Bezpieczeństwo domyślne 24H2/25H2 — SMB, NTLM, LSA, usunięte składniki i druk IPP

□□ Typ: fiszka **□□ Poziom: średniozaawansowany**

□□ Dotyczy: Windows 11 24H2/25H2, Windows Server 2025, flota mieszana (czyste instalacje i aktualizacje z Windows 10)

□ Czas: ~40 min

Efekt: wiemy, które zabezpieczenia Windows 11 24H2 i 25H2 włącza domyślnie, a które tylko na czystych instalacjach; audytujemy skryptem podpisywanie SMB, LSA protection, użycie NTLM, skrypty z VBScript i WMIC oraz kolejki wydruku, które przeskoczyły na sterownik klasy IPP — i wiemy, co z tego trzeba naprawić, zanim samo się zepsuje.

□□ Skróty użyte na tej stronie (37)

Skrót	Co znaczy
ACPI	Advanced Configuration and Power Interface: opis sprzętu i zasilania dla systemu
AD	Active Directory: katalog kont, komputerów i zasad w domenie Windows
ASR	Attack Surface Reduction: reguły Defendera blokujące typowe techniki ataku
CIM	Common Information Model: standard, na którym stoi WMI i cmdlety *-CimInstance
DES	Data Encryption Standard: stary, słaby szyfr blokowy
eSCL	protokół skanowania sieciowego oparty na HTTP, obsługiwany bez sterownika producenta
ESS	Enhanced Sign-in Security: izolacja biometrii Windows Hello w VBS
GPO	Group Policy Object: obiekt zasad grupy w Active Directory
HTML	HyperText Markup Language: język stron WWW

Skrót	Co znaczy
HVCI	Hypervisor-protected Code Integrity: w interfejsie „Integralność pamięci”; sprawdza sterowniki przed jądrem
IAKerb	Initial and Pass Through Authentication Using Kerberos: Kerberos przez pośrednika, bez linii wzroku do DC
IPP	Internet Printing Protocol: standardowy protokół druku sieciowego
KB	Knowledge Base: numer artykułu i aktualizacji Microsoftu (np. KB5124008)
KDC	Key Distribution Center: usługa wydająca bilety Kerberos
LANMAN	LAN Manager: najstarszy protokół uwierzytelniania sieciowego Microsoftu
LPD	Line Printer Daemon: stara usługa druku z Uniksa (klient: LPR)
LPR	Line Printer Remote: stary protokół druku z Uniksa
LSA	Local Security Authority: podsystem Windows obsługujący logowanie i sekrety
LSASS	Local Security Authority Subsystem Service: proces lsass.exe przechowujący sekrety logowania
NAS	Network Attached Storage: dysk sieciowy z własnym systemem
NTLM	NT LAN Manager: starszy protokół uwierzytelniania Windows, poprzednik Kerberosa w domenie
PC	Personal Computer: komputer osobisty
PIN	Personal Identification Number: kod liczbowy, np. do odblokowania wydruku poufnego
QUIC	protokół transportowy na UDP, używany m.in. przez HTTP/3 i SMB over QUIC
SDEV	Secure Devices table: tabela ACPI wskazująca urządzenia do izolacji w VBS
SMB	Server Message Block: protokół udziałów plików i drukarek Windows
TLS	Transport Layer Security: szyfrowanie połączeń, np. w HTTPS
TPM	Trusted Platform Module: układ przechowujący klucze i pomiary rozruchu
UEFI	Unified Extensible Firmware Interface: współczesny firmware płyty głównej
VBA	Visual Basic for Applications: język makr w pakiecie Office
VBS	Virtualization-Based Security: izolowany hipernadzorcą obszar pamięci Windows
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
WDAC	Windows Defender Application Control: dawna nazwa App Control for Business
WinRM	Windows Remote Management: zdalne zarządzanie Windowsem, podstawa PowerShell Remoting
WMI	Windows Management Instrumentation: interfejs zarządzania i inwentaryzacji Windows
WMIC	WMI Command-line: stare narzędzie wiersza poleceń do WMI
WS-Scan	Web Services for Devices Scan: protokół skanowania sieciowego Microsoftu

