NTLM-Audit, Datenschutz und Betriebsrat: was du beachten musst



WISSEN
Wie der NTLM Diagnostiker rein lesend zeigt, wo noch NTLM läuft, und die Daten dabei bei dir lässt.
› NTLM Diagnostiker

BERATUNG
NTLM-Audit mit Zweckbestimmung, Löschkonzept und Unterlagen für Datenschutz und Betriebsrat planen.
› Beratung zur NTLM-Ablösung

SCHULUNG
Auditing, Auswertung und datensparsame Berichte im Team sicher beherrschen.
› Schulung zum NTLM Diagnostiker

Es gibt zwei Arten, ein NTLM-Audit zu starten. Bei der ersten schaltest du am Montag das Auditing per Gruppenrichtlinie ein, sammelst drei Wochen lang Ereignisse und präsentierst stolz eine Excel-Tabelle mit 480.000 Zeilen. Bei der zweiten sitzt du vorher eine Stunde mit dem Datenschutz und dem Betriebsrat zusammen. Die erste Variante ist schneller. Bis zu dem Moment, in dem jemand aus dem Betriebsrat die Tabelle sieht, nach dem eigenen Namen filtert und fragt, warum die IT weiß, dass er jeden Morgen um 7:58 Uhr seinen Rechner entsperrt.

Dann bist du nicht mehr der Admin, der NTLM ablöst. Dann bist du der Admin, der eine Überwachungsanlage betreibt, und das Projekt steht still, bis eine Einigung gefunden ist. Dabei hast du gar nichts falsch gemacht, technisch jedenfalls. Du hast nur übersehen, dass NTLM-Ereignisse Benutzernamen, Rechnernamen und Zeitstempel enthalten. Und dass genau diese Kombination in Deutschland zwei Instanzen auf den Plan ruft: die Datenschutz-Grundverordnung und die Mitbestimmung.

Der Zeitdruck macht die Sache nicht entspannter. Seit dem Windows-Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 NTLMv1 für Single Sign-on standardmäßig, zu erkennen an den Ereignissen 4024 und 4025. Mit der nächsten Windows-Server-Version ist NTLM standardmäßig abgeschaltet. Wer jetzt nicht misst, wo NTLM noch läuft, erfährt es später durch Störungsmeldungen. Den Zeitplan im Detail findest du in NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet.

Dieser Beitrag zeigt dir, welche personenbezogenen Daten in einem NTLM-Audit anfallen, wie du Zweck, Speicherdauer und Zugriff sauber festlegst, wer informiert werden muss und warum

Netzwerkmitschnitte die heikelste Disziplin sind. Am Ende steht eine Checkliste, die du in dein Projekt übernehmen kannst.

WICHTIG · Keine Rechtsberatung

Dieser Beitrag ist eine praxisnahe Orientierung aus Sicht der IT, keine Rechtsberatung. Ob eine Datenschutz-Folgenabschätzung nötig ist, welche Rechtsgrundlage greift und welche Form der Beteiligung dein Betriebs- oder Personalrat verlangt, klärst du mit deinem Datenschutzbeauftragten und gegebenenfalls mit der Rechtsabteilung. Die gute Nachricht: Mit den Unterlagen aus diesem Beitrag sind diese Gespräche kurz.

Was in NTLM-Ereignissen wirklich steht

Aus Sicht der IT ist ein NTLM-Ereignis eine technische Notiz: Ein Client hat sich per NTLM bei einem Ziel angemeldet, weil Kerberos aus einem bestimmten Grund nicht ging. Aus Sicht des Datenschutzes ist es ein Datensatz, der eine Person, einen Ort im Netz und einen Zeitpunkt miteinander verknüpft. Beide Sichtweisen sind richtig, und du brauchst beide.

Die Ereignisse im Überblick

Seit dem erweiterten NTLM-Auditing, das Microsoft in KB5064479 beschreibt, liefern Windows eine ganze Familie von Ereignissen. Die Clients und Server protokollieren ausgehende und eingehende NTLM-Anmeldungen, die Domänencontroller die Pass-through-Authentifizierung. Für die Ablösung ist das ein Segen, denn erstmals steht in jedem Ereignis eine Reason ID, also der Grund, warum nicht Kerberos verwendet wurde.

Ereignisse	Wo sie entstehen	Was sie enthalten (Auswahl)
4020, 4021	Client, ausgehende Anmeldung	Benutzer, Target Machine, Prozess, Reason ID, NTLM Version
4022, 4023	Server, eingehende Anmeldung	Benutzer, Clientrechner, Reason ID, NTLM Version
4030 bis 4033	Domänencontroller	Benutzer, Clientrechner, Zielserver, Reason ID
4024, 4025	Client, NTLMv1 für Single Sign-on	Benutzer, Ziel, Hinweis auf Überwachung oder Blockade
8001 bis 8004	klassische Restrict-NTLM-Überwachung	Benutzer, Rechner, Ziel, ohne Reason ID

FAKTEN · Systemvoraussetzungen laut KB5064479

Das erweiterte Auditing mit den Ereignissen 4020 bis 4023 und 4030 bis 4033 gibt es ab Windows 11 24H2 und Windows Server 2025 sowie auf Windows Server 2022 und 2019 mit den Updates ab dem 13.10.2026. Die Reason IDs reichen von 0 bis 11. Die klassischen Ereignisse 8001 bis 8004 aus den Restrict-NTLM-Richtlinien stehen auch auf älteren Systemen zur Verfügung.

