Landesamt für Sicherheit in der Informationstechnik

LSI-Info T#06b

WINDOWS DOMÄNEN TEIL2: DOMÄNENCONTROLLER

BESSERER SCHUTZ VON DOMÄNENCONTROLLERN

Version 1.2 vom: 16.05.2022

Management Summary

Im Rahmen des Active Directory (AD) stellen Domänencontroller Dienste zur zentralen Authentifizierung und Verwaltung von Ressourcen im Netzwerk bereit. Solche zentralen Server, welche Zugriff auf Dienste und deren Administration gewähren, sollten besonders geschützt werden. Im Falle eines Angriffs wäre es möglich, beispielsweise mit Golden oder Silver Tickets, dass das gesamte Netzwerk kompromittiert wird. Diese LSI-Info zeigt auf, mit welchen Möglichkeiten Domänencontroller besser abgesichert werden können. An dieser Stelle sei noch darauf hingewiesen, dass die Tipps zur Absicherung von Domänencontrollern nur eine Ergänzung zu anderen Basismaßnahmen sind und alleine keinen ausreichenden Schutz bieten.

AUTHENTIFIZIERUNGSPROTOKOLL KERBEROS

Aktuelle Windows Server Betriebssysteme setzen als Standard-Authentifizierungsverfahren Kerberos ein, was im Gegensatz zu älteren Authentifizierungsverfahren mehr Sicherheit bietet. Kerberos löst somit die Authentifizierungsprotokolle NTLM(v1) und NTLMv2 sowie LM ab. Dabei sollte aus Sicherheitsgründen dringend auf NTLM(v1) und LM verzichtet werden (siehe Abbildung 1). Allerdings müsste vor einer Umstellung geprüft werden, ob alle angeschlossenen Systeme diese Authentifizierungsverfahren unterstützen.

