NTLM in der Klinik: Medizintechnik, Labor und Fachanwendungen



WISSEN
Wie der NTLM Diagnostiker rein lesend zeigt, welche Geräte und Anwendungen in deiner Klinik noch NTLM sprechen.
› **NTLM Diagnostiker**

BERATUNG
Messung, Herstellerabstimmung und Wellenplan für Medizintechnik, Labor und KIS gemeinsam aufsetzen.
› **Beratung zur NTLM-Ablösung**

SCHULUNG
Ereignisse, Reason IDs und Mitschnitte so lesen, dass dein Team die Befunde selbst bewertet.
› **Schulung zum NTLM Diagnostiker**

In einem Krankenhaus stirbt Technik selten. Sie wird alt, bekommt einen Aufkleber „Nicht ausschalten!“, wandert in einen Nebenraum und läuft dort weiter, bis der Hersteller insolvent ist oder das Gebäude abgerissen wird. Das Röntgengerät mit Windows 7 Embedded, der Laborautomat, der seine Ergebnisse per IP-Adresse auf eine Freigabe schreibt, die Schnittstelle zum KIS, die irgendwann 2014 jemand mit einem Dienstkonto namens „svc_hl7_alt“ eingerichtet hat: Sie alle sprechen NTLM. Und sie alle sind wichtiger als dein Wartungsfenster.

Gleichzeitig zieht Microsoft das Tempo an. 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 sichtbar in den Ereignissen 4024 und 4025. Phase 2 bringt IAKerb und ein lokales KDC, und mit der nächsten Windows-Server-Version ist NTLM standardmäßig abgeschaltet. Was das im Einzelnen heißt, steht in NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet und in NTLMv1 blockiert: was seit Oktober 2026 nicht mehr geht.

Dieser Beitrag ist für Administratoren, Medizintechnikerinnen und Medizintechniker sowie IT-Leitungen in Kliniken. Er erklärt, warum ausgerechnet dein Haus so viele NTLM-Altlasten hat, welche Rolle Hersteller und Zulassung spielen, wie du abschaltest, ohne dass auf Station etwas stehen bleibt, und was das alles mit Informationssicherheit und KRITIS zu tun hat. Ohne Paragraphenreiterei, versprochen.

FAKTEN · NTLM im Krankenhaus: die Lage auf einen Blick

NTLMv1 ist seit dem Update vom 13.10.2026 auf Windows 11 ab 24H2 und Windows Server 2025 für Single Sign-on standardmäßig blockiert (BlockNtlmv1SSO, Ereignisse 4024 und 4025). Alte Medizintechnik ist die wahrscheinlichste Quelle für NTLMv1 in deinem Netz.

Das erweiterte NTLM-Auditing nach Microsoft KB5064479 liefert die Ereignisse 4020 bis 4023 auf Clients und Servern und 4030 bis 4033 auf Domänencontrollern, jeweils mit einer Reason ID von 0 bis 11. Es läuft ab Windows 11 24H2 und Windows Server 2025 sowie auf Windows Server 2022 und 2019 mit den Updates ab 13.10.2026.

Ältere Systeme liefern nur die klassischen Restrict-NTLM-Ereignisse 8001 bis 8004, ohne Ursache. Medizingeräte mit eingebettetem Windows liefern oft gar nichts, was du je zu sehen bekommst.

Mit der nächsten Windows-Server-Version ist NTLM standardmäßig abgeschaltet. Die Zulassungszyklen deiner Medizintechnik richten sich nicht nach diesem Termin.

Warum Kliniken besonders viele NTLM-Altlasten haben

Ein mittelständischer Maschinenbauer hat vielleicht fünf Systeme, bei denen er nicht selbst schrauben darf. Ein Krankenhaus der Regelversorgung hat davon schnell ein paar hundert. Der Grund ist nicht Nachlässigkeit, sondern Struktur: Medizintechnik, Labor und klinische Fachanwendungen leben in Zyklen, die mit Windows-Versionen nichts zu tun haben.



Skizze: Schichten der Kliniklandschaft nach Änderbarkeit, vereinfacht

Medizingeräte mit langer Zulassung

Ein Medizinprodukt wird mit einer bestimmten Software-Konfiguration bewertet und in Verkehr gebracht. Ändert jemand diese Konfiguration, steht schnell die Frage im Raum, ob das Gerät noch so betrieben wird, wie der Hersteller es vorgesehen hat. Deshalb installiert niemand mal eben ein Sicherheitsupdate auf dem Steuerrechner eines CT oder stellt am Monitoring-Server die Authentifizierung um. Die Geräte laufen zehn, fünfzehn Jahre. Das Windows darin ist bei Auslieferung oft schon nicht mehr taufrisch.

Für NTLM heißt das: Viele dieser Geräte schreiben Bilder, Protokolle oder Exporte auf Windows-Freigaben, und sie tun das mit dem Authentifizierungsverfahren, das zum Zeitpunkt der Zulassung eingebaut war. Häufig mit einem lokalen Konto, häufig per IP-Adresse, manchmal mit NTLMv1. Kerberos ist bei diesen Geräten kein Konfigurationsschalter, sondern ein Wunschzettel.

