NTLM abschalten im Krankenhaus: Medizingeräte, Altanwendungen und Kerberos



Wissen

Alle Beiträge der Serie rund um Kliniken, Klinikverbünde und Microsoft 365:

Microsoft 365 im Krankenhaus

Beratung

Fahrplan, Ereignisauswertung und Kerberos-Bereinigung mit erfahrener Begleitung:

Microsoft-365-Beratung für Krankenhäuser

Schulung

Wissen für IT-Team und Medizintechnik, damit die Umstellung im Haus bleibt:

Microsoft-365-Schulung für Krankenhäuser

Es gibt Protokolle, die in Würde in den Ruhestand gehen. NTLM gehört nicht dazu. Seit den Neunzigern im Dienst, unzählige Male nachgebessert, vom eigenen Hersteller abgekündigt – und trotzdem läuft es in praktisch jedem Kliniknetz noch irgendwo mit: am Ultraschallgerät in der Funktionsdiagnostik, am Dienstkonto des Laborsystems, am Multifunktionsgerät auf Station, das seit Jahren klaglos Unterlagen in einen Netzwerkordner scannt und von dem niemand mehr weiß, wer es eigentlich eingerichtet hat.

Wer **NTLM im Krankenhaus abschalten** will, merkt schnell: Die Technik ist der kleinere Teil des Problems. Der größere sitzt an der Schnittstelle zwischen IT, Medizintechnik und Herstellern. Ein Medizinprodukt mit eingebettetem Windows darf man nicht einfach umkonfigurieren, ein Subsystem mit Wartungsvertrag auch nicht, und eine Sperre, die nachts um drei die Befundübertragung aus dem Labor lahmlegt, ist in einem 24/7-Betrieb mit Rufbereitschaft kein Lernerlebnis, sondern ein Vorfall.

Dieser Beitrag zeigt, warum NTLM trotzdem weg muss, warum es gerade in Kliniken so zäh ist und wie Sie in vier Stufen vorgehen: überwachen, auswerten, bereinigen, stufenweise sperren. Er gehört zur Serie Microsoft 365 im Krankenhaus. Dass ein Artikel über ein lokales Anmeldeprotokoll in einer Microsoft-365-Serie steht, ist kein Versehen: Ihr lokales Active Directory ist in fast jedem Klinik-Tenant die Quelle der synchronisierten Identitäten. Wer dort per Pass-the-Hash Domänen-Admin wird, steht kurz darauf auch vor der Tür Ihres Tenants.

Warum NTLM weg muss

Ein Protokoll aus der Zeit vor dem Patientenportal

NTLM ist ein Challenge-Response-Verfahren: Der Server schickt eine Zufallszahl, der Client antwortet mit einem Wert, den er aus dieser Zahl und dem Hash des Benutzerkennworts berechnet. Klingt solide, hat aber drei Konstruktionsfehler, die sich nicht wegpatchen lassen:

- **Keine Prüfung des Gegenübers.** Der Client weiß nicht, mit welchem Server er wirklich spricht. Kerberos dagegen bindet jedes Ticket an einen konkreten Dienst.
- **Der Hash ist das Passwort.** Wer den NT-Hash eines Kontos besitzt, kann sich damit anmelden, ohne das Klartextkennwort je zu kennen.
- **Schwache Kryptografie in den Altvarianten.** NTLMv1 ist mit heutiger Rechenleistung in überschaubarer Zeit zu knacken; auch NTLMv2 hilft nicht gegen Relay und Pass-the-Hash.

Kerberos löst diese Probleme nicht vollständig, aber deutlich besser: gegenseitige Authentifizierung, zeitlich begrenzte Tickets, keine Kennwort-Hashes auf der Leitung und mit AES eine Verschlüsselung, die dem Stand der Technik entspricht. Wenn Sie tiefer in die Funktionsweise einsteigen wollen, finden Sie die Grundlagen im Kompetenzbereich Kerberos.

NTLM-Relay: Der Mann in der Mitte freut sich

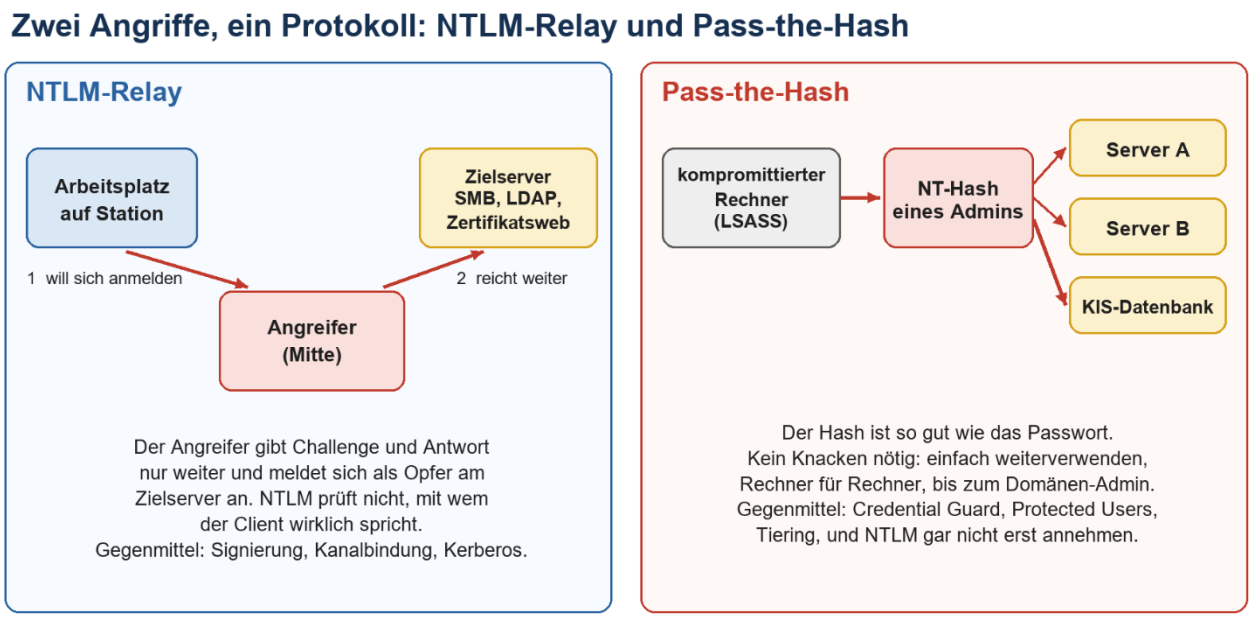
Beim Relay-Angriff lockt ein Angreifer einen Rechner dazu, sich bei ihm anzumelden – etwa über eine manipulierte Namensauflösung im lokalen Netz oder über einen präparierten Link auf eine Freigabe. Die NTLM-Anmeldung reicht er unverändert an einen anderen Server weiter und ist dort angemeldet, und zwar mit den Rechten des Opfers. Besonders begehrt sind Ziele, die viel Macht verleihen: Dateiserver ohne SMB-Signierung, Domänencontroller per LDAP ohne Signierung und Kanalbindung und die Webregistrierung der Zertifikatsdienste, über die sich ein Angreifer im ungünstigsten Fall ein Zertifikat für einen Domänencontroller ausstellen lässt.