Was die einzelnen Reason IDs bedeuten, steht in NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat. Wie du das Auditing einschaltest, zeigt Erweitertes NTLM-Auditing einschalten: Schritt für Schritt.

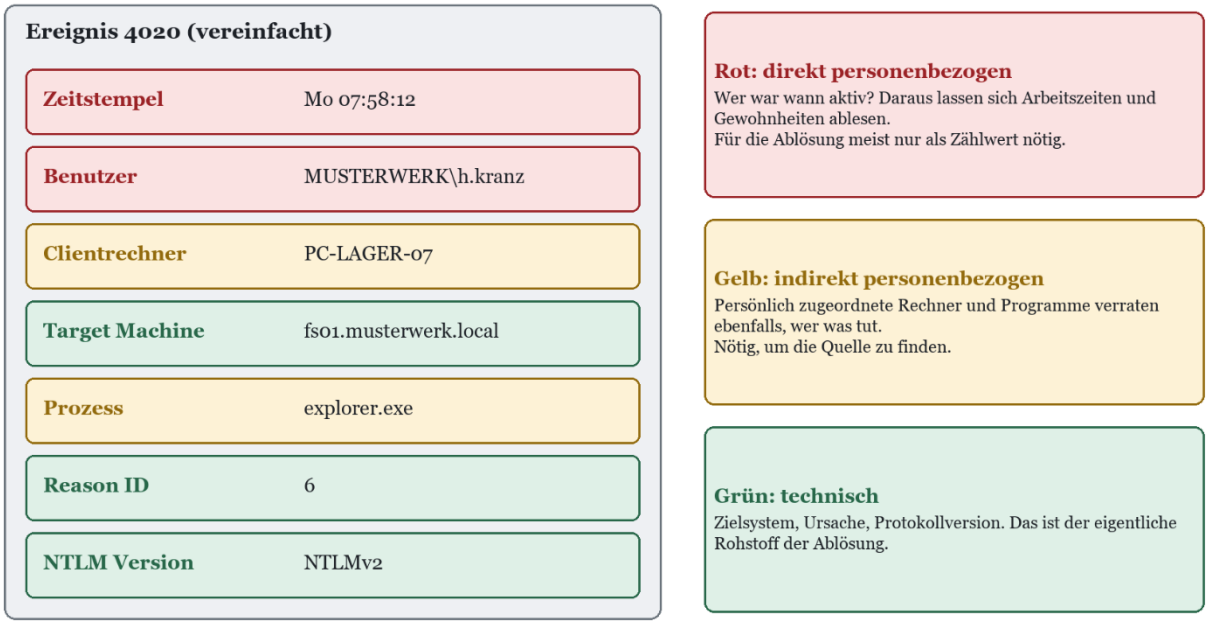
Wo der Personenbezug steckt

Der Benutzername ist offensichtlich personenbezogen. Weniger offensichtlich: Auch ein Rechnername wie PC-LAGER-07 ist personenbezogen, sobald dieser Rechner einer bestimmten Person zugeordnet ist, und im Mittelstand ist er das fast immer. Gleiches gilt für den

Prozessnamen. Wer weiß, dass um 7:58 Uhr der Explorer auf dem Rechner von Frau Kranz eine Freigabe geöffnet hat, weiß, wann Frau Kranz angefangen hat zu arbeiten.

Was ein NTLM-Ereignis über Menschen verrät

Technisch gedacht, personenbezogen gelesen: dieselben Felder, zwei Brillen.



Skizze: Felder eines NTLM-Ereignisses nach Personenbezug, Werte fiktiv

Feld	Personenbezug	Für die Ablösung nötig?	Empfehlung
Benutzer	direkt	selten im Detail	nur zur Unterscheidung Dienstkonto oder Person auswerten
Clientrechner	indirekt	ja, um die Quelle zu finden	auswerten, aber nicht mit Uhrzeiten koppeln
Target Machine, Zielserver	kaum	ja, zentral	voll auswerten
Prozess	indirekt	ja, für die Ursache	auswerten, nicht pro Person berichten
Zeitstempel	in Kombination stark	nur grob	auf Tage oder Wochen verdichten
Reason ID, NTLM Version	keiner	ja, zentral	voll auswerten