Laborsysteme und Analysegeräte

Im Labor sitzt eine eigene Welt: Analysegeräte mit eingebettetem Windows, eine Middleware, die Aufträge verteilt und Ergebnisse einsammelt, und ein Laborinformationssystem, das am KIS hängt. Ergebnisdateien wandern oft über Dateifreigaben von Station zu Station. Die Middleware greift mit einem Dienstkonto zu, das Analysegerät mit einem lokalen Konto, und beide adressieren das Ziel so, wie der Techniker es bei der Installation eingetippt hat, also gern als IP-Adresse.

KIS-Schnittstellen und Kommunikationsserver

Das Krankenhausinformationssystem ist selten ein einzelnes Programm, sondern ein Geflecht aus Client, Anwendungsserver, Datenbank, Kommunikationsserver und Dutzenden Schnittstellen zu Labor, Radiologie, Abrechnung und Pflegedokumentation. Viele davon laufen unter Dienstkonten, deren Passwort seit Jahren niemand anfasst, weil niemand weiß, wo es überall hinterlegt ist. Wo Webanwendungen im Spiel sind, ist NTLM oft fest als Anmeldeverfahren eingestellt statt Negotiate. Wie du solche Konten aufspürst, beschreibt Dienstkonten als NTLM-Quelle: finden, prüfen, umstellen.

Befundablagen per IP-Adresse

Der Klassiker: Ein Gerät exportiert Befunde nach \\10.20.30.40\befunde. Eine IP-Adresse hat keinen Service Principal Name, also kann der Client kein Kerberos-Ticket anfordern und fällt auf NTLM zurück. In der Büro-IT ist das ein Fall für Suchen und Ersetzen. In der Medizintechnik steht der Pfad in einer Gerätekonfiguration, die nur der Servicetechniker des Herstellers ändern darf, der nächste Woche kommt, vielleicht. Die Technik dahinter erklärt NTLM wegen IP-Adresse: Laufwerke und Skripte auf DNS-Namen umstellen.

Systemklasse	Typischer NTLM-Grund	Wer darf ändern?	Realistische Lösung
Büro-IT, Verwaltung	IP-Adresse, fehlender SPN, Alias	IT selbst	Ursache beheben
KIS-Client und -Server	Dienstkonto ohne SPN, NTLM fest konfiguriert	IT mit Hersteller	Konfiguration, Update
Kommunikationsserver	Dienstkonten, Freigaben per IP	IT mit Hersteller	SPN, DNS-Namen, gMSA wo unterstützt
Labor-Middleware	lokale Konten, IP-Pfade	Hersteller, Laborleitung	Update, Ausnahme befristet
Analysegeräte	eingebettetes Windows, NTLMv1 möglich	nur Hersteller	Segment plus Ausnahme
Modalitäten, Monitoring	Firmware ohne Kerberos	nur Hersteller	Segment, Ausnahme, Gerätetausch im Investitionsplan

WICHTIG · Das Problem ist selten das Gerät, sondern der Server dahinter

Medizingeräte selbst sind meist Clients. Die NTLM-Anmeldung landet auf deinem Befund- oder Dateiserver und wird am Domänencontroller geprüft, sofern ein Domänenkonto im Spiel ist. Genau dort, auf Windows-Systemen, die du verwaltest, entstehen die Ereignisse. Das ist die gute Nachricht: Du musst das Gerät nicht anfassen, um zu sehen, was es tut.

Hersteller und Zulassung: wer was ändern darf

In der Büro-IT bist du der Chef. In der Medizintechnik bist du bestenfalls Gast. Die Verantwortung für das Medizinprodukt teilen sich Hersteller und Betreiber, und die Medizintechnik im Haus achtet zu Recht darauf, dass niemand diese Aufteilung durch eine spontane Gruppenrichtlinie durcheinanderbringt. Für die NTLM-Ablösung heißt das: Ohne die Medizintechnik am Tisch planst du an der Realität vorbei.

Die richtigen Fragen an den Hersteller

„Unterstützen Sie Kerberos?“ ist eine schlechte Frage, weil die Antwort fast immer „ja“ lautet und nichts bedeutet. Besser sind konkrete Fragen, die sich auf deine Messung beziehen. Eine ausführliche Vorlage findest du in Wenn die Anwendung NTLM fest eingebaut hat: Hersteller richtig fragen.

