Domain Controller - Secure Connection Binding

Ab Mitte des Jahres 2020 wird Microsoft das LDAP Channel Binding & LDAP Signing erzwingen.

Diese beiden Methoden sollen zur Erhöhung der Sicherheit in der Netzwerkkommunikation zwischen Clients und Domain Controllern dienen.

Betroffen sind folgende Dienste:

- AD DS (Active Directory-Domänendienste)
- AD LDS (Active Directory-Lightweight Directory-Dienste)

Im März wird Microsoft ein Sicherheitsupdate veröffentlichen, mit dem im Nachgang, das LDAP Channel Bindung und das LDAP Signing weiter gehärtet werden kann und forciert wird!

Auslöser des Sicherheitsupdate und das Forcieren des Bindings & Signings sind:

Wer die LDAP Standard-Einstellungen auf einem Domain Controller belässt (ohne Bindung und Signierung), der geht das Risiko ein, das ein Angreifer durch Erschleichung erhöhter Rechte weiterhin in der Lage wäre, eine Authentifizierungsanforderung erfolgreich an einen LDAP Server (AD DS oder AD LDS) weiterzuleiten.

Am 13. August wurde die ADV190023 bereits veröffentlicht, siehe hier:

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190023

Ab jetzt sind noch 3 Monate Zeit, die eigene Umgebung dahingehend zu prüfen, ob die Durchsetzung also die Erzwingung von Binding&Signing ein Problem darstellen würde.

Was sollte geprüft werden:

- Drucker mit einer Scan to Mail Funktion
- Proxys
- SecureMail Gateways
- Dritt-Anbieter Anwendungen uvm.

Wer sein Environment bisher immer aktuell gehalten hat, wird diese Beispiele wohl nicht prüfen müssen. Aber ein Blick unter Haube lohnt sich immer.

Welche Systeme kommunizieren denn überhaupt mit einer schwachen Verschlüsselung?

Dazu hatte ich bereits eine Dokumentation geschrieben „LDAP unsichere Verbindungen".

Auf allen Domain Controllers muss dazu das entsprechende Logging eingeschaltet werden. Das geht am Besten über den Import eines Registry-Keys:

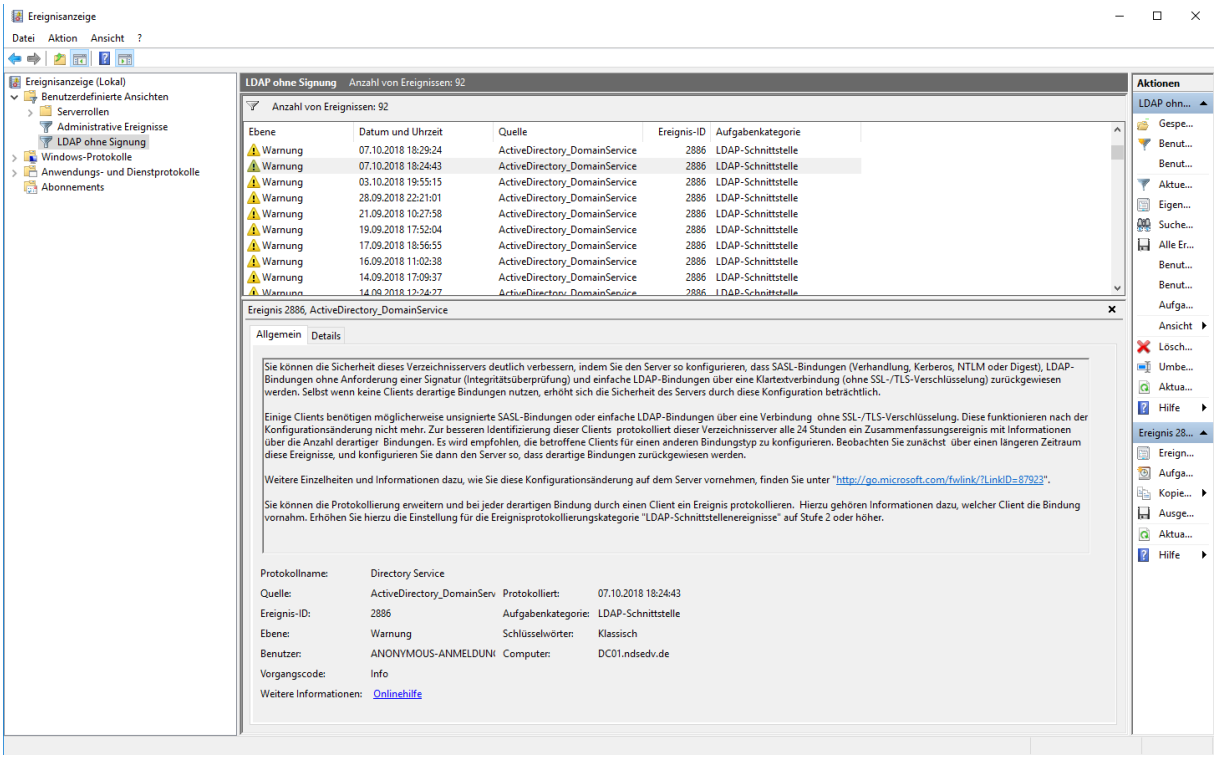
```
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics /v "16 LDAP Interface Events" /t REG_DWORD /d 2
```