TIPP · Dienstkonten sind keine Menschen

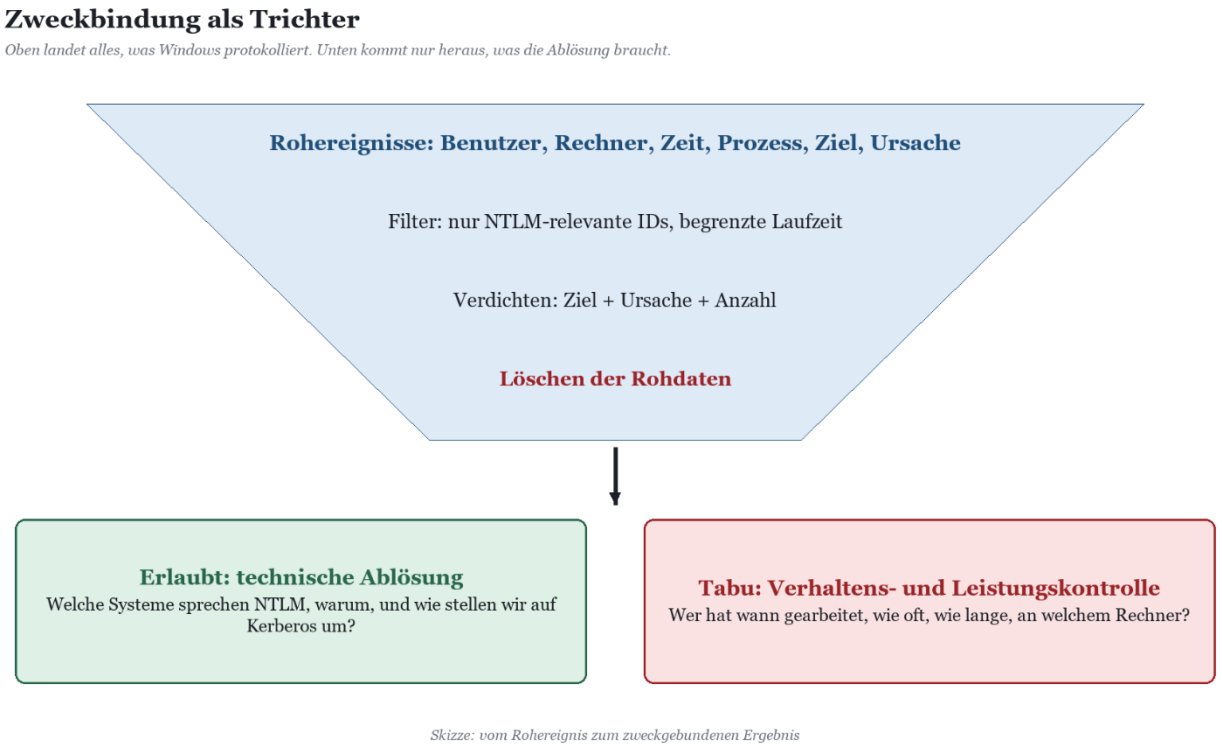
Ein großer Teil der NTLM-Last stammt erfahrungsgemäß von Dienstkonten, geplanten Aufgaben und Geräten. Diese Daten sind für das Projekt am wertvollsten und datenschutzrechtlich am unproblematischsten. Wenn du zuerst die technischen Konten auswertest und persönliche Konten nur als Zählwert betrachtest, entschärfst du die Diskussion, bevor sie beginnt.

Der Rahmen: Zweckbindung, Rechtsgrundlage, Mitbestimmung

Du musst kein Jurist werden. Aber drei Begriffe solltest du so sicher beherrschen, dass du sie in einer Betriebsratssitzung erklären kannst, ohne auf den Fußboden zu schauen.

Zweckbindung und Datenminimierung

Artikel 5 der DSGVO verlangt, dass personenbezogene Daten für festgelegte, eindeutige Zwecke erhoben und nicht für andere Zwecke weiterverarbeitet werden. Dazu kommen Datenminimierung und Speicherbegrenzung. Für dein Audit heißt das: Der Zweck lautet „technische Ablösung des NTLM-Protokolls“ und nichts anderes. Keine Fehlersuche bei einzelnen Personen, keine Anwesenheitskontrolle, keine Auswertung, wer wie oft auf welche Freigabe zugreift.



Skizze: vom Rohereignis zum zweckgebundenen Ergebnis

Klingt selbstverständlich, ist es aber nicht. Die Versuchung kommt garantiert, meist in Form einer harmlosen Frage aus der Führungsebene: „Wenn ihr eh schon seht, wer sich wann anmeldet, könnt ihr dann mal schauen, ob der Kollege aus dem Vertrieb wirklich um acht da ist?“ Die einzig richtige Antwort ist ein freundliches Nein mit Verweis auf die Zweckbestimmung. Schreib sie deshalb vorher auf, dann musst du nicht improvisieren.

Rechtsgrundlage und Dokumentation

In der Praxis stützen Unternehmen solche Auswertungen meist auf ihr berechtigtes Interesse an einem sicheren IT-Betrieb, flankiert von der Pflicht zur Sicherheit der Verarbeitung nach Artikel 32 DSGVO. Die Ablösung eines unsicheren Authentifizierungsverfahrens ist dafür ein gutes Beispiel. Welche Grundlage bei dir trägt, entscheidet der Datenschutz. Deine Aufgabe ist es, die Verarbeitung so zu beschreiben, dass er entscheiden kann: welche Daten, welche Systeme, wie lange, wer hat Zugriff, wann wird gelöscht. Das gehört ins Verzeichnis der Verarbeitungstätigkeiten. Ob zusätzlich eine Datenschutz-Folgenabschätzung nötig ist, hängt vom Umfang ab und davon, ob Daten über viele Personen systematisch zusammengeführt werden.