Fiszka

□□ TYLKO ODCZYT

Wymóg podpisywania SMB po stronie klienta i serwera

```
Get-SmbClientConfiguration | FL RequireSecuritySignature
Get-SmbServerConfiguration | FL RequireSecuritySignature
```

Od **24H2** edycje Enterprise, Pro i Education wymagają podpisywania SMB przychodzącego i wychodzącego; Home — nie. `True` po obu stronach to stan domyślny na 24H2. Wymóg podpisywania **wyłącza dostęp gościa**, a Windows 11 Pro nie pozwala już domyślnie na połączenia gościa — to najczęstsza przyczyna, dla której po przejściu na 24H2 przestają działać NAS-y, skanowanie do folderu i stare urządzenia wielofunkcyjne.

Przykład (wynik ilustracyjny, nie z dokumentacji):

```
RequireSecuritySignature : True
```

□□ **SMB** = Server Message Block: protokół udziałów plików i drukarek Windows

□□ TYLKO ODCZYT

Stan LSA protection: RunAsPPL

```
# polecenie pomocnicze; nazwa i znaczenie wartości z dokumentacji Microsoftu
Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Control\Lsa -Name RunAsPPL -ErrorAction
SilentlyContinue
```

`1` — ochrona z blokadą UEFI (rejestrem się jej nie wyłączy, potrzebne jest narzędzie opt-out), `2` — bez blokady UEFI (22H2+), `0` albo brak wartości — wyłączona. LSA protection jest domyślnie włączona tylko na **nowych** instalacjach Windows 11 22H2+ przyłączonych do przedsiębiorstwa (AD, Entra albo hybrydowo) i zdolnych do HVCI — maszyna zaktualizowana z Windows 10 zwykle jej nie ma.

□□ **AD** = Active Directory: katalog kont, komputerów i zasad w domenie Windows · **HVCI** = Hypervisor-protected Code Integrity: w interfejsie „Integralność pamięci”; sprawdza sterowniki przed jądrem · **LSA** = Local Security Authority: podsystem Windows obsługujący logowanie i sekrety · **UEFI** = Unified Extensible Firmware Interface: współczesny firmware płyty głównej

□□ ZMIENIA SYSTEM

Tryb audytu LSA przed włączeniem ochrony: AuditLevel = 8

```
# ścieżka klucza i wartość z dokumentacji Microsoftu (Configuring additional LSA protection)
$ifeo = 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LSASS.exe'
# bez New-Item -Force: na istniejącym kluczu rejestru -Force tworzy go od nowa i kasuje jego wartości
if (-not (Test-Path $ifeo)) { New-Item -Path $ifeo | Out-Null }
Set-ItemProperty -Path $ifeo -Name AuditLevel -Value 8 -Type DWord
Restart-Computer
```

Zanim włączymy LSA protection na maszynie zaktualizowanej z Windows 10, uruchamiamy audyt: system nie blokuje jeszcze niczego, tylko zapisuje zdarzenia **3065** i **3066** dla wtyczek i sterowników, które nie spełniają wymagań podpisu i po włączeniu ochrony przestałyby się ładować do procesu LSASS. Zbieramy je przez kilka dni normalnej pracy, w tym logowań VPN, kart inteligentnych i agentów bezpieczeństwa. Audyt włączamy najpierw na kilku maszynach testowych; wycofanie to usunięcie wartości `AuditLevel` z tego klucza (`Remove-ItemProperty -Path $ifeo -Name AuditLevel`) i restart.

