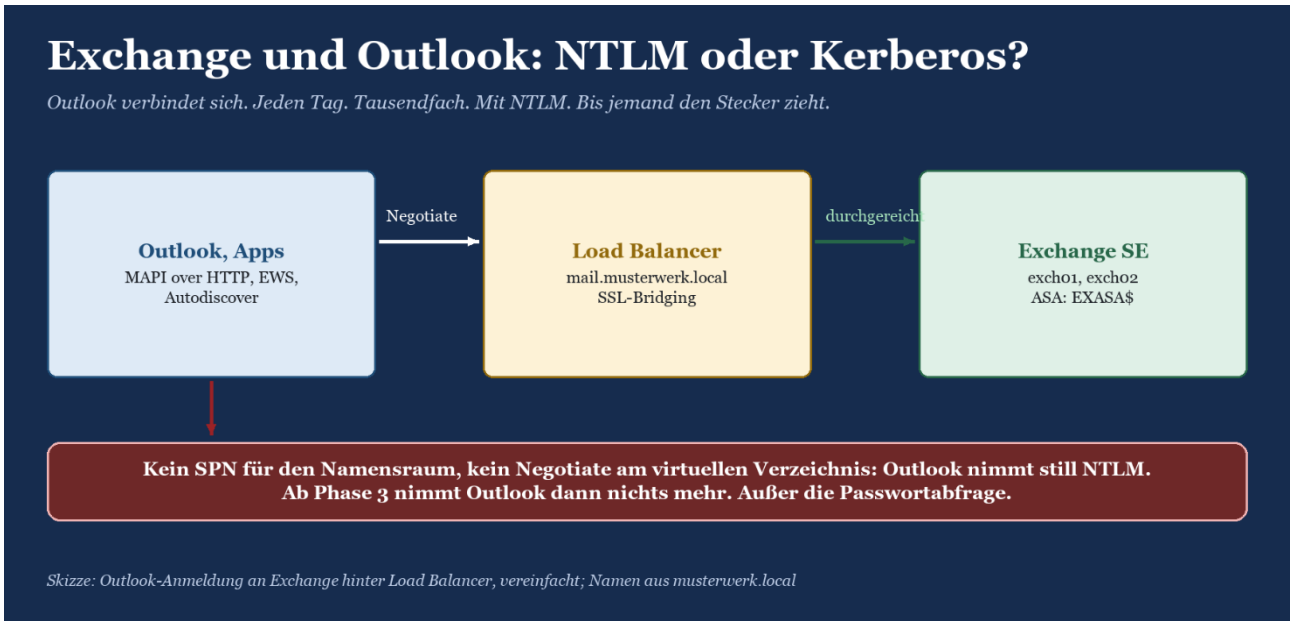
Exchange Server und Outlook: NTLM bei MAPI over HTTP und EWS



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

BERATUNG
Exchange hinter Load Balancer, Extended Protection, Hybrid? Wir sortieren mit.
› Beratung zur NTLM-Ablösung

SCHULUNG
NTLM-Ereignisse lesen, SPNs prüfen, Abschaltung testen: praxisnah für dein Team.
› Schulung zum NTLM Diagnostiker

Exchange ist in jeder NTLM-Auswertung der Dauerbrenner. Jeder Outlook-Client im Haus meldet sich mehrmals pro Stunde am Postfachserver an, holt Autodiscover, synchronisiert über MAPI over HTTP, fragt Frei/Gebucht-Zeiten per EWS ab und lädt das Offline-Adressbuch. Dazu kommen die Fachanwendungen, die per EWS Termine eintragen, Mails archivieren oder Tickets aus Postfächern fischen. Und all das läuft in sehr vielen Häusern mit NTLM. Nicht, weil jemand das so entschieden hat, sondern weil Exchange hinter einem Load Balancer ohne zusätzliches Konto schlicht kein Kerberos kann.

Solange NTLM erlaubt ist, merkt das niemand. Mit der nächsten Windows-Server-Version ist NTLM aber standardmäßig abgeschaltet, und dann wird aus dem stillen Rückfall die Passwortabfrage in Outlook, die sich auch durch dreimaliges Eintippen nicht beeindrucken lässt. Wer nach exchange ntlm kerberos sucht, will diesen Montag verhindern. In diesem Beitrag siehst du, wo Exchange Server und Outlook NTLM nutzen, wie du Kerberos hinter dem Load Balancer mit einem alternativen Dienstkonto (ASA) einrichtest, welche SPNs der Namensraum braucht, was Extended Protection damit zu tun hat und wie du die Anwendungen mit EWS-Zugriff findest, die beim Abschalten als Erste umfallen.

Die Phasen der Ablösung und den Zeitplan erklärt NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet. Das allgemeine Prinzip von Negotiate im IIS steht in NTLM in IIS und Webanwendungen: Negotiate statt NTLM. Hier geht es nur um Exchange Server, also Exchange 2016, 2019 und die Subscription Edition (SE) on-premises.

FAKTEN · Exchange, Outlook und Kerberos in 30 Sekunden

Outlook für Windows meldet sich per Negotiate an. Negotiate versucht Kerberos und fällt still auf NTLM zurück, wenn der Client kein Dienstticket für den angefragten Namen bekommt.

Für einen gemeinsamen Namensraum wie mail.musterwerk.local hinter einem Load Balancer brauchen alle Exchange-Server mit Clientzugriffsdiensten dasselbe alternative Dienstkonto (ASA). Die SPNs des Namensraums gehören an dieses Konto, nicht an einen einzelnen Server.

Microsoft empfiehlt als ASA ein Computerkonto. Gruppenverwaltete Dienstkonten (gMSA) werden von Exchange on-premises dafür nicht unterstützt.

Extended Protection ist seit Exchange 2019 CU14 standardmäßig aktiv und verträgt sich nicht mit SSL-Offloading und nicht mit NTLMv1.

Wo Exchange und Outlook NTLM nutzen

Exchange ist kein einzelner Dienst, sondern eine Sammlung virtueller Verzeichnisse im IIS. Jedes hat eigene Authentifizierungseinstellungen, und jedes kann NTLM anbieten. Für die NTLM-Ablösung zählen vor allem die Wege, über die sich Windows-Clients und Anwendungen mit ihrer Domänenanmeldung melden.

Wo Exchange überall Windows-Anmeldung annimmt

Jedes virtuelle Verzeichnis ist eine eigene Tür, und jede Tür hat ihr eigenes Schloss

Zugriffsweg	Wer klopft an	SPN, den der Client sucht	Typisches Risiko
/mapi	Outlook für Windows	HTTP/mail.musterwerk.local	kein ASA, kein Negotiate
/EWS	Outlook, Mac, Fach-Apps	HTTP/mail.musterwerk.local	Apps per IP oder nur NTLM
/Autodiscover	Outlook, Apps	HTTP/autodiscover.musterwerk.local	SPN vergessen
/OAB	Outlook	HTTP/mail.musterwerk.local	folgt dem Namensraum
/rpc (Outlook Anywhere)	Altclients	HTTP/mail.musterwerk.local	steht oft auf Ntlm
/owa, /ecp	Browser	Formularanmeldung	kein Thema, solange FBA

Skizze: typische Belegung; prüfe die tatsächlichen URLs mit Get-...VirtualDirectory

MAPI over HTTP und Outlook Anywhere

MAPI over HTTP ist seit Exchange 2016 das Standardprotokoll von Outlook für Windows. Ob der Server hier Kerberos überhaupt anbietet, steuert die Eigenschaft IISAuthenticationMethods des MAPI-Verzeichnisses. Steht dort nur Ntlm (und in Hybridumgebungen OAuth), bekommt Outlook gar keine Chance auf Kerberos. Erst mit Negotiate in der Liste darf der Client ein Ticket vorlegen. Für ältere Clients über Outlook Anywhere (RPC over HTTP) gilt dasselbe für InternalClientAuthenticationMethod, das in gewachsenen Umgebungen gern noch auf Ntlm steht.

```
# Was bieten die Verzeichnisse an? (Exchange Management Shell)
Get-MapiVirtualDirectory | Format-List Server, InternalUrl, IISAuthenticationMethods
Get-OutlookAnywhere | Format-List Server, InternalHostname, InternalClientAuthenticationMethod
Get-WebServicesVirtualDirectory | Format-List Server, InternalUrl, WindowsAuthentication
```

```
Get-ClientAccessService | Format-List Name, AutoDiscoverServiceInternalUri
```

Die Ausgabe ist gleichzeitig deine Namensliste: Jeder Hostname in InternalUrl, InternalHostname und AutoDiscoverServiceInternalUri wird später ein SPN. Steht dort statt des Namensraums der Servername, etwa exch01.musterwerk.local, geht Outlook direkt an diesen Server. Das ist für Kerberos sogar unkritisch, weil das Computerkonto über den HOST-SPN ohnehin passt, aber dann brauchst du deinen Load Balancer auch nicht.

EWS, Autodiscover und Offline-Adressbuch

Outlook nutzt EWS für Frei/Gebucht, Abwesenheitsnotizen und einige Add-Ins, Autodiscover für die Konfiguration und das OAB-Verzeichnis für das Offline-Adressbuch. Alle drei laufen über dieselben Namen wie MAPI, meist mail.musterwerk.local und autodiscover.musterwerk.local, und nutzen im IIS die Windows-Authentifizierung mit den Anbietern Negotiate und NTLM. Fehlt der SPN für autodiscover.musterwerk.local, holt sich Outlook seine Konfiguration also mit NTLM, auch wenn MAPI danach sauber Kerberos spricht. Das ist der Klassiker der halben Umstellung.

Anwendungen mit EWS-Zugriff

Der eigentliche Ärger kommt selten von Outlook, sondern von allem, was sich sonst noch per EWS an Exchange anmeldet: CRM-Systeme, die Termine schreiben, Archivlösungen, Ticketsysteme, die ein Funktionspostfach leeren, Telefonanlagen mit Kalenderabgleich, Raumbuchungssysteme und das selbstgeschriebene Skript aus dem Jahr 2015. Diese Programme laufen meist unter einem Dienstkonto auf einem Anwendungsserver, und sie haben drei typische Gewohnheiten, die Kerberos verhindern:

- **Die URL enthält eine IP-Adresse.** Für https://10.20.0.25/EWS/Exchange.asmx gibt es keinen SPN. Ergebnis: NTLM, jedes Mal.
- **Die Bibliothek kann nur NTLM oder Basic.** Ältere EWS-Bibliotheken, besonders in Java oder in eingebetteten Systemen, sprechen gar kein Negotiate. Hier hilft kein SPN, sondern nur ein Update oder ein anderer Anmeldeweg.
- **Die Anmeldedaten stehen im Klartext in der Konfiguration.** Dann meldet sich das Programm mit Benutzername und Kennwort an, und ob daraus Kerberos oder NTLM wird, entscheidet die Bibliothek. Mit einer guten Bibliothek und dem richtigen Namen klappt auch hier Kerberos.

Wie Java-Anwendungen grundsätzlich zu Kerberos kommen, steht in Java-Anwendungen und NTLM: Kerberos mit SPNEGO. Dienstkonten, die in Konfigurationsdateien vergessen wurden, behandelt Dienstkonten als NTLM-Quelle: finden, prüfen, umstellen.

So sieht das in den Ereignissen aus

Auf dem Client landet die NTLM-Anmeldung als Ereignis 4020 oder 4021 im Protokoll Microsoft-Windows-NTLM/Operational, sofern das erweiterte Auditing aktiv ist. Für Exchange erkennst du sie an einem ProcessName wie OUTLOOK.EXE oder dem Prozess deiner Fachanwendung und an einem TargetService der Form HTTP/mail.musterwerk.local. Auf den Exchange-Servern selbst siehst du die eingehende Seite in 4022 und 4023 mit RemoteClientMachine und ClientIP, in der klassischen Überwachung als 8003 mit dem anfragenden Client im Feld Workstation. Wie du das Auditing einschaltest, steht in Erweitertes NTLM-Auditing einschalten: Schritt für Schritt; die passende Gruppenrichtlinie baut dir das NTLM-Audit-GPO-Skript.

Feld	Typischer Wert bei Exchange	Was es dir sagt
ProcessName	OUTLOOK.EXE, crmsync.exe, w3wp.exe	wer anfragt: Outlook, Fachanwendung, Webanwendung
TargetService	HTTP/mail.musterwerk.local	welcher SPN gesucht wurde; Namensraum

