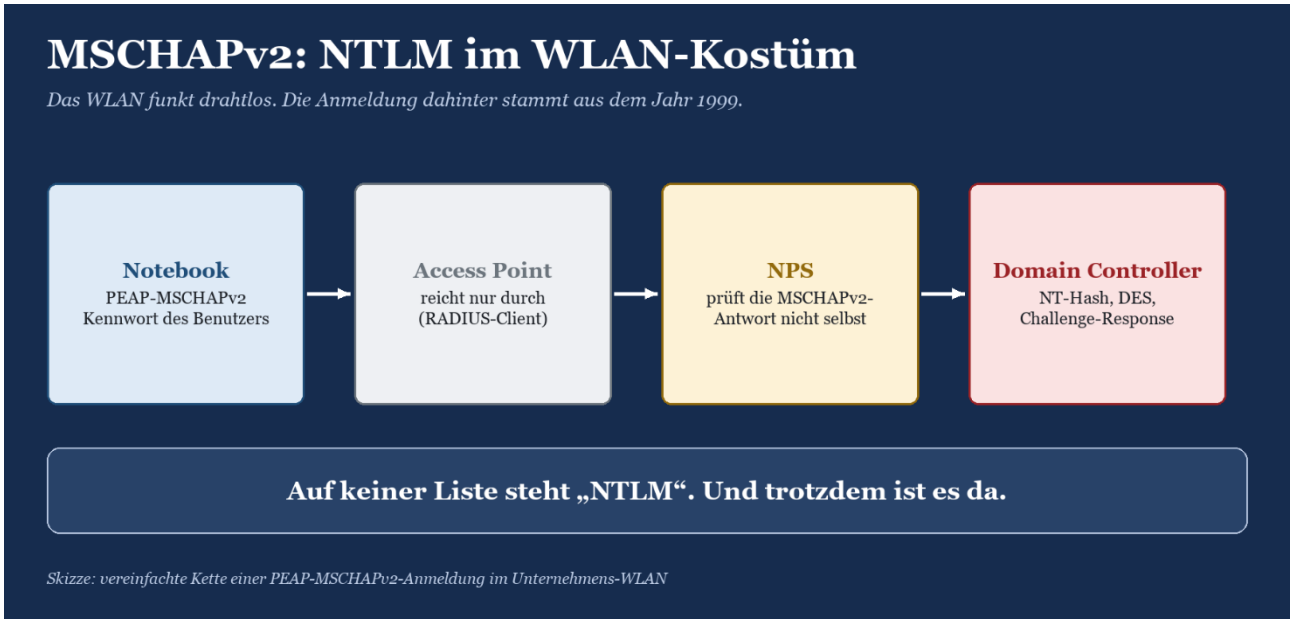
MSCHAPv2, NPS und WLAN: die versteckte NTLM-Abhängigkeit



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

BERATUNG
WLAN auf Zertifikate umstellen, ohne dass Montag die halbe Firma offline ist? Wir planen mit.
› **Beratung zur NTLM-Ablösung**

SCHULUNG
NTLM-Ereignisse, NPS-Protokolle und Umstellung: praxisnah für dein Team.
› **Schulung zum NTLM Diagnostiker**

Du hast die Liste gemacht. Dateiserver, Druckserver, das Fachverfahren der Lohnbuchhaltung, der Scanner im Flur. Alles, was NTLM spricht, steht drauf, sauber nach Ursache sortiert. Und dann kommt der Dienstag, an dem die ersten Notebooks nach dem Update morgens nicht mehr ins WLAN kommen, beziehungsweise nur noch nach Eingabe des Kennworts. Auf deiner Liste stand das WLAN nicht. Warum auch? Da steht ja „PEAP“ und „RADIUS“, nicht „NTLM“.

Genau das ist die versteckte Abhängigkeit, um die es hier geht: mschapv2 ntlm. PEAP-MSCHAPv2 und EAP-MSCHAPv2, die Klassiker für Unternehmens-WLAN, 802.1X am Switch und VPN-Zugänge über den Netzwerkrichtlinienserver (NPS), rechnen mit demselben Kennwort-Hash und derselben DES-Challenge-Response-Mathematik wie NTLMv1. Microsoft formuliert es nüchtern: WLAN- und VPN-Endpunkte auf MS-CHAPv2-Basis sind ähnlichen Angriffen ausgesetzt wie NTLMv1. Wer NTLM ablöst und MSCHAPv2 vergisst, hat den Keller aufgeräumt und den Dachboden ignoriert.

In diesem Beitrag erfährst du, wie die Kette Client, Access Point, NPS und Domain Controller funktioniert, warum Credential Guard die einmalige Anmeldung mit MSCHAPv2 bricht, wie du mit Bordmitteln herausfindest, wer bei dir noch per MSCHAPv2 anmeldet, und wie der Weg zu EAP-TLS oder PEAP-TLS mit eigener PKI aussieht. Den großen Rahmen der Ablösung findest du im Der Fahrplan zur NTLM-Abschaltung; hier geht es um das Funknetz und seine Verwandtschaft.

FAKTEN · MSCHAPv2 und NTLM in 30 Sekunden

MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol Version 2) bildet die Antwort aus dem NT-Hash des Kennworts und DES, genau wie NTLMv1. Nur die Verpackung ist eine andere.

PEAP-MSCHAPv2 legt einen TLS-Tunnel mit dem Zertifikat des NPS-Servers um diese Anmeldung. Der Tunnel schützt den Transport, ändert aber nichts an dem, was darin steckt.

NPS prüft die MSCHAPv2-Antwort nicht selbst, sondern lässt sie über den sicheren Kanal (Netlogon) von einem Domain Controller prüfen, also über denselben Weg wie eine durchgereichte NTLM-Anmeldung.

Credential Guard blockiert bei MS-CHAP laut Microsoft nur die einmalige Anmeldung (SSO). Mit Kennworteingabe klappt es weiter. Seit Windows 11 22H2 und Windows Server 2025 ist Credential Guard auf geeigneten, domänengebundenen Geräten standardmäßig eingeschaltet.