Betriebsrat und Personalrat

Hier wird es für viele IT-Abteilungen überraschend. Nach § 87 Absatz 1 Nummer 6 des Betriebsverfassungsgesetzes hat der Betriebsrat mitzubestimmen bei der Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Nach ständiger Rechtsprechung des Bundesarbeitsgerichts genügt es, dass eine Einrichtung objektiv dazu geeignet ist. Ob du das vorhast, spielt keine Rolle. Ein Ereignisprotokoll mit Benutzername und Uhrzeit ist geeignet. Punkt.

In Verwaltungen tritt an die Stelle des Betriebsrats der Personalrat, und die Personalvertretungsgesetze von Bund und Ländern enthalten vergleichbare Mitbestimmungsrechte bei technischen Einrichtungen. Kliniken und Einrichtungen in kirchlicher Trägerschaft haben eine Mitarbeitervertretung mit eigenem Regelwerk. Viele Häuser haben bereits eine Rahmenvereinbarung zu IT-Systemen und Protokollierung. Prüfe zuerst, ob das NTLM-Audit dort hineinpasst. Oft reicht dann eine Information oder eine kurze Protokollnotiz statt einer neuen Vereinbarung.

Wer	Wann einbinden	Was du mitbringst
Datenschutzbeauftragter	vor dem Einschalten des Auditings	Zweck, Datenarten, Systeme, Frist, Zugriffsrechte, Löschkonzept
Betriebsrat, Personalrat, Mitarbeitervertretung	vor dem Einschalten, nach dem Datenschutz	Zweckbestimmung, Ausschluss der Leistungskontrolle, Beispielbericht
Informationssicherheit	bei Netzwerkmitschnitten zwingend	Umfang, Dauer, Speicherort, Löschnachweis
IT-Leitung oder Geschäftsführung	zu Projektbeginn	Projektauftrag mit festgeschriebenem Zweck
Dienstleister, Systemhaus	vor Zugriff auf Daten	Auftragsverarbeitungsvertrag prüfen

WARNUNG · Erst einschalten, dann fragen, ist der teuerste Weg

Wird das Auditing ohne Beteiligung eingeschaltet, kann der Betriebsrat verlangen, dass es wieder abgeschaltet wird, bis eine Einigung steht. Dann verlierst du nicht nur Zeit, sondern auch die bisher gesammelten Daten, und der nächste Anlauf beginnt mit Misstrauen. Bei einer festen Frist wie der Abschaltung von NTLM in der nächsten Windows-Server-Version ist das ein echtes Projektrisiko.

Wie du das Audit in einen Projektplan mit Rollen und Meilensteinen einbettest, beschreibt NTLM-Ablösung als Projekt: Zeitplan, Rollen, Aufwand. Die Datenschutzschritte gehören dort in die Vorbereitungsphase, nicht in einen Nachtrag.

Speicherdauer, Zugriff und Netzwerkmitschnitte

Zweckbindung ist Theorie. Speicherdauer und Zugriffsrechte sind die Praxis, in der sich zeigt, ob die Theorie ernst gemeint war.

Wie lange darf was liegen bleiben?

Für eine belastbare NTLM-Analyse brauchst du einige Wochen, damit auch Monatsabschlüsse, Quartalsjobs und der Drucker im Keller, der nur dienstags scannt, im Protokoll auftauchen. Danach brauchst du die Rohdaten nicht mehr, sondern nur noch das Ergebnis: welches Ziel, welche Ursache, wie viele Anmeldungen. Eine sinnvolle Staffelung sieht so aus:

Datenart	Vorschlag Aufbewahrung	Begründung
Rohereignisse auf Clients und Servern	Protokollgröße begrenzen, laufendes Überschreiben	Windows verwirft alte Einträge ohnehin, wenn das Protokoll voll ist
Zentral gesammelte Ereignisse	Dauer der Erfassung plus Auswertung, etwa 4 bis 8 Wochen	danach ist der Zweck erreicht
Exporte mit Benutzernamen	nur so lange wie nötig, nicht in Postfächern	Kopien sind das größte Leck
Verdichtete Ergebnisse ohne Personen	bis zum Projektende und darüber hinaus	Nachweis, warum ein System eine Ausnahme bekommt

Netzwerkmitschnitte	Stunden bis wenige Tage, dann Löschen	enthalten Nutzdaten und angreifbare Anmeldedaten

Mit Bordmitteln steuerst du die Größe des NTLM-Betriebsprotokolls über wevtutil oder zentral per Gruppenrichtlinie. Ein Protokoll, das nach einigen Tagen überschreibt, ist auf dem einzelnen Client datensparsamer als eines mit einem Gigabyte. Wer das Auditing mit dem NTLM-Audit-GPO-Skript einrichtet, sollte die Protokollgröße gleich mit festlegen.

```
# Größe des NTLM-Betriebsprotokolls anzeigen und auf 20 MB begrenzen
wevtutil gl Microsoft-Windows-NTLM/Operational
wevtutil sl Microsoft-Windows-NTLM/Operational /ms:20971520

# Nach Projektende: Protokoll leeren (vorher Ergebnis sichern!)
wevtutil cl Microsoft-Windows-NTLM/Operational
```