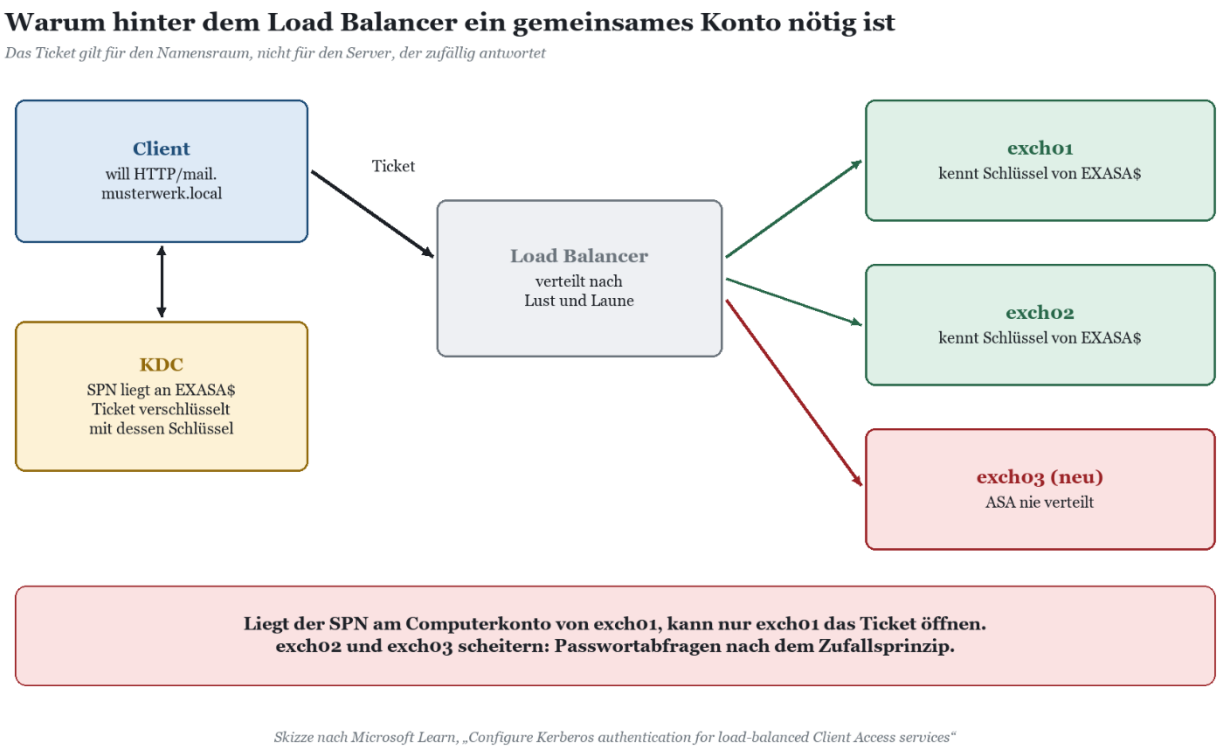
		statt Server
TargetIP	10.20.0.25	Zugriff per IP: hier gibt es keinen SPN
NtlmUsageReason	Begründungstext, z. B. Ziel nicht auflösbar	die eigentliche Ursache; der Text zählt, nicht die Nummer
ChannelBindingStatus	vorhanden oder fehlend	ob Extended Protection greifen kann
Mic Status	vorhanden oder fehlend	Integritätsschutz der NTLM-Nachricht
NtlmVersion	NTLMv2 oder NTLMv1	NTLMv1 und Extended Protection schließen sich aus

Die Reason-ID in NtlmUsageId ist nur ein Hinweis. Microsoft dokumentiert in KB5064479 die Nummern 0 bis 11, in der Praxis taucht auch 12 auf, und Nummer und Text passen nicht immer zusammen. Maßgeblich ist der Begründungstext in NtlmUsageReason; Details in NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat. Und weil per Event Forwarding weitergeleitete Ereignisse manchmal einen leeren Meldungstext haben, filterst du immer über die EventData-Felder, nicht über den Text. Fertige Abfragen dafür findest du in NTLM-Ereignisse mit PowerShell auswerten: Get-WinEvent-Rezepte.

```
# NTLM-Anmeldungen gegen HTTP-Ziele auf einem Client, nach Ziel und Prozess gruppiert
Get-WinEvent -LogName 'Microsoft-Windows-NTLM/Operational' -FilterXPath '*[System[(EventID=4020
or EventID=4021)]]' |
  ForEach-Object { $x = [xml]$_.ToXml(); $d = @{}
    $x.Event.EventData.Data | ForEach-Object { $d[$_.Name] = $_.'#text' }
    [pscustomobject]@{ Prozess = $d.ProcessName; Ziel = $d.TargetService; Grund =
$d.NtlmUsageReason } } |
  Where-Object { $_.Ziel -like 'HTTP/*' } | Group-Object Prozess, Ziel, Grund | Sort-Object
Count -Descending
```

Kerberos hinter dem Load Balancer: das alternative Dienstkonto

Hier liegt der Kern des Problems. Ein Kerberos-Ticket wird für einen SPN ausgestellt und mit dem Schlüssel des Kontos verschlüsselt, an dem dieser SPN hängt. Outlook fragt nach HTTP/mail.musterwerk.local. Der Load Balancer schickt die Verbindung aber an exch01, exch02 oder exch03, und jeder dieser Server muss das Ticket öffnen können. Mit seinem eigenen Computerkonto kann er das nicht. Die Lösung von Microsoft heißt Alternate Service Account Credential, kurz ASA: ein gemeinsames Konto, dessen Kennwort alle Exchange-Server mit Clientzugriffsdiensten kennen.



Skizze nach Microsoft Learn, „Configure Kerberos authentication for load-balanced Client Access services"

WARNUNG · Der Kurzschluss, den du nicht machen willst

Der schnelle Trick „ich hänge HTTP/mail.musterwerk.local einfach an das Computerkonto von exch01" funktioniert genau so lange, wie der Load Balancer zufällig exch01 erwischt. Alle anderen Server können das Ticket nicht entschlüsseln. Ergebnis: Passwortabfragen nach dem Zufallsprinzip, die niemand reproduzieren kann. Prüfe vor jeder Änderung, ob der SPN schon irgendwo hängt.

ASA anlegen und verteilen

Microsoft empfiehlt ein Computerkonto, weil es keine interaktive Anmeldung erlaubt. Es braucht keine besonderen Rechte, nur die Mitgliedschaft in Domänencomputer. Alle Server, die denselben Namensraum bedienen, müssen dasselbe ASA verwenden; in der Regel reicht eines je Gesamtstruktur und Exchange-Version. Gruppenverwaltete Dienstkonten unterstützt Exchange on-premises dafür nicht, so verlockend der Gedanke ist. Verteilt wird das Konto ausschließlich mit dem Skript RollAlternateServiceAccountPassword.ps1 aus dem Scripts-Ordner der Exchange-Installation.

```
# 1. Computerkonto als ASA anlegen, AES aktivieren
New-ADComputer -Name EXASA -SamAccountName EXASA -Enabled $true `
  -Description 'Alternate Service Account für Exchange' `
  -AccountPassword (Read-Host 'Kennwort' -AsSecureString)
Set-ADComputer EXASA -Add @{'msDS-SupportedEncryptionTypes'=28}

# 2. Auf den ersten Server verteilen (Exchange Management Shell, Ordner V15\Scripts)
.\RollAlternateServiceAccountPassword.ps1 -ToSpecificServer exch01.musterwerk.local `
  -GenerateNewPasswordFor 'MUSTERWERK\EXASA$'

# 3. Auf alle weiteren Server kopieren
.\RollAlternateServiceAccountPassword.ps1 -ToSpecificServer exch02.musterwerk.local `
  -CopyFrom exch01.musterwerk.local

# 4. Kontrolle je Server
Get-ClientAccessService exch02 -IncludeAlternateServiceAccountCredentialStatus |
  Format-List Name, AlternateServiceAccountConfiguration
```