LSA = Local Security Authority: podsystem Windows obsługujący logowanie i sekrety · **LSASS** = Local Security Authority Subsystem Service: proces lsass.exe przechowujący sekrety logowania · **VPN** = Virtual Private Network: szyfrowany tunel do sieci firmowej

TYLKO ODCZYT

Zdarzenia audytu LSA: 3065 i 3066

```
# polecenie pomocnicze; numery zdarzeń i dziennik (Applications and Services Logs → Microsoft → Windows → CodeIntegrity → Operational) z dokumentacji Microsoftu
Get-WinEvent -FilterHashtable @{ LogName = 'Microsoft-Windows-CodeIntegrity/Operational'; Id = 3065, 3066 } `
    -MaxEvents 100 -ErrorAction SilentlyContinue |
    Select-Object TimeCreated, Id, Message | Format-Table -Wrap
```

Pusty wynik po kilku dniach audytu znaczy, że żaden składnik nie zostałby zablokowany. Jeśli zdarzenia są, w treści jest nazwa pliku — sprawdzamy u producenta, czy jest nowsza, podpisana wersja, zanim przejdziemy dalej.

LSA = Local Security Authority: podsystem Windows obsługujący logowanie i sekrety

□□ ZMIENIA SYSTEM

Włączenie LSA protection bez blokady UEFI: RunAsPPL = 2

```
# wartość z dokumentacji Microsoftu
Set-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Control\Lsa -Name RunAsPPL -Value
2 -Type DWord
Restart-Computer
```

Wariant `2` (22H2+) chroni proces LSA tak samo, ale bez zapisu blokady w zmiennej UEFI — w razie problemu wyłączymy go zmianą rejestru. Wariantu `1` z blokadą UEFI nie używamy na pilotażu, bo jego wyłączenie wymaga osobnego narzędzia opt-out. Przed zmianą robimy kopię klucza (`reg export HKLM\SYSTEM\CurrentControlSet\Control\Lsa C:\Temp\lsa-przed.reg /y`, katalog musi istnieć), zmianę robimy najpierw na maszynach z grupy testowej, które przeszły audyt bez zdarzeń 3065/3066. Po włączeniu ochrony zablokowane ładowanie wtyczki trafia do tego samego dziennika CodeIntegrity jako zdarzenie **3033** albo **3063**. Wycofanie według dokumentacji Microsoftu: `RunAsPPL` = `0` albo usunięcie wartości, restart; jeśli ochronę włączono GPO „Configures LSASS to run as a protected process”, trzeba ją tam ustawić jawnie na wyłączoną — „Nie skonfigurowano” nie czyści wcześniejszego ustawienia.

□□ **LSA** = Local Security Authority: podsystem Windows obsługujący logowanie i sekrety · **UEFI** = Unified Extensible Firmware Interface: współczesny firmware płyty głównej

□□ TYLKO ODCZYT

Użycie NTLM w sieci: dziennik NTLM/Operational

```
# polecenie pomocnicze; nazwa dziennika z dokumentacji Microsoftu
Get-WinEvent -LogName 'Microsoft-Windows-NTLM/Operational' -MaxEvents 200 -ErrorAction
SilentlyContinue |
    Select-Object TimeCreated, Id, Message | Format-Table -Wrap
```

Dziennik zapełnia się po włączeniu audytu zasadami **Network security: Restrict NTLM: Audit…** (GPO zabezpieczeń). Z treści zdarzeń wyciągamy, kto i do czego uwierzytelnia się przez NTLM: aplikacje, drukarki, NAS-y, skrypty, maszyny bez linii wzroku do kontrolera. To lista rzeczy, które przestaną działać, gdy sieciowy NTLM zostanie domyślnie wyłączony.