Auch die Auswertung selbst kann datensparsam sein. Statt alle Felder zu exportieren, zählst du nur, was die Ablösung braucht. Das folgende Beispiel verdichtet die ausgehenden NTLM-Ereignisse eines Rechners auf Ereignis-ID und Anzahl, ohne einen einzigen Benutzernamen anzufassen:

```
Get-WinEvent -LogName 'Microsoft-Windows-NTLM/Operational' `
  -FilterXPath '*[System[(EventID=4020 or EventID=4021)]]' -ErrorAction SilentlyContinue |
  Group-Object Id, MachineName |
  Select-Object Count, Name |
  Sort-Object Count -Descending
```

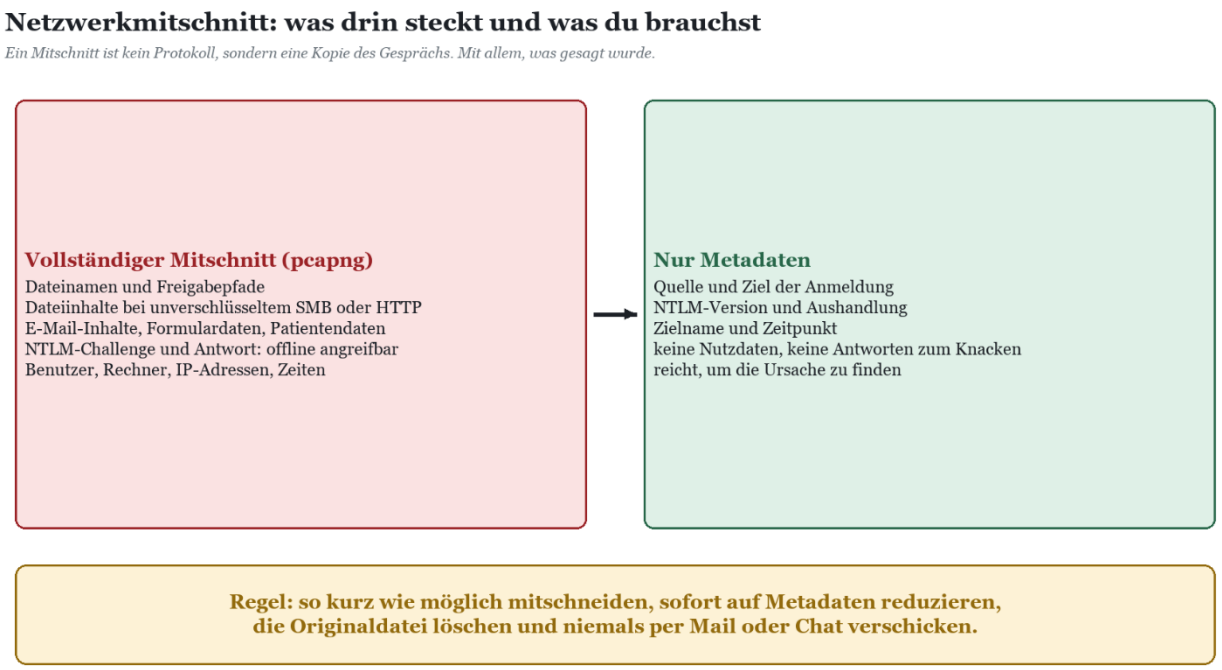
Wer darf hineinschauen?

Rohdaten mit Benutzernamen gehören in die Hände weniger Personen im Projektteam, nicht auf ein Netzlaufwerk, auf das die halbe IT Lesezugriff hat. Leg fest, wer die Daten sieht, wo sie liegen und wie sie gelöscht werden. Wenn ein externer Dienstleister mitarbeitet, prüfe, ob der Auftragsverarbeitungsvertrag diesen Zugriff abdeckt. Systemhäuser, die das bei vielen Kunden tun, finden ein wiederholbares Vorgehen in NTLM-Ablösung im Systemhaus: viele Kunden, ein Vorgehen.

Wenn du die Ereignisse zentral sammelst, hast du einen weiteren Vorteil: Es gibt genau einen Ort, an dem die Daten liegen, und genau einen Ort, an dem du sie löschst. Wie das mit Bordmitteln geht, steht in NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding. Der Sammelserver braucht dann aber auch ein eigenes, restriktives Berechtigungskonzept.

Netzwerkmitschnitte: die heikelste Disziplin

Bei Geräten ohne Ereignisprotokoll, also NAS, Druckern, Scannern oder Maschinensteuerungen, führt oft kein Weg an einem Mitschnitt vorbei. Und hier wird es ernst. Ein Ereignisprotokoll ist eine Notiz über ein Gespräch, ein Mitschnitt ist die Aufnahme des Gesprächs selbst. Darin stehen Dateinamen, je nach Protokoll auch Dateiinhalte, Formulardaten und in der Klinik womöglich Patientendaten. Und, das vergessen viele: die NTLM-Challenge mit der Antwort des Clients. Die lässt sich offline angreifen, bei schwachen Kennwörtern mit Erfolg.



Skizze: Inhalte eines Mitschnitts im Vergleich zur Metadatensicht

WARNUNG · Ein Mitschnitt ist ein Sicherheitsvorfall auf Vorrat

Eine pcapng-Datei mit NTLM-Anmeldungen ist für einen Angreifer wertvoll. Lege sie nie auf Freigaben, schicke sie nicht per Mail oder Chat und lade sie nicht in Online-Analysedienste hoch. Schneide nur so lange mit, wie nötig, filtere schon bei der Aufnahme auf die betroffenen Geräte und reduziere das Ergebnis so schnell wie möglich auf Metadaten.

