IT-PRO-BERLIN.DE

Frühlingserwachen: Das LDAPS-Ding

Was ist dran? Was ist zu tun?

Windows Server User Group Berlin | 20.02.2020

Get-SpeakerInfo -Brief

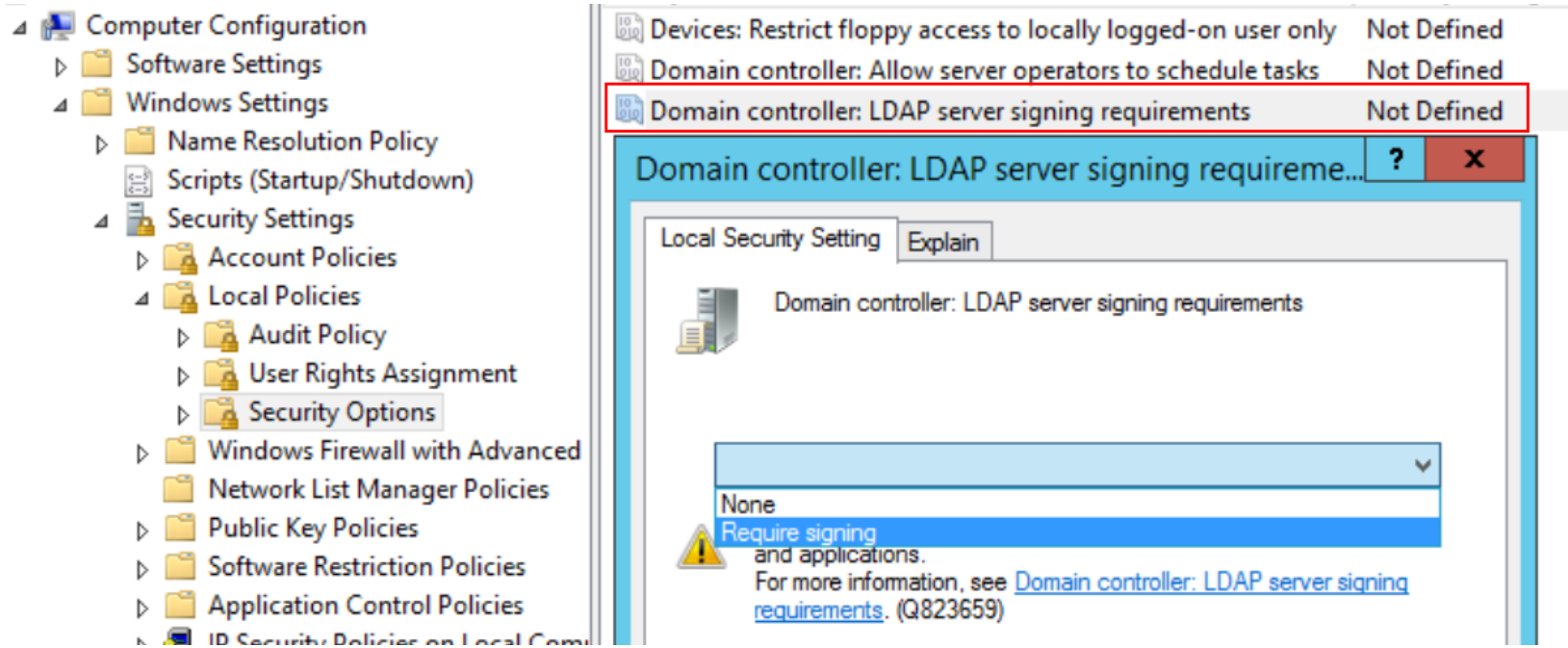
- **Name:** Evgenij Smirnov
- **YearOfBirth:** 1972
- **JobTitle:** { Consultant, Project Mgr. }
- **TwitterID:** @cj_berlin
- **Employer:** DTS Systeme GmbH
- **MVP:** False
- **Certifications:** { MCSE, MCSA, VCP, VCAP, VCIX, CCA, QCIC }
- **UserGroups:** { WSUG-B, EXUSG, PSUGB }

Was ist eigentlich das Problem?

- **Das Thema ist nicht neu!**
- **MSRC: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190023**
- **Es sind zwei Sachverhalte, die miteinander technisch nicht viel zu tun haben:**
  - LDAP Signing
  - LDAP Channel Binding
- **Beide sind per Default abgeschaltet (können aber aktiviert werden)**
- **Microsoft möchte nun per Default beide einschalten**
- **Nicht alle nachgelagerten Systeme sind Stand heute kompatibel**
  - Nicht alle Systeme, die LDAPS verwenden, sind zwangsläufig bekannt!