Frage an den Hersteller	Warum sie wichtig ist
Welches Authentifizierungsverfahren nutzt das Gerät für den Zugriff auf Windows-Freigaben?	Trennt Negotiate mit Kerberos-Fähigkeit von fest eingebautem NTLM.
Unterstützt das Gerät NTLMv2, und ist NTLMv1 abschaltbar?	NTLMv1 ist seit Oktober 2026 für Single Sign-on blockiert; hier droht der erste Ausfall.
Kann das Ziel als DNS-Name statt als IP-Adresse eingetragen werden?	Oft die schnellste Umstellung, wenn das Gerät Kerberos grundsätzlich kann.
Ist die Änderung durch die Zweckbestimmung gedeckt, oder braucht es ein Update?	Klärt, ob der Servicetechniker es vor Ort darf oder ob ein Release nötig ist.
Gibt es eine Version mit Kerberos-Unterstützung, und ab wann?	Liefert das Ablaufdatum für deine Ausnahme.
Welche Konten nutzt das Gerät, lokal oder in der Domäne?	Lokale Konten führen zwingend zu NTLM, egal wie gut dein DNS ist.

Lokale Konten sind in der Medizintechnik besonders verbreitet. Warum sie Kerberos grundsätzlich ausschließen und wie du sie im Protokoll erkennst, erklärt Lokale Konten und NTLM: Dienste, Aufgaben und Altlasten finden.

WARNUNG · Nicht am Medizinprodukt herumkonfigurieren

Kein Registrierungswert, kein Gruppenrichtlinien-Objekt, kein Agent auf einem Gerät, das als Medizinprodukt betrieben wird, ohne Abstimmung mit Hersteller und Medizintechnik. Wenn dein Sicherheitsupdate das Gerät außerhalb seiner Zweckbestimmung betreibt, hast du ein Problem geschaffen, das größer ist als NTLM. Steht ein solches Gerät in der Domäne und in einer OU mit allgemeinen Härtungs-GPOs, nimm es heraus, bevor du dort irgendetwas verschärfst.

AUS DER PRAXIS · Das Klinikum, das nicht Klinikum heißen darf

Ein Haus der Regelversorgung, im Folgenden Klinikum Musterstadt mit der Domäne klinikum-musterstadt.local, hatte das erweiterte Auditing auf den Servern aktiviert. Nach drei Wochen standen 41 Quellen auf der Liste, die NTLM zum Befundserver sprachen. Die IT hatte mit acht gerechnet. 26 davon waren Arbeitsplätze mit einem Laufwerk per IP-Adresse, in einer Woche erledigt. Neun waren Ultraschallgeräte zweier Baureihen, sechs Laborgeräte. Für die Ultraschallgeräte lieferte der Hersteller ein Update mit DNS-Namen-Unterstützung, für die Laborgeräte gab es eine befristete Ausnahme im eigenen Segment. Niemand auf Station hat davon etwas gemerkt. So soll es sein.

Erst messen: was Bordmittel zeigen und wo es eng wird

Bevor irgendetwas abgeschaltet wird, brauchst du ein Bild: Wer spricht NTLM mit wem, unter welchem Konto, in welcher Version, und warum nicht Kerberos? Die gute Nachricht: Windows liefert das inzwischen ziemlich vollständig, wenn du es fragst.

Auditing auf Servern und Domänencontrollern einschalten

Das erweiterte Auditing schaltest du per Gruppenrichtlinie ein: auf Clients und Servern über die Richtlinie für die erweiterte NTLM-Protokollierung, auf Domänencontrollern zusätzlich über die domänenweite Protokollierung im Netlogon-Bereich. Die Schritt-für-Schritt-Anleitung steht in Erweitertes NTLM-Auditing einschalten: Schritt für Schritt, eine fertige Vorlage liefert das NTLM-Audit-GPO-Skript. In der Klinik gilt dabei: Aktiviere das Auditing auf deinen Windows-Servern und DCs, nicht auf den Medizingeräten. Die Befund- und Dateiserver sehen den eingehenden Verkehr der Geräte in den Ereignissen 4022 und 4023, der DC sieht die Prüfung in 4030 bis 4033.

Weil NTLM-Ereignisse Benutzernamen und Arbeitsplätze enthalten, gehören Datenschutz und Personalvertretung früh dazu. In einem Krankenhaus ist das kein Formalismus; wie du das sauber regelst, beschreibt NTLM-Audit, Datenschutz und Betriebsrat: was du beachten musst.

Ereignisse mit PowerShell und wevtutil lesen

Für einen ersten Blick auf einem Befundserver reicht PowerShell. Das folgende Beispiel zieht die eingehenden NTLM-Ereignisse der letzten sieben Tage aus dem Protokoll Microsoft-Windows-NTLM/Operational und gruppiert sie nach Meldungstext:

```
$seit = (Get-Date).AddDays(-7)
Get-WinEvent -FilterHashtable @{
    LogName   = 'Microsoft-Windows-NTLM/Operational'
    Id        = 4022, 4023
    StartTime = $seit
} | Group-Object Id | Select-Object Count, Name

# Export für die Medizintechnik, ohne Interpretation
wevtutil epl Microsoft-Windows-NTLM/Operational C:\Temp\bef01-ntlm.evtx

# Hat der Befundserver die nötigen SPNs?
setspn -L BEF01
```

Im Meldungstext findest du unter anderem „Reason ID“, „NTLM Version“ und den Namen des Ziels. Die Reason ID sagt dir, warum Windows nicht Kerberos benutzt hat. In der Klinik tauchen besonders häufig die Fälle IP-Adresse, lokales Konto und fehlende Sichtverbindung zum DC auf. Die vollständige Liste von 0 bis 11 erklärt NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat. Fehlt die Sichtverbindung, weil das Gerät in einem abgeschotteten Netz steht, ist Keine Sichtverbindung zum DC: Reason-ID 9, IAKerb und lokales KDC der passende Beitrag.