Die Aufgabe besteht nun darin die Systeme zu identifizieren die noch über ldap simple bind kommunizieren.

Die Ergebnisse lesen wir im Event-Log unter Applications and Services aus. Dazu navigieren wir zu Directory Service. Das Logging sollte mindestens 50 Stunden laufen, denn ein Eintrag wird nur alle 24 Stunden geschrieben.

Domain Controller - Secure Connection Binding

Gefiltert in Verzeichnisdienst (Directory Services) > Aufgabenkategorie LDAP-Schnittstelle > Events 2886, 2887, 2888, 2889



Text etwas vergrößert

Sie können die Sicherheit dieses Verzeichnisservers deutlich verbessern, indem Sie den Server so konfigurieren, dass SASL-Bindungen (Verhandlung, Kerberos, NTLM oder Digest), LDAP-Bindungen ohne Anforderung einer Signatur (Integritätsüberprüfung) und einfache LDAP-Bindungen über eine Klartextverbindung (ohne SSL-/TLS-Verschlüsselung) zurückgewiesen werden. Selbst wenn keine Clients derartige Bindungen nutzen, erhöht sich die Sicherheit des Servers durch diese Konfiguration beträchtlich.

Einige Clients benötigen möglicherweise unsignierte SASL-Bindungen oder einfache LDAP-Bindungen über eine Verbindung ohne SSL-/TLS-Verschlüsselung. Diese funktionieren nach der Konfigurationsänderung nicht mehr. Zur besseren Identifizierung dieser Clients protokolliert dieser Verzeichnisserver alle 24 Stunden ein Zusammenfassungsereignis mit Informationen über die Anzahl derartiger Bindungen. Es wird empfohlen, die betroffene Clients für einen anderen Bindungstyp zu konfigurieren. Beobachten Sie zunächst über einen längeren Zeitraum diese Ereignisse, und konfigurieren Sie dann den Server so, dass derartige Bindungen zurückgewiesen werden.

Weitere Einzelheiten und Informationen dazu, wie Sie diese Konfigurationsänderung auf dem Server vornehmen, finden Sie unter "http://go.microsoft.com/fwlink/?LinkID=87923".

Sie können die Protokollierung erweitern und bei jeder derartigen Bindung durch einen Client ein Ereignis protokollieren. Hierzu gehören Informationen dazu, welcher Client die Bindung vornahm. Erhöhen Sie hierzu die Einstellung für die Ereignisprotokollierungskategorie "LDAP-Schnittstellenereignisse" auf Stufe 2 oder höher.

Event-ID 2886
Event-ID 2887
Event-ID 2888
Event-ID 2889

Erstellt von Jörn Walter **17.12.2019**