Gegenmittel gibt es: SMB-Signierung, LDAP-Signierung und Kanalbindung, erweiterter Schutz für die Authentifizierung an Webdiensten. Windows 11 ab Version 24H2 und Windows Server 2025 verlangen die SMB-Signierung inzwischen standardmäßig. Das ist gut, betrifft aber nur neue Systeme – und genau die sind im Kliniknetz selten das Problem. Wie Sie die Zertifikatsdienste gegen Relay härten, beschreibt der Beitrag PKI im Krankenhaus: Zertifikate für Geräte, WLAN, Anmeldung und Klinikanwendungen.

Pass-the-Hash: Das Passwort, das keins sein muss

Pass-the-Hash ist der Klassiker jeder Ransomware-Kette. Ein Angreifer übernimmt einen Rechner, liest aus dem Speicher des Anmeldedienstes die Hashes angemeldeter Konten aus und meldet sich damit am nächsten System an. Hat sich auf dem ersten Rechner irgendwann ein Administrator mit Domänenrechten angemeldet, ist der Weg zum Domänencontroller kurz. Credential Guard, die Gruppe „Protected Users“ und ein sauberes Ebenenmodell für Administratoren erschweren das erheblich. Mitglieder der Gruppe „Protected Users“ können sich übrigens gar nicht mehr per NTLM anmelden – ein guter erster Schritt für Ihre Admin-Konten, den Sie nicht mit dem Medizingerät auf der Intensivstation abstimmen müssen.

Wie solche Ketten in Kliniken typischerweise ablaufen und wo Microsoft 365 ins Spiel kommt, beschreibt der Beitrag Ransomware im Krankenhaus: Der Weg über Konten und Microsoft 365 und was wirklich hilft.



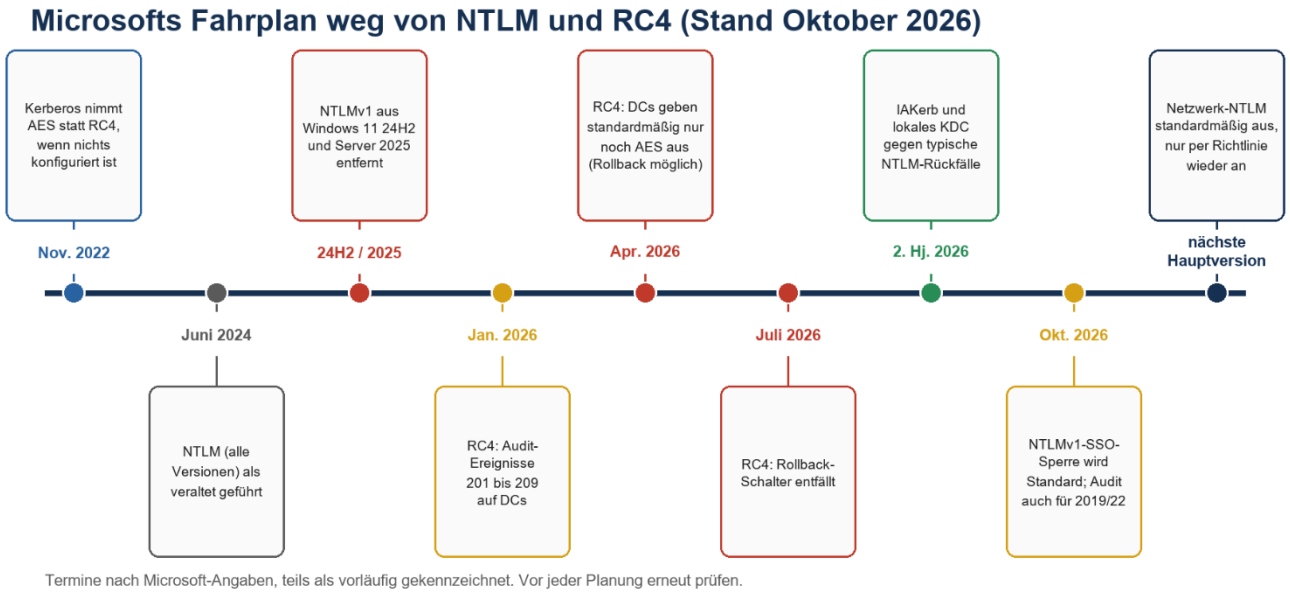
Skizze 1: NTLM-Relay und Pass-the-Hash. Beide Angriffe brauchen keine geknackten Kennwörter, nur ein Protokoll, das zu gutgläubig ist.

Microsofts Abkündigungsfahrplan: Stand Oktober 2026

Microsoft führt NTLM in allen Versionen seit 2024 als veraltet und hat einen Fahrplan in drei Phasen veröffentlicht. Er ist nicht als harte Abschaltung bestehender Systeme angelegt, sondern als Abschaltung per Standardeinstellung in künftigen Versionen. Für Ihre Planung heißt das: Sie haben Zeit, aber Sie sollten sie nutzen.

Fakten: Der Fahrplan in Zahlen (Stand 15.10.2026)

- **Phase 1 – erweiterte Überwachung:** Neue NTLM-Ereignisse im Protokoll Microsoft-Windows-NTLM/Operational, verfügbar ab Windows 11 24H2 und Windows Server 2025, laut Microsoft für Windows Server 2019 und 2022 mit Updates ab dem 13. Oktober 2026.
- **Phase 2 – Kerberos statt Rückfall:** IAKerb und ein lokales KDC sollen typische Gründe für den NTLM-Rückfall beseitigen, etwa fehlende Sichtverbindung zum Domänencontroller oder lokale Konten. Angekündigt für die zweite Jahreshälfte 2026 für Windows Server 2025 und Windows 11 ab 24H2.
- **Phase 3 – standardmäßig aus:** In der nächsten Hauptversion von Windows Server und den zugehörigen Client-Versionen ist Netzwerk-NTLM standardmäßig deaktiviert und muss per Richtlinie bewusst wieder eingeschaltet werden. Bereits ausgelieferte Versionen unterstützen NTLM weiter; der Code bleibt vorerst im System.
- **NTLMv1:** In Windows 11 24H2 und Windows Server 2025 entfernt. Für die Nutzung von NTLMv1-abgeleiteten Anmeldedaten bei Einmalanmeldung wechselt der Standard des Registrierungswerts BlockNTLMv1SSO im Oktober 2026 von Überwachen auf Erzwingen, sofern der Wert nicht gesetzt ist und Credential Guard nicht aktiv ist. Betroffen sind etwa WLAN- und VPN-Anmeldungen mit MS-CHAPv2.
- **RC4 in Kerberos:** Seit Januar 2026 protokollieren Domänencontroller die Ereignisse 201 bis 209 der Quelle KDCSVC, seit April 2026 nehmen sie für Konten ohne gesetzte Verschlüsselungstypen standardmäßig nur noch AES an, und seit Juli 2026 ist der Schalter zum Zurückrollen entfallen.