Stille Geräte: was nur im Mitschnitt auftaucht

Manche Medizintechnik meldet sich gar nicht als Windows-Anmeldung an einem System, das du auswertest, etwa weil das Ziel ein eingebettetes System im selben Segment ist oder weil die Ereignisse auf einem Gerät entstehen, an das du nicht herankommst. Dann bleibt der Netzwerkmitschnitt am Spiegelport des Switches. Er ist für Medizintechnik ideal, weil er das Gerät nicht berührt: kein Agent, keine Konfigurationsänderung, keine Freigabe am Medizinprodukt. Wie du NTLM im Mitschnitt erkennst und welche Filter du brauchst, steht in NTLM im Netzwerkmitschnitt finden: Wireshark richtig einsetzen. Für Drucker, Scanner und NAS gilt Ähnliches, siehe NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll.

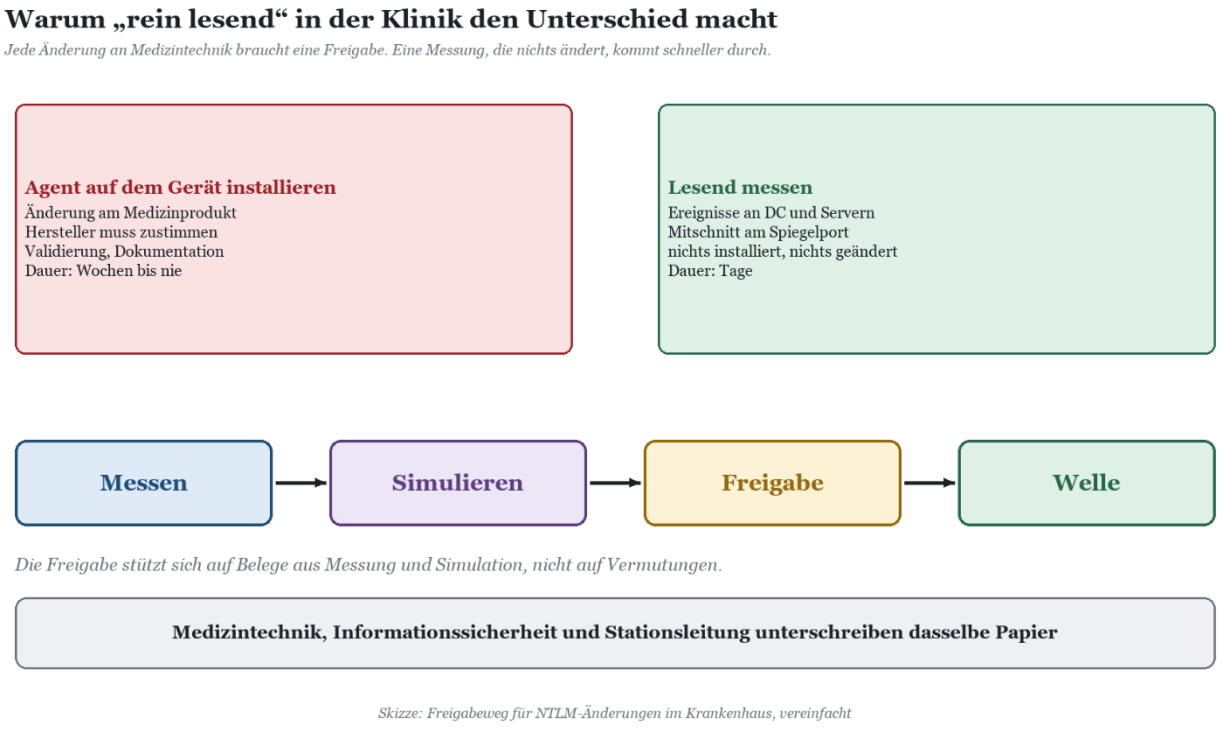
TIPP · Mitschnitt mit der Medizintechnik planen, nicht an ihr vorbei

Lege Mitschnitte in Zeiträume, in denen das Gerät typisch arbeitet: Ultraschall am Vormittag, Labor in der Nachtschicht, Archivexporte am Monatsende. Ein Mitschnitt vom Sonntagnachmittag zeigt dir vor allem, dass am Sonntagnachmittag wenig los ist. Und speichere Mitschnitte so, wie du Patientendaten speicherst, denn genau die können darin stecken.