Der Wert 28 für msDS-SupportedEncryptionTypes stammt aus der Microsoft-Anleitung und schaltet RC4 und beide AES-Varianten frei. Wenn du RC4 in deiner Umgebung schon zurückdrängst, stimme den Wert mit deiner Kerberos-Strategie ab; Hintergründe dazu findest du unter Microsoft Kerberos. Für das ASA verantwortlich ist auf jedem Server der Dienst Microsoft Exchange Service Host (MSExchangeServiceHost). Läuft der nicht, gibt es kein Kerberos.

SPNs für den Namensraum

Erst wenn das ASA auf mindestens einem Server angekommen ist, hängst du die SPNs daran. Microsoft ist da deutlich: Andersherum gibt es Kerberos-Fehler. Für Outlook Anywhere, MAPI over HTTP, EWS, Autodiscover und OAB genügt die Dienstklasse http. Die SPN-Namen richten sich nach den Namen am Load Balancer, nicht nach den Servern. Und vor dem Setzen prüfst du gesamtstrukturweit, dass niemand anderes den SPN schon trägt.

```
setspn -F -Q http/mail.musterwerk.local          # muss leer zurückkommen
setspn -F -Q http/autodiscover.musterwerk.local
setspn -S http/mail.musterwerk.local MUSTERWERK\EXASA$
setspn -S http/autodiscover.musterwerk.local MUSTERWERK\EXASA$
setspn -L MUSTERWERK\EXASA$
```

Situation	SPNs am ASA	Worauf du achtest
Ein Standort, ein Namensraum	http/mail..., http/autodiscover...	alle Server hinter dem Load Balancer bekommen dasselbe ASA
Mehrere Standorte, eigene Namen	je Standort eigene Namen, z. B. http/mail-nord...	je Standort ein eigenes ASA, so beschreibt es Microsoft
Namensraum als DNS-CNAME	http/<Name, den der Client sieht>	Microsoft empfiehlt A-Einträge, damit der Client nach dem gemeinsamen Namen fragt
Koexistenz mit Exchange 2010	nicht teilbar	Exchange 2010 und 2016 können kein gemeinsames ASA nutzen
Interner und externer Name verschieden	beide, wenn interne Clients beide nutzen	maßgeblich ist der Name, den Outlook tatsächlich anfragt

Warum CNAMEs und Aliasnamen bei Kerberos so oft überraschen, steht ausführlich in CNAME, Aliasnamen und hosts-Datei: warum Kerberos den Namen nicht findet.

Negotiate einschalten und prüfen

Jetzt öffnest du die Türen. Für Outlook Anywhere setzt du die interne Authentifizierung auf Negotiate, für MAPI ergänzt du Negotiate in IISAuthenticationMethods. In Hybridumgebungen oder bei intern genutztem OAuth hängst du Negotiate an die bestehende Liste an, statt sie zu überschreiben, sonst ist OAuth weg.

```
Get-OutlookAnywhere -Server exch01 | Set-OutlookAnywhere -InternalClientAuthenticationMethod
Negotiate
$m = Get-MapiVirtualDirectory -Server exch01
$m | Set-MapiVirtualDirectory -IISAuthenticationMethods ($m.IISAuthenticationMethods +=
'Negotiate')
```

Die Kontrolle hat zwei Seiten. Auf dem Server zeigt das HttpProxy-Protokoll unter Logging\HttpProxy\Mapi im Exchange-Installationspfad den AuthenticationType; Microsoft wertet Negotiate dort als Zeichen für erfolgreiches Kerberos. Auf dem Client machst du die Gegenprobe mit klist: Ein Ticket für HTTP/mail.musterwerk.local muss im Cache liegen, und neue Ereignisse 4020 mit diesem Ziel bleiben aus. Wie du klist richtig liest, steht in Mit klist prüfen, ob Kerberos wirklich greift.

TIPP · Kennwortwechsel nicht vergessen

Das ASA-Kennwort läuft als Computerkonto nicht ab, Microsoft empfiehlt trotzdem einen regelmäßigen Wechsel, wieder mit RollAlternateServiceAccountPassword.ps1, gern als geplante Aufgabe. Überwache diese Aufgabe. Ein halb ausgerollter Kennwortwechsel ist exakt der Fehler aus der Skizze oben, nur an einem Freitagnachmittag.

WICHTIG · Große Tickets, kurze Köpfe

Mitglieder vieler Gruppen haben große Kerberos-Tickets. Die passen nicht immer in die Standardgrenzen von HTTP.sys für Anfragekopfzeilen, und dann antwortet der Server mit HTTP 400 statt mit dem Postfach. Teste deshalb gezielt mit einem Konto aus vielen Gruppen, bevor du Erfolg meldest. Unter NTLM tritt das Problem nicht auf, was es so schön tückisch macht.

Und der Load Balancer?