Skizze 2: Microsofts Weg weg von NTLM und RC4. Einige Termine sind von Microsoft als vorläufig gekennzeichnet.

Zwei Dinge fallen auf. Erstens: Die RC4-Abkündigung in Kerberos ist bereits durch. Wer im Frühjahr 2026 auf dem Domänencontroller plötzlich Fehler bei alten Dienstkonten oder Speichersystemen gesehen hat, kennt den Grund. Zweitens: Die eigentliche NTLM-Abschaltung kommt mit der nächsten Server-Generation. Spätestens wenn Ihre Domänencontroller und Dateiserver auf diese Version wechseln, müssen Sie wissen, wer noch NTLM spricht – sonst schalten Sie es per Ausnahmerichtlinie wieder ein und haben nichts gewonnen außer einer weiteren Gruppenrichtlinie.

Stand der Technik: Was § 391 SGB V und das BSIG damit zu tun haben

§ 391 SGB V verpflichtet Krankenhäuser, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zu treffen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme zu vermeiden. Die Vorschrift hat seit dem NIS2-Umsetzungsgesetz vom 6. Dezember 2025 eine neue Fassung; für Häuser, die als Betreiber kritischer Anlagen ohnehin den Pflichten des BSI-Gesetzes unterliegen, gelten stattdessen diese Pflichten. Als Weg zur Erfüllung nennt das Gesetz einen branchenspezifischen Sicherheitsstandard – in der Praxis den B3S „Medizinische Versorgung“ der Deutschen Krankenhausgesellschaft, aktuell in Version 1.3.1 vom 10. Oktober 2025.

NTLM steht in keinem dieser Texte. Das müssen Sie aber auch nicht: Ein Anmeldeprotokoll, das sein eigener Hersteller abkündigt und in der nächsten Version standardmäßig abschaltet, ist schwer als Stand der Technik zu verkaufen – weder dem Prüfer noch nach einem Vorfall. Die Einordnung für Microsoft 365 insgesamt finden Sie im Beitrag NIS2, § 391 SGB V und B3S: Was die Sicherheitspflichten für Microsoft 365 bedeuten.

Wichtig: Keine Rechtsberatung

Dieser Beitrag beschreibt technische Maßnahmen und ordnet sie in den Rechtsrahmen ein. Ob und wie Ihr Haus unter § 391 SGB V oder unter die Pflichten des BSI-Gesetzes fällt und welche Nachweise im Einzelfall verlangt werden, klären Sie mit Ihrem Informationssicherheitsbeauftragten und gegebenenfalls mit rechtlicher Beratung. Landesrecht – insbesondere Landeskrankenhausgesetze und Landesdatenschutzgesetze – unterscheidet sich je Bundesland.

Warum NTLM abschalten im Krankenhaus besonders zäh ist

In einem Mittelständler mit einer Domäne, ein paar Dateiservern und einem Druckerpark ist NTLM ein Projekt von überschaubarer Länge. Im Krankenhaus kommen Gerätegruppen dazu, die nicht der IT gehören, Anwendungen, deren Konfiguration ein Hersteller verantwortet, und ein Betrieb, der keine Wartungsfenster im klassischen Sinn kennt. Die folgende Skizze zeigt, aus welchen Ecken das NTLM typischerweise kommt.



Skizze 3: Die üblichen Verdächtigen. Die Farbe zeigt, wie viele Parteien Sie zur Lösung an den Tisch holen müssen.

Medizingeräte mit eingebettetem Windows

Modalitäten in der Radiologie, Ultraschallgeräte, Messplätze in der Funktionsdiagnostik, Analysegeräte im Labor: Viele davon laufen auf einem eingebetteten oder angepassten Windows. Die Bilder und Befunde selbst gehen meist per DICOM oder HL7 an PACS und Subsysteme – das ist kein NTLM-Thema. Aber Export-Freigaben, Berichtsablagen, Protokollordner und Fernwartungswege laufen häufig über SMB, und das Gerät steht oft in einer Arbeitsgruppe mit lokalem Konto. Ein Gerät, das nicht Mitglied der Domäne ist, kann sich gegenüber einem Domänendienst nicht per Kerberos ausweisen – also NTLM.

Das Entscheidende: Ein Medizinprodukt ändern Sie nicht nach Gusto. Konfiguration, Betriebssystemstand und Netzwerkeinstellungen gehören zum Zustand, den der Hersteller verantwortet. Eine eigenmächtige Änderung kann Gewährleistung und Konformität berühren, und die Medizintechnik in Ihrem Haus hat dafür zu Recht ein Wörtchen mitzureden. Wo die Gerätenachweise und Einweisungen dokumentiert sind, beschreibt der Beitrag Medizinproduktebuch, Einweisungen, Gerätenachweise: MPBetreibV-Dokumentation zwischen CAFM und SharePoint.

Subsysteme mit Dienstkonten

LIS, RIS, PACS, Kommunikationsserver, Archivsysteme, Dokumentenmanagement: Jedes Subsystem bringt eigene Dienstkonten mit, oft angelegt bei der Erstinstallation vor vielen Jahren, mit nie geändertem Kennwort und ohne sauberen Service Principal Name (SPN). Fehlt der SPN oder ist er doppelt vergeben, kann der Client kein Kerberos-Ticket bekommen und fällt stillschweigend auf NTLM zurück. Niemand merkt etwas – bis jemand NTLM sperrt.

Ein Klassiker ist SQL Server unter Klinikanwendungen: Der Datenbankdienst läuft unter einem Domänenkonto, der SPN für den Dienst wurde nie registriert, und alle Clients verbinden sich per NTLM. Kommt eine Weiterleitung über einen Anwendungsserver dazu, scheitert auch die Kerberos-Delegierung, und die Anwendung weicht auf SQL-Anmeldungen oder hinterlegte Kennwörter aus. Mehr dazu im Beitrag SQL Server unter Klinikanwendungen: Warum Subsysteme langsam werden und was wirklich hilft und im Kompetenzbereich SQL Server.

Herstellerfreigaben und Wartungsverträge

Die meisten Subsysteme und alle Medizinprodukte laufen unter einer Herstellerfreigabe: Betriebssystemstand, Datenbankversion, Virenschutz, Netzwerkeinstellungen. „Kerberos mit AES“ steht in vielen Freigabedokumenten schlicht nicht drin – nicht weil es nicht ginge, sondern weil nie jemand gefragt hat. Ihr wichtigstes Werkzeug ist deshalb die Frage an den Hersteller, schriftlich und mit Frist: Unterstützt Ihr Produkt Kerberos? Mit AES? Ist der Betrieb ohne NTLM freigegeben? Wenn nein, wann?

> **Tipp: Beschaffung als Hebel**
>
> Nehmen Sie Kerberos-Fähigkeit mit AES, Domänenmitgliedschaft oder zertifikatsbasierte Anmeldung und den Betrieb ohne NTLM als Anforderung in Ihre Lastenhefte und Ausschreibungen für Medizintechnik und Subsysteme auf. Jedes Gerät, das heute ohne diese Anforderung beschafft wird, steht in zehn Jahren auf Ihrer Ausnahmeliste.

Druck- und Scanlösungen

Multifunktionsgeräte auf Station und in der Verwaltung scannen gern in Netzwerkordner – mit einem lokalen oder einem Sammelkonto, häufig per IP-Adresse statt per Namen und mit einer Firmware, die Kerberos nur auf ausdrücklichen Wunsch beherrscht. Hinzu kommen Druckserver-Lösungen und Follow-me-Printing, die Benutzer gegen das Verzeichnis prüfen. Gute Nachricht: Hier hilft oft ein Firmware-Update plus Umstellung auf Namen statt IP-Adressen. Schlechte Nachricht: Sie müssen es Gerät für Gerät tun, und auf jeder Station steht eins.

Vertrauensstellungen und Altdomänen im Klinikverbund

Klinikverbünde wachsen durch Zukäufe und Fusionen, und mit jedem Haus kommt oft eine eigene Domäne. Externe Vertrauensstellungen zu solchen Altdomänen und fehlendes Namenssuffix-Routing führen dazu, dass Anmeldungen über die Domänengrenze hinweg auf NTLM zurückfallen. Wer NTLM abschalten will, muss die Vertrauensstellungen mitdenken – oder die Gelegenheit nutzen, sie zu konsolidieren. Den Weg dahin beschreibt der Beitrag Active Directory im Klinikverbund: Vertrauensstellungen, Altdomänen und der Weg zur Konsolidierung.

NTLM-Quelle	Typischer Grund	Lösungsweg	Wer muss mit an den Tisch
Medizingerät mit eingebettetem Windows	Arbeitsgruppe, lokales Konto, SMB-Export	Hersteller-Update, eigenes Segment, befristete Ausnahme bis zum Gerätetausch	Medizintechnik, Hersteller, ISB
Subsystem (LIS, RIS, PACS)	Dienstkonto ohne SPN, Zugriff per IP-Adresse oder Alias	SPN registrieren, Namen statt IP, AES für Dienstkonto, gMSA prüfen	Systembetreuer, Hersteller
SQL-Server-	fehlender MSSQLSvc-	SPN setzen, eingeschränkte	Datenbankbetreuung,

Anwendung	SPN, Delegierung	Delegierung konfigurieren	Hersteller
Multifunktionsgerät	Scan-to-Folder mit lokalem Konto, IP-Adresse	Firmware, Kerberos aktivieren, Zielpfad per Name	IT, Druckdienstleister
Altdomäne im Verbund	externe Vertrauensstellung, fehlendes Suffix-Routing	Gesamtstruktur-Vertrauensstellung oder Konsolidierung	IT der Standorte, Geschäftsführung
Webanwendung im Intranet	Windows-Authentifizierung nur mit NTLM-Anbieter	Negotiate mit Kerberos, SPN für HTTP-Dienst	Anwendungsbetreuung
Admin-Werkzeuge und Skripte	Zugriff per IP-Adresse, lokale Konten	Namen verwenden, LAPS, Admin-Konten in Protected Users	IT-Betrieb

Der Fahrplan in vier Stufen: Überwachen statt Abschalten

Der häufigste Fehler beim NTLM-Projekt ist Ungeduld. Wer eine Sperre setzt, um zu sehen, „was dann passiert“, erfährt es zuverlässig – meist von der Station, selten zu einer günstigen Uhrzeit. Der bessere Weg folgt vier Stufen, zwischen denen jeweils eine bewusste Freigabe steht.



Skizze 4: Fahrplan in vier Stufen. Jede Stufe endet mit einer Entscheidung, nicht mit einem Datum im Kalender.

Stufe 1: Überwachen

Am Anfang wird nichts gesperrt, sondern nur gezählt. Dafür aktivieren Sie per Gruppenrichtlinie die NTLM-Überwachung – auf allen Domänencontrollern aller Domänen und auf den wichtigsten Mitgliedsservern:

- **Netzwerksicherheit: NTLM einschränken: NTLM-Authentifizierung in dieser Domäne überwachen** auf den Domänencontrollern, Einstellung „Alle aktivieren“.
- **Netzwerksicherheit: NTLM einschränken: Eingehenden NTLM-Datenverkehr überwachen** auf Servern.

- **Netzwerksicherheit: NTLM einschränken: Ausgehender NTLM-Datenverkehr zu Remoteservern** auf Clients, zunächst ebenfalls nur „Alle überwachen“.
- **Erweiterte NTLM-Protokollierung** über die administrativen Vorlagen „NTLM Enhanced Logging“ und für Domänencontroller „Log Enhanced Domain-wide NTLM Logs“, wo die Betriebssystemversion es hergibt.

Sammeln Sie die Ereignisse zentral – per Windows-Ereignisweiterleitung, in Ihrem SIEM oder, sofern lizenziert und angebunden, über Microsoft Defender for Identity. Wichtig ist der Zeitraum: Ein Monat reicht im Krankenhaus selten. Manche Prozesse laufen nur zum Monatsabschluss, zum Quartalsende, zur jährlichen Statistik oder nur dann, wenn die Rufbereitschaft nachts einen bestimmten Fernwartungsweg nutzt. Planen Sie so, dass mindestens ein Quartalswechsel in die Überwachung fällt.