Wo es mühsam wird

Bis hierhin klingt alles machbar. In einer echten Klinik sieht es dann so aus: 30 Server, 6 Domänencontroller, 2 500 Arbeitsplätze, ein paar hundert Geräte ohne Ereignisprotokoll. Nach einer Woche Auditing hast du sechsstellige Ereigniszahlen, verteilt auf Protokolle, die je nach Betriebssystem unterschiedliche Ereignisse liefern. Ein Teil der Server ist noch Windows Server 2016 und kennt nur 8001 bis 8004, ohne Ursache. Die Mitschnitte liegen als Dateien auf einem Laptop. Und die eigentliche Frage, nämlich was ausfällt, wenn du am Befundserver NTLM verweigerst, beantwortet keines dieser Werkzeuge direkt.

Genau für diese Lage ist der NTLM Diagnostiker gebaut. Er führt Ereignisse und Mitschnitte zusammen, ermittelt die Ursache und simuliert das Abschalten, bevor du es tust. Für ein Krankenhaus ist dabei eine Eigenschaft wichtiger als jede Auswertung: Er arbeitet ausschließlich lesend.



Skizze: Freigabeweg für NTLM-Änderungen im Krankenhaus, vereinfacht

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Medizintechnik messen, ohne sie anzufassen

Der NTLM Diagnostiker arbeitet ausschließlich lesend. Er installiert nichts auf Medizingeräten, ändert keine Gruppenrichtlinie, keinen Registrierungswert und keine Gerätekonfiguration. Das ist in der Klinik das Argument, mit dem die Freigabe durch Medizintechnik und Informationssicherheit schnell gelingt.

Ereignisse holt er direkt vom DC, über einen vorhandenen Windows Event Collector oder per Direktabfrage von deinen Servern. Abdeckungsmonitor und OS-Landkarte zeigen, welche Systeme

erweitertes Auditing liefern, welche nur 8001 bis 8004 und welche schweigen.

Für stille Medizintechnik importierst du Mitschnitte vom Spiegelport über den Wireshark-Import. Die Geräte erscheinen dann neben den Windows-Quellen in derselben Kommunikationsmatrix, samt Konten-Sicht: welches Gerät, welches Ziel, welches Konto.

Die Ursachen-Engine mit SPN- und DNS-Prüfung trennt Fälle, die du selbst lösen kannst, von denen, die beim Hersteller liegen. Die NTLMv1-Hitliste zeigt, welche Geräte noch NTLMv1 sprechen, die Sicherheitsflaggen markieren riskante Kombinationen.

Die Abschalt-Simulation zeigt, welche Verbindungen ausfallen würden, wenn du am Befundserver oder domänenweit verweigerst. Die Readiness-Ampel fasst zusammen, wie weit ein Bereich ist.

Für die Freigabesitzung gibt es den Word-Bericht, für die Medizintechnik und den Hersteller den Excel/CSV-Export mit genau den Geräten, um die es geht.

Zum Einstieg liefert die kostenlose Edition Express einen Fünf-Minuten-Befund, der volle Umfang lässt sich sieben Tage testen. Lizenziert wird pro aktivem Computerkonto. Ein Anwendungskatalog, ein Phasenplan und ein Kerberos-Gegencheck sind als Ausbaustufen geplant.

Abschalten ohne Patientengefährdung

Der wichtigste Satz dieses Kapitels: Ein Ausfall in der Büro-IT ist ärgerlich, ein Ausfall in der Befundübermittlung kann eine Behandlung verzögern. Deshalb gelten in der Klinik dieselben Werkzeuge wie überall, nur mit mehr Geduld und einem Rückweg, den jemand nachts um drei ohne Anruf beim Hersteller gehen kann. Die allgemeine Methode beschreibt NTLM schrittweise abschalten, ohne dass etwas ausfällt; hier geht es um das, was im Krankenhaus anders ist.

