine Richtlinie, keinen SPN und keinen DNS-Eintrag. Damit passt er auch in Umgebungen, in denen jede Änderung durch ein Change-Board muss.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Bestandsaufnahme und Nachweis im Projekt

Readiness-Ampel: zeigt auf einen Blick, wie weit die Umgebung von einer Abschaltung entfernt ist. Das ist die Folie für den Lenkungsausschuss.

Abdeckungsmonitor und OS-Landkarte: zeigen, welche Rechner Ereignisse liefern, welche schweigen und auf welchen Systemen erweitertes Auditing überhaupt möglich ist.

Ursachen-Engine mit SPN- und DNS-Prüfung: macht aus Ereignissen Ursachen, also aus Phase 1 direkt die Arbeitsliste für Phase 3.

NTLMv1-Hitliste: priorisiert das, was seit Oktober 2026 ohnehin brennt.

Kommunikationsmatrix und Konten-Sicht: zeigen, wer mit wem per NTLM spricht und welche Konten beteiligt sind. Sicherheitsflaggen markieren auffällige Verbindungen.

Abschalt-Simulation: zeigt vor einer Welle, was mit verweigertem NTLM nicht mehr funktionieren würde.

Wireshark-Import: holt Geräte ohne Ereignisprotokoll aus Netzwerkmitschnitten in dieselbe Sicht.

Word-Bericht sowie Excel- und CSV-Export: liefern den Nachweis für Management, Revision und Abschlussdokumentation.

Zum Einstieg gibt es die kostenlose Edition Express mit einem Fünf-Minuten-Befund und einen Testzeitraum von 7 Tagen. Lizenziert wird pro aktivem Computerkonto, also nach der Größe der Umgebung, die du im Projekt tatsächlich bearbeitest.

Geplant sind außerdem ein Anwendungskatalog, ein Ausnahmelisten- und Skript-Generator, ein Phasenplan, ein Kerberos-Gegencheck und ein Verlauf. Diese Funktionen gibt es derzeit noch nicht.

Lizenz und Projektbudget

Weil der Diagnostiker pro aktivem Computerkonto lizenziert wird, lässt sich der Posten früh beziffern. Für eine erste Größenordnung reicht ein Blick ins Active Directory:

```
# Aktivierte Computerkonten mit Anmeldung in den letzten 90 Tagen zählen
$grenze = (Get-Date).AddDays(-90)
Get-ADComputer -Filter 'Enabled -eq $true' -Properties LastLogonTimestamp |
    Where-Object { [DateTime]::FromFileTime($_.LastLogonTimestamp) -gt $grenze } |
    Measure-Object
```

Nebenbei bekommst du damit die erste Kennzahl für den Abdeckungsabgleich: So viele Rechner sollten im Laufe der Bestandsaufnahme mindestens einmal auftauchen oder bewusst als „ohne NTLM“ bestätigt werden.

Interne Kräfte, Beratung oder beides

Viele Häuser haben das Wissen im Team, aber nicht die Zeit. Andere haben die Zeit, aber noch nie eine NTLM-Bestandsaufnahme gemacht. Eine bewährte Aufteilung: Planung, Bestandsaufnahme und Analyse mit externer Begleitung, Bereinigung und Wellen weitgehend intern, mit Unterstützung bei den schwierigen Fällen. Wie wir dich dabei begleiten, von der Projektplanung über die Auswertung bis zum Abschaltplan, beschreibt die Beratung zur NTLM-Ablösung. Wenn dein Team die Auswertung selbst übernehmen soll, ist die Schulung zum NTLM Diagnostiker der passende Einstieg. Systemhäuser, die das Vorgehen bei vielen Kunden wiederholen wollen, finden ihr Modell in NTLM-Ablösung im Systemhaus: viele Kunden, ein Vorgehen.

TIPP · Die Kosten-Folie für das Management

Stell drei Zahlen gegenüber: Personentage mit manueller Auswertung, Personentage mit Werkzeug und Begleitung, und die geschätzten Kosten eines ungeplanten Ausfalls einer kritischen Anwendung für einen Tag. Die dritte Zahl beendet die Diskussion meistens.

Projektsteuerung: Kennzahlen und Nachweis

Ein Lenkungsausschuss will keine Ereignis-IDs sehen, sondern Fortschritt. Leg deshalb von Anfang an wenige Kennzahlen fest und berichte sie in festen Abständen. Das schützt auch dich: Wenn ein Hersteller blockiert, steht das schwarz auf weiß im Bericht und nicht nur in deinem Kopf.

