Wie Administratoren ihr Active Directory absichern

# Mit aller Härte

**Marco Wohler**

Zu den elementaren Punkten bei der Absicherung eines Active Directory gehören verschiedene Härtungsmaßnahmen. Im Zentrum stehen dabei Klassiker wie der Umgang mit Passwörtern oder das Deaktivieren nicht benötigter Dienste.

Nachdem sich die bereits erschienenen Teile der Artikelserie rund um das Active Directory (AD) detailliert mit den Angriffen auf den Verzeichnisdienst beschäftigten [1–7], beschreibt der achte Teil, wie Systemverwalter das AD absichern können und sicherstellen, dass der Betrieb auch nach einem Worst Case schnell wieder aufgenommen werden kann. Der Artikel stellt verschiedene Konzepte, Ressourcen und Tools vor, mit denen sich die Sicherheit einer Domänenlandschaft verbessern lässt. Für einen Blick nach links und rechts finden Interessierte Hinweise zu externen Ressourcen, die eine weitere Vertiefung des Themas ermöglichen.

Es wird davon ausgegangen, dass Leserinnen und Leser die vorangegangenen Artikel [1–7] kennen und die darin konkret beschriebenen Fehlkonfigurationen oder Nachlässigkeiten vermeiden, beispielsweise ein Passwort in eine Benutzerbeschreibung zu schreiben [2] oder uneingeschränkte Delegierung [6] auf einem Rechner zu hinterlegen. Nicht alle bislang angeschnittenen Themen oder Angriffswerkzeuge werden in diesem Artikel explizit erwähnt.

## Vier Stufen zum Erfolg

Um einen gesamtheitlichen Blick auf die Verteidigung zu werfen, genügt es nicht, lediglich die präventiven Maßnahmen zu berücksichtigen, auch wenn dieser Artikel sich darauf konzentriert. Wie unter anderem seit Stuxnet [8] bekannt ist, können auch sehr gut gesicherte Systeme erfolgreich kompromittiert werden. Also gehört zu einer guten Vorbereitung nicht nur das Verhindern eines Angriffs, sondern auch das frühzeitige Erkennen und das Wiederherstellen des Betriebs sowie das Lernen aus Vorfällen. Stufe eins wäre demnach die Prävention, Stufe zwei das Erkennen von Vorfällen, Stufe drei beinhaltet Backup und Recovery sowie Business Continuity und Stufe vier sogenannte Lessons Learned (zu Deutsch: gewonnene Erkenntnisse).

Dieser Artikel behandelt die Prävention, das Absichern der AD-Umgebung. Wie man Angriffe erkennen kann, stellen kommende Artikel der Serie ausführlicher dar, ebenso das Thema Backup, das entscheidend dafür sein kann, ob es ein Unternehmen nach einem Worst Case noch gibt oder nicht [1]. Bleiben die Lessons Learned: Nach einem Incident (in diesem Kontext ein Ereignis, das die Informationssicherheit betrifft), den man bewältigen konnte, sollte immer mit den für die Lösung des Vorfalls wichtigen Personen ein Meeting stattfinden, mit dem Ziel, aus den Geschehnissen zu lernen. Denn selten erfährt man so viel über die eigene Infrastruktur und deren Schwächen wie bei der Bewältigung eines Incidents [9].

Mit den nachfolgend vorgestellten Techniken lässt sich der Domänencontroller (DC) beziehungsweise die gesamte Domäneninfrastruktur absichern. Die meisten Maßnahmen zeigen ihre volle Wirkung jedoch erst in Kombination miteinander. Wird zum Beispiel eine lokale Firewall auf einem Server mit offenem Remote-Desktop-Zugang (RDP) installiert und der RDP-Benutzer verwendet ein leicht zu erratendes Passwort ohne zweiten Faktor, wird sich ein Angreifer nicht die Zähne an der Firewall ausbeißen müssen, um an andere, abgeschirmte Dienste zu gelangen.

## Härtung per Gruppenrichtlinien

Das Setzen von Einstellungen per Gruppenrichtlinien (Group Policy, GPO) ist äußerst effizient [2]. Die Administratorin kann die gewünschten Werte zentral definieren und an mehrere Geräte auf einmal verteilen. Viele der Einstellungen werden erzwungen, sodass Anwender sich nicht über die Richtlinien hinwegsetzen können. Da in Windows fast alles per GPO konfiguriert werden kann, ist es auch für Sicherheitsmaßnahmen ein mächtiges Werkzeug.

Viele empfohlene sicherheitsbezogene Einstellungen lassen sich durch GPOs einfach implementieren und verteilen.

Die aus Sicht des Autors wichtigsten Maßnahmen, die so umgesetzt werden können, sind:

- UAC (User Access Control, Benutzerkontensteuerung);
- LDAP-Signierung;
- SMB-Signierung;
- SChannel-Signierung (Secure Channel, sicherer Kanal);
- das Ausschalten alter und entsprechend unsicherer Authentisierungs- oder Übertragungsprotokolle;
- Einstellungen zu Log-Größen;
- Einsatz von NLA (Network Level Authentication, Authentifizierung auf Netzwerkebene) bei Remote-Desktop-Verbindungen;
- das Einrichten von PowerShell-Logging (siehe ix.de/z2py; über diesen Link sind alle im Folgenden erwähnten Artikel, Blogbeiträge, Hilfestellungen etc. zu finden);
- das Verhindern des Hinzufügens neuer Computer zum AD durch beliebige Domänenbenutzer.

Diese GPO-Einstellungen, die einen eigenen Artikel füllen könnten, wurden vom Autor in einem Blogbeitrag ausführlich beschrieben (ix.de/z2py).

Im Internet gibt es verschiedene Ressourcen, die Einstellungen empfehlen oder fertige Policies bereitstellen. Bekannte Vertreter sind die Microsoft Windows Security Baselines oder die Benchmarks des Center for Internet Security (CIS). Bei Microsoft können Interessierte die Empfehlungen als fertige GPOs herunterladen. Das CIS veröffentlicht Benchmarks für unterschiedliche Systeme, die auf seiner Webseite kostenlos als PDF erhältlich sind.

Für Windows Server, Clients und Software beschreiben die CIS-Benchmarks, welche Einstellungen in den GPOs aus welchen Gründen mit welchen Werten ausgestattet werden sollten. Sie unterteilen die einzelnen Empfehlungen in zwei Level: Level 1 kann meist ohne negative Auswirkung auf den Betrieb verteilt werden. Bei Level 2 hingegen sollte man gut überlegen, ob das Ändern eines Werts nicht zu unerwünschten Nebeneffekten führt. Abwägen und Testen sind beim Härten immer gute Strategien: Wer denkt, man könne die GPOs von Microsoft ungetestet und ohne Bedenken produktiv im Unternehmen anwenden, wird meist schnell zurück auf Start gehen, da die Wahrscheinlichkeit groß ist, dass irgendetwas nicht mehr richtig läuft.

Quelle: CIS Password Policy Guide

| Passwortlänge | mögliche Kombinationen | Zeit in Stunden |
|---|---|---|
| 6 | 782 757 789 696 | 0,002 |
| 7 | 75 144 747 810 816 | 0,21 |
| 8 | 7 213 895 789 838 340 | 20,04 |
| 9 | 692 533 995 824 480 000 | 1923,71 |
| 10 | 66 483 263 599 150 100 000 | 184 675,73 |

**Passwortlänge in Relation zur Zeit, die bei Brute Force zum Herausfinden des Passworts benötigt wird (Abb. 1).**

Wenn sinnvolle Einstellungen per GPO verteilt werden, kann das die individuelle Angriffsfläche der einzelnen Systeme und somit der gesamten Infrastruktur verringern. Gerade dann, wenn sich ein Angreifer bereits im Netzwerk einnisten konnte, können solche Maßnahmen ihn oder die Schadsoftware in ihrem Tun behindern. Im Zusammenspiel mit einigen nachfolgend beschriebenen Maßnahmen kann zum Beispiel die Ausbreitung im Netzwerk oder der Angriff auf zentrale, wichtige Systeme effektiv unterbunden werden.

## Updates einspielen

Eine der wichtigsten und sinnvollsten Maßnahmen allgemein beim Härten ist das zeitnahe Einspielen von Sicherheitsupdates. Dabei sind interne Systeme wie ein DC nicht weniger zu berücksichtigen als exponierte Systeme. Für das Eindringen in Netzwerke bevorzugen Angreifer zwar meist eine einfachere Art als das mühsame Ausnutzen komplizierter Sicherheitslücken, nämlich das Social Engineering, zum Beispiel per E-Mail, oder das Verwenden gestohlener oder schwacher Passwörter im Zusammenhang mit Remote-Zugängen (oft RDP).

Sollte sich ein Angreifer jedoch im Netzwerk befinden, können interne Systeme ohne aktuelle Updates ihm eine Privilege Escalation (Rechteausweitung) oder Lateral Movement (seitliche Bewegung, die weitere Ausbreitung im Netzwerk) ermöglichen [10]. Daher sollten Updates regelmäßig geplant und eingespielt werden. Es können verschiedene Strategien für das Ausrollen entwickelt und verfolgt werden. So kann man etwa Testsysteme und weniger wichtige Zonen etwas früher mit den Aktualisierungen versorgen, um zu sehen, ob die Patches unerwünschte Nebenwirkungen mit sich bringen. Bei kritischen Sicherheitsupdates sollten betroffene Systeme möglichst bald auf einen aktuellen Stand gebracht werden.

In Microsoft-Umgebungen können Einstellungen zu Updates per GPO ausgerollt und zum Beispiel per Windows Server Update Service (WSUS) oder System Center Configuration Manager (SCCM) freigegeben und verteilt werden. Kleinere Netzwerke ohne WSUS können gut verschiedene Segmente der Server und Clients mit unterschiedlichen Update-Präferenzen per GPO ausstatten, sodass die Updates zeitlich etwas verteilt auf den Geräten und Servern ankommen. So sind im Falle eines fehlerverursachenden Updates nicht alle Benutzer und Dienste gleichzeitig betroffen. Sind wichtige Systeme wie der Domänencontroller redundant ausgelegt, wiegt ein Ausfall eines Servers durch ein Update in der Regel nicht schwer.

Härtung sowie Updates sind sehr wichtig, bringen jedoch wenig, wenn man einem Angreifer die entsprechenden Zugangsdaten frei Haus liefert.

## Ungenutzte und alte Protokolle abschalten

In den meisten Windows-Umgebungen laufen noch alte oder nicht benötigte Protokolle, insbesondere LLMNR (Link-Local Multicast Name Resolution), NetBIOS und WPAD (Web Proxy Autodiscovery).

LLMNR ist ein Protokoll zur Namensauflösung in Ad-hoc-Netzwerken, bei denen kein DNS-Server zum Einsatz kommt.

### iX-TRACT

- Der Umgang mit Passwörtern wird vielerorts noch immer unterschätzt – das trifft beim Active Directory genauso zu wie in der restlichen IT-Welt. Auch das Abschalten ungenutzter Protokolle ist nicht weit genug verbreitet.
- Gerade bei privilegierten Benutzern helfen starke Passwörter und deren sichere Verwahrung gegen viele Angriffe, insbesondere gegen die Rechteausweitung.
- Das Härten per Group Policy deckt zahlreiche Protokolle und Einstellungen zentral ab – wenn man es nutzt.

**Empfehlungen für eine Passwort-Policy**

| Einstellung | Wert |
|---|---|
| Passwortlänge (min.) | **mit MFA:** 10*;<br>**ohne MFA:** 14 |
| Komplexität | **mit MFA:** keine;<br>**ohne MFA:** mindestens ein Zeichen, das nicht dem Alphabet zugehört (in der Domäne Komplexität auf „aktiviert“ stellen) |
| Passwortalter (max.) | Unbeschränkt, wird aufgrund von Ereignissen sofort geändert. Ereignisse können z. B. Policy-Änderungen oder Sicherheitsvorfälle sein. |
| Passwortalter (min.) | >= 1 Tag |
| Kennwortchronik vorangegangener Passwörter | >= 5 |
| Kontosperrschwelle | fünf Fehlversuche |
| Kontosperrdauer | >= 15 Minuten |
| Bildschirmsperre | <= 15 Minuten |

* von CIS-Richtlinie abweichende Empfehlung

Anfragen per LLMNR werden an das ganze Netzwerk versendet, die Antworten darauf werden nicht auf Authentizität überprüft. Angreifer können diesen Mechanismus ausnutzen, indem sie solche Abfragen abhören und Antworten fälschen – und so das Opfer dazu bringen, bösartigen Servern zu vertrauen. Um LLMNR zu deaktivieren, muss in der Gruppenrichtlinie „Multicastnamensauflösung deaktivieren“ auf „aktiviert“ gesetzt werden. Pfad: „Computerkonfiguration\Administrative Vorlagen\Netzwerk\DNS-Client“.

NetBIOS zu deaktivieren ist schwieriger. Es muss auf jedem Netzwerkadapter separat eingestellt werden. Kommen neue hinzu, ist darauf NetBIOS wieder aktiv. Eine einfache Lösung ist das Unterbinden von NetBIOS per Firewall. Kommunikation auf den Ports TCP/137-139 kann, wenn NetBIOS nicht verwendet wird, blockiert werden. Das Angriffsszenario per NetBIOS wurde in [1] beschrieben.

## „Man in the Middle“ vermeiden

WPAD ist ein Protokoll zur automatischen Proxykonfiguration. Es kann je nach Netzwerk Man-in-the-Middle-Attacken (MITM) begünstigen. Auf Servern, die in der Regel in statischen Netzwerken installiert werden, kann der Proxy fix konfiguriert und WPAD abgeschaltet werden. Auf Clients lässt sich WPAD ebenfalls deaktivieren, wenn es nicht benötigt wird. Man geht dazu folgendermaßen vor: In den Einstellungen von Windows muss bei der Konfiguration des Proxys „Einstellungen automatisch erkennen“ auf „aus“ gestellt werden. Zudem muss der folgende Registry-Schlüssel gesetzt werden: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinHttpAutoProxySvc; Wert von „Start“ von 3 (manuell) auf 4 (deaktiviert) umstellen.

Wie man mit alten Authentifizierungsprotokollen verfährt, beschreibt der oben erwähnte Blogartikel zu den GPO-Einstellungen. Sollte im Unternehmen nur IPv4 verwendet werden, lässt sich IPv6 unter Windows deaktivieren (siehe ix.de/z2py) oder per Firewall blockieren. Das verhindert das Ausnutzen von IPv6 [6].

Schließlich wird allgemein empfohlen, ungenutzte Dienste zu deaktivieren. Microsoft pflegt eine Liste für Windows Server, die beschreibt, welche Dienste man grundsätzlich ohne Probleme abschalten kann (siehe ix.de/z2py). Zum Beispiel sollte der Druckerspooler auf dem Domänencontroller deaktiviert werden, da sonst Angriffe wie der „Printer Bug“ [6] möglich sind.

## Passwörter und Berechtigungen

In den meisten Domänen wird nach wie vor ein Passwort zur Authentisierung der Benutzer verwendet. In Organisationen, in denen Smartcards eingesetzt werden, laufen trotzdem viele Dienste mit einem Service Account, für den es ein Passwort gibt. Oft haben auch Administratoren ein Passwort als Alternative, um sich remote zum Beispiel per PowerShell anmelden zu können. Neue Verfahren wie FIDO2 sind vor allem im Web auf dem (langsamen) Vormarsch. An vielen Stellen wird leider noch immer auf einen zweiten Faktor beim Log-in verzichtet.

Ein Schritt in Richtung starke Passwörter ist die Passwort-Policy. Sie wird per GPO verteilt und ist dort unter „Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Kontorichtlinien“ zu finden. Bezüglich der optimalen Werte gibt es unterschiedliche Ansätze. Werden mehrere Wörter und ganze Sätze als Passwort eingesetzt, spricht man von Passphrasen. Sie erreichen die Sicherheit über die Länge und müssen daher nicht extra komplex gehalten werden. Für Passphrasen gibt es außerdem erst wenige Listen und Ressourcen, die ein Knacken durch Ausprobieren (Brute Force) vereinfachen.

Lange Passphrasen verhindern Attacken wie Passwort-Spraying [4] und das Offline-Brechen, etwa bei Kerberoasting [5], effektiv – solange für sie nicht das Lieblingszitat verwendet wird, das auf Facebook großzügig geteilt wurde. Ein weiterer Vorteil von Wörtern und Sätzen ist das leichtere Auswendiglernen. Passwörter wie „DXm:-ECa+weR“ lassen sich offensichtlich weniger gut einprägen als „schnell Segen ihren Münze“. Beides wären jedoch gute Passwörter, wenn sie nicht in diesem Heft stehen würden.

## Technische Maßnahmen plus Sensibilisierung

Passphrasen lassen sich in der klassischen Domäne leider mehr schlecht als recht technisch implementieren. Theoretisch könnte man die minimale Passwortlänge auf 25 stellen und dafür die erforderliche Komplexität minimieren – empfohlen wird dies jedoch nicht. Besser ist eine Policy, die auf Passwörter ausgelegt ist, und zusätzlich das Schulen und Sensibilisieren der Benutzer.

Die per GPO forcierte Länge und Komplexität der Passwörter orientiert sich grundsätzlich an der Brute-Force-Geschwindigkeit: Je nach Länge des Passworts sowie der Anzahl der zur Verfügung stehenden Zeichen dauert es unterschiedlich lange, bis die Angreiferin alle möglichen Kombinationen durchprobiert hat. Abbildung 1 zeigt, in welcher Zeit ein gut ausgestatteter Hacker Passwörter verschiedener Länge mit einer Basis von 96 Zeichen durchprobieren kann. In der Realität werden neben dem einfachen Durchprobieren weitere Strategien angewandt, um schneller mehr Passwörter zu knacken. So werden etwa bekannte Muster berücksichtigt, infrage kommende Wörter priorisiert oder Passwortsammlungen aus anderen Hacks durchprobiert.

Ein Passwort mit neun Zeichen lässt sich in maximal 1923 Stunden durch reines Durchprobieren herausfinden (siehe Abbildung 1). Daher lautet die Empfehlung für die Länge: mindestens zehn Zeichen für normale Benutzer, zwölf für Administratoren oder Benutzer mit besonderen Berechtigungen. Für Dienstkonten sollte man lange und automatisch generierte Passwörter vergeben, da diese ohnehin in einem Passwortmanager gespeichert werden sollten.

Die Tabelle „Empfehlungen für eine Passwort-Policy“ enthält sinnvolle Vorgaben für eine Passwortrichtlinie. Die Einstellungen stammen aus dem CIS Password Policy Guide (siehe ix.de/z2py). Je nachdem, ob weitere Schutzmechanismen wie MFA oder 2FA (Multi-Factor/Second-Factor Authentication) eingesetzt werden, weichen die Werte etwas voneinander ab.

Die beste Passwort-Policy nützt allerdings nicht viel, wenn die Benutzer einfach zu erratende Passwörter verwenden oder einen Notizzettel an den Bildschirm oder unter die Tastatur kleben.

## In der Stärke liegt Sicherheit

Um starke Passwörter zu generieren, zu verwenden und zu speichern, eignen sich Passwortmanager. Sie helfen, für jeden Dienst ein anderes Passwort einzusetzen und es nicht zu vergessen. Die Manager enthalten meist einen Generator zum Erstellen neuer Passwörter. