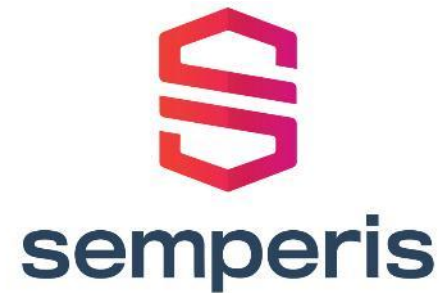


# 10 Maßnahmen, die nichts kosten

und jedes Active Directory sofort etwas sicherer machen

Bechtle MVP Community Week | 24.04.2026

Vielen Dank!

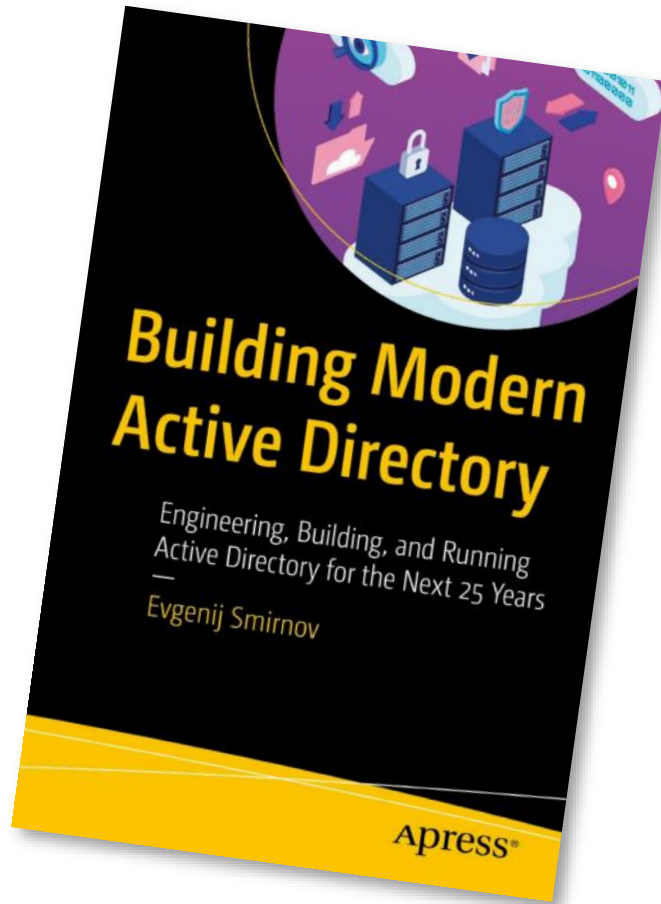


## Get-SpeakerInfo -Brief

- **Name:** Evgenij Smirnov
- **YearOfBirth:** 1972
- **JobTitle:** Principal Solutions Architect
- **Employer:** Semperis
- **MVP:** { Identity & Security, PowerShell }
- **Certifications:** { MCSE, MCSA, VCP, VCAP, VCIX, CCA, QCIC }
- **UserGroups:** { WSUG-B, EXUSG, PSUGB }
- **BlueSkyHandle:** @it-pro-berlin.de



## Kleine Werbung am Rande...



**Heinemann Verlag**  
Im Dialog mit Spezialisten.

Suchbegriff ...

0,00 €\*

Abonnements Sonderhefte Einzelhefte Digital Mehrfachlizenzen Bücher **Seminare** Extras

Administrator Website

Seminare

### Online-Intensivseminar Active-Directory-Security



1.785,00 €\*

Preis inkl. MwSt. [Lieferschlussinformation](#)

Hybridpreise bei Moonster-Registrierung  
Stellen Sie bereits registriert sein, zum Login

- Versandkostenlos
- Sofort verfügbar

Veranstaltungsort/-datum

ONLINE: 30. Juni - 02. Juli 2025

1

In den Warenkorb

[Zum Merkzettel hinzufügen](#)

Produktnummer: ITA-23-SEM-2823.2

<https://ad2049.com>

Nächste Gruppe: 01.07 – 03.07.2026

## Kleine Werbung am Rande...



<https://ntlminator.com>

- > AUFTRAG: AD VERTEIDIGEN
- > WO: HANNOVER, DEUTSCHLAND
- > VON: 2026-05-04
- > BIS: 2026-05-08
- > WIRD DEINE FIRMA UEBERLEBEN?
- > DIE UHR LAEFT...
- > \_
- > BUCHUNG: [ADGATOR.ORG/BOOTCAMP](https://adgator.org/bootcamp)

Nächste Gruppe: 04.05 – 08.05.2026

## In dieser Session

- **Warum AD- und Windows-Härtung so ein Thema ist**
- **10 Maßnahmen, die nichts kosten (aber etwas bewirken)**
- **Bonus Track: Trusts (wer hat)**
- **Bonus Track: Enterprise PKI, besonders ADCS (wer hat)**

# Warum AD-Härtung so ein Thema ist...

**Your job is not to stop the enemy but to slow it down...**

Your security controls force the enemy to behave abnormally, making it an anomaly, that your SOC can detect and stop...