Ereignis	Protokoll	Bedeutung
4624	Sicherheit	Erfolgreiche Anmeldung; das Feld für das Authentifizierungspaket zeigt NTLM und die Version (V1 oder V2)
8001 bis 8004	Microsoft-Windows-NTLM/Operational	Klassische NTLM-Überwachung: ausgehend am Client, eingehend am Server, domänenweit am Domänencontroller (8004)
4020 / 4021	Microsoft-Windows-NTLM/Operational	Erweiterte Protokollierung am Client: ausgehende NTLM-Anmeldung mit aufrufendem Prozess und Grund; Warnstufe bei Herabstufung wie NTLMv1
4022 / 4023	Microsoft-Windows-NTLM/Operational	Erweiterte Protokollierung am Server: eingehende NTLM-Anmeldung
4030 bis 4033	Microsoft-Windows-NTLM/Operational	Erweiterte Protokollierung am Domänencontroller, getrennt nach eigener Domäne und domänenübergreifend
4024 / 4025	Microsoft-Windows-NTLM/Operational	Einmalanmeldung mit NTLMv1-abgeleiteten Anmeldedaten: überwacht beziehungsweise blockiert
201 bis 209	System, Quelle KDCSVC	RC4-Nutzung in Kerberos: Warnungen sowie blockierte oder verweigerte Anfragen

Die Zuordnung der Ereignisnummern hat Microsoft in einer eigenen Übersicht zur erweiterten NTLM-Überwachung beschrieben. Prüfen Sie vor dem Bau von Auswertungen an einem echten Ereignis aus Ihrer Umgebung, ob Felder und Stufen so ankommen, wie Sie es erwarten – die Protokollierung hat sich über die Versionen mehrfach verändert.

Stufe 2: Auswerten

Nach einigen Wochen haben Sie viele Ereignisse und wenig Erkenntnis. Jetzt beginnt die eigentliche Arbeit: Gruppieren Sie nach Quellrechner, Zielserver, Konto und – bei der erweiterten Protokollierung – aufrufendem Prozess. Daraus entsteht eine Liste von Verbindungen, nicht von Ereignissen. Jede Verbindung bekommt eine Ursache und einen Besitzer.

Ursachen-Kategorie	Erkennungsmerkmal	Typische Abhilfe
Zugriff per IP-Adresse	Ziel ist eine IP, kein Name	Namen verwenden; Kerberos mit IP-SPN nur

		als Notlösung
Fehlender oder doppelter SPN	Dienstkonto mit Kerberos-Fehlern, setspn -X meldet Duplikate	SPN registrieren oder bereinigen
DNS-Alias ohne SPN	Zugriff über einen CNAME-Namen	SPN für den Alias ergänzen
Lokales Konto	Kontoname ohne Domäne oder mit Rechnername	Domänenkonto oder gMSA, bei Admins LAPS
Gerät nicht in der Domäne	Quellrechner unbekannt im Verzeichnis	Domänenbeitritt prüfen, sonst Ausnahme mit Kompensation
Keine Sichtverbindung zum DC	Segment ohne Zugang zu Port 88	Firewall-Regel oder künftig IAKerb
Domänenübergreifend	Ereignisse 4030 / 4031, fremde Domäne	Vertrauensstellung prüfen, Suffix-Routing, Konsolidierung
NTLMv1	Paketversion V1 im Ereignis 4624	sofort angehen; Geräte mit NTLMv1 sind der erste Kandidat für Austausch

Tipp: Die Pareto-Regel gilt auch für NTLM

In aller Regel verursachen wenige Quellen den Großteil der Ereignisse: ein Druckserver, ein Überwachungssystem, das per IP-Adresse alle Server abfragt, ein Skript mit lokalem Konto. Räumen Sie diese zuerst ab, dann wird die Liste übersichtlich – und die verbleibenden Einträge sind die, über die Sie wirklich reden müssen.

Stufe 3: Bereinigen – RC4 nach AES

NTLM und RC4 sind zwei Baustellen mit denselben Bewohnern. Konten, deren Kennwort seit der Einführung von AES in der Domäne nie geändert wurde, haben keine AES-Schlüssel; Geräte, die kein AES können, können oft auch kein sauberes Kerberos. Seit der Umstellung im April 2026 nehmen Domänencontroller für Konten ohne gesetzte Verschlüsselungstypen standardmäßig nur noch AES an. Was nicht passt, taucht in den Ereignissen 201 bis 209 auf – oder als Störungsmeldung.

- **Inventur:** Microsoft stellt dafür Skripte bereit, die aus den Ereignissen 4768 und 4769 die verwendeten Verschlüsselungstypen und verfügbaren Schlüssel je Konto ermitteln. Details liefert die Anleitung von Microsoft zum Erkennen und Beheben von RC4 in Kerberos.
- **Kennwort neu setzen:** Konten ohne AES-Schlüssel erhalten diese erst durch eine Kennwortänderung. Bei Dienstkonten heißt das: abgestimmter Termin mit dem Systembetreuer.
- **Verschlüsselungstypen setzen:** Für Dienstkonten mit SPN das Attribut `msDS-SupportedEncryptionTypes` auf AES128 und AES256 setzen (Wert 0x18). Explizite RC4-Freigaben nur als dokumentierte Ausnahme.
- **Altgeräte:** Domänencontroller ab Windows Server 2025 stellen keine RC4-Ticket-Granting-Tickets mehr aus. Ein Gerät, das nur RC4 kann, kann sich damit nicht mehr selbst per Kerberos anmelden.

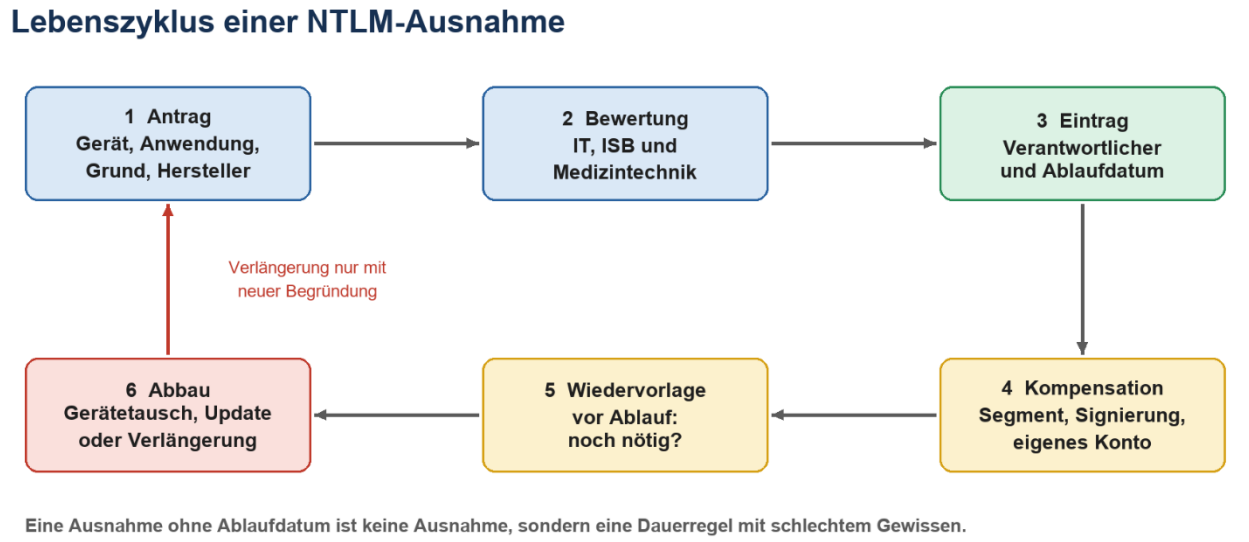
Stufe 3: Bereinigen – Dienstkonten mit SPN sauber machen