Ausnahmen eng fassen

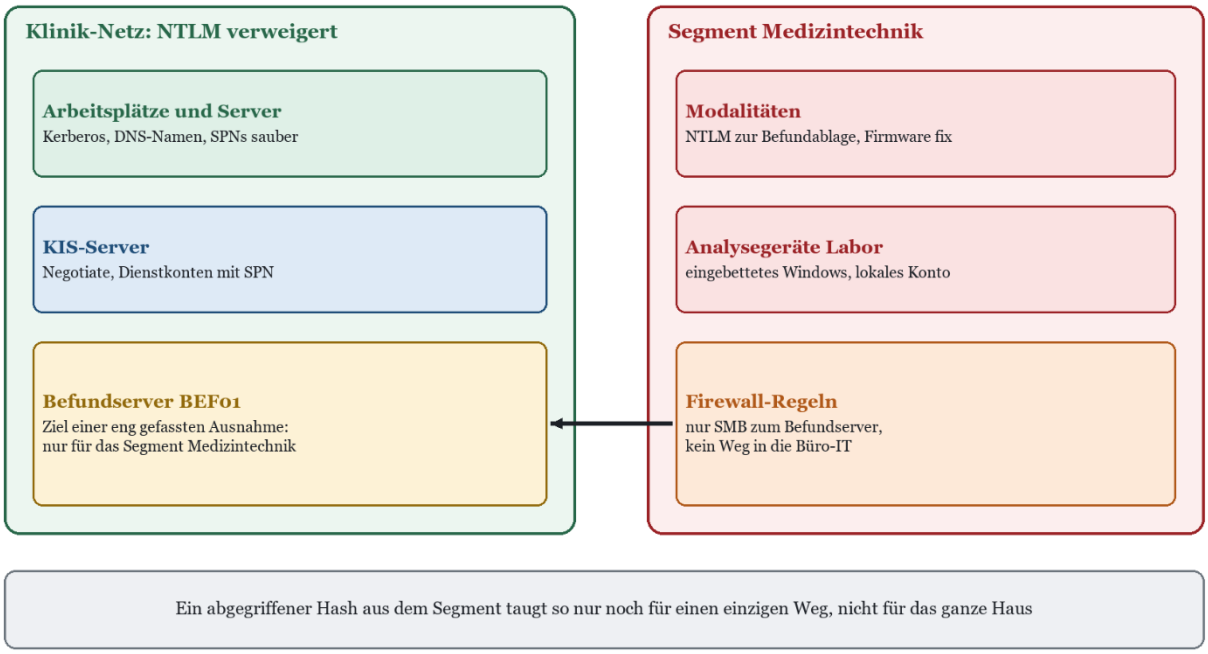
Für Medizintechnik, die NTLM behalten muss, sind Ausnahmen kein Versagen, sondern das Werkzeug der Wahl. Die Restrict-NTLM-Richtlinien erlauben Ausnahmen pro Zielserver, und in einer Klinik ist das Ziel fast immer derselbe Befund- oder Archivserver. Trag genau diesen Server ein, nicht ein Muster, und dokumentiere Gerät, Hersteller, Begründung und Ablaufdatum. Wie die Listen technisch funktionieren, steht in Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern, wie du sie pflegst, in Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren.

Netzsegmentierung als zweite Hälfte der Ausnahme

Eine Ausnahme sagt: Hier darf NTLM weiterlaufen. Die Segmentierung sagt: aber nur hier. In vielen Kliniken gibt es ohnehin eigene Netze für Medizintechnik. Nutze sie. Wenn die Geräte im Segment nur den einen Befundserver per SMB erreichen und nichts sonst, ist ein abgegriffener NTLM-Hash dort deutlich weniger wert. Ergänzend gehört auf den Zielserver alles, was NTLM-Relay erschwert, also SMB-Signierung und erweiterter Schutz, soweit die Geräte damit klarkommen. Die Details stehen in NTLM-Relay verhindern: MIC, Kanalbindung und erweiterter Schutz.

Ausnahme plus Zaun: NTLM nur noch dort, wo es muss

Was NTLM behalten muss, bekommt ein eigenes Segment und eine eng gefasste Ausnahme.



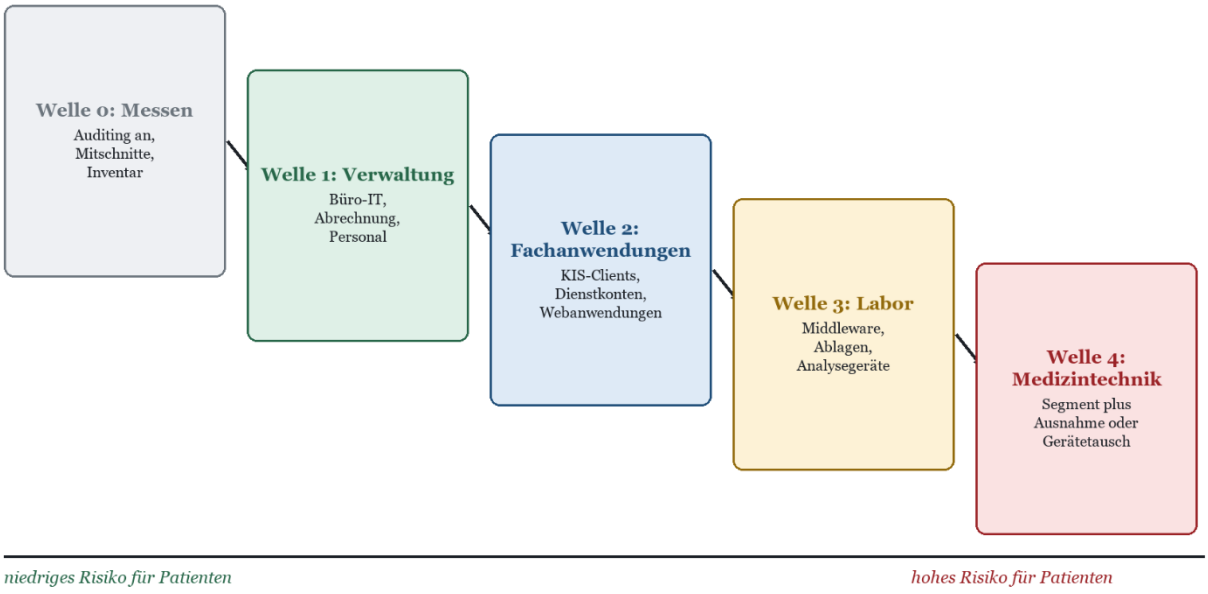
Skizze: Netzsegmentierung mit Ausnahme, Namen fiktiv