Bei Berufsgeheimnisträgern wie Steuerberatern, Ärzten oder Kliniken gilt das doppelt, denn Mitschnitte können geschützte Mandanten- oder Patientendaten enthalten.

Wie du den Mitschnitt technisch so gestaltest, dass er möglichst wenig enthält, beschreibt NTLM im Netzwerkmitschnitt finden: Wireshark richtig einsetzen. Für Kliniken mit Medizintechnik und Laborgeräten lohnt zusätzlich ein Blick in NTLM in der Klinik: Medizintechnik, Labor und Fachanwendungen.

Wo es mit Bordmitteln unübersichtlich wird

Mit wevtutil, PowerShell und einer Gruppenrichtlinie kommst du bei zwanzig Rechnern gut zurecht. Bei Hunderten Maschinen entstehen neben den Tausenden Ereignissen vor allem viele Kopien: evtx-Dateien auf Admin-Laptops, CSV-Exporte im Download-Ordner, eine Excel-Datei, die per Mail an drei Kollegen ging, und ein Mitschnitt, von dem niemand mehr weiß, wo er liegt. Das Löschkonzept steht auf Papier, die Daten liegen überall. Wenn der Datenschutz nach sechs Wochen fragt, ob alles gelöscht ist, lautet die ehrliche Antwort meistens „wahrscheinlich“.

Dazu kommt das inhaltliche Problem: Selbst wenn du sauber sammelst, fehlt dir in den Rohdaten die Ursache. Du siehst Reason IDs, aber nicht, ob der SPN fehlt oder der DNS-Eintrag falsch ist. Also schaust du länger und tiefer in die Daten, als es für den Zweck nötig wäre. Für Datensparsamkeit ist das das Gegenteil von hilfreich. Einen ehrlichen Vergleich der Werkzeuge findest du in NTLM-Analyse im Vergleich: Bordmittel, Skripte und NTLM Diagnostiker.

Genau an dieser Stelle setzt der NTLM Diagnostiker an. Er arbeitet ausschließlich lesend, ändert also nichts an deiner Domäne, und hält die Daten an einem Ort, nämlich bei dir. Statt Rohdaten in

Tabellen zu wälzen, bekommst du Ursachen und Zusammenhänge, und damit genau die verdichtete Sicht, die die Zweckbindung verlangt.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Datenschutzfreundlich auswerten

Daten bleiben lokal: Der Diagnostiker verarbeitet die Ereignisse in deiner Umgebung. Für die Lizenz wird lediglich die Domänen-SID verwendet, und zwar nur als Hashwert. Benutzer- und Rechnernamen verlassen dein Netz nicht.

Ausschließlich lesend: Ereignisquellen sind der Domänencontroller direkt, ein Windows Event Collector oder die Direktabfrage einzelner Systeme. Es wird nichts konfiguriert und nichts verändert.

Mitschnitte nur als Metadaten: Beim Wireshark-Import übernimmt der Diagnostiker nur die Metadaten der NTLM-Anmeldungen. Danach kannst du die Originaldatei löschen, wie es dein Löschkonzept vorsieht.

Ursache statt Rohdaten: Die Ursachen-Engine mit SPN- und DNS-Prüfung, die NTLMv1-Hitliste, die Kommunikationsmatrix und die Konten-Sicht zeigen, welche Systeme und Konten betroffen sind und warum. Readiness-Ampel, Abdeckungsmonitor und OS-Landkarte zeigen den Stand, Sicherheitsflaggen markieren Auffälligkeiten, die Abschalt-Simulation zeigt, was beim Verweigern ausfallen würde.

Unterlagen für die Gremien: Der Word-Bericht eignet sich als Beispielbericht für Betriebsrat und Datenschutz. Excel- und CSV-Exporte erzeugst du nur bei Bedarf und behandelst sie nach deinem Löschkonzept.

Zum Einstieg zeigt dir die kostenlose Edition Express mit einem Fünf-Minuten-Befund, was überhaupt sichtbar wird, ideal, um es den Gremien vorab zu zeigen. Danach gibt es einen Testzeitraum von 7 Tagen, lizenziert wird pro aktivem Computerkonto. Ein Anwendungskatalog, Generatoren für Ausnahmelisten und Skripte, ein Phasenplan, ein Kerberos-Gegencheck und ein Verlauf sind als Ausbaustufen geplant.