□□ **GPO** = Group Policy Object: obiekt zasad grupy w Active Directory · **NTLM** = NT LAN Manager: starszy protokół uwierzytelniania Windows, poprzednik Kerberosa w domenie

□□ TYLKO ODCZYT

Skrypty VBScript i wywołania WMIC w skryptach logowania

```
# polecenie pomocnicze; moduł ActiveDirectory
$domena = (Get-ADDomain).DNSRoot
Get-ChildItem "\\$domena\SYSVOL\$domena\Policies" -Recurse -Include *.vbs -ErrorAction
SilentlyContinue |
    Select-Object FullName
Get-ChildItem "\\$domena\NETLOGON" -Recurse -Include *.vbs, *.bat, *.cmd, *.ps1 -
ErrorAction SilentlyContinue |
    Select-String -Pattern '\bwmic\b' -List | Select-Object Path
```

Pierwsza lista to skrypty `.vbs` podpięte w GPO — w domenach z lat 2000. bardzo częste, a VBScript jest przestarzały od października 2023 i ma zniknąć z systemu. Druga — skrypty, które wywołują `wmic`, usunięty z 24H2+ i niedostępny już nawet jako funkcja na żądanie. Jedne i drugie przepisujemy na PowerShell 5.1 albo 7.x i `Get-CimInstance`; samo WMI pozostaje w pełni wspierane. Gdy inwentaryzacja przez CIM zwraca błędy repozytorium, pomaga strona o naprawie liczników wydajności i repozytorium WMI: diagnostyka liczników i WMI.

CIM = Common Information Model: standard, na którym stoi WMI i cmdlety *-CimInstance · **GPO** = Group Policy Object: obiekt zasad grupy w Active Directory · **WMI** = Windows Management Instrumentation: interfejs zarządzania i inwentaryzacji Windows · **WMIC** = WMI Command-line: stare narzędzie wiersza poleceń do WMI

TYLKO ODCZYT

Kolejki wydruku na sterowniku klasy IPP

```
# polecenie pomocnicze; moduł PrintManagement
Get-Printer | Select-Object Name, DriverName, PortName |
    Sort-Object DriverName | Format-Table -AutoSize
```

Od **1 lipca 2026** ranking sterowników drukarek zawsze preferuje wbudowany sterownik klasy IPP — po nowej instalacji drukarki Windows może wybrać **Microsoft IPP Class Driver** zamiast sterownika producenta, co zmienia dostępne funkcje: tace, zszywanie, kody PIN i druk poufny. Na serwerze druku i na stacjach sprawdzamy, które kolejki mają w `DriverName` sterownik klasy, a miały sterownik producenta.

IPP = Internet Printing Protocol: standardowy protokół druku sieciowego · **PIN** = Personal Identification Number: kod liczbowy, np. do odblokowania wydruku poufnego

TYLKO ODCZYT

Audyt bezpieczeństwa domyślnego na całej flocie

```
# polecenie pomocnicze; nazwy wartości z dokumentacji Microsoftu
$komputery = Get-Content .\komputery.txt
Invoke-Command -ComputerName $komputery -ScriptBlock {
    $lsa = Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Control\Lsa -ErrorAction
SilentlyContinue
    $dg  = Get-CimInstance -Namespace root\Microsoft\Windows\DeviceGuard -ClassName
Win32_DeviceGuard -ErrorAction SilentlyContinue
    [pscustomobject]@{
        Wydanie        = (Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion').DisplayVersion
        SMBKlientPodp  = (Get-SmbClientConfiguration).RequireSecuritySignature
        SMBSerwerPodp  = (Get-SmbServerConfiguration).RequireSecuritySignature
        RunAsPPL       = $lsa.RunAsPPL
        MII            = $lsa.MachineIdentityIsolation
        VBSDziala      = ($dg.VirtualizationBasedSecurityStatus -eq 2)
        WMICObecny     = [bool](Get-Command wmic.exe -ErrorAction SilentlyContinue)
        VBScriptFoD    = (Get-WindowsCapability -Online | Where-Object Name -like
'*VBSCRIPT*').State -join ','
        DrukarkiIPP    = @(Get-Printer -ErrorAction SilentlyContinue | Where-Object
DriverName -like '*IPP*').Count
    }
} -Credential (Get-Credential) |
    Select-Object PSComputerName, Wydanie, SMBKlientPodp, SMBSerwerPodp, RunAsPPL, MII,
VBSDziala, WMICObecny, VBScriptFoD, DrukarkiIPP |
    Export-Csv .\bezpieczenstwo-domyslne.csv -NoTypeInformation -Encoding UTF8
```

Jedna tabela pokazuje obie polityki bezpieczeństwa, które flota mieszana ma na tej samej wersji Windows: czyste instalacje z `RunAsPPL` i VBS, zaktualizowane maszyny bez nich. Kolumna `MII` z wartością 2 odsyła do Machine Identity Isolation po KB5124008. Wymaga WinRM — WinRM — zarządzanie zdalne.

VBS = Virtualization-Based Security: izolowany hipernadzorcą obszar pamięci Windows · **WinRM** = Windows Remote Management: zdalne zarządzanie Windowsem, podstawa PowerShell Remoting

Po co to istnieje

W latach 2022–2026 Windows 11 przesunął granicę „bezpiecznie domyślnie” o kilka lat do przodu naraz, a wiele z tych zmian trafia do firm nie przez nową wersję, tylko przez comiesięczne aktualizacje albo wyłącznie na nowych instalacjach. **Administrator floty mieszanej — maszyny zaktualizowane z Windows 10 obok czystych instalacji — ma w efekcie dwie różne polityki bezpieczeństwa na tej samej wersji Windows.** Ta strona zbiera te zmiany w jednym miejscu i daje skrypty, które pokazują, po której stronie stoi każda maszyna.

Jak to działa

SMB: podpisywanie tak, szyfrowanie nie

Pakiet utwardzania SMB w 24H2 i Windows Server 2025 obejmuje: wymóg podpisywania (Pro, Enterprise, Education), **ogranicznik prób uwierzytelnienia** — domyślnie 2 sekundy opóźnienia po nieudanej próbie NTLM lub Kerberos, więc 90 000 prób trwa ok. 50 godzin zamiast minut — zarządzanie dialektami od 2.0.2 do 3.1.1, **blokowanie NTLM dla wychodzących połączeń SMB**, brak domyślnych połączeń gościa w Pro, SMB over QUIC we wszystkich edycjach Server 2025 i usunięcie portów NetBIOS z domyślnych reguł zapory. Klient **może** wymagać szyfrowania wszystkich połączeń wychodzących (SMB 3.0+), ale nie robi tego domyślnie — „szyfrowanie SMB domyślne” jest mitem. Wymóg podpisywania wyłącza się GPO „Microsoft network client: Digitally sign communications (always)”; robimy to tylko dla konkretnego urządzenia, którego nie da się naprawić, i z datą powrotu.

NTLM: harmonogram wycofania

Kiedy	Co
X 2023	pierwsza zapowiedź wycofania NTLM
VI 2024	wszystkie wersje NTLM, w tym LANMAN, NTLMv1 i NTLMv2, „nie są już aktywnie rozwijane i są przestarzałe”
XI 2024	„NTLMv1 usunięto, począwszy od Windows 11 24H2 i Windows Server 2025”
faza 1 (od ok. 30 I 2026)	rozszerzony audyt użycia NTLM w 24H2 i Server 2025
faza 2 (II poł. 2026)	IAKerb i Local KDC dla scenariuszy, w których dziś następuje przejście na NTLM: brak linii wzroku do kontrolera, konta lokalne
faza 3 (przyszłość, bez ogłoszonej wersji)	**sieciowy NTLM wyłączony domyślnie**, z możliwością ponownego włączenia polityką

Microsoft: „Wyłączenie NTLM domyślnie nie oznacza jeszcze całkowitego usunięcia NTLM z Windows”. W domenie z Machine Identity Isolation awaria Kerberosa kończy się dziś przejściem na NTLM — po domyślnym wyłączeniu NTLM skończy się brakiem logowania. Dlatego audyt robimy teraz, a nie w dniu zmiany.

LSA protection, Windows Hello ESS i klucze dostępu

Windows Hello Enhanced Sign-in Security izoluje algorytmy biometryczne w VBS, a kanały zabezpiecza przez TPM; wymaga czujników zgodnych z ESS (kamery z tabelą ACPI SDEV, czytniki z dopasowaniem na układzie). Wszystkie Copilot+ PC mają ESS domyślnie włączone. Od 24H2 użytkownik może ESS wyłączyć (Konta → Opcje logowania → Dodatkowe ustawienia) — wtedy działają zewnętrzne kamery i czytniki Hello, przy włączonym nie. Weryfikacja: zdarzenie 1108 (czujniki izolowane w Virtual Secure Mode) i VBS „Running” w `msinfo32`. Ponieważ Recall wymaga ESS, laptop Copilot+ z zewnętrzną kamerą Hello na biurku to konflikt do rozstrzygnięcia polityką.

Klucze dostępu (passkeys) są zarządzane natywnie od Windows 11 22H2 z KB5030310: klucz prywatny na urządzeniu, odblokowanie Windows Hello, telefon jako uwierzytelniacz przez Bluetooth i internet. Od 24H2 aplikacje pytają o zgodę na dostęp do kluczy (Ustawienia → Prywatność i zabezpieczenia → Dostęp do kluczy dostępu); widoczność tej strony Ustawień w firmie steruje `Settings/PageVisibilityList`, a polityki dla firm miały być ogólnie dostępne do czerwca 2026. Obsługa zewnętrznych menedżerów kluczy dostępu jako dostawców systemowych była zapowiadana w 2025 roku; daty nie potwierdziłem. W firmie Smart App Control jest w praktyce nieobecny — wymaga czystej instalacji, a flota jest aktualizowana z Windows 10 i zarządzana — jego rolę pełnią App Control for Business (dawniej WDAC) i reguły ASR w Defenderze.

Co usunięto i co jest na liście

Komponent	Status	Co robimy
Windows PowerShell 2.0	usunięty z 24H2 od VIII 2025; PowerShell 5.1 i 7.x zostają	skrypty wymagające 2.0 już nie działają — przepisać
WMIC	przestarzały od 21H1; według listy z VIII 2026 i omówień KB5124008 usunięty z 24H2+, niedostępny nawet jako funkcja na żądanie (w samej nocie KB tego zdania nie ma); WMI w pełni wspierane	`wmic` → `Get-CimInstance`
VBScript	przestarzały od X 2023; ma przejść w funkcję na żądanie, potem zniknąć	inwentaryzacja `.vbs` w GPO; makra VBA korzystające z VBScript, np. `RegExp`
WordPad	usunięty ze wszystkich edycji od 24H2	—
NTLMv1; DES w Kerberosie	usunięte od 24H2 (DES — IX 2025)	audyt NTLM

Komponent	Status	Co robimy
Windows Information Protection; Defender Application Guard for Edge	usunięte / niedostępne od 24H2	—
Windows Mixed Reality	usunięta w 24H2; gogle działają ze Steam do XI 2026	—
DirectAccess	przestarzały od VI 2024 — „zalecamy migrację na Always On VPN”	migracja na Always On VPN
TLS 1.0 i 1.1	domyślnie wyłączone od kompilacji z IX 2023	stare urządzenia i aplikacje z własnym stosem TLS
Remote Mailslots; LPR/LPD	Remote Mailslots przestarzałe (XI 2023) i domyślnie wyłączone; LPR/LPD — przypomnienie o wycofaniu z II 2025	klienci uniksowi drukujący przez LPD przestaną działać
Steps Recorder, aplikacja Porady; stary WebView EdgeHTML i aplikacje HTML/JS z Windows 8	przestarzałe (XI 2023; IX 2025)	—
Paint 3D / 3D Viewer / Mapy	usunięte ze Sklepu 4 XI 2024 / 1 VII 2026 / VII 2025	—

> Harmonogram VBScript w fazach — funkcja na żądanie włączona domyślnie od 24H2, wyłączona domyślnie około 2027, potem usunięcie — pochodzi z pamięci branżowej, bo wpis Microsoftu z terminami nie dał się pobrać. Traktujemy go jako kierunek, nie jako datę.

Druk: sterownik klasy IPP i koniec sterowników firm trzecich

Data	Co się zmienia
15 I 2026	koniec publikowania nowych sterowników drukarek firm trzecich w Windows Update dla Windows 11 i Server 2025 (wyjątki: drukarki nie do certyfikacji Mopria, sterowniki dla Windows 10 i starszych, natywne ARM64)
1 VII 2026	ranking sterowników **zawsze preferuje wbudowany sterownik klasy IPP**
1 VII 2027	koniec aktualizacji sterowników firm trzecich poza poprawkami bezpieczeństwa; instalacja z pakietów producenta nadal możliwa

Zastępstwem są **Microsoft IPP Class Driver** dla drukarek zgodnych z Mopria i **Print Support Apps** ze Sklepu; urządzenia wielofunkcyjne drukują i faksują przez IPP, a skanują przez WS-Scan

albo eSCL. Tryb **Windows Protected Print**, w którym działa wyłącznie nowoczesny stos druku, Microsoft wymienia w Windows Resiliency Initiative jako sposób na pozbycie się sterowników firm trzecich; nazwy polityki GPO i dostępności od 24H2 nie potwierdziłem.

Analogia

Czysta instalacja Windows 11 24H2 i maszyna zaktualizowana z Windows 10 do tej samej wersji są jak dwa mieszkania w tym samym bloku po remoncie klatki schodowej: nowi lokatorzy dostali od razu drzwi antywłamaniowe, domofon z kamerą i nowe zamki, a starzy lokatorzy — tę samą klatkę, ale z drzwiami, które mieli wcześniej, bo nikt nie wymienia drzwi, za którymi ktoś mieszka, bez pytania. Administrator widzi w ewidencji jeden blok i jeden standard, a w praktyce ma dwa. Ograniczenie analogii: część zmian — podpisywanie SMB, usunięcie WMIC, ranking sterowników druku — dotyczy wszystkich lokatorów naraz, niezależnie od tego, kiedy się wprowadzili, i to właśnie te zmiany psują rzeczy, które działały latami.

Częste błędy

Mylenie podpisywania z szyfrowaniem SMB. 24H2 domyślnie podpisuje; szyfrowanie wszystkich połączeń klient może wymusić, ale nie robi tego sam. Raport „SMB jest szyfrowany, bo mamy 24H2” jest nieprawdziwy.

Wyłączanie podpisywania SMB na całej flocie, żeby wrócił stary NAS. Jedno urządzenie bez wsparcia dla podpisywania nie jest powodem do obniżenia zabezpieczeń wszystkich stacji — wyjątek stosujemy celowo i z terminem wymiany urządzenia.

Włączenie LSA protection bez audytu. Wtyczka logowania albo sterownik bez wymaganego podpisu przestaje się ładować do LSASS i objawia się awarią logowania, VPN-u albo kart inteligentnych. Najpierw `AuditLevel` = 8 i zdarzenia 3065/3066.

Uznanie NTLM za „usunięty”. Usunięto NTLMv1; NTLMv2 jest przestarzały, a domyślne wyłączenie sieciowego NTLM zaplanowano na przyszłe wydanie. Audyt, który dziś niczego nie znajduje, bo nie był włączony, niczego nie dowodzi.