Gestaffelte Wellen

Fang am unkritischen Rand an und arbeite dich zur patientennahen Mitte vor. Jede Welle beginnt mit Überwachen, geht nach einer Beobachtungszeit ins Verweigern und endet erst, wenn auch die Monatsabschlüsse und Quartalsläufe durch sind.

Gestaffelte Wellen statt Big Bang

Vom unkritischen Rand zur patientennahen Mitte. Jede Welle beginnt mit Überwachen und endet mit Beobachten.



Skizze: Wellenplan für die NTLM-Ablösung im Krankenhaus, Reihenfolge als Richtwert

Welle	Bereich	Beobachtungszeit	Wer muss zustimmen?
0	Messen: Auditing, Mitschnitte,	4 bis 8 Wochen	IT-Leitung, Datenschutz,

	Inventar		Personalvertretung
1	Verwaltung, Büro-IT, Abrechnung	2 Wochen inkl. Monatsabschluss	IT-Leitung
2	KIS-Clients, Fachanwendungen, Dienstkonten	4 Wochen	IT, Anwendungsbetreuung, Hersteller
3	Labor, Middleware, Ablagen	4 Wochen inkl. Nachtbetrieb	IT, Laborleitung, Hersteller
4	Medizintechnik	pro Gerätetyp	Medizintechnik, Hersteller, Informationssicherheit

Die Zeiten sind Richtwerte. Ein Bereich, in dem einmal pro Quartal ein Export läuft, braucht eine Beobachtungszeit von einem Quartal, egal was die Tabelle sagt.

Rückweg und Bereitschaft

Jede Welle braucht einen dokumentierten Rückweg: Welche GPO wird zurückgenommen, wer darf das, wie lange dauert die Wirkung? Restrict-NTLM-Richtlinien greifen laut Microsoft ohne Neustart, aber erst nach der nächsten Richtlinienaktualisierung. Plane Umstellungen nicht auf Freitagnachmittag und nicht in die Woche, in der die Notaufnahme sowieso brennt. Sprich mit der Stationsleitung, bevor du anfängst, nicht hinterher.

TIPP · Die Bereitschaft muss wissen, was NTLM ist

Wenn nachts um drei ein Laborgerät keine Ergebnisse mehr ablegt, landet der Anruf bei der IT-Bereitschaft. Gib ihr eine einseitige Anleitung: welche Welle gerade aktiv ist, welches Ereignis auf dem Befundserver auf eine NTLM-Blockade hinweist und wie der Rückweg funktioniert. Eine Ausnahme, die eine Viertelstunde zu spät eingetragen wird, ist ärgerlicher als jede Sicherheitslücke, die du in drei Monaten schließt.

KRITIS und Informationssicherheit, ohne Paragraphenreiterei

Krankenhäuser gehören zu den Einrichtungen, an die der Gesetzgeber besondere Anforderungen an die Informationssicherheit stellt, größere Häuser als kritische Infrastruktur. Du musst die Paragraphen nicht auswendig können, um die Konsequenz zu verstehen: Wer ein angemessenes Sicherheitsniveau nachweisen muss, kann bekannte Schwachstellen nicht stillschweigend weiterlaufen lassen. NTLM ist eine bekannte Schwachstelle, NTLMv1 eine sehr bekannte.

Gleichzeitig verlangt dasselbe Regelwerk, dass die Versorgung funktioniert. Die Lösung ist nicht, NTLM über Nacht abzuschalten, sondern nachvollziehbar zu machen, wo es noch läuft, warum, wie lange und mit welcher Absicherung. Genau das fragen Prüfer und Auditoren auch: nicht „Ist NTLM weg?“, sondern „Kennen Sie Ihre Risiken und behandeln Sie sie?“

Was die Informationssicherheit wissen will	Was du aus der NTLM-Ablösung lieferst
Inventar der betroffenen Systeme	Messung mit Quelle, Ziel, Konto, NTLM-Version und Ursache
Risikobewertung	NTLMv1-Geräte, lokale Konten, Ziele mit hohem Schutzbedarf
Behandlung des Restrisikos	Ausnahmen mit Begründung und Ablaufdatum, Netzsegmentierung
Nachweis der Wirksamkeit	wiederholte Messung nach jeder Welle, Ereignisse 4024 und 4025 im Blick
Planung	Wellenplan, Herstellertermine, Gerätetausch im Investitionsplan

WICHTIG · Ausnahmen gehören ins Risikoregister

Jede NTLM-Ausnahme für Medizintechnik ist ein akzeptiertes Restrisiko. Behandle sie so: mit Eigentümer, Begründung, Ablaufdatum und Verweis auf die Herstellerantwort. Dann ist die Ausnahme kein Befund im nächsten Audit, sondern ein Beleg dafür, dass dein Haus seine Risiken steuert.