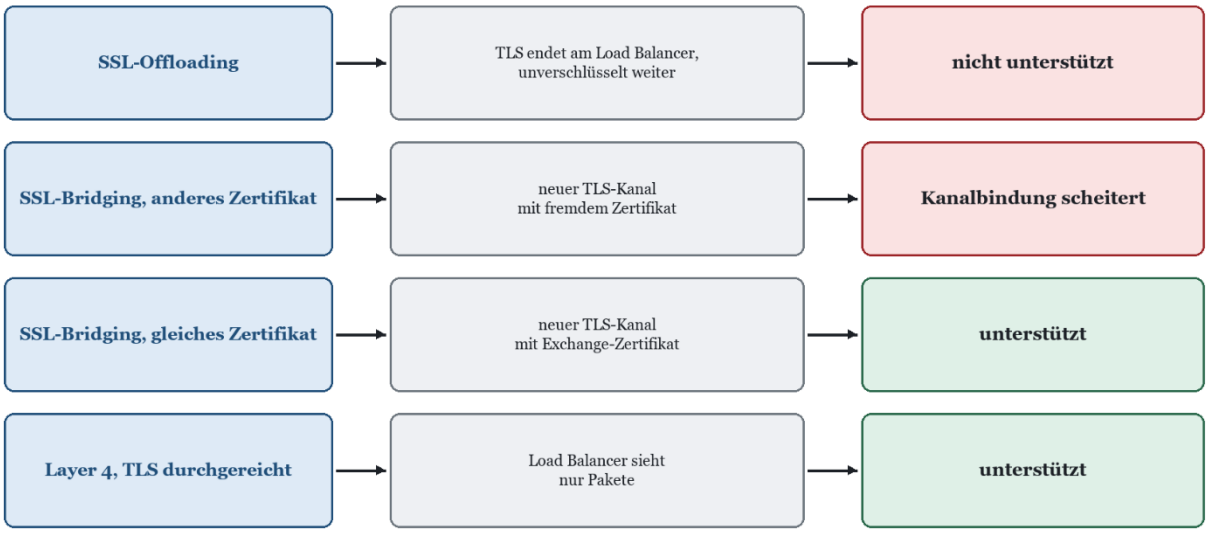
Solange der Load Balancer nur verteilt und selbst nicht anmeldet, reicht er das Negotiate-Token einfach durch und braucht für Kerberos nichts. Das gilt für Layer-4-Verteilung ebenso wie für SSL-Bridging. Anders wird es, wenn das Gerät selbst vorab authentifiziert, etwa bei der Vorab-Anmeldung mit eingeschränkter Delegierung, wie sie Kemp LoadMaster für die Exchange-Veröffentlichung anbietet. Dann braucht das Gerät ein eigenes Konto, eigene SPNs und Delegierungsrechte auf die Exchange-SPNs. Das ist ein eigenes Projekt mit eigener Testphase.

Extended Protection: NTLM absichern, solange es noch da ist

Bis NTLM verschwindet, ist Extended Protection der Gurt, den Exchange anlegt. Es bindet die Windows-Anmeldung über ein Channel Binding Token an den TLS-Kanal, über den sie kommt. Ein Angreifer, der eine NTLM-Anmeldung abgreift und an Exchange weiterreicht, scheitert dann, weil sein TLS-Kanal nicht zum Token passt. Seit Exchange 2019 CU14 schaltet das Setup Extended Protection automatisch ein; ältere Versionen ab dem Sicherheitsupdate vom August 2022 bekommen es über das Skript ExchangeExtendedProtectionManagement.ps1. Wie Kanalbindung, MIC und Signierung gegen Relay zusammenspielen, erklärt NTLM-Relay verhindern: MIC, Kanalbindung und erweiterter Schutz.

Extended Protection: was der Load Balancer darf und was nicht

Kanalbindung prüft, ob der TLS-Kanal von Outlook auch der ist, an dem Exchange hängt



Skizze nach „Exchange Server support for Windows Extended Protection" (Microsoft Learn)

Voraussetzung	Warum	Prüfschritt
Kein SSL-Offloading	TLS-Abbruch am Load Balancer zerstört die Kanalbindung	Load-Balancer-Konfiguration ansehen; Outlook Anywhere ohne SSL-Offloading
Gleiches Zertifikat bei SSL-Bridging	sonst passt das Channel Binding Token nicht	Fingerabdruck am Load Balancer und am Exchange-Frontend vergleichen
Kein NTLMv1	NTLMv1 und Extended Protection funktionieren nicht zusammen	LmCompatibilityLevel mindestens 3, besser 5, auf Clients und Servern
Einheitliche TLS-Konfiguration	Abweichungen zwischen Servern brechen Verbindungen	Health Checker von Microsoft ausführen
Kein Proxy in der Mitte	lokale Proxys von Virenschutzlösungen gelten als Mann in der Mitte	Drittprodukte vor dem Einschalten testen

Der NTLMv1-Punkt ist für die NTLM-Ablösung besonders interessant: Ein Client, der noch NTLMv1 spricht, bekommt bei aktivem Extended Protection Passwortabfragen ohne Ausweg. Wie du LmCompatibilityLevel ohne Ausfall hochziehst, steht in LmCompatibilityLevel richtig setzen: NTLMv2 erzwingen ohne Ausfall. Seit dem Windows-Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 NTLMv1 für Single Sign-on ohnehin standardmäßig, sichtbar an den Ereignissen 4024 und 4025.

WARNUNG · Zertifikatswechsel mit Extended Protection

Beim SSL-Bridging muss das Zertifikat am Load Balancer und auf Exchange identisch sein. Microsoft beschreibt für die Erneuerung deshalb einen Ablauf, in dem Extended Protection vorübergehend ausgeschaltet, das Zertifikat auf beiden Seiten getauscht und Extended Protection danach wieder eingeschaltet wird. Wer nur auf einer Seite tauscht, erntet Anmeldefenster in Outlook. Plane den jährlichen Zertifikatswechsel also als kleines Wartungsfenster, nicht als Nebenbei-Klick.

FAKTEN · Was Extended Protection nicht ist

Extended Protection ersetzt NTLM nicht, es macht NTLM nur schwerer missbrauchbar. Kerberos über das ASA ist davon unabhängig und funktioniert mit und ohne Extended Protection. Wer

Exchange zusätzlich mit moderner Authentifizierung betreibt, etwa Hybrid Modern Authentication, nimmt Outlook damit ebenfalls aus der NTLM-Schusslinie; Microsoft nennt HMA und Extended Protection ausdrücklich verträglich. Ein Teil der Umgebung braucht Windows-Anmeldung aber weiterhin, und für den gilt alles in diesem Beitrag.

Die Originaldokumentation findest du unter Exchange Server support for Windows Extended Protection und für das ASA unter Configure Kerberos authentication for load-balanced Client Access services.

Von drei Clients zu dreitausend: Exchange-Verursacher im Griff behalten

Für einen Testclient ist das alles schnell erledigt: klist, ein Blick ins HttpProxy-Protokoll, fertig. In einer Klinik mit zweitausend Arbeitsplätzen, zwei Rechenzentren und einem Exchange-Verbund mit vier Servern sieht es anders aus. Outlook erzeugt NTLM-Ereignisse auf jedem Client, verteilt über Hunderte Maschinen, ein paar Tausend pro Tag. Dazwischen verstecken sich die wirklich kritischen Fälle: das Archivsystem, das per IP-Adresse auf EWS zugreift, die Telefonanlage mit ihrer Java-Bibliothek, der Terminalserver, auf dem Outlook aus einem anderen Grund NTLM nimmt. Und die Frage, ob nach dem ASA-Rollout wirklich alle Clients umgestiegen sind, beantwortet kein einzelnes Protokoll.