LDAP Signing

- **Garantiert die Integrität im LDAP-Verkehr (keine Möglichkeit der Änderung durch MitM)**
- **Wird auch mit den jetzigen Defaults verwendet, wenn der Client es anfordert**
- **“Require” erzwingt nur dann Signierung, wenn TLS nicht verwendet wird**
- **Default jetzt: None**
- **Default später: Require**



LDAP Channel Binding

- **Verhinderung von Replay-Angriffen durch ein einmaliges Token**
  - setzt LDAPS voraus
- **CVE-2017-8563 → Sicherheitsupdate auf LDAP-Clients**
  - sollte aber bereits vorhanden sein, seit 2017 ist einiges passiert ;-)
- **Registry Key auf Domain Controllern:**
  `HKLM\System\CurrentControlSet\Services\NTDS\Parameters\`
  `LdapEnforceChannelBindings`
- **Default jetzt: nicht vorhanden (entspricht 0) = deaktiviert**
- **Default später: nicht vorhanden (entspricht 1) = aktiviert, falls unterstützt**
- **Auch möglich: 2 = aktiviert, immer**

Was sind die wirklichen Problemfälle?

- **Ältere proprietäre Systeme (oder seit 2016 ungepatchte Server 2008 ;-))**
  - manche können gar kein LDAPS
  - andere kommen mit SHA-2-Zertifikaten nicht klar
  - usw…

- **Load Balancing-Konstrukte für LDAP (hat noch nie besonders gut funktioniert)**
  - Signing kann man durch LDAPS abwenden, Channel Binding wird aber nicht gehen
  - möglichst auf Applikationsebene abbilden
  - Eine nicht nur “LDAP-fähige”, sondern “AD-fähige” Anwendung muss SRV Records nutzen, um einen LDAP-Server oder KDC zu finden!

Was ist zu tun?

- **SSL aktivieren JETZT (ändert erst einmal nichts am *status quo ante*)**
  - Falls möglich, Domain Controller-Zertifikate per Autoenrollment verteilen
  - **`gpupdate /force`**, danach NTDS oder den DC durchstarten
- **LDAP-Diagnostik benutzen:**
  - mit dem März-Update sollen neue Audit-Events kommen, die sie erleichtern sollen
  - Bereits heute per Default: **Event 2887** im Directory Services Log sagt aus, dass es unerwünschte Anmeldungen hat und wieviele, nicht jedoch welche.
  - **`reg add HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics /v "16 LDAP Interface Events" /t REG_DWORD /d 2`**
  - Danach nach dem **Event 2889** Ausschau halten
- **Die gemeldeten Systeme (IP-Adressen) prüfen und Konfiguration anpassen**
  - Kompatibilität vom Hersteller bestätigen lassen
  - Zum Testen kann man einen DC umstellen, der sonst kein Ziel für LDAP ist

Log hunting-Beispiel

```
$events = Get-WinEvent -ComputerName "MYDC4711"
      -FilterHashtable @{
            'logname' = 'Directory Service';
            'id' = 2889  }
$events.foreach( {
     $ip = ($_.Properties.Value[0] -split ":")[0]
     $user = $_.Properties.Value[1]
     $bind = $_.Properties.Value[2]
     if ($bind -eq 1) {
         Write-Information "No TLS:   $user from $ip"
     } else {
         Write-Information "Unsigned: $user from $ip"
     }
} )
```

“Offizielle” Ressource

https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/ldap-channel-binding-and-ldap-signing-requirements-march-update/ba-p/921536

Updates in diesem Artikel sind zu erwarten, wenn das März-Update und dann das richtige rauskommt, also am besten bookmarken.

Und was, wenn ich nicht bis H2 härten kann?

- **Wer Anwendungen hat, die auch noch in H2 2020 kein Channel Binding können werden, hat folgende Möglichkeiten:**
  - Das bisherige Verhalt per Gruppenrichtlinie fest konfigurieren (also quasi die Niederlage eingestehen). *Der oder die Hersteller sollte(n) einen bösen Brief erhalten, da seint-/ bzw. Ihretwegen die Sicherheit der gesamten Umgebung herabgesetzt wird…*
  - Eine LDS-Instanz oder ein anderes Verzeichnis als Proxy vorschalten.

Happy hardening!

Bei Fragen → einfach fragen ☺