Damit das Ganze nicht als Nebenbei-Projekt der Systemadministration versandet, braucht es Rollen, Zeitplan und Budget. Wie du das aufsetzt, beschreibt NTLM-Ablösung als Projekt: Zeitplan, Rollen, Aufwand. Wenn du dafür Unterstützung von außen möchtest, etwa für die Abstimmung mit Herstellern und Medizintechnik, hilft dir die Beratung zur NTLM-Ablösung.

FAQ: NTLM im Krankenhaus

Muss ich auf Medizingeräten das NTLM-Auditing aktivieren?

Nein, und meist darfst du es auch nicht ohne Abstimmung. Die Geräte sind in der Regel Clients. Die Ereignisse entstehen auf deinen Windows-Servern und Domänencontrollern, die du verwaltest. Was dort nicht auftaucht, findest du im Netzwerkmitschnitt.

Was passiert mit Geräten, die nur NTLMv1 können?

Seit dem Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 NTLMv1 für Single Sign-on standardmäßig, sichtbar in den Ereignissen 4024 und 4025. Betroffene Geräte gehören ganz oben auf die Liste für Herstellergespräche. Details stehen in NTLMv1 blockiert: was seit Oktober 2026 nicht mehr geht.

Darf ich einen Mitschnitt im Medizintechnik-Netz machen?

Technisch berührt ein Mitschnitt am Spiegelport das Gerät nicht. Organisatorisch können darin Patientendaten stecken. Stimm Zweck, Zeitraum und Speicherort mit Datenschutz und Medizintechnik ab, und lösche den Mitschnitt, sobald die Auswertung steht.

Reicht eine Ausnahme, oder muss ich zusätzlich segmentieren?

Die Ausnahme regelt, wohin NTLM noch darf. Die Segmentierung regelt, wer überhaupt dorthin kommt. Erst beides zusammen begrenzt das Risiko wirksam.

Verändert der NTLM Diagnostiker etwas an meinen Systemen?

Nein. Er arbeitet ausschließlich lesend, sowohl bei Ereignissen als auch beim Wireshark-Import. Das macht ihn für Freigabeprozesse in der Klinik besonders geeignet.

Wie lange dauert die NTLM-Ablösung in einer Klinik?

Die Büro-IT schaffst du oft in wenigen Monaten. Die Medizintechnik folgt den Lebenszyklen der Geräte und damit eher Jahren. Plane deshalb nicht auf ein Enddatum für alles, sondern auf kontrollierte Ausnahmen für den Rest, bevor die nächste Windows-Server-Version NTLM standardmäßig abschaltet.

Was hat Kerberos damit zu tun?

Alles, was du von NTLM wegholst, muss danach per Kerberos funktionieren: DNS-Namen, saubere SPNs, Sichtverbindung zum DC. Hintergründe findest du im Kompetenzbereich Microsoft Kerberos.

Fazit: Erst die Fakten, dann die Freigabe, dann die Welle

Kliniken haben nicht mehr NTLM-Altlasten, weil dort schlechter gearbeitet wird, sondern weil Medizintechnik, Labor und Fachanwendungen länger leben und nicht dir gehören. Die NTLM-

Ablösung gelingt trotzdem, wenn du in der richtigen Reihenfolge vorgehst: rein lesend messen, die selbst behebbaren Ursachen in der Büro-IT abräumen, mit den Herstellern über konkrete Befunde reden, Medizintechnik segmentieren und eng gefasst ausnehmen, und in Wellen vom Rand zur Mitte abschalten.

Die nächste Windows-Server-Version wartet nicht auf die Zulassung deines Ultraschallgeräts. Aber wer jetzt misst, hat die Ausnahmen begründet, die Segmente gezogen und die Hersteller angeschrieben, bevor der Termin kommt. Alle anderen erfahren es von der Station, und die ruft nicht an, um sich zu bedanken. Wenn dein Team Befunde und Mitschnitte selbst bewerten soll, hilft die Schulung zum NTLM Diagnostiker.

WEITERLESEN · Weiter in dieser Serie

› NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet
› NTLMv1 blockiert: was seit Oktober 2026 nicht mehr geht
› Erweitertes NTLM-Auditing einschalten: Schritt für Schritt
› Wenn die Anwendung NTLM fest eingebaut hat: Hersteller richtig fragen
› NTLM im Netzwerkmitschnitt finden: Wireshark richtig einsetzen
› Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren
› NTLM schrittweise abschalten, ohne dass etwas ausfällt
› NTLM-Relay verhindern: MIC, Kanalbindung und erweiterter Schutz