Landesamt für Sicherheit in der Informationstechnik

LSI-Info T#06a

WINDOWS DOMÄNEN TEIL 1: DOMÄNENADMINISTRATOREN

SCHUTZ VON PRIVILEGIERTEN BENUTZERKONTEN

Version 1.1 vom: 16.05.2022

Management Summary

Domänenadministratoren haben Vollzugriff auf alle Daten in der Domäne. Neben dem Zugriff auf Daten im Dateisystem betrifft dies administrativen Vollzugriff auf alle Computer in der Domäne und auf das Active Directory (u.v.a. Gruppenrichtlinien). Da sich mit diesen Benutzerkonten zentral alle IT-Ressourcen in der Domäne verwalten lassen, können administrative Prozesse effizienter gestalten werden. Dadurch werden diese Benutzerkonten aber auch ein beliebtes Angriffsziel und ein Einfallstor, um komplette Netzwerke zu kompromittieren. Daher haben derart mächtige Benutzerkonten einen sehr hohen Schutzbedarf und sollten somit besonders abgesichert werden.

ALLGEMEIN

Für Angreifer sind Benutzerkonten mit erweiterten Berechtigungen ein lohnenswertes Ziel, um möglichst viel Schaden in einem Netzwerk anzurichten.
Leider wird immer wieder festgestellt, dass mit Administratorkonten sorglos umgegangen und diese folglich nicht ausreichend geschützt werden. Außerdem werden diese häufig für nicht-administrative Aufgaben verwendet, womit Einfallstore geschaffen werden. Dabei ist es gerade bei Benutzerkonten mit erweiterten Berechtigungen wichtig, diese besonders zu schützen und nur für die ihnen zugedachten Aufgaben zu verwenden. Vor allem Domänenadministratoren mit domänenweiten Rechten haben administrativen Vollzugriff auf alle Daten und Computer in der Domäne sowie das Active Directory (siehe Abbildung 1) und sollten daher besonders abgesichert werden.

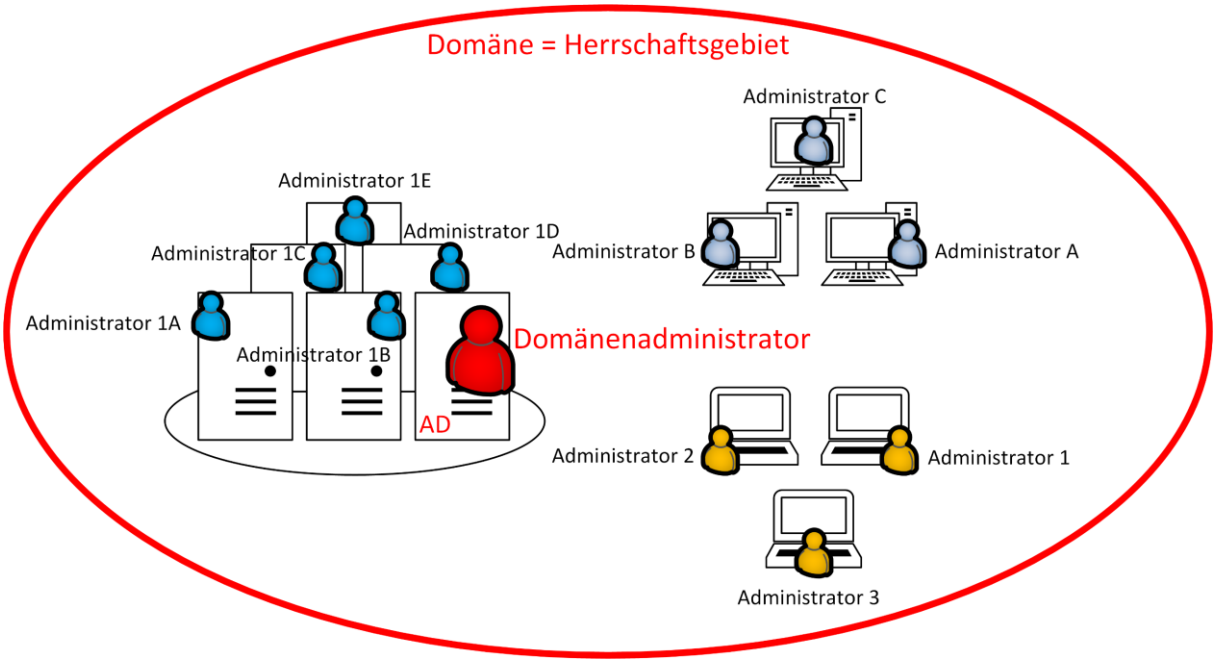

Abbildung 1: Herrschaftsgebiet eines Domänenadministrators

Ein starkes Passwort alleine kann aber auch nicht als ultimativer Schutz gesehen werden. Beispielsweise reicht es bei Pass the Hash (PtH) oder Pass the Ticket (PtT) Angriffen aus, die sich im Arbeitsspeicher befindlichen verschlüsselten Passwörter (Hashes) eines Domänenadministrators auszulesen, womit sich beispielsweise Ticket-Granting-Tickets (TGT) erstellen lassen. Somit kann sich ein Angreifer Zugang zum gesamten Netzwerk verschaffen ohne sich selbst authentisieren zu müssen.

AUSLESEN VON PASSWÖRTERN

Speziell bei PtH oder PtT Angriffen werden die benötigten Informationen aus dem Arbeitsspeicher ausgelesen. Damit eine Privilegien-Eskalation möglich wird, ist es notwendig, dass die Informationen von Benutzern mit erweiterten Berechtigungen ausgelesen werden, wie zum Beispiel die von Domänenadministratoren. Die erlangten Daten können dann für weitere Aktionen, wie zum Beispiel die Erstellung eines Golden und Silver Tickets verwendet oder die Hash-Werte mit spezieller Software durch unterschiedliche Verfahren erraten (Offline-Cracking) werden.

SCHUTZMAßNAHMEN GEGEN DAS AUSLESEN VON PASSWÖRTERN

Die Anzahl der Administratorkonten sollte auf ein notwendiges Maß reduziert werden, gleichzeitig soll mit einem Administratorkonto aber auch nur bestimmte Tätigkeiten ausgeführt werden. Beispielsweise je ein Administratorkonto nur für die Verwaltung der Benutzerkonten oder der Gruppenrichtlinien. Zudem sollte jedes Administratorkonto personalisiert sein und verschiedene komplexe Passwörter (Klein-, Großbuchstaben, Zahlen und Sonderzeichen) mit einer angemessenen Passwortkomplexität zugewiesen bekommen und auch in regelmäßigen Abständen geändert werden (weitere Informationen zu dem Umgang mit Passwörtern, sind in der LSI-Info A#03: Umgang mit Passwörtern beschrieben). Für die Verwaltung vieler komplexer Passwörter bietet sich die Verwendung eines Passwort-Managers an, wodurch Passwörter dokumentiert und verschlüsselt auf dem Computer gespeichert werden können.
Weiterhin müssen auch normale Benutzerkonten der Mitarbeiter geschützt werden. Hierfür empfiehlt es sich eine Kennwortlichtlinie zu erstellen und dafür zu sorgen, dass diese mittels einer Gruppenrichtlinien umgesetzt wird (siehe Abbildung 2). Sofern Anpassungen unter anderem an Gruppenrichtlinien vorgenommen werden und jeder Administrator die Möglichkeit haben muss diese nachvollziehen zu können, sollten diese Änderungen dokumentiert werden.

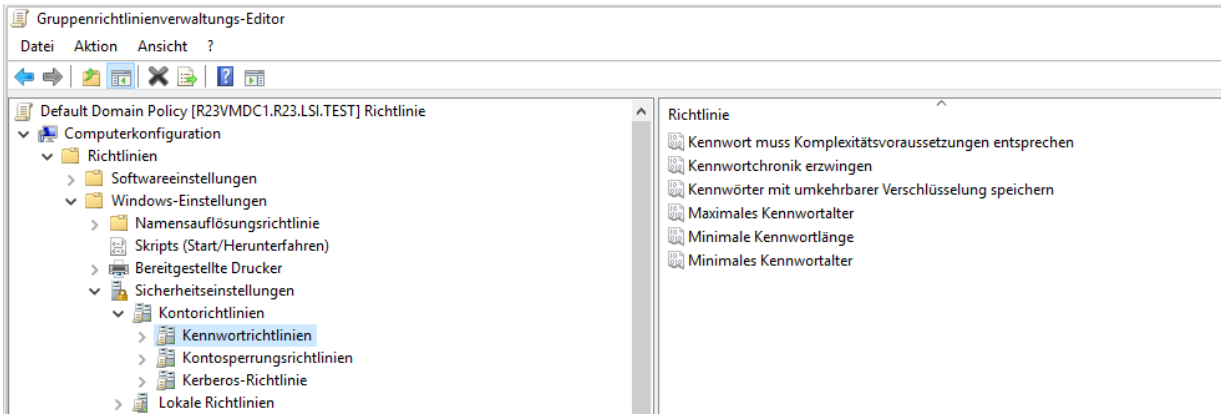

Abbildung 2: Gruppenrichtlinie - Kennwortrichtlinien

Falls es kompromittierte Benutzerkonten gibt, lassen sich diese unter Umständen identifizieren, indem unerwartetes Verhalten überwacht wird. Dies kann zum Beispiel durch die Konfiguration der Gruppenrichtlinie „Erweiterte Überwachungsrichtlinien“ erfolgen, durch welche die entsprechenden Ereignisse erzeugt werden. Natürlich reicht die reine Protokollierung an dieser Stelle nicht aus. Die Ereignisse müssen auch, entweder manuell oder mit Hilfe entsprechender Software, kontrolliert und ausgewertet werden.

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 zu Bausteinen
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Umsetzungshinweise/Umsetzungshinweise.html

- Schützen des privilegierten Zugriffs
  https://docs.microsoft.com/de-de/security/compass/overview

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

- LSI-Info A#03: Umgang mit Passwörtern
  https://lsi.bayern.de/mam/aktuelles/lsi-info_a03_umgang_mit_passwoer-tern_v1.0.pdf

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.