**NIC REBEL EDITION**

**COHESIVE STREAM**

**EVASIVE MANUEVER**

**PATH COMPARISON: GROUP VS. INDIVIDUAL**

## Die Philosophie (die nicht jeder teilen muss)

**Eine technische, nicht von Tools abhängende, Maßnahme,  
die nichts in Umsetzung und Unterhalt kostet,  
aber \*irgendwas\* tatsächlich verhindert,  
sollte stets realisiert werden,  
damit man sich darum^^  
in Zukunft nicht mehr  
kümmern muss 😊**

# The Final Countdown

Alles Dinge, die ihr schon tausendmal gehört habt.

# #1 LLMNR, mDNS und NetBIOS\* deaktivieren

- **Gefühlt 50% der Hacking-Übungen beginnen mit Responder und LLMR**
- **Policy: „Turn off multicast name resolution“ → Enabled**
  - HKLM\Software\Policies\Microsoft\Windows NT\DNSClient\EnableMulticast = 0
- **Policy: „Configure multicast DNS protocol“ → Disabled (neue Templates!)**
  - HKLM\Software\Policies\Microsoft\Windows NT\DNSClient\EnableMDNS = 0
- **Policy: „Allow NetBT queries for FQDN“ → Disabled**
  - HKLM\Software\Policies\Microsoft\Windows NT\DNSClient\QueryNetBTfqdn = 0
- **Policy: „Turn off smart protocol reordering“ → Enabled**
  - HKLM\Software\Policies\Microsoft\Windows NT\DNSClient\DisableSmartProtocolReordering = 1

## #2 RID-500 zum Break-Glass umfunktionieren

### ▪ **Ganz einfach:**

- Wenn's nicht anders geht, eine Kopie machen und ab sofort diese benutzen
  - **Ordentliche Separation von Berechtigungen ist natürlich noch besser**
- Alle SPNs von RID-500 entfernen
  - **Und wenn sie wirklich noch im Betrieb waren... nun ja, entschärfen**
- Kennwort durch die gesamte History durchrollen, ein neues langes (aber tippbares) generieren und in den Safe sperren
- In eine OU verschieben, wo niemand aus Versehen das Kennwort rollt
  - **Besserer Schutz wird wegen AdminSDHolder schwierig, aber nicht ganz unmöglich**

### ▪ **Warum?**

- RID-500 kann man nicht wirkungsvoll deaktivieren
- Im Zweifel wirken auf ihn keine Einschränkungen wie AuthN Policies

## #3 Print Spooler auf DCs deaktivieren

- **Das Original-PrintingNightmare ist zwar weggepatcht worden, aber es gibt immer wieder neue Angriffstechniken**
- **Einfach per GPO oder GPP:**
  - GPO stoppt den Dienst nicht, bei GPP kann man das angeben
- **Im AD veröffentlichte Drucker müssen dann manuell gelöscht werden**
- **Alternative, falls man die Spooler-Funktion wirklich braucht:**
  - Auf dem PDCe (fokussiert per WMI) laufen lassen → nur per GPP
  - Und einen RPC-Filter auf der Firewall  
(nicht einfach, aber möglich: <https://firewall.dsinternals.com/ADDS/>)

## #4 Unconstrained Delegation entsorgen

### ▪ Wenn Delegation gebraucht wird:

- Constrained für die richtigen Ziele (und Dienste, aber das ist weniger wichtig)
- Oder RBCD ← Einschränkungen am richtigen Ort anwenden

### ▪ Warum?

- Bei Constrained Delegation → Angreiferin bekommt Service Tickets
- Bei Unconstrained → Angreiferin bekommt TGTs...
- ...und das Kerberos-Ticket wird doppelt so groß (nicht der LSA Token!)

### ▪ Identifizierung:

```
(& (userAccountControl:1.2.840.113556.1.4.803:=524288)
(! (userAccountControl:1.2.840.113556.1.4.803:=1048576))
(! (primaryGroupID=516)))
```

## #5 Delegation für privilegierte Accounts deaktivieren

- Sollte 2026 nicht mehr nötig sein...
- ...und eröffnet viele „schöne“ Angriffsszenarien
- Identifizierung (maximal vereinfacht):  
(`& (adminCount=1)`  
`(objectCategory=person)`  
`(!(userAccountControl:1.2.840.113556.1.4.803:=1048576))`)
- Auch die Mitgliedschaft in „Protected Users“ hat diese Wirkung!

## #6 LMCompatibilityLevel auf 3 (oder höher)

- **Hindert betroffene Maschinen daran, für ausgehende Verbindungen NTLMv1 oder gar LM zu verwenden**
  - Auf allen Tier 0-Systemen einstellen!
- **Wert 3 hindert nicht betroffene Maschinen nicht daran, NTLMv1 oder LM zu verwenden!**
- **Wert 4 hindert nicht betroffene Maschinen nicht daran, NTLMv1 zu verwenden!**
- **Doch selbst Wert 5 hindert eine gewiefte Angreiferin nicht daran, NTLMv1 anzufordern.**
  - Korrekt programmierte Anwendungen werden der LSA-Einstellung aber folgen.

## #7 GPOs mit Kennwörtern entsorgen

- **Nur in GPPs, dafür aber in vielen:**

- Users & Groups
- Files & Folders
- Scheduled Tasks
- ODBC Data Sources

- **Falsch: Microsoft hat das 2014 weggepatcht**

- **Richtig: Microsoft hat die Bearbeitung im Editor 2014 weggepatcht**

- Die Anwendung funktioniert nach wie vor...
- ...genauso wie das Entschlüsseln durch interessierte Dritte ☹️

- **Identifizierung:**

```
$files = Get-ChildItem -Path '\\localhost\SYSTEM\demo.mvp\Policies' -Recurse -File -Include '*.xml'  
select-String -Path $files.FullName -Pattern 'cpassword\="\S+\\"'
```

## #8 Überschüssige PKI-Zertifikate raus aus NTAUTH

- **Wenn eine CA keine Kerberos-Zertifikate ausstellen soll...**
- **...hat ihr Zertifikat auch nichts in NTAUTH verloren. So einfach ist es.**
  - Das hat nichts mit dem Vertrauen in diese Zertifizierungsstelle zu tun!
- **Und falls doch einmal benötigt?**
- **Die Reparatur ist trivial und sogar mit der GUI (pkiview.msc) möglich 😊**

## #9 Domain Join durch User deaktivieren

- **Wie kontrolliere ich als Angreiferin am einfachsten einen Computer im AD?**
- **Indem ich ihn selbst erzeuge!**
  
- **Mit Standard-Einstellungen kann das jeder Benutzer (und sogar Computer)**
  
- **Deaktivieren: Domain Root + DDCP**
  
- **Identifizieren:  
(ms-DS-CreatorSID=\*)**

## #10 SPNs und RC4 von privilegierten Accounts entfernen

- Einfaches Kennwort + SPN + RC4-Verschlüsselung = Kerberoasting
- Einfaches Kennwort + SPN + RC4-Verschlüsselung + hohe Rechte = ☠
- **Klassiker:**
  - SQL (Domain Admin)
  - SharePoint (Replikation)
  - Irgendwas mit WebUI (Verwendung von Admins oder Delegation)

- **Identifizieren:**

```
(& (servicePrincipalName=*)(!(userAccountControl:1.2.840.113556.1.4.803:=2))
(userAccountControl:1.2.840.113556.1.4.803:=66048)
(|
(msDS-SupportedEncryptionTypes:1.2.840.113556.1.4.803:=4)
(! (msDS-SupportedEncryptionTypes=*))
)
)
```

- **Eliminieren: je nachdem, wozu der Account noch genutzt wird**

# Bonus: Trusts

Auch ein einseitiger Trust braucht Liebe!

## Trust auf der vertrauten (wertvollen) Seite härten

- **In beiden Forests vorhanden: trustedDomain Objekt für die Gegenseite**
- **Nur im vertrauten Forest: Ein User-Objekt mit dem Namen der Gegenseite**
  - Bis DFL 2016: Mitglied in -513 (Users)
  - DFL 2025: Mitglied in -528 / -529 (Forest / External)
- **Diese teilen ein (automatisch rotiertes) Kennwort**
  
- **Beste Härtung:**
  - AuthN Policy mit einer Bedingung, die nie zutrifft (z.B. ein nicht existierendes Silo)

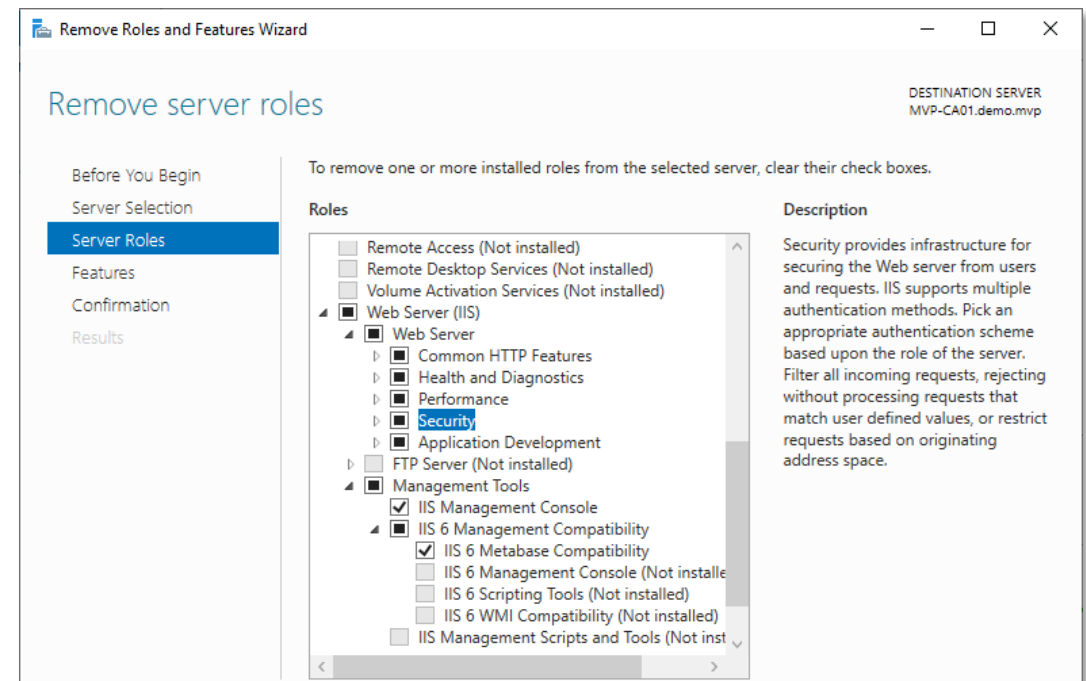
# Bonus: Enterprise PKI

Weil den Zertifikatskram eh keiner versteht...

## Web Enrollment endlich in Rente schicken

- **Nicht wirklich benutzbar im Jahre 2026...**
  - ASP-Code aus 1998 wird nicht wirklich gepflegt
  - ActiveX-Controls nicht mehr möglich oder zumindest nicht mehr empfohlen
- **...dafür anfällig für eine Vielzahl von Angriffen**

- **Lösung: einfach deinstallieren**
  - An die IIS-Komponenten denken!
- **Identifizieren: nicht immer einfach**
  - Inventur hilft, falls man hat
  - Ansonsten: scannen...



## ADCS: Berechtigungen restriktiv regeln

- **Manage CA → Tier 0-Aufgabe**
- **Manage Certificates → kommt darauf an**
  - Wenn AuthN-fähige Zertifikate ausgestellt werden → Tier 0
  - Wenn Server-Zertifikate für Tier 0-Systeme ausgestellt werden → Tier 0
  - Andernfalls → Tier 1
- **Manager-Freigabe für Zertifikate ist ein sehr wirkungsvolles Mittel**
  - Wo Autoenrollment notwendig ist → Separate Issuing CA mit Einschränkung der EKUs
- **ADCS hat eine Einstellung, wonach „Manage CA“ und „Manage Certs“ zwangsläufig getrennt werden müssen → zu überlegen**
- **Templates:**
  - Bearbeiten → Tier 0
  - Enroll → siehe nächsten Tip

## ADCS: Tame My Certs einsetzen

- **Kostet nichts (aber man kann Support vom Autor kaufen)**
- **Ist schnell installiert**
  - Uwe Gradenegger hat aber leider beschlossen, auf .NET 10 umzusteigen ☹️
- **Verändert nicht das Verhalten der CA, wenn man nichts einstellt...**
- **...aber macht sie sehr wohl viel sicherer, wenn man kritische Vorlagen konfiguriert!**

# Bonus: Andere Maßnahmen

Dafür ist heute keine Zeit → kommt zu mir ins Seminar 😊

## 10 Maßnahmen, die evtl. etwas kosten und/oder kaputt machen

- **Pre-Windows-2000-Compatible-Access Gruppe ausleeren**
- **LAPS überall, außer für DSRM**
- **Signierung überall: LDAP + SMB + HTTP (*heißt EPA bei IIS*)**
- **NTLM zumindest für privilegierte Accounts deaktivieren, besser für alle**
- **Service Accounts mit AuthN Policies einhegen oder durch gMSA ersetzen**
- **Tier 0 Assets mit AuthN Policies einhegen**
- **WDAC oder zumindest AppLocker – ja, auch auf Servern**
- **BitLocker – ja, auch auf Servern**
- **Alte Accounts aufräumen, Computer sind unter Umständen wichtiger als User**
- **AD-Backups in den Griff kriegen und dennoch KRBTGT- und DSRM-Rotation**



# Happy Hardening!

Bei Fragen → einfach fragen ☺