Kennzahl	Aussage	Zielwert vor der Abschaltung
Abdeckung	Anteil der Rechner, die Ereignisse liefern oder geprüft sind	nahe 100 Prozent
NTLMv1-Quellen	Systeme, die noch NTLMv1 verwenden	null
Offene Ursachen	Ursachen ohne Lösung	nur dokumentierte Ausnahmen
Ausnahmen	Einträge in Ausnahmelisten, jeweils mit Besitzer und Ablaufdatum	so wenige wie möglich
NTLM-Ereignisse pro Tag	Trend über die Projektlaufzeit	stetig fallend

FAKTEN · Was in den Abschlussbericht gehört

Umfang und Zeitraum der Bestandsaufnahme, Liste der Ursachen mit Lösung, verbleibende Ausnahmen mit Begründung und Ablaufdatum, Ergebnisse jeder Welle, Vereinbarungen mit Datenschutz und Betriebs- oder Personalrat sowie der Prozess für die Nachsorge. Damit hast du für Revision, Versicherung und Wirtschaftsprüfung einen sauberen Nachweis.

FAQ zur NTLM-Ablösung als Projekt

Wie lange muss die Bestandsaufnahme mindestens laufen?

Mindestens 30 Tage, besser ein voller Monatszyklus mit Monatsabschluss. Wo Quartals- oder Jahresprozesse wichtig sind, lohnt sich ein längerer Zeitraum oder eine gezielte Prüfung dieser Prozesse.

Können wir nicht einfach auf die nächste Windows-Server-Version warten?

Kannst du, aber dann beginnt dein Projekt unter Zeitdruck. NTLMv1 ist für Single Sign-on schon heute standardmäßig blockiert, und die Ursachen, die in Phase 3 auffallen, sind dieselben, die du jetzt in Ruhe finden könntest.

Wer muss vor dem Einschalten des Auditings zustimmen?

Kläre den Zweck mit dem Datenschutz und beteilige den Betriebs- oder Personalrat, bevor die Protokollierung startet. Details stehen in NTLM-Audit, Datenschutz und Betriebsrat: was du beachten musst.

Was ist der größte Kostentreiber?

In fast allen Projekten die Bereinigung, und dort die Abhängigkeit von Herstellern. Der zweitgrößte ist eine unvollständige Bestandsaufnahme, weil sie die Kosten in die Abschaltung verschiebt.

Hilft Phase 2 von Microsoft nicht ohnehin?

Teilweise. IAKerb und das lokale KDC helfen bei fehlender Sichtverbindung zum Domain Controller und bei lokalen Konten. Gegen IP-Adressen in Skripten, fehlende SPNs und Anwendungen, die NTLM direkt aufrufen, helfen sie nicht.

Ändert der NTLM Diagnostiker etwas an unserer Umgebung?

Nein. Er arbeitet ausschließlich lesend. Änderungen an Richtlinien, SPNs oder DNS nimmst du selbst vor, so wie es dein Change-Prozess vorsieht.

Brauchen wir externe Unterstützung?

Nicht zwingend. Sinnvoll ist sie vor allem bei Planung, Bestandsaufnahme und Analyse, weil dort Erfahrung am meisten Zeit spart. Ansprechpartner findest du über die Beratung zur NTLM-Ablösung.

Fazit: Erst der Plan, dann die Richtlinie

Die NTLM-Ablösung ist kein technisches Kunststück, sondern ein Organisationsprojekt mit technischem Kern. Fünf Phasen, mindestens 30 Tage Erfassung, eine Ursachenliste mit Besitzern, Hersteller auf dem kritischen Pfad, Datenschutz und Betriebs- oder Personalrat von Anfang an dabei und eine Abschaltung in Wellen mit getestetem Rückweg: Mit diesem Gerüst kommst du in sechs bis achtzehn Monaten ans Ziel, je nach Umgebung und Herstellerlage.

Ohne dieses Gerüst kommst du auch ans Ziel. Nur heißt das Ziel dann nicht „NTLM ist aus“, sondern „NTLM ist wieder an, und wir reden nächstes Jahr noch einmal darüber“. Fang mit der Bestandsaufnahme an, solange der Stichtag noch eine Zahl im Kalender ist und kein Anruf aus der Buchhaltung.

WEITERLESEN · Weiter in dieser Serie

› NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet

› NTLM-Nutzung ermitteln: der komplette Leitfaden

› Erweitertes NTLM-Auditing einschalten: Schritt für Schritt
› NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat
› Wenn die Anwendung NTLM fest eingebaut hat: Hersteller richtig fragen
› NTLM schrittweise abschalten, ohne dass etwas ausfällt
› Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren
› NTLM-Audit, Datenschutz und Betriebsrat: was du beachten musst
› Beratung zur NTLM-Ablösung