Dienstkonten mit SPN sind das Lieblingsziel beim sogenannten Kerberoasting: Jeder Benutzer der Domäne kann ein Dienstticket anfordern und offline versuchen, das Kennwort des Dienstkontos zu erraten. Das funktioniert umso besser, je schwächer die Verschlüsselung und je älter das Kennwort ist. Beim Aufräumen schlagen Sie deshalb zwei Fliegen mit einer Klappe:

- Alle Konten mit SPN auflisten und jedem Konto einen Verantwortlichen und eine Anwendung zuordnen. Konten ohne Besitzer sind Kandidaten für die Deaktivierung – nach Rücksprache, nicht nach Gefühl.
- Doppelte SPNs mit setspn -X finden und bereinigen; sie sind eine der häufigsten Ursachen für unerklärliche NTLM-Rückfälle.
- Wo die Anwendung es unterstützt: auf gruppenverwaltete Dienstkonten (gMSA) umstellen. Kennwörter mit 120 Zeichen, die sich selbst wechseln, sind gegen Kerberoasting praktisch immun.
- Wo die Anwendung es nicht unterstützt: lange, zufällige Kennwörter, AES erzwingen, Anmeldung auf die tatsächlich nötigen Server beschränken und einen Wechselrhythmus vereinbaren.
- Delegierung prüfen: Uneingeschränkte Delegierung auf Anwendungsservern ist ein Geschenk an Angreifer. Eingeschränkte oder ressourcenbasierte Delegierung reicht fast immer.

Stufe 3: Die Ausnahmeliste – mit Verantwortlichem und Ablaufdatum

Es wird Geräte geben, die Sie nicht bereinigen können: das Analysegerät, das noch drei Jahre unter Wartungsvertrag steht, die Modalität, deren Hersteller ein Update erst mit der nächsten Gerätegeneration anbietet. Für diese Fälle brauchen Sie eine Ausnahmeliste. Nicht als Excel-Datei auf einem persönlichen Laufwerk, sondern als gelenktes Dokument mit klaren Regeln.



Skizze 5: Lebenszyklus einer NTLM-Ausnahme. Ohne Wiedervorlage wird aus jeder Ausnahme eine Dauerlösung.

Feld	Inhalt	Warum
Gerät oder Anwendung	Bezeichnung, Standort, Inventarnummer aus dem Medizintechnik-Bestand	eindeutige Zuordnung, auch nach Umzug auf eine andere Station
Quelle und Ziel	Rechner oder Segment, Zielserver, Dienst	Grundlage für die technische Serverausnahme

Grund	z. B. fehlende Herstellerfreigabe für Kerberos	dokumentiert, warum die Regel nicht greift
Verantwortlicher	eine benannte Person, kein Postfach	jemand muss die Wiedervorlage beantworten
Ablaufdatum	konkretes Datum, höchstens zwölf Monate	erzwingt die erneute Prüfung
Kompensation	eigenes Netzsegment, SMB-Signierung, eigenes Konto mit minimalen Rechten	begrenzt den Schaden, solange die Ausnahme besteht
Ausstiegsplan	Update, Austausch, Ende des Wartungsvertrags	macht aus der Ausnahme ein Projekt mit Ende

Die Serverausnahmen selbst tragen Sie technisch über die Richtlinie **Netzwerksicherheit: NTLM einschränken: Serverausnahmen in dieser Domäne hinzufügen** beziehungsweise auf Clientseite über die Ausnahmen für Remoteserver ein. Wichtig: Die technische Liste und die organisatorische Liste müssen übereinstimmen. Prüfen Sie das bei jeder Wiedervorlage. Im Krankenhaus bietet es sich an, das Verfahren als Verfahrensanweisung ins QM-Handbuch aufzunehmen – dann hat es einen Prüf- und Freigabeprozess, den Ihre Organisation ohnehin beherrscht. Wie das mit SharePoint aussieht, beschreibt der Beitrag QM-Handbuch mit SharePoint: Dokumentenlenkung im Krankenhaus, die im Audit hält.

Stufe 4: Stufenweise sperren

Erst wenn die Liste der offenen Verbindungen leer oder vollständig durch Ausnahmen abgedeckt ist, wird gesperrt – und auch dann nicht auf einen Schlag. Eine bewährte Reihenfolge:

- **NTLMv1 abschalten:** LAN-Manager-Authentifizierungsebene auf „Nur NTLMv2-Antworten senden. LM und NTLM verweigern“. Das ist der Schritt mit dem besten Verhältnis von Nutzen zu Risiko.
- **Admin-Konten absichern:** Domänen-Admins und andere hoch privilegierte Konten in die Gruppe „Protected Users“. Ab jetzt kann sich kein Admin mehr per NTLM anmelden.
- **Ebene 0 sperren:** Domänencontroller, Zertifizierungsstellen und Verwaltungssysteme der Identität nehmen kein eingehendes NTLM mehr an, abgesehen von dokumentierten Ausnahmen.
- **Servergruppen nacheinander:** Dateiserver, Anwendungsserver, Datenbankserver – jeweils mit Beobachtungszeit und vorbereitetem Rückweg.
- **Domänenweite Sperre:** „NTLM-Authentifizierung in dieser Domäne“ auf Verweigern, mit der Serverausnahmeliste. Ausgehendes NTLM auf Clients zuletzt.

Jede Stufe wird als Änderung geplant, freigegeben und angekündigt: außerhalb der Visitenzeiten, nicht zum Monatsabschluss, nicht vor einem Wochenende mit dünner Besetzung, und mit einem Rückweg, den die Rufbereitschaft nachts ohne Rückfrage ausführen kann. Das Zurücksetzen einer Gruppenrichtlinie dauert Minuten; bis sie auf allen Systemen angekommen ist, kann es länger dauern. Testen Sie den Rückweg, bevor Sie ihn brauchen – zum Beispiel im Rahmen einer Notfallübung für die Klinik-IT.