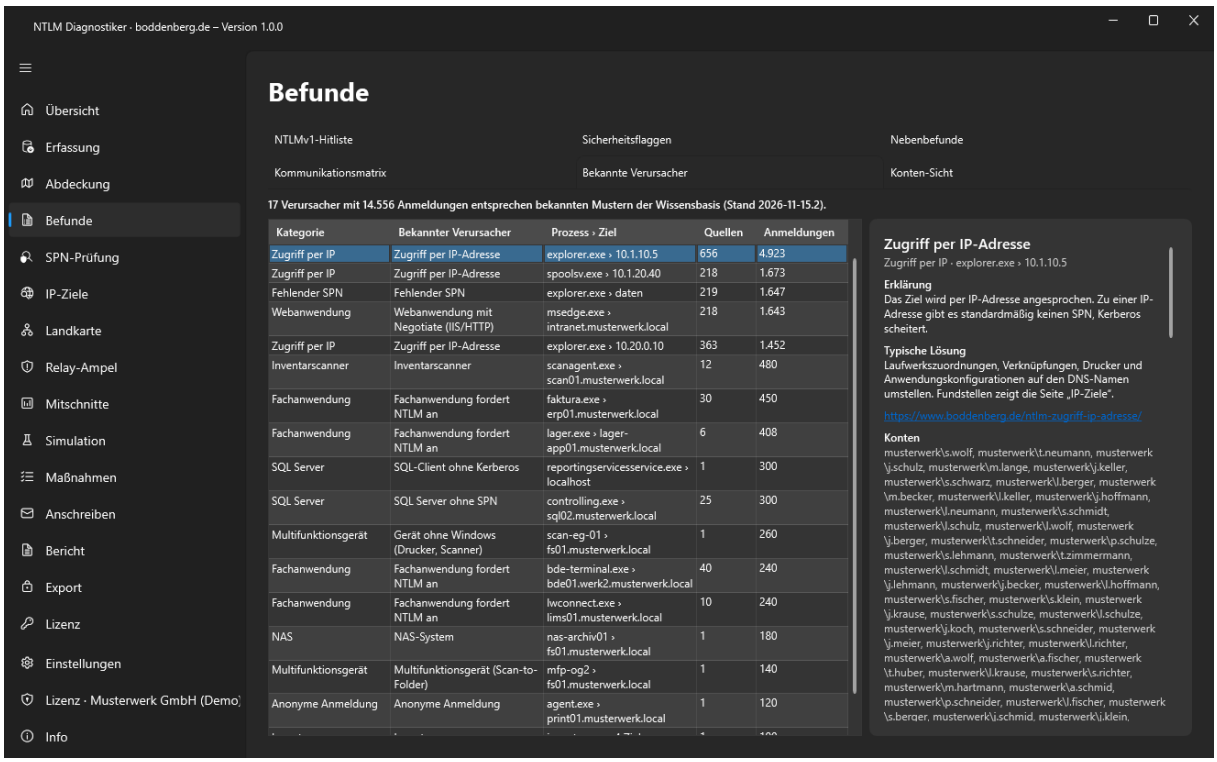
Mit Bordmitteln heißt das: Ereignisse von allen Clients einsammeln, über die EventData-Felder nach TargetService und ProcessName gruppieren, jeden HTTP-Namen gegen das Active Directory halten und für jede Fachanwendung herausfinden, wer sie betreut. Machbar, aber in Excel wird daraus schnell eine Doktorarbeit. Genau diese Fleißarbeit nimmt dir der NTLM Diagnostiker ab. Er arbeitet ausschließlich lesend, sammelt die NTLM-Ereignisse direkt vom Domain Controller, über einen Windows Event Collector, per Direktabfrage oder aus importierten Dateien und fasst gleichartige Verbindungen nach Ursache, Prozess und Ziel zusammen. Aus 6.000 Outlook-Ereignissen wird so eine Zeile.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Exchange-Ziele in Befunden und Wissensbasis

In den Befunden fasst der Diagnostiker gleichartige Verbindungen zu Verursachern zusammen: Kategorie, erkannter Verursacher, Prozess-zu-Ziel-Paar, Zahl der Quellen und Anmeldungen. OUTLOOK.EXE gegen HTTP/mail.musterwerk.local auf 1.800 Clients erscheint dort als ein Eintrag, nicht als 1.800. Das Archivsystem, das EWS per IP-Adresse anspricht, steht als eigener Verursacher „Zugriff per IP-Adresse“ daneben.

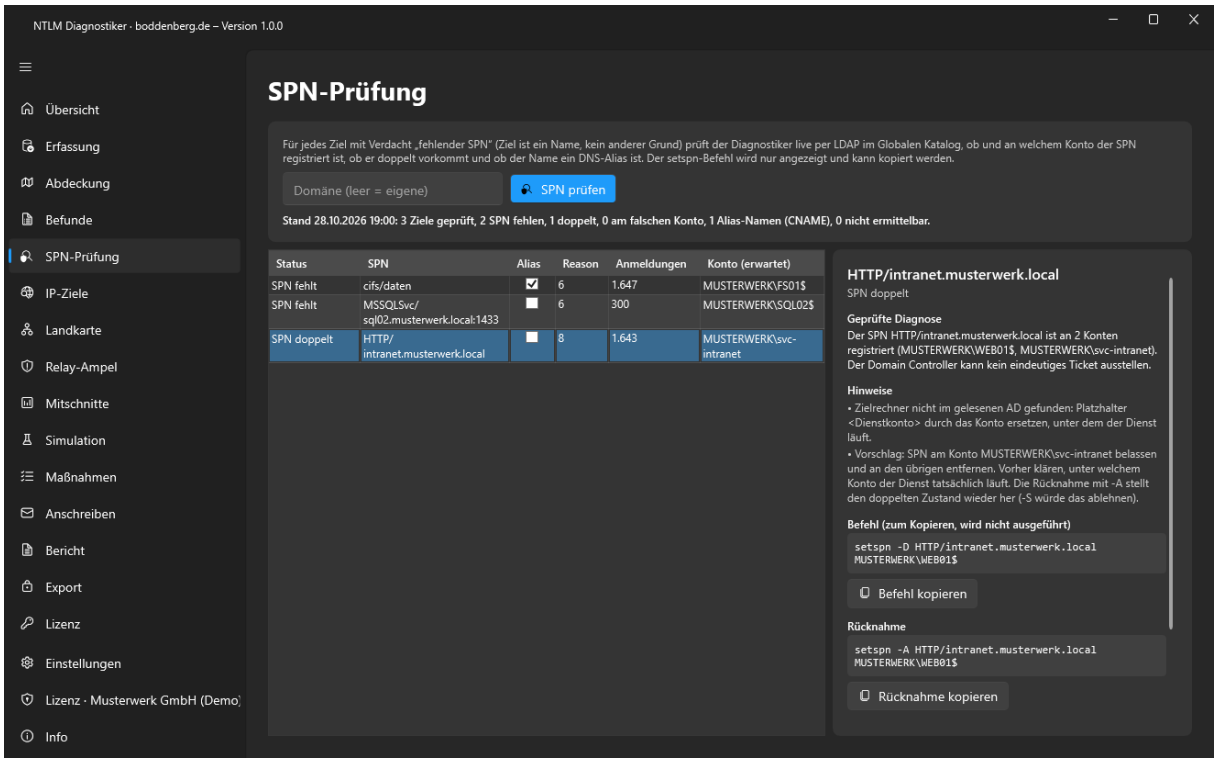
Für jeden Treffer liefert die Wissensbasis bekannter Verursacher rechts im Detailbereich eine Erklärung, eine typische Lösung und die Liste der betroffenen Konten. Die Ursachen-Engine wertet dafür den Begründungstext in NtlmUsageReason aus, nicht nur die Nummer. So siehst du sofort, ob der Namensraum keinen SPN hat oder ob eine Anwendung gar nicht erst nach einem Namen fragt.