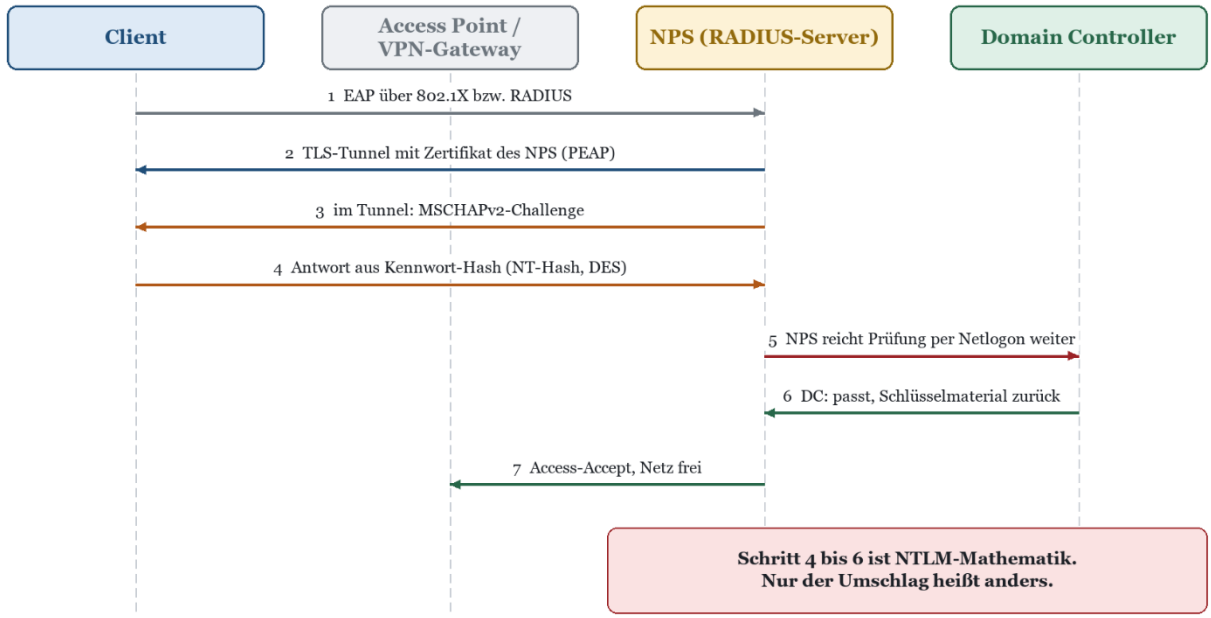
Microsofts Empfehlung: weg von PEAP-MSCHAPv2 und EAP-MSCHAPv2, hin zu zertifikatsbasiertem PEAP-TLS oder EAP-TLS. Credential Guard blockiert zertifikatsbasierte Anmeldungen nicht.

Warum MSCHAPv2 ein NTLM-Verfahren in Verkleidung ist

Schauen wir in die Kette. Ein Notebook der Musterwerk GmbH will ins WLAN „MW-Corp“. Der Access Point kann selbst niemanden prüfen, er ist nur RADIUS-Client und reicht die EAP-Nachrichten an den NPS weiter. Der NPS baut mit dem Notebook einen TLS-Tunnel auf (das ist das P in PEAP) und stellt darin eine MSCHAPv2-Challenge. Das Notebook antwortet mit einem Wert, der aus dem NT-Hash des Benutzerkennworts gerechnet ist. Und jetzt der entscheidende Punkt: Der NPS kennt diesen Hash nicht. Er schickt Challenge und Antwort an einen Domain Controller, der rechnet nach und meldet zurück, ob es passt.

Wer prüft eigentlich das Kennwort?

PEAP-MSCHAPv2 über NPS, vereinfacht: TLS-Tunnel außen, NTLM-Verwandtschaft innen



Skizze vereinfacht; Ablauf und Zuständigkeiten nach der Microsoft-Dokumentation zu NPS und PEAP

Wer schon einmal eine NTLM-Anmeldung an einem Mitgliedsserver verfolgt hat, erkennt das Muster: Challenge vom Server, Antwort vom Client, Durchreichen der Prüfung an den DC. Dass außen ein TLS-Tunnel liegt, ist gut gegen Mitlesen im Funk, macht aber aus der Kennwortanmeldung keine Zertifikatsanmeldung. Und weil die Mathematik im Inneren die von NTLMv1 ist, gilt auch dieselbe Schwäche: Wer einen Austausch abgreift, kann offline auf das

Kennwort losgehen. Ein falsch konfigurierter Client, der das NPS-Zertifikat nicht prüft, liefert diesen Austausch einem gefälschten Access Point frei Haus.

Was im Ereignisprotokoll davon ankommt

Hier wird es für die NTLM-Bestandsaufnahme spannend und ein wenig tückisch. MSCHAPv2 läuft nicht über die NTLM-Sicherheitsschnittstelle, die auf dem Client die Ereignisse 8001 oder 4020/4021 schreibt. Das Notebook taucht für die WLAN-Anmeldung also nicht als ausgehende NTLM-Verbindung auf. Sichtbar wird der Vorgang dort, wo die Prüfung tatsächlich stattfindet: auf dem NPS, der die Anmeldung an den DC durchreicht, und auf dem Domain Controller. Prüfe in deiner Umgebung, welche Spuren dort ankommen: das NPS-eigene Ereignis 6272 (Zugriff gewährt) oder 6273 (Zugriff verweigert) im Sicherheitsprotokoll des NPS, dazu Ereignis 4776 auf dem DC mit dem NPS als anfragender Station. Wie du 4776 liest, steht im Beitrag Ereignis 4776 auf dem Domain Controller: NTLM-Anmeldungen im Sicherheitsprotokoll.