Warnung: Nie ohne Rücksprache mit Medizintechnik und Hersteller sperren

Eine NTLM-Sperre, die ein Medizinprodukt trifft, ist keine IT-Störung, sondern kann die Patientenversorgung berühren: Befunde kommen nicht an, Geräte können Ergebnisse nicht

ablegen, Fernwartung funktioniert im Ernstfall nicht. Sperren Sie deshalb nie ein Segment, einen Server oder eine Domäne, über die Medizinprodukte kommunizieren, ohne vorherige schriftliche Abstimmung mit der Medizintechnik und – wo nötig – mit dem Hersteller. Legen Sie fest, wer im Störungsfall die Sperre zurücknehmen darf, und sorgen Sie dafür, dass die Rufbereitschaft das weiß.

Phase	Maßnahme	Werkzeug	Risiko
1 Überwachen	NTLM- und RC4-Überwachung auf allen DCs und wichtigen Servern, zentrale Sammlung	Gruppenrichtlinien, Ereignisweiterleitung, SIEM, Defender for Identity (sofern lizenziert)	gering; Mitbestimmung und Speicherbedarf beachten
2 Auswerten	Verbindungen gruppieren, Ursachen zuordnen, Besitzer finden	PowerShell, SIEM-Abfragen, Microsoft-Skripte zu Kerberos-Verschlüsselung	gering; Gefahr der Analyse ohne Ende
3 Bereinigen	SPNs setzen, Dienstkonten auf AES, gMSA, Namen statt IP, Firmware-Updates, Ausnahmeliste	setspn, Active-Directory-Verwaltung, Herstellerkontakt, QM-Verfahrensanweisung	mittel; Kennwortwechsel an Dienstkonten kann Anwendungen stoppen
4 Sperren	NTLMv1 aus, Protected Users, Ebene 0, Servergruppen, domänenweit mit Ausnahmen	Gruppenrichtlinien „NTLM einschränken“, Änderungsverfahren, Rückweg	hoch ohne Vorarbeit; Ausfall von Subsystemen und Medizingeräten möglich

Aus der Praxis: Die NTLM-Roadmap eines Krankenhausverbunds

In einem Krankenhausverbund mit mehreren Standorten, den ich über viele Jahre begleitet habe, war die NTLM-Abschaltung kein Einzelprojekt, sondern Teil einer größeren Aufräumarbeit: Vertrauensstellungen zwischen den Domänen der Häuser, Kerberos-Bereinigung und der Aufbau und die Härtung einer eigenen PKI liefen ineinander.

Drei Erfahrungen daraus tragen über diesen Einzelfall hinaus. Erstens: Die Überwachung muss über alle Domänen laufen, sonst sehen Sie die domänenübergreifenden Anmeldungen nur zur Hälfte. Zweitens: Die Ausnahmeliste mit benanntem Verantwortlichen und Ablaufdatum war das eigentliche Steuerungsinstrument – technisch ist eine Serverausnahme schnell eingetragen, organisatorisch ist sie nur dann beherrschbar, wenn jemand sie wieder austragen will. Drittens: Wer NTLM abschaltet, landet zwangsläufig bei Kerberos, bei Zertifikaten und bei den Vertrauensstellungen. Wer diese Themen getrennt plant, plant dreimal.

Wer am Tisch sitzen muss

Ein NTLM-Projekt im Krankenhaus ist zu 30 Prozent Gruppenrichtlinie und zu 70 Prozent Abstimmung. Das ist keine Schwäche des Projekts, sondern die Realität einer Organisation, in der IT, Medizintechnik und Hersteller gemeinsam für den Betrieb verantwortlich sind.

Rolle	Aufgabe im NTLM-Projekt
Geschäftsführung	Auftrag erteilen, Ressourcen bereitstellen, Restrisiken bei Ausnahmen bewusst tragen
IT-Leitung	Fahrplan verantworten, Lenkungskreis führen, Prioritäten zwischen Standorten festlegen
Active-Directory-Administratoren	Überwachung, Auswertung, SPN- und Dienstkonto-Bereinigung, Sperrrichtlinien
Medizintechnik	Gerätebestand, Herstellerkontakte, Bewertung jeder Sperre mit Bezug zu Medizinprodukten
Hersteller und Systembetreuer	Aussagen zu Kerberos, AES und NTLM-freiem Betrieb, Updates, Freigaben
Informationssicherheitsbeauftragter	Risikobewertung, Ausnahmen mitzeichnen, Einordnung in B3S oder BSIG-Pflichten
Datenschutzbeauftragter	Bewertung der Auswertung von Anmeldeereignissen mit Personenbezug, Löschfristen
Qualitätsmanagementbeauftragter	Ausnahmeverfahren als Verfahrensanweisung im QM-Handbuch lenken
Betriebsrat, Personalrat oder MAV	Mitbestimmung bei der Auswertung von Anmelde- und Nutzungsdaten

Mitbestimmung: Anmeldeereignisse sind personenbezogen

NTLM-Ereignisse enthalten Benutzernamen, Rechnernamen und Uhrzeiten. Damit lässt sich – theoretisch – nachvollziehen, wer wann an welchem Arbeitsplatz gearbeitet hat. Je nach Trägerschaft greifen das Betriebsverfassungsgesetz, das Personalvertretungsrecht des Bundes oder des jeweiligen Landes oder die kirchlichen Mitarbeitervertretungsordnungen, und diese Regelungen unterscheiden sich im Detail. Klären Sie früh, ob eine bestehende Vereinbarung zu Protokolldaten die NTLM-Auswertung abdeckt oder ob Sie eine Ergänzung brauchen. Hilfreich sind eine klare Zweckbindung auf IT-Sicherheit und Fehleranalyse, eine Auswertung nach Rechnern und Diensten statt nach Personen und kurze Aufbewahrungsfristen. Die Unterschiede je Trägerschaft beschreibt der Beitrag Betriebsrat, Personalrat oder MAV: Mitbestimmung bei Microsoft 365 je nach Trägerschaft.

Wichtig: Mitbestimmung ist keine Formsache

Ob und in welchem Umfang die Auswertung von Anmeldeereignissen mitbestimmungspflichtig ist, hängt von Trägerschaft, Bundesland und bestehenden Vereinbarungen ab. Dieser Hinweis ersetzt keine Rechtsberatung. Binden Sie die Interessenvertretung ein, bevor die Überwachung startet – nicht erst, wenn die erste Auswertung auf dem Tisch liegt.