In der Kommunikationsmatrix taucht der Exchange-Namensraum als Webziel auf, mit allen Prozessen und Konten, die ihn per NTLM ansprechen. Damit hast du die Liste der EWS-Anwendungen, die dir sonst niemand geben kann.



So siehst du in den Befunden, welche Prozesse und Ziele NTLM verursachen, und bekommst Erklärung, Lösung und betroffene Konten aus der Wissensbasis (Demodaten).

Der zweite Stolperstein bei Exchange sind doppelte SPNs, etwa wenn jemand vor Jahren http/mail.musterwerk.local an ein Serverkonto gehängt hat und jetzt das ASA denselben SPN bekommen soll. Die SPN-Prüfung hält jedes Ziel aus den Ereignissen gegen das Active Directory und meldet fehlende und doppelte SPNs sowie Aliasnamen. Den passenden setspn-Befehl samt Rücknahme zeigt sie dir zum Kopieren an. Ausführen tust du ihn selbst; der Diagnostiker ändert nichts an deinem Active Directory.



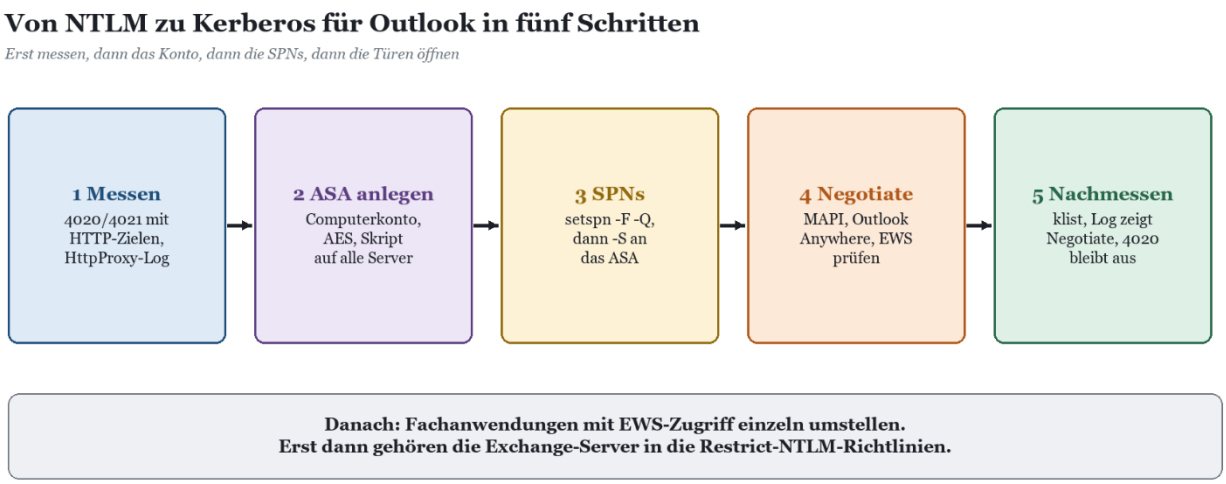
So erkennst du in der SPN-Prüfung einen doppelt registrierten HTTP-SPN und siehst den angebotenen setspn-Befehl zur Bereinigung (Demodaten).

Readiness-Ampel, Abdeckungskarte, Top-10-Verursacher und Hinweise aus der Wissensbasis bekommst du in der kostenlosen Express-Edition als Fünf-Minuten-Befund direkt vom Domain Controller. Kommunikationsmatrix und SPN-Prüfung testest du im siebentägigen Testzeitraum, einmal pro Domäne. Wenn du ASA, Extended Protection und Hybrid lieber gemeinsam planst, ist die Beratung zur NTLM-Ablösung der richtige Ansprechpartner.

AUS DER PRAXIS · Trendforge Digital und das Kalenderskript

Bei der Trendforge Digital GmbH lief Outlook nach dem ASA-Rollout sauber mit Kerberos. Trotzdem blieben täglich rund 900 NTLM-Anmeldungen gegen den Exchange-Namensraum übrig. Absender: ein Webserver, Prozess w3wp.exe, Ziel nicht HTTP/mail.musterwerk.local, sondern eine IP-Adresse. Dahinter steckte das Intranet-Raumbuchungssystem, das per EWS Termine in Raumpostfächer schrieb, mit der IP des alten Exchange 2013 in der Konfiguration, die inzwischen als virtuelle IP auf dem Load Balancer lag. Eine Zeile in der Konfigurationsdatei, ein Neustart des Anwendungspools, und die 900 Anmeldungen waren Kerberos. Gesucht hatte man vorher drei Wochen lang auf den Clients.

Umstellen ohne Passwort-Popup-Festival: Reihenfolge und Erfolgskontrolle



Skizze: Reihenfolge beispielhaft für die Musterwerk GmbH

Die Reihenfolge ist bei Exchange wichtiger als anderswo, weil jeder Fehler sofort bei allen Anwenderinnen und Anwendern als Anmeldefenster aufschlägt. Deshalb gilt: messen, ASA verteilen, SPNs prüfen und setzen, erst dann Negotiate einschalten, und zwar Server für Server.