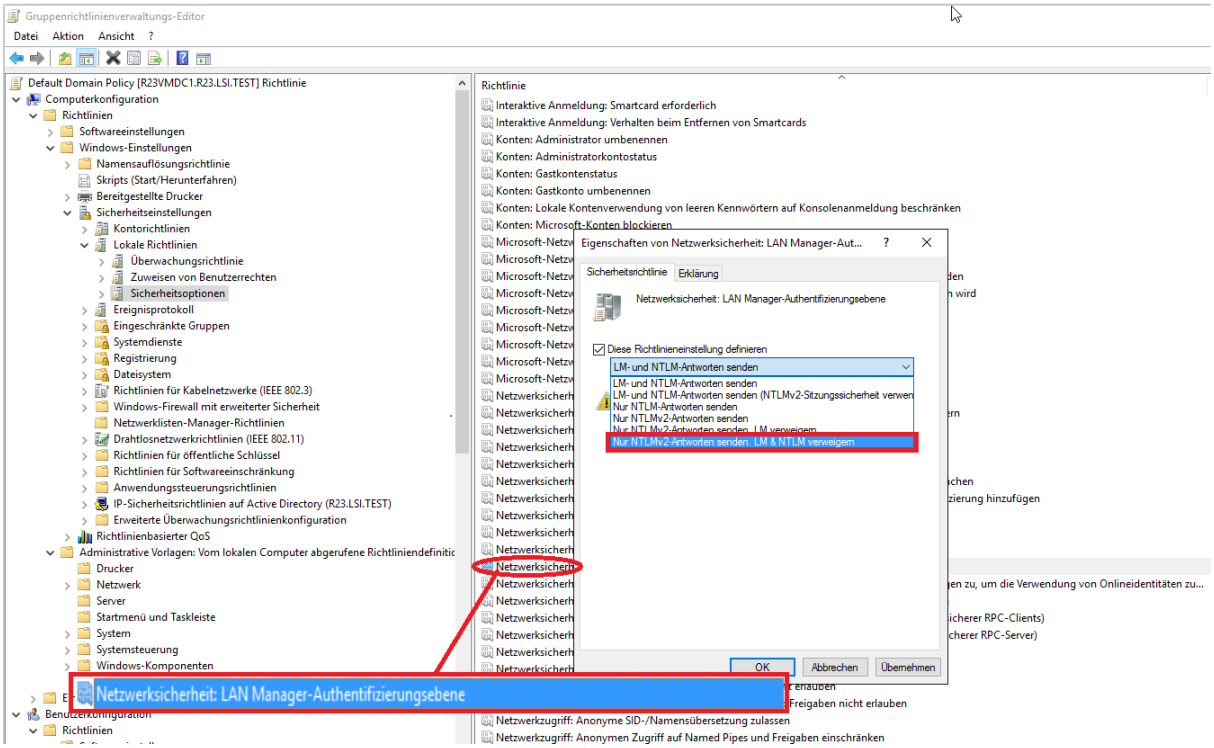

Abbildung 1: Gruppenrichtlinie LAN-Manager

Generell muss auch gerade bei älteren Betriebssystemen das Ende des Supportzeitraums (End-of-Life) im Auge behalten und rechtzeitig ein Umstieg auf ein aktuelles Betriebssystem geplant und vorgenommen werden. Dadurch wird gewährleistet, dass aktuelle Protokolle genutzt und Sicherheitsupdates eingespielt werden können.

GOLDEN UND SILVER TICKET ANGRIFFE

Ein Golden Ticket-Angriff verschafft dem Angreifer umfassenden und vollständigen Zugriff auf die gesamte Domäne – auf alle Computer, Dateien, Ordner und vor allem den Domänencontroller. Unter einem Golden Ticket versteht man ein Ticket-Granting-Ticket (TGT) mit einer Laufzeit von standardmäßig 10 Jahren, welche aber beim Erstellen

auch selbst gewählt werden kann. Mit einem solchen Ticket können über diese Dauer Service Tickets ausgestellt werden, ohne dass eine erneute Authentifizierung notwendig ist.
Das TGT ist also in der Hierarchie das oberste Ticket, dem der Ticket Granting Service (TGS) vertraut und aufgrund dessen Service Tickets ausgestellt werden. Das TGT wird mit dem Passwort des Benutzerkontos mit dem Namen *krbtgt* im AD verschlüsselt, für die Erzeugung eines Golden Tickets ist hier allerdings nur der Hashwert des Passworts notwendig, welcher durch Pass the Hash (PtH) bzw. Pass the Ticket (PtT) Angriffe oder Zugriff auf unverschlüsselte Backups ausgelesen werden kann. Ein Golden Ticket bleibt auch nach einer Passwortänderung des Benutzerkontos *krbtgt* noch gültig (s. Kerberos-Reset weiter unten).
Silver Tickets sind im Gegensatz zum Golden Ticket keine TGTs, sondern gefälschte Service Tickets um Zugriff zu einem speziellen Dienst zu erlangen. Hierfür wird nicht der Hashwert des *krbtgt*-Benutzerpassworts benötigt, sondern der Hashwert des Benutzerkontos unter welchem der entsprechende Dienst läuft.

SCHUTZMAßNAHMEN GEGEN GOLDEN UND SILVER TICKET ANGRIFFE

Um sich bestmöglich vor Golden und Silver Ticket Angriffen zu schützen, ist es empfehlenswert, alle nicht benötigten Benutzer, Rollen, Erweiterungen und Dienste auf dem Server zu deaktivieren und den Einsatz unsicherer Protokolle wie zum Beispiel LM und NTLM(v1) zu unterbinden (Minimalprinzip). Hinzu kommt das zeitnahe Einspielen von Sicherheitsupdates (Patch-Management) und die Verschlüsselung der Datenträger. Auch der Zugriff auf Domänencontroller sollte eingeschränkt werden, sodass sich nur bestimmte Benutzer direkt dort anmelden können. Generell kann per Gruppenrichtlinie festgelegt werden, an welchem System sich welcher Benutzer und welche Benutzergruppe anmelden darf. Die Nutzung eines Choke Points (Engpass/Nadelöhr) in Form eines Terminalservers oder eines, nur für diesen Zweck genutzten, dedizierten Clients, der ausschließlich und exklusiven administrativen Zugriff auf den Domänencontroller hat, stellt eine weitere Schutzmaßnahme dar.
Da der Passworthash des Benutzerkontos *krbtgt* auch aus einem Backup gewonnen werden kann, ist es wichtig Backups vor unberechtigtem Zugriff zu schützen.
Bei virtuellen Maschinen (VM) gibt es die Möglichkeit, den Bootvorgang abzusichern, die VM zu verschlüsseln und virtuelle Trusted Platform Modules (TPM) einzusetzen, um diese sicherer zu machen.
Strukturierungsmaßnahmen wie der Einsatz von sogenannten Schichten (Tier) kann darüber hinaus dabei helfen, Zugriffe auf einen bestimmten Bereich einzuschränken.

Ein Beispiel für eine entsprechende Strukturierungsmaßnahme könnte so aussehen:

- Tier 0 = besonders schützenswerte Systeme wie bspw. Domänencontroller
- Tier 1 = Server die nicht im Tier 0 sind
- Tier 2 = Clients

Jede Schicht hat unterschiedliche Administratorkonten und die Einschränkung, dass die Administratoren und Benutzer sich nur innerhalb der jeweiligen Schicht auf Systemen authentisieren können. Somit hätte ein Angreifer, der einen Client übernommen hat, nicht direkt Zugriff auf stärker abgesicherte und schützenswertere Systeme.

Da mit dem Hashwert des deaktivierten *krbtgt*-Benutzerkontos Golden Tickets erstellt werden können, können diese bis zu einem Kerberos-Reset dieses Benutzers verwendet werden. Daher ist es empfehlenswert in regelmäßigen Abständen einen Kerberos-Reset des Benutzerkontos auf allen Domänencontrollern durchzuführen. Da für Benutzerkonten das aktuelle und das vorherige Passwort im Verlauf gespeichert werden, sollte das Passwort immer zwei Mal geändert werden. Nach einem einmaligen Passwortwechsel bleiben bestehende Tickets für deren Dauer weiterhin gültig. Microsoft stellt für einen Kerberos-Reset ein entsprechendes PowerShell-Skript[1] bereit. Für einen Kerberos-Reset muss dies Script auch zweimal ausgeführt werden. Bevor dieser Reset des *krbtgt*-Benutzers durchgeführt wird, sollte geprüft werden, ob die sich im Netz befindlichen Systeme wie Linux-Server, dies unterstützen.
In den Gruppenrichtlinien können die von Kerberos unterstützten Verschlüsselungsdatentypen eingestellt werden, welche für das Anfordern und Ausstellen von Tickets verwendet werden. Hierbei sollte darauf geachtet werden, dass nur nach aktuellem Stand der Technik sichere Verschlüsselungsverfahren (Beispielsweise AES256, SHA256, SHA 512) zugelassen sind.

DIENSTE AUF DOMÄNENCONTROLLERN

Bei Schwachstellen oder durch Fehlkonfiguration kann grundsätzlich jeder Dienst ein gewisses Risiko darstellen.
Daher sollten gerade auf wichtigen Systemen wie Domänencontrollern nur notwendige Dienste aktiviert sein. Beispielsweise für Print- oder Fileserver bietet sich an, diese

[1] https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51

Dienste auf eigene Systeme auszulagern um die Angriffsvektoren auf den Domänencontroller zu minimieren.

ACTIVE DIRECTORY DATENBANK

Die Dateien der AD-Datenbank sind in einer laufenden AD-Umgebung vor unberechtigtem Zugriff gekapselt und damit vor direktem Zugriff geschützt. Dies betrifft jedoch nicht Datensicherungen, diese haben keinen nativen Zugriffschutz durch das AD und können manipuliert werden. Aus diesem Grunde empfiehlt es sich, Sicherungsdateien des ADs auf dauerhaft angeschlossenen Datenträgern über Datenträger- und zusätzliche Dateiverschlüsselung zu schützen.

REFERENZEN

- APP.2.2 Active Directory
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

- SYS.1.2.2 Windows Server 2012
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

- Umsetzungshinweise zum Baustein SYS.1.2.2 Windows Server 2012
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Umsetzungshinweise/Umsetzungshinweise.html

- AD-Gesamtstruktur Wiederherstellung: Zurücksetzen des krbtgt-Kennworts
  https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/manage/ad-forest-recovery-resetting-the-krbtgt-password

- Übersicht über geschütztes Fabric und abgeschirmte VMs
  https://docs.microsoft.com/de-de/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-and-shielded-vms

- Michael Kofler et al. (2018), Hacking & Security (1. Auflage, 3. Korrigierter Nachdruck), Rheinwerk Verlag

KONTAKT

Weitere Informationen finden Sie unter:

https://lsi.bayern.de/kommunen/

Für Unterlagen und Beratung wenden Sie sich bitte per E-Mail an:

Beratung-Kommunen@lsi.bayern.de.

Gerne ist das kommunale Beratungsteam auch telefonisch unter 0911 21549-523 für Sie erreichbar.

Landesamt für Sicherheit in der Informationstechnik – Leitfaden T#06b Windows Domänen Teil 2: Domänencontroller (Stand: 16.05.2022)