Kommunikation in den Häusern

Pflegekräfte und Ärzte merken von einem gut gemachten NTLM-Projekt im Idealfall nichts. Damit das so bleibt, sollte die Stationsleitung wissen, wen sie anruft, wenn nach einer Umstellung ein Scanner, ein Etikettendrucker oder eine Gerätefreigabe streikt – und die Rufbereitschaft muss wissen, dass eine NTLM-Sperre als Ursache in Frage kommt. Eine kurze Information an Pflegedirektion und Funktionsbereiche vor jeder Sperrstufe ist billiger als jede Fehlersuche. Wo die Anmeldung am Stationsarbeitsplatz selbst betroffen ist, lohnt der Blick in den Beitrag Anmeldung am Stationsarbeitsplatz: Citrix, Entra ID, Karte und schneller Benutzerwechsel.

Wenn Sie den Fahrplan nicht allein aufsetzen wollen: Die Microsoft-365-Beratung für Krankenhäuser umfasst Ereignisauswertung, Kerberos- und PKI-Bereinigung sowie die Abstimmung mit Medizintechnik und Herstellern. Damit das Wissen anschließend im Haus bleibt, gibt es die Microsoft-365-Schulung für Krankenhäuser – auch für IT-Teams, die Active Directory, Kerberos und die Microsoft-365-Anbindung gemeinsam im Blick behalten müssen.

Häufige Fragen zum NTLM-Abschalten im Krankenhaus

Schaltet Microsoft NTLM in unseren bestehenden Servern einfach ab?

Nein. Nach Microsofts Angaben unterstützen bereits ausgelieferte Windows- und Windows-Server-Versionen NTLM weiter. Standardmäßig abgeschaltet wird Netzwerk-NTLM in der nächsten Hauptversion; es lässt sich dort per Richtlinie wieder einschalten. Ausnahme: NTLMv1 ist in Windows 11 24H2 und Windows Server 2025 bereits entfernt, und bei der Einmalanmeldung mit NTLMv1-abgeleiteten Anmeldedaten wechselt der Standard im Oktober 2026 auf Blockieren.

Reicht es, nur NTLMv1 abzuschalten?

Es ist der wichtigste erste Schritt, aber nicht das Ziel. NTLMv2 schützt nicht vor Relay-Angriffen und nicht vor Pass-the-Hash. Wer bei NTLMv2 stehen bleibt, hat die Tür abgeschlossen und das Fenster offen gelassen.

Wie lange sollten wir überwachen, bevor wir sperren?

So lange, bis alle relevanten Betriebszyklen einmal durchgelaufen sind. Im Krankenhaus heißt das in aller Regel mindestens ein Quartalswechsel, besser mit Jahresabschluss oder anderen seltenen Prozessen. Wichtiger als die Dauer ist, dass die Liste der offenen Verbindungen am Ende jeder Auswertung kürzer wird.

Was machen wir mit einem Medizingerät, das nur NTLM kann?

Es kommt auf die Ausnahmeliste – mit Verantwortlichem aus der Medizintechnik, Ablaufdatum, Kompensation (eigenes Netzsegment, Zugriff nur auf einen dedizierten Zielserver, eigenes Konto mit minimalen Rechten) und einem Ausstiegsplan. Parallel fragen Sie beim Hersteller nach Update oder Nachfolgegerät und schreiben die Anforderung in die nächste Ausschreibung.

Bricht die RC4-Umstellung unsere Subsysteme?

Sie kann es, wenn Dienstkonten keine AES-Schlüssel haben oder Geräte nur RC4 beherrschen. Seit April 2026 nehmen Domänencontroller für Konten ohne gesetzte Verschlüsselungstypen standardmäßig nur noch AES an. Prüfen Sie die Ereignisse 201 bis 209 im Systemprotokoll Ihrer Domänencontroller; dort sehen Sie, welche Konten und Geräte betroffen sind.

Hat NTLM etwas mit Microsoft 365 zu tun?

Nicht direkt – Microsoft 365 und Entra ID verwenden moderne Protokolle. Indirekt sehr wohl: Ihr lokales Active Directory ist in aller Regel die Quelle der synchronisierten Identitäten. Wer lokal per Pass-the-Hash die Kontrolle über privilegierte Konten oder den Synchronisierungsserver erlangt,

hat einen kurzen Weg in den Tenant. Mehr dazu im Kompetenzbereich Microsoft Entra ID und im Kompetenzbereich Microsoft 365 Security.

Brauchen wir für die Überwachung Zusatzprodukte?

Nein. Die Bordmittel – Gruppenrichtlinien, Ereignisprotokolle, Ereignisweiterleitung und PowerShell – reichen für die Erhebung. Ein SIEM oder Microsoft Defender for Identity macht die Auswertung komfortabler. Welche Lizenzen Ihr Haus dafür hat, klären Sie vorab; die Methode funktioniert auch ohne.

Fazit: Vier Stufen, eine Liste und viel Geduld

NTLM abzuschalten ist im Krankenhaus kein Wochenendprojekt, sondern eine Reihe kleiner, gut abgestimmter Schritte. Die Technik ist bekannt und von Microsoft gut dokumentiert: überwachen, auswerten, RC4 nach AES, SPNs und Dienstkonten aufräumen, stufenweise sperren. Was Kliniken anders macht, sind Medizingeräte mit eingebettetem Windows, Subsysteme unter Herstellerfreigabe und ein Betrieb ohne Pause. Dafür gibt es keine Gruppenrichtlinie, sondern nur Abstimmung, eine ehrliche Ausnahmeliste mit Verantwortlichen und Ablaufdaten und die Geduld, Ausnahmen wirklich wieder abzubauen.

Der Zeitpunkt ist günstig: Die RC4-Umstellung hat viele Altlasten ohnehin sichtbar gemacht, die erweiterte NTLM-Überwachung ist auf den aktuellen Systemen verfügbar, und die nächste Server-Generation wird NTLM standardmäßig nicht mehr anbieten. Wer jetzt mit Stufe 1 beginnt, hat beim nächsten Serverwechsel eine Liste statt einer Überraschung. Und die Station merkt im besten Fall: nichts.

Weiter im Thema

› Kompetenzbereich Kerberos

› Active Directory im Klinikverbund: Vertrauensstellungen, Altdomänen und der Weg zur Konsolidierung

› PKI im Krankenhaus: Zertifikate für Geräte, WLAN, Anmeldung und Klinikanwendungen

› NIS2, § 391 SGB V und B3S: Was die Sicherheitspflichten für Microsoft 365 bedeuten

› Ransomware im Krankenhaus: Der Weg über Konten und Microsoft 365 und was wirklich hilft

› SQL Server unter Klinikanwendungen: Warum Subsysteme langsam werden und was wirklich hilft