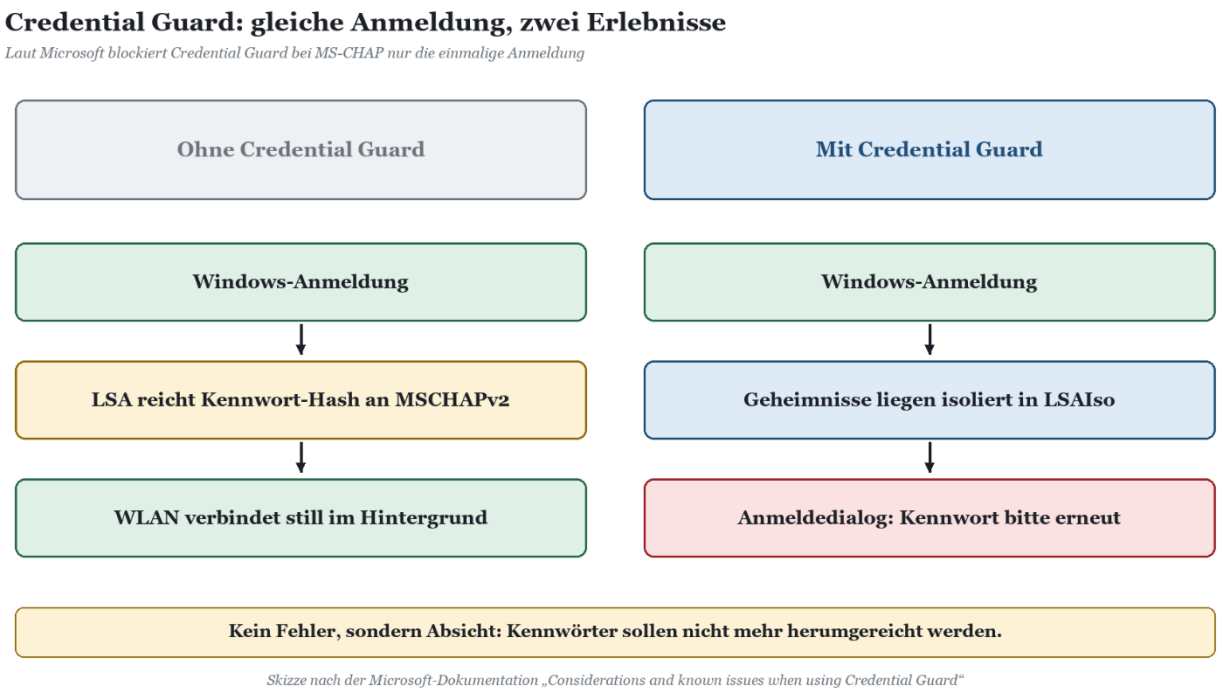
Wo	Ereignis	Was du siehst	Nutzen für die NTLM-Ablösung
NPS	6272 / 6273 (Sicherheitsprotokoll)	Benutzer, Client-Rechner, RADIUS-Client (Access Point), Netzwerkrichtlinie, Authentifizierungs- und EAP-Typ, bei 6273 ein Grundcode	Hauptquelle: Hier zählst du, wer per MSCHAPv2 hereinkommt.
Domain Controller	4776	Konto und anfragende Station; bei durchgereichten Prüfungen steht der NPS als Station drin	Bestätigt, dass der DC Anmeldungen im NTLM-Verfahren für den NPS prüft.
NPS und DC	8003 / 8004 bzw. 4022/4023, 4030–4033	nur, wenn erweitertes oder klassisches NTLM-Auditing aktiv ist; ob MSCHAPv2-Prüfungen dort erscheinen, prüfst du im Test	Ergänzend; nicht darauf verlassen, ohne es gesehen zu haben.
Client mit Credential Guard	4013 / 4014 (Microsoft-Windows-NTLM/Operational)	Hinweis, dass Credential Guard NTLMv1 bzw. den Zugriff auf Anmeldeschlüssel blockiert hat	Belegt, warum das SSO im WLAN plötzlich nicht mehr funktioniert.

WARNUNG · Der Client prüft das NPS-Zertifikat nicht? Dann schenkst du Angreifern Hashes

PEAP schützt nur, wenn das Notebook das Serverzertifikat des NPS gegen eine vertrauenswürdige Stammzertifizierungsstelle und den erwarteten Servernamen prüft. Steht im WLAN-Profil „Serverzertifikat nicht überprüfen“ oder dürfen Benutzer unbekannten Zertifikaten einfach vertrauen, reicht ein gefälschter Access Point mit gleichem Netzwerknamen. Der fängt die MSCHAPv2-Antwort ab, und der Rest ist Rechenzeit. Prüfe das WLAN-Profil in der Gruppenrichtlinie, bevor du irgendetwas anderes tust.

Credential Guard bricht die einmalige Anmeldung

Jetzt zum Dienstag mit den Kennwortdialogen. Credential Guard isoliert seit Windows 11 22H2 auf geeigneten, domänengebundenen Rechnern mit Enterprise- oder Education-Lizenz standardmäßig die Geheimnisse der lokalen Sicherheitsautorität in einer virtualisierungsbasierten Umgebung. Auf Windows Server 2025 gilt das für domänengebundene Server, die keine Domain Controller sind. Das Ziel: NTLM-Hashes und Kerberos-Tickets sollen nicht mehr aus dem Speicher zu klauen sein. Der Nebeneffekt: Verfahren, die für die einmalige Anmeldung genau diese Geheimnisse brauchen, gehen leer aus.



Microsoft listet die betroffenen Verfahren in den bekannten Problemen zu Credential Guard ausdrücklich auf. Für MS-CHAP, WDigest und NTLMv1 ist nur die einmalige Anmeldung blockiert. Das heißt: Das WLAN-Profil mit „Windows-Anmeldenamen und -kennwort automatisch verwenden“ funktioniert nicht mehr still im Hintergrund. Windows fragt nach dem Kennwort, in jeder neuen Sitzung, und kann es laut Microsoft auch nicht dauerhaft speichern. Das betrifft drahtlose und kabelgebundene 802.1X-Netze ebenso wie VPN-Verbindungen, die auf kennwortbasierten, unsicheren Verfahren beruhen. Die Einzelheiten stehen auf der Microsoft-Seite Considerations and known issues when using Credential Guard.