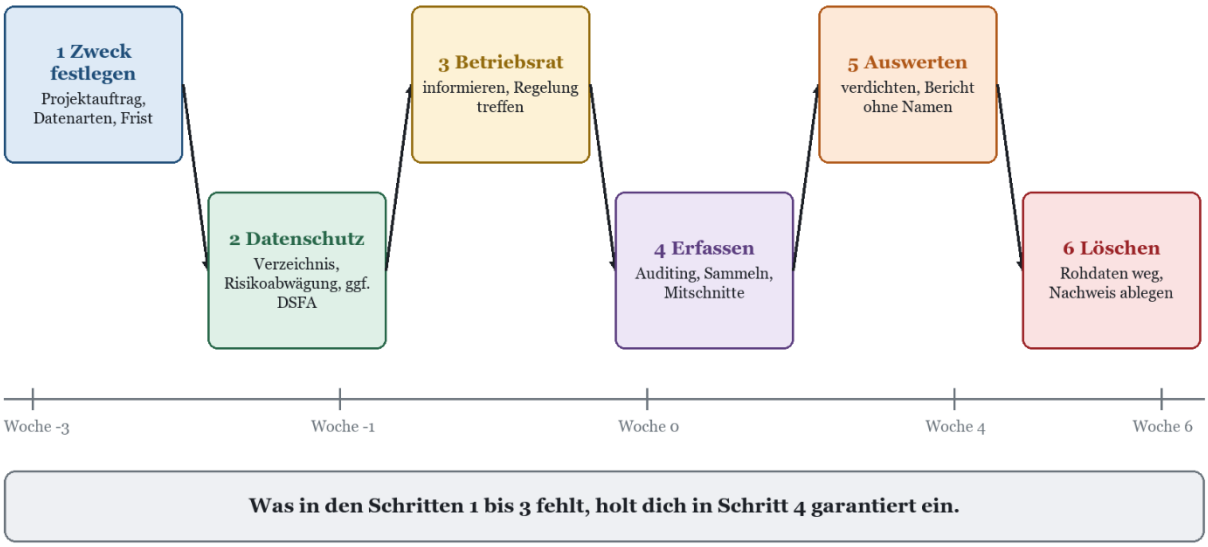
Wenn du Zweckbestimmung, Löschkonzept und den Termin mit dem Betriebsrat nicht allein vorbereiten willst, hilft dir die Beratung zur NTLM-Ablösung mit erprobten Unterlagen und einem Vorgehen, das Gremien in der Regel ohne lange Schleifen mittragen.

Die Praxis-Checkliste für dein NTLM-Audit

Die folgende Checkliste ersetzt keine Prüfung durch deinen Datenschutz, aber sie sorgt dafür, dass du mit vollständigen Unterlagen in das Gespräch gehst. Arbeite sie vor dem Einschalten des Auditings ab, nicht danach.

Ablauf: vom ersten Gespräch bis zur Löschung

Der Datenschutz-Teil kostet ein bis drei Wochen Vorlauf. Plane ihn ein, bevor das Auditing läuft.



Skizze: Datenschutz und Mitbestimmung im Ablauf eines NTLM-Audits, Zeiten beispielhaft

Nr.	Punkt	Verantwortlich	Erledigt
1	Zweck schriftlich festlegen: technische NTLM-Ablösung, keine Verhaltens- oder Leistungskontrolle	IT-Leitung	
2	Datenarten auflisten: Benutzer, Rechner, Zeitstempel, Prozess, Ziel, Reason ID, NTLM Version	Projektteam	
3	Systeme und Ereignis-IDs benennen, auf denen Auditing eingeschaltet wird	Projektteam	
4	Erfassungszeitraum und Löschfristen festlegen, Protokollgrößen begrenzen	Projektteam	
5	Zugriffsberechtigte Personen und Speicherort festlegen	IT-Leitung	
6	Datenschutz informieren, Verzeichnis ergänzen, DSFA-Bedarf prüfen lassen	Datenschutz	
7	Betriebs- oder Personalrat informieren, bestehende Vereinbarungen prüfen	IT-Leitung	
8	Netzwerkmitschnitte gesondert freigeben lassen: Dauer, Filter, Löschung	Informationssicherheit	
9	Auswertung verdichten, Berichte ohne personenbezogene Rankings	Projektteam	
10	Rohdaten und Exporte löschen, Löschung dokumentieren	Projektteam	

Musterformulierung für die Zweckbestimmung

TIPP · Zum Übernehmen und Anpassen

„Die Protokollierung von NTLM-Anmeldungen dient ausschließlich der technischen Vorbereitung der Ablösung des NTLM-Protokolls durch Kerberos. Ausgewertet werden Zielsysteme, Ursachen und Häufigkeiten. Eine Auswertung zur Verhaltens- oder Leistungskontrolle einzelner Mitarbeiterinnen und Mitarbeiter findet nicht statt. Die Rohdaten werden spätestens acht Wochen nach Beginn der Erfassung gelöscht. Zugriff haben ausschließlich die namentlich benannten Mitglieder des Projektteams.“

Warum das Ziel Kerberos heißt und wie es funktioniert, erklärt der Kompetenzbereich Microsoft Kerberos.

Drei Fälle aus der Praxis

AUS DER PRAXIS · Musterwerk GmbH: der Betriebsrat als Verbündeter

In der Musterwerk GmbH stellte die IT dem Betriebsrat vor dem Start einen Beispielbericht vor, in dem nur Server, Ursachen und Anzahlen standen. Die Frage nach Namen kam, die Antwort war einfach: Persönliche Konten tauchen nur als Summe auf. Der Betriebsrat stimmte nach einer Sitzung zu und bat am Ende sogar darum, das Projekt zu beschleunigen, weil ihm die NTLMv1-Funde auf der Hitliste mehr Sorgen machten als das Audit.

AUS DER PRAXIS · Sparfuchs & Partner Steuerberatungs GmbH: der Mitschnitt im Postfach

Bei Sparfuchs & Partner wurde für den Multifunktionsdrucker ein Mitschnitt angefertigt und zur Analyse an einen externen Techniker gemailt. Darin: gescannte Mandantenunterlagen und NTLM-Anmeldungen der Partnerinnen und Partner. Die Mail wurde gelöscht, das Postfach des Technikers geprüft, der Vorfall dokumentiert. Seitdem gilt: Mitschnitte nur mit Filter, nur lokal, nur als Metadaten weiterreichen.

AUS DER PRAXIS · Trendforge Digital GmbH: die Excel-Datei, die nicht sterben wollte

Trendforge Digital hatte ein vorbildliches Löschkonzept. Leider existierte der Export mit allen Benutzernamen am Ende in elf Kopien, eine davon im Teams-Kanal „Allgemein“. Die Lehre: Ein Löschkonzept ist nur so gut wie die Anzahl der Orte, an denen Daten entstehen. Je weniger Exporte, desto weniger Kopien, desto ruhiger der Schlaf.

FAQ: NTLM-Audit und Datenschutz

Muss der Betriebsrat einem NTLM-Audit zustimmen?

Sehr wahrscheinlich ist er zu beteiligen, weil die Ereignisse objektiv geeignet sind, Verhalten zu überwachen. Ob eine bestehende IT-Rahmenvereinbarung genügt oder eine neue Regelung nötig ist, klärst du mit dem Gremium und deiner Rechtsabteilung. Eine frühe Information spart fast immer Zeit.

Ist ein NTLM-Audit eine Verhaltenskontrolle?

Nach dem Zweck nicht, nach der Eignung schon. Genau deshalb schreibst du den Zweck fest, verdichtest die Auswertung und schließt personenbezogene Rankings ausdrücklich aus.

Brauche ich eine Datenschutz-Folgenabschätzung?

Das hängt vom Umfang und von der Art der Auswertung ab und entscheidet dein Datenschutz. Ein zeitlich begrenztes, zweckgebundenes Audit mit verdichteter Auswertung ist in vielen Fällen überschaubar, systematische Mitschnitte über lange Zeiträume eher nicht.

Wie lange darf ich die Ereignisse aufbewahren?

So lange, wie du sie für die Ablösung brauchst. In der Praxis sind das einige Wochen Erfassung plus Auswertung. Verdichtete Ergebnisse ohne Personenbezug darfst du länger behalten, etwa als Nachweis für Ausnahmen.

Darf ich Netzwerkmitschnitte machen?

Technisch ja, organisatorisch nur mit klarem Rahmen: kurze Dauer, Filter auf die betroffenen Geräte, gesicherter Speicherort, schnelle Reduktion auf Metadaten und dokumentierte Löschung. Bei Berufsgeheimnisträgern ist besondere Vorsicht geboten.

Schickt der NTLM Diagnostiker Daten an den Hersteller?

Nein. Die Daten bleiben lokal. Für die Lizenzprüfung wird ausschließlich ein Hashwert der Domänen-SID verwendet, keine Benutzer- oder Rechnernamen.

Was ist mit Ereignissen auf Domänencontrollern, die ohnehin protokolliert werden?

Die Sicherheitsprotokolle der Domänencontroller sind meist schon geregelt. Das zusätzliche NTLM-Auditing mit den Ereignissen 4030 bis 4033 erweitert den Umfang aber, deshalb gehört es ausdrücklich in die Zweckbestimmung.

Fazit: erst reden, dann loggen

Ein NTLM-Audit ist technisch notwendig und datenschutzrechtlich gut beherrschbar, wenn du es von Anfang an richtig aufsetzt. Der Zweck ist klar umrissen, die Datenmenge lässt sich begrenzen, die Speicherdauer ist kurz, und das Ergebnis braucht keine Namen. Was es braucht, ist eine Stunde Vorbereitung mit Datenschutz und Betriebs- oder Personalrat, bevor die erste Gruppenrichtlinie greift.

Netzwerkmitschnitte behandelst du wie radioaktives Material: nur mit Handschuhen, nur kurz, und am Ende fachgerecht entsorgt. Und wenn dich jemand fragt, ob man mit den Daten nicht auch mal eben nachschauen könnte, wann der Kollege aus dem Vertrieb kommt, zeigst du auf die Zweckbestimmung. Die hast du ja vorher aufgeschrieben. Die anderen schreiben sie hinterher, mit dem Betriebsrat am Tisch und dem Fahrplan von Microsoft im Nacken.

WEITERLESEN · Weiter in dieser Serie

› NTLM-Nutzung ermitteln: der komplette Leitfaden
› Erweitertes NTLM-Auditing einschalten: Schritt für Schritt
› NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding
› NTLM im Netzwerkmitschnitt finden: Wireshark richtig einsetzen
› NTLM-Ablösung als Projekt: Zeitplan, Rollen, Aufwand
› Ereignis 4024 und 4025: NTLMv1 im Protokoll erkennen
› NTLM-Analyse im Vergleich: Bordmittel, Skripte und NTLM Diagnostiker