Traktowanie zmiany sterownika drukarki jako awarii drukarki. Po 1 lipca 2026 nowa instalacja kolejki może dostać sterownik klasy IPP i zgubić tace czy druk poufny — przyczyną jest ranking sterowników, nie sprzęt.

□□ Ćwiczenia

> Ćwiczenia wymagają jednej czystej instalacji Windows 11 24H2 lub 25H2 i jednej maszyny zaktualizowanej z Windows 10, obu w domenie testowej.

Ćwiczenie 1 — dwie polityki na jednej wersji

```
# polecenie pomocnicze
Import-Csv .\bezpieczenstwo-domyslne.csv |
    Group-Object RunAsPPL, VBSDziala |
    Select-Object Count, Name
```

Po uruchomieniu audytu z ostatniej karty Fiszki na obu maszynach grupujemy wynik. Czym różnią się wiersze, skoro obie maszyny mają ten sam `DisplayVersion`?

Odpowiedź

Na czystej instalacji przyłączonej do domeny i zdolnej do HVCI LSA protection jest domyślnie włączona (`RunAsPPL` ma wartość), a VBS i HVCI działają; na maszynie zaktualizowanej z Windows 10 LSA protection zwykle nie ma, a VBS często pozostaje wyłączony. Ta sama wersja systemu, dwie różne polityki bezpieczeństwa — i dwa różne zachowania przy hotpatch, który wymaga VBS.

Ćwiczenie 2 — gość i podpisywanie

```
# polecenie pomocnicze
Get-SmbClientConfiguration | FL RequireSecuritySignature
New-PSDrive -Name T -PSProvider FileSystem -Root \\adres-nas\udzial
```

Próbujemy podłączyć udział z urządzenia, które pozwala wyłącznie na dostęp gościa. Dlaczego się nie udaje, choć przed aktualizacją do 24H2 działało?

Odpowiedź

Od 24H2 edycje Pro, Enterprise i Education wymagają podpisywania SMB, a wymóg podpisywania wyłącza dostęp gościa; dodatkowo Pro nie pozwala już domyślnie na połączenia gościa. Właściwa naprawa to konto na urządzeniu i podpisywanie po jego stronie albo wymiana

urządzenia — a nie wyłączenie podpisywania na stacji.

Pytania kontrolne

1. Gdzie szukamy śladów użycia NTLM i dlaczego pusty dziennik nie musi znaczyć, że NTLM nie jest używany?

Odpowiedź

Po włączeniu audytu zasadami „Network security: Restrict NTLM: Audit…” zdarzenia trafiają do dziennika Microsoft-Windows-NTLM/Operational. Bez włączonego audytu dziennik jest pusty także wtedy, gdy NTLM jest intensywnie używany — pusty dziennik bez audytu niczego nie dowodzi.

2. Czym różni się RunAsPPL = 1 od RunAsPPL = 2 i dlaczego na pilotażu wybieramy 2?

Odpowiedź

Wartość 1 zapisuje blokadę w zmiennej UEFI — ochrony nie da się potem wyłączyć zmianą rejestru, potrzebne jest osobne narzędzie opt-out. Wartość 2 (22H2+) daje tę samą ochronę bez blokady UEFI, więc na pilotażu da się ją wycofać zwykłą zmianą rejestru.

Powiązane: Windows 11 w firmie 2026 — przegląd zmian · Machine Identity Isolation po KB5124008 · WinRM — zarządzanie zdalne · diagnostyka liczników i WMI · Skrypty audytowe Active Directory

Źródła: podpisywanie SMB · utwardzanie SMB · BleepingComputer — plan NTLM · LSA protection · Windows Hello ESS · passkeys · Smart App Control · funkcje przestarzałe · funkcje usunięte · Pureinfotech o KB5124008 · koniec serwisowania sterowników drukarek

Revision #3
Created 2026-09-27 17:44:22 UTC by Tomasz Konieczny
Updated 2026-10-18 23:00:54 UTC by Tomasz Konieczny