Verfahren	Wirkung von Credential Guard	Was der Benutzer merkt
PEAP-MSCHAPv2 / EAP-MSCHAPv2	nur SSO blockiert	Kennwortdialog statt automatischer Verbindung; vor der Windows-Anmeldung kein Benutzer-WLAN
NTLMv1	nur SSO blockiert	Kennwortabfrage bzw. Abbruch; Ereignis 4013 im NTLM-Betriebsprotokoll
WDigest	nur SSO blockiert	Kennwortabfrage
CredSSP-Delegierung	gespeicherte und SSO-Anmeldedaten nicht nutzbar	Remotedesktop mit gespeicherten Anmeldedaten scheitert, siehe Geschwister-Beitrag zu RDP
Kerberos ohne Einschränkung delegiert, DES	vollständig blockiert	Anwendung bricht
PEAP-TLS / EAP-TLS	nicht blockiert	nichts, es funktioniert einfach

Die Abkürzung, die keine ist

Die schnellste Lösung steht ebenfalls bei Microsoft, nur mit deutlichem Beipackzettel: Credential Guard abschalten. Es gibt keine Ausnahme je Protokoll oder Anwendung, nur an oder aus. Wer abschaltet, macht die gespeicherten Domänenanmeldedaten wieder diebstahlfähig, also genau das, wogegen Pass-the-Hash-Angriffe so gut funktionieren. Du tauschst eine nervige Kennwortabfrage

gegen eine offene Flanke. Das ist ungefähr so klug, wie den Rauchmelder abzuhängen, weil er beim Toasten piept.

Wichtig für die Planung: Wer Credential Guard vor dem Upgrade ausdrücklich deaktiviert hat, bekommt es nicht automatisch wieder eingeschaltet. Viele Umgebungen haben deshalb Credential Guard nicht wegen MSCHAPv2 aus, sondern aus Versehen. Wie Credential Guard sonst noch mit NTLM zusammenspielt, beschreibt der Beitrag Credential Guard und NTLM: was danach nicht mehr funktioniert. Für Remotedesktop gibt es einen eigenen Artikel: RDP, NLA und CredSSP: wann Remotedesktop auf NTLM zurückfällt.

TIPP · So bestätigst du den Verdacht auf einem betroffenen Notebook

Öffne die Ereignisanzeige und gehe zu Anwendungs- und Dienstprotokolle › Microsoft › Windows › NTLM › Operational. Ereignis 4013 (Warnung) meldet einen blockierten NTLMv1-Versuch, Ereignis 4014 (Fehler) einen von Credential Guard blockierten Zugriff auf den Anmeldeschlüssel. Ob Credential Guard läuft, zeigt dir msinfo32 unter „Ausgeführte Dienste für virtualisierungsbasierte Sicherheit“.

Was das für die NTLM-Ablösung heißt: Bestand mit Bordmitteln

Drei Konsequenzen solltest du dir an die Wand hängen. Erstens: MSCHAPv2 gehört auf deine NTLM-Liste, auch wenn es in keinem Ereignis 8001 eines Clients erscheint. Zweitens: Jede Schraube, die du am Domain Controller in Richtung „weniger NTLM“ drehst, kann den NPS treffen. Das gilt für die Einschränkungsrichtlinien aus dem Beitrag Die Restrict-NTLM-Richtlinien richtig einsetzen ebenso wie für die Stufe 5 der LAN Manager-Authentifizierungsebene aus LmCompatibilityLevel richtig setzen: NTLMv2 erzwingen ohne Ausfall. Plane für beide einen Test mit echter WLAN-Anmeldung über den NPS ein, bevor du sie auf den DCs scharf schaltest. Drittens: Mit der nächsten Windows-Server-Version ist NTLM standardmäßig abgeschaltet (Phase 3). Verlass dich nicht darauf, dass kennwortbasiertes WLAN dann ungeschoren davonkommt, sondern plane die Umstellung auf Zertifikate so, dass die Frage gar nicht mehr gestellt werden muss.

Schritt 1: NPS-Überwachung einschalten

Die Ereignisse 6272 und 6273 schreibt der NPS nur, wenn die Unterkategorie „Netzwerkrichtlinienserver“ der erweiterten Überwachungsrichtlinie für Erfolg und Fehler aktiv ist. Auf dem NPS prüfst und setzt du das so:

```
auditpol /get /subcategory:"Network Policy Server"
auditpol /set /subcategory:"Network Policy Server" /success:enable /failure:enable
```

Dauerhaft gehört das natürlich in eine Gruppenrichtlinie für die OU der NPS-Server, nicht in eine Konsolensitzung. Die NTLM-Überwachung auf DCs und Servern richtest du parallel ein, wie in Erweitertes NTLM-Auditing einschalten beschrieben; das NTLM-Audit-GPO-Skript nimmt dir die Klickarbeit ab.

Schritt 2: Wer meldet sich per MSCHAPv2 an?

Mit PowerShell zählst du die gewährten Zugriffe nach EAP-Typ und Netzwerkrichtlinie. Wie immer gilt: Werte aus den Ereignisfeldern lesen, nicht aus dem Meldungstext, denn weitergeleitete Ereignisse kommen gern ohne Text an. Die Feldnamen prüfst du einmal mit einem Beispielereignis, bevor du dich auf das Skript verlässt:

```
# Feldnamen eines Beispielereignisses anzeigen
$e = Get-WinEvent -FilterHashtable @{LogName='Security'; Id=6272} -MaxEvents 1
([xml]$e.ToXml()).Event.EventData.Data | Format-Table Name, '#text' -AutoSize
```

```
# Zugriffe der letzten 7 Tage nach EAP-Typ und Richtlinie
Get-WinEvent -FilterHashtable @{LogName='Security'; Id=6272; StartTime=(Get-Date).AddDays(-7)}
|
  ForEach-Object {
    $d = @{}; ([xml]$_.ToXml()).Event.EventData.Data | ForEach-Object { $d[$_.Name] =
$_.'#text' }
    [pscustomobject]@{ Benutzer=$d['SubjectUserName']; Rechner=$d['SubjectMachineName'];
                       Richtlinie=$d['NetworkPolicyName']; EAP=$d['EAPType'] }
  } | Group-Object Richtlinie, EAP | Sort-Object Count -Descending |
  Select-Object Count, Name
```

Alles, was als „Microsoft: Gesichertes Kennwort (EAP-MSCHAP v2)“ oder in der englischen Fassung als „Microsoft: Secured password (EAP-MSCHAP v2)“ erscheint, ist dein MSCHAPv2-Bestand. Weitere Rezepte zum Filtern und Gruppieren findest du in NTLM-Ereignisse mit PowerShell auswerten: Get-WinEvent-Rezepte. Fehlgeschlagene Anmeldungen in 6273 tragen einen Grundcode; bei Kennwortproblemen landest du auf dem DC oft bei 0xC000006D, den der Beitrag Fehlercodes 0xC000006D und Co.: fehlgeschlagene NTLM-Anmeldungen deuten erklärt.

Schritt 3: Die Ausnahmen aufschreiben

Der Bestand ist selten homogen. Typisch ist dieses Bild bei der Sparfuchs & Partner Steuerberatungs GmbH: 140 Notebooks im Mitarbeiter-WLAN, dazu zwölf Smartphones mit Kennwort, drei Etikettendrucker, die per 802.1X mit einem Dienstkonto ins Netz gehen, und ein VPN-Zugang für die Partner im Homeoffice. Jede dieser Gruppen braucht einen eigenen Weg.

Gerätegruppe	Heute	Ziel	Knackpunkt
Domänen-Notebooks	PEAP-MSCHAPv2 mit Benutzerkennwort	EAP-TLS mit Computer- und/oder Benutzerzertifikat	Autoenrollment, Zertifikatsvorlagen
Smartphones und Tablets	PEAP-MSCHAPv2 mit Benutzerkennwort	EAP-TLS mit Zertifikat aus der Geräteverwaltung	Zertifikatsverteilung über das MDM prüfen
Drucker, Scanner, IoT im 802.1X-Netz	PEAP-MSCHAPv2 mit Dienstkonto	EAP-TLS, sofern das Gerät es kann; sonst eigenes Netz mit MAC-Filter und Segmentierung	Herstellerfrage, Firmware
VPN (RAS über NPS)	EAP-MSCHAPv2 oder MS-CHAPv2	zertifikatsbasiertes EAP	Gateway und Client müssen mitspielen
Gäste	irgendwas mit Kennwort am Empfang	getrenntes Gastnetz ohne Domänenanmeldung	gehört gar nicht an den NPS mit Domänenkonten

Wo es mit Bordmitteln mühsam wird

Für einen NPS und ein WLAN ist das alles gut machbar. In echten Umgebungen sieht es anders aus: zwei oder drei NPS-Server für Ausfallsicherheit, getrennte Richtlinien für WLAN, LAN und VPN, dazu Hunderte Clients, deren NTLM-Ereignisse auf ganz andere Server zeigen. Die WLAN-Spur liegt im NPS-Protokoll, die NTLM-Spur auf DCs und Mitgliedsservern, und den Zusammenhang stellst du per Tabellenkalkulation her. Bis der Abgleich fertig ist, hat sich die Hälfte der Notebooks schon wieder neu angemeldet. Und spätestens beim Abschalten willst du nicht schätzen, sondern wissen, welche Konten und Geräte noch an diesem einen Server hängen.

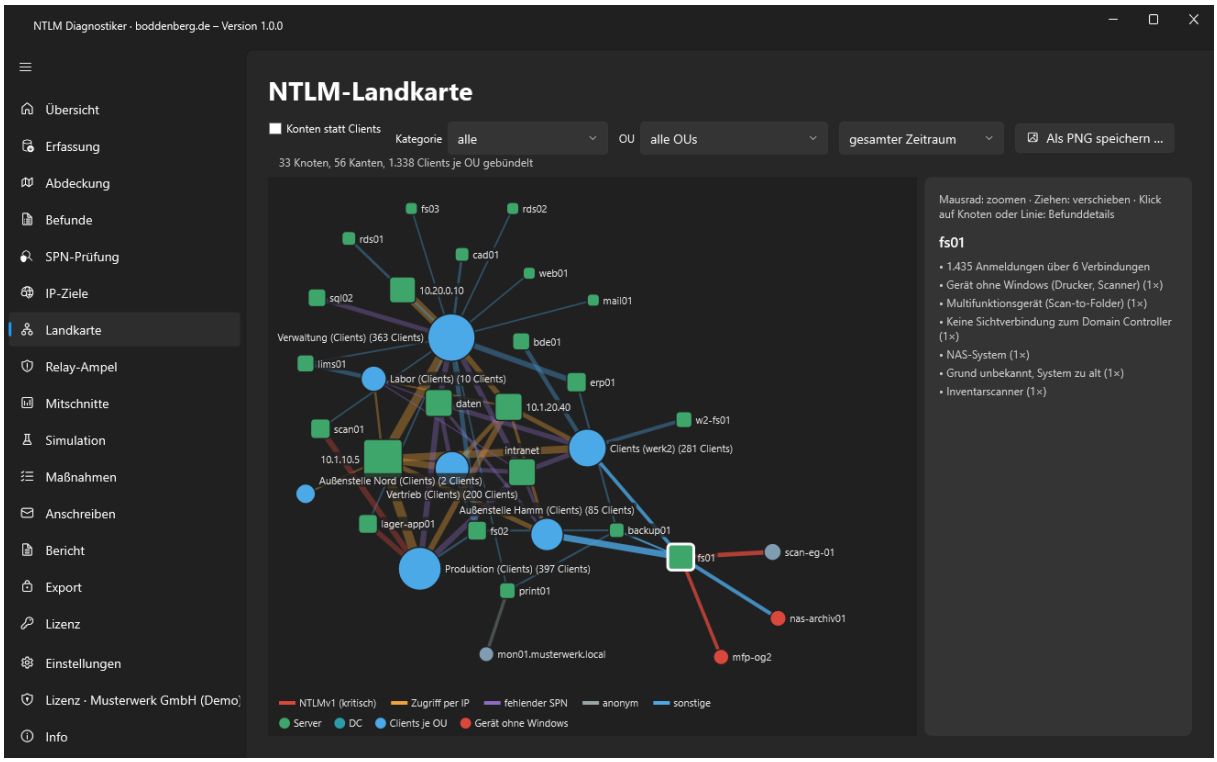
Genau für diese Frage ist der NTLM Diagnostiker gebaut. Er liest NTLM-Ereignisse vom Domain Controller, über einen Windows Event Collector, per Direktabfrage oder aus importierten Dateien, fasst gleichartige Verbindungen zusammen und zeigt, wer mit wem per NTLM spricht. Er arbeitet ausschließlich lesend: Er ändert keine Richtlinie, keinen SPN und keine NPS-Einstellung.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Den NPS als NTLM-Ziel sichtbar machen

In der Kommunikationsmatrix erscheint dein NPS-Server als Ziel, an dem sich Konten im NTLM-Verfahren anmelden. Damit steht er auf derselben Liste wie Dateiserver und Fachanwendungen, statt in einem separaten Protokoll zu verschwinden. Die Konten-Sicht zeigt dir, welche Benutzer- und Dienstkonten dort auftauchen, etwa das Dienstkonto der Etikettendrucker.

Die NTLM-Landkarte stellt das grafisch dar: Server, Clients je OU, Domain Controller und Geräte ohne Windows als Knoten, die Verbindungen farbig nach Kategorie wie NTLMv1, Zugriff per IP oder fehlender SPN. Mit den Filtern für Kategorie, OU und Zeitraum grenzt du ein, ein Klick auf einen Server zeigt rechts Anmeldezahlen und Befunde. Über „Als PNG speichern“ landet die Karte direkt in deiner Projektdokumentation.

Vor dem Umbau beantwortet der Abschalt-Simulator die Frage „Was bricht, wenn ich NTLM jetzt abdrehe?“ mit einem Vertrauenswert aus der Abdeckung. Die Abdeckungskarte verrät dir, ob deine NPS-Server überhaupt Ereignisse liefern oder zu den stillen Maschinen gehören. Ausnahmelisten und Befehle zeigt der Diagnostiker zum Kopieren an; ausgeführt werden sie von dir.



So siehst du auf der NTLM-Landkarte, welche Server, Clients und Geräte per NTLM miteinander sprechen, hier mit Details zum Server fs01 (Demodaten der Musterwerk GmbH).

Für den Einstieg reicht die kostenlose Edition Express: ein Fünf-Minuten-Befund direkt vom DC mit Readiness-Ampel, Abdeckungskarte, Top-10-Verursachern, Hinweisen aus der Wissensbasis und einem NTLMv1-Alarm mit Anzahl und Top 5. Den vollen Funktionsumfang mit Kommunikationsmatrix, Landkarte und Simulator kannst du sieben Tage je Domäne testen. Wer die Umstellung auf Zertifikate nicht allein stemmen will, findet in der Beratung zur NTLM-Ablösung Unterstützung von der Bestandsaufnahme bis zur neuen NPS-Richtlinie.

Der Ausweg: EAP-TLS oder PEAP-TLS mit eigener PKI

Die gute Nachricht: Die Lösung ist seit Jahren dieselbe und gut dokumentiert. Statt eines Kennworts weist sich der Client mit einem Zertifikat aus. Bei EAP-TLS geschieht das direkt im

TLS-Handshake, bei PEAP-TLS innerhalb des PEAP-Tunnels. Kein NT-Hash, kein DES, keine Challenge-Response, nichts, was ein gefälschter Access Point offline knacken könnte. Und weil Credential Guard zertifikatsbasierte Anmeldungen nicht blockiert, ist auch der Kennwortdialog Geschichte.

Wer ist NTLM-abhängig, wer nicht?

Authentifizierungsverfahren für WLAN, LAN und VPN im Vergleich

Verfahren	Kennwort	SSO mit Credential Guard	NTLM-Verwandtschaft	Bewertung
PEAP-MSCHAPv2	ja	nein	ja	ablösen
EAP-MSCHAPv2 (VPN)	ja	nein	ja	ablösen
MS-CHAP (Version 1)	ja	nein	ja	sofort weg
PEAP-TLS	nein	ja	nein	Ziel
EAP-TLS	nein	ja	nein	Ziel

Skizze nach den Empfehlungen von Microsoft zu Credential Guard; vereinfacht

Kriterium	PEAP-MSCHAPv2	PEAP-TLS	EAP-TLS
Nachweis des Clients	Kennwort (NT-Hash)	Zertifikat im Tunnel	Zertifikat
Zertifikat auf dem NPS	ja	ja	ja
Zertifikat auf jedem Client	nein	ja	ja
NTLM-Verwandtschaft	ja, Mathematik wie NTLMv1	nein	nein
SSO mit Credential Guard	nein	ja	ja
Offline-Angriff nach Abfangen	möglich	nicht auf ein Kennwort	nicht auf ein Kennwort
Aufwand	gering, schon da	PKI nötig	PKI nötig
Typischer Einsatz	Altbestand	wenn PEAP-Infrastruktur bleiben soll	Standard für Neuplanung

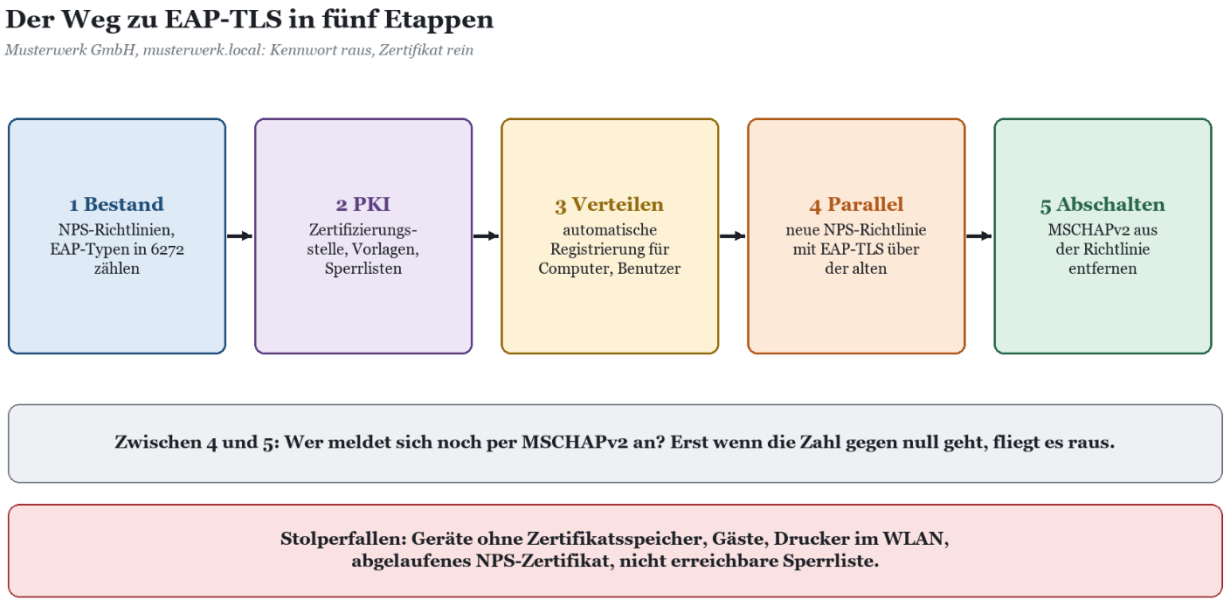
Was die PKI liefern muss

Eine eigene Unternehmens-PKI mit den Active Directory-Zertifikatdiensten ist der übliche Unterbau. Sie liefert drei Dinge: ein Serverzertifikat für jeden NPS mit dem Zweck Serverauthentifizierung, Client-Zertifikate für Computer oder Benutzer mit dem Zweck Clientauthentifizierung, verteilt per automatischer Registrierung über Gruppenrichtlinie, und erreichbare Sperrlisten. Der letzte Punkt ist der, an dem die meisten Umstellungen am ersten Tag scheitern: Kann der NPS die Sperrliste der ausstellenden Zertifizierungsstelle nicht abrufen, lehnt er die Anmeldung ab. Ein abgelaufenes NPS-Zertifikat hat denselben Effekt, nur mit größerem Publikum.

- **Computerzertifikat:** Das Gerät kommt vor der Benutzeranmeldung ins Netz. Gruppenrichtlinien, Anmeldeskripte und Kennwortänderungen funktionieren, auch für Benutzer, die sich zum ersten Mal anmelden.
- **Benutzerzertifikat:** Die Netzanmeldung hängt am Menschen, nicht am Gerät. Nützlich für unterschiedliche VLANs je Abteilung, aber erst nach der Windows-Anmeldung verfügbar.
- **Beides:** Computeranmeldung beim Start, Benutzeranmeldung danach. Mehr Flexibilität, mehr Testaufwand.

Umstellung ohne Funkstille

Der Trick ist die Parallelphase. Du legst im NPS eine neue Netzwerkrichtlinie mit EAP-TLS an und setzt sie in der Reihenfolge vor die alte MSCHAPv2-Richtlinie. Clients mit Zertifikat und neuem WLAN-Profil treffen die neue Regel, alle anderen fallen weiter auf die alte. Über die Ereignisse 6272 siehst du jeden Tag, wie der Anteil der MSCHAPv2-Anmeldungen sinkt. Erst wenn er gegen null geht und die verbleibenden Geräte erklärt sind, entfernst du MSCHAPv2 aus der Richtlinie.



Skizze: Reihenfolge beispielhaft; Dauer hängt vor allem an Etappe 2 und deinen Exoten

AUS DER PRAXIS · Trendforge Digital GmbH: die drei Etikettendrucker

Bei der Trendforge Digital GmbH (trendforge.local) lief die Umstellung der Notebooks in zwei Wochen durch. Übrig blieben drei Etikettendrucker im Versand, die ausschließlich PEAP-MSCHAPv2 konnten und sich mit einem gemeinsamen Dienstkonto anmeldeten. Das Kennwort dieses Kontos war seit 2019 nicht geändert worden, weil man ja sonst an alle drei Drucker hätte müssen. Die Lösung war unspektakulär: eigenes SSID für die Drucker, eigenes VLAN, Zugriff nur auf den Druckserver, MSCHAPv2 nur in genau dieser einen NPS-Richtlinie, und ein Termin für den Gerätetausch im Investitionsplan. Ausnahme dokumentiert, Risiko begrenzt, Kennwort endlich geändert.

WICHTIG · Vor dem Abschalten von MSCHAPv2 prüfen

Hat jeder NPS ein gültiges Serverzertifikat, und vertrauen alle Clients dessen Stammzertifizierungsstelle?

Ist die Sperrliste der ausstellenden Zertifizierungsstelle vom NPS aus erreichbar, auch bei Ausfall

eines Webservers?

Bekommen neue Geräte ihr Zertifikat, bevor sie das WLAN brauchen? Plane für die Erstinstallation einen kabelgebundenen oder separaten Bereitstellungszugang ein.

Sind alle Geräte ohne Zertifikatsspeicher erfasst und mit eigener Ausnahme versehen?

Gibt es einen Rückweg: alte Netzwerkrichtlinie deaktiviert, nicht gelöscht?

Wie viel Arbeit das insgesamt bedeutet, hängt fast nur an der PKI. Steht sie schon, ist die WLAN-Umstellung ein überschaubares Projekt. Fehlt sie, ist sie die eigentliche Baustelle. Eine Einordnung für die Budgetplanung findest du in Was kostet die NTLM-Ablösung? Aufwand realistisch schätzen.

FAQ zu MSCHAPv2 und NTLM

Ist MSCHAPv2 dasselbe wie NTLM?

Nicht dasselbe Protokoll, aber dieselbe Kryptografie. MSCHAPv2 berechnet die Antwort aus dem NT-Hash des Kennworts mit DES, wie NTLMv1. Microsoft schreibt, dass MS-CHAPv2-basierte WLAN- und VPN-Endpunkte ähnlichen Angriffen ausgesetzt sind wie NTLMv1.

Schützt der TLS-Tunnel von PEAP nicht ausreichend?

Er schützt den Transport, solange der Client das Serverzertifikat sauber prüft. Gegen einen gefälschten Access Point bei nachlässig konfigurierten Clients hilft er nicht, und an der Kennwortbasis der Anmeldung ändert er nichts.

Warum fragt Windows nach dem Update plötzlich nach dem WLAN-Kennwort?

Sehr wahrscheinlich, weil Credential Guard eingeschaltet wurde. Seit Windows 11 22H2 ist es auf geeigneten, domänengebundenen Geräten standardmäßig aktiv und blockiert bei MS-CHAP die einmalige Anmeldung. Die Ereignisse 4013 und 4014 im NTLM-Betriebsprotokoll bestätigen den Verdacht.

Kann ich Credential Guard nur für das WLAN ausnehmen?

Nein. Laut Microsoft gibt es keine Richtlinien je Protokoll oder Anwendung, nur an oder aus. Abschalten macht die gespeicherten Domänenanmeldedaten wieder angreifbar.

Sehe ich MSCHAPv2-Anmeldungen in den NTLM-Ereignissen der Clients?

In der Regel nicht, denn die WLAN-Anmeldung läuft nicht über die NTLM-Schnittstelle des Clients. Die belastbare Quelle sind die Ereignisse 6272 und 6273 auf dem NPS sowie die Prüfungen auf dem Domain Controller, bei denen der NPS als anfragende Station erscheint.

Bricht das WLAN, wenn ich die Domain Controller auf LmCompatibilityLevel 5 setze?

Das hängt von deiner Umgebung ab und ist nicht pauschal zu beantworten. Teste es mit einer echten WLAN-Anmeldung über den NPS gegen einen DC mit Stufe 5, bevor du produktiv umstellst. Der Beitrag LmCompatibilityLevel richtig setzen: NTLMv2 erzwingen ohne Ausfall beschreibt die Reihenfolge.

Brauche ich für EAP-TLS zwingend eine eigene PKI?

Du brauchst eine Zertifizierungsstelle, der NPS und Clients vertrauen, und eine Verteilung der Client-Zertifikate. In Active Directory-Umgebungen ist das meist eine eigene Unternehmens-PKI mit automatischer Registrierung per Gruppenrichtlinie.

Was ist mit Geräten, die kein EAP-TLS können?

Erfassen, isolieren, befristen. Eigene SSID oder eigenes VLAN, Zugriff nur auf das Nötigste, eine eigene NPS-Richtlinie für genau diese Geräte, ein dokumentierter Austauschtermin. Dienstkonten solcher Geräte bekommen starke, regelmäßig geänderte Kennwörter.

Gehört das WLAN wirklich in ein NTLM-Projekt?

Ja. Es nutzt dieselbe Kennwort-Mathematik, dieselbe Prüfkette über den DC und wird von denselben Härtungsmaßnahmen getroffen. Nimm es auf deine Checkliste vor dem NTLM-Stichtag: 25 Prüfpunkte mit auf.

Fazit: Das WLAN gehört auf die NTLM-Liste

MSCHAPv2 ist der Gast auf der NTLM-Party, den niemand eingeladen hat und den trotzdem alle kennen. Er heißt anders, sitzt in einem TLS-Tunnel und taucht in den üblichen Client-Ereignissen nicht auf. Aber er rechnet wie NTLMv1, lässt sich vom Domain Controller prüfen wie eine durchgereichte NTLM-Anmeldung und verliert mit Credential Guard seine einmalige Anmeldung. Spätestens wenn die Belegschaft morgens Kennwortdialoge wegklickt, ist er nicht mehr zu übersehen.

Der Weg raus ist klar: Bestand über die NPS-Ereignisse erheben, PKI aufbauen oder aufräumen, EAP-TLS oder PEAP-TLS parallel einführen, MSCHAPv2 auf erklärte Ausnahmen zurückdrängen. Das ist kein Wochenendprojekt, aber eines mit sichtbarem Ende. Und danach ist dein WLAN nicht nur NTLM-frei, sondern auch gegen den Klassiker mit dem gefälschten Access Point gewappnet. Schwarzer Humor zum Schluss: Das einzige, was dann noch per Kennwort ins Netz kommt, ist der Besuch am Empfang. Und der landet im Gastnetz.

WEITERLESEN · Weiter in dieser Serie

› Credential Guard und NTLM: was danach nicht mehr funktioniert
› LmCompatibilityLevel richtig setzen: NTLMv2 erzwingen ohne Ausfall
› Ereignis 4776 auf dem Domain Controller: NTLM-Anmeldungen im Sicherheitsprotokoll
› Die Restrict-NTLM-Richtlinien richtig einsetzen
› RDP, NLA und CredSSP: wann Remotedesktop auf NTLM zurückfällt
› NTLM schrittweise abschalten
› Checkliste vor dem NTLM-Stichtag: 25 Prüfpunkte