Schritt	Werkzeug	Erfolgskriterium
NTLM gegen Exchange-Namen erfassen	Ereignisse 4020/4021 und 8003, HttpProxy-Protokoll	Liste aus Prozess, Ziel, Begründung, Anzahl
ASA anlegen und auf alle Server verteilen	New-ADComputer, RollAlternateServiceAccountPassword.ps1	Get-ClientAccessService zeigt überall dasselbe ASA
SPNs prüfen und setzen	setspn -F -Q, setspn -S, setspn -L	jeder Namensraum-SPN genau einmal, am ASA

Negotiate einschalten	Set-MapiVirtualDirectory, Set-OutlookAnywhere	HttpProxy-Protokoll zeigt Negotiate
Große Tickets testen	Testkonto mit vielen Gruppen	kein HTTP 400
EWS-Anwendungen umstellen	Konfiguration der Anwendung, Herstelleranfrage	FQDN statt IP, Bibliothek mit Negotiate
Nachmessen	klist, NTLM-Ereignisse	keine neuen 4020 mit HTTP-Zielen

Terminalserver und virtuelle Desktops verdienen einen eigenen Blick, weil Outlook dort unter anderen Bedingungen startet; mehr in Citrix und virtuelle Desktops: NTLM in VDI- und Terminalserver-Umgebungen. Wenn auch das Intranet über den Browser auf Exchange oder SharePoint zugreift, hilft Edge, Chrome und Firefox: Browser für Kerberos im Intranet einstellen, und für die SharePoint-Seite SharePoint Server: Kerberos statt NTLM für Webanwendungen. Erst wenn keine NTLM-Anmeldungen gegen die Exchange-Namen mehr auftauchen, nimmst du die Exchange-Server in die Restrict-NTLM-Richtlinien auf, wie in Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern beschrieben. Dass danach nichts zurückfällt, überwachst du wie in Nach der Abschaltung: Rückfälle erkennen und NTLM-frei bleiben.

WARNUNG · Kerberos ausschalten ist auch ein Rückweg

Microsoft beschreibt den Rückbau so: SPNs vom ASA entfernen, ASA mit Set-ClientAccessServer -RemoveAlternateServiceAccountCredentials von den Servern nehmen. Clients mit Negotiate fallen dann wieder auf NTLM zurück. Halte diese Schritte im Änderungsantrag als Rücknahme fest, bevor du anfängst. Nach der NTLM-Abschaltung gibt es diesen Rückweg nicht mehr.

FAQ zu Exchange, NTLM und Kerberos

Nutzt Outlook mit Exchange on-premises NTLM oder Kerberos?

Outlook für Windows meldet sich per Negotiate an. Ob daraus Kerberos wird, hängt davon ab, ob der Client ein Ticket für den angefragten Namen bekommt und ob das virtuelle Verzeichnis Negotiate anbietet. Hinter einem Load Balancer ohne ASA ist das Ergebnis praktisch immer NTLM.

Brauche ich das ASA auch ohne Load Balancer?

Wenn Outlook direkt den Servernamen anspricht, passt das Computerkonto des Servers, und Kerberos funktioniert ohne ASA. Sobald mehrere Server einen gemeinsamen Namen bedienen, brauchst du es.

Kann ich ein gruppenverwaltetes Dienstkonto als ASA nehmen?

Nein. Microsoft unterstützt gMSA für das ASA in Exchange on-premises nicht. Empfohlen ist ein Computerkonto, ein Benutzerkonto ist möglich.

Welche SPNs braucht Exchange für Kerberos?

Mindestens http/ für jeden Namen, den Clients für Outlook Anywhere, MAPI over HTTP, EWS, Autodiscover und OAB verwenden, typischerweise http/mail.<domäne> und http/autodiscover.<domäne>. Alle hängen am ASA und dürfen in der Gesamtstruktur nur einmal vorkommen.

Woran erkenne ich, dass Kerberos wirklich greift?

Auf dem Client mit klist an einem Ticket für HTTP/mail.<domäne> und am Ausbleiben neuer Ereignisse 4020 mit diesem Ziel. Auf dem Server am AuthenticationType Negotiate im HttpProxy-Protokoll.

Was passiert mit EWS-Anwendungen, wenn NTLM abgeschaltet wird?

Anwendungen, die per IP-Adresse zugreifen oder nur NTLM beherrschen, können sich dann nicht mehr anmelden. Stelle die URL auf den Namensraum um und prüfe, ob die Bibliothek Negotiate kann. Wenn nicht, ist der Hersteller gefragt.

Verträgt sich Extended Protection mit Kerberos?

Ja. Extended Protection bindet Windows-Anmeldungen an den TLS-Kanal und schützt so vor allem NTLM gegen Relay. Kerberos über das ASA funktioniert unabhängig davon. Wichtig sind kein SSL-Offloading und beim SSL-Bridging dasselbe Zertifikat am Load Balancer und auf Exchange.

Warum bekommen einige Benutzer nach der Umstellung HTTP 400?

Häufig, weil ihr Kerberos-Ticket zu groß für die Kopfzeilengrenzen von HTTP.sys ist, typisch bei Konten mit sehr vielen Gruppenmitgliedschaften. Prüfe die Gruppenanzahl des Kontos und die Microsoft-Empfehlungen zu den HTTP.sys-Grenzwerten, bevor du an Exchange selbst zweifelst.

Fazit: Exchange kann Kerberos. Es braucht nur einen gemeinsamen Schlüsselbund.

Exchange ist kein NTLM-Problem, sondern ein Namensraumproblem mit NTLM als Symptom. Hinter dem Load Balancer fehlt einfach das gemeinsame Konto, an dem die SPNs hängen könnten, und so fällt Outlook seit Jahren still auf NTLM zurück. Mit einem ASA als Computerkonto, sauberen SPNs für mail und autodiscover, Negotiate an den virtuellen Verzeichnissen und einem Blick auf die EWS-Anwendungen im Haus ist der größte NTLM-Brocken der Clientlandschaft in wenigen Tagen erledigt. Extended Protection hält NTLM bis dahin im Zaum.

Und wenn die nächste Windows-Server-Version NTLM standardmäßig abdreht, sieht die Belegschaft am Montag genau das, was sie immer sieht: ihren Posteingang. Kein Anmeldefenster, kein Anruf beim Helpdesk, kein Krisenstab. Langweilig. Genau so soll es sein.

WEITERLESEN · Weiter in dieser Serie

› NTLM in IIS und Webanwendungen: Negotiate statt NTLM
› Reason-ID 6: wenn der Zielname nicht auflösbar ist
› CNAME, Aliasnamen und hosts-Datei: warum Kerberos den Namen nicht findet
› Mit klist prüfen, ob Kerberos wirklich greift
› NTLM-Relay verhindern: MIC, Kanalbindung und erweiterter Schutz
› LmCompatibilityLevel richtig setzen: NTLMv2 erzwingen ohne Ausfall
› Java-Anwendungen und NTLM: Kerberos mit SPNEGO
› Checkliste vor dem NTLM-Stichtag: 25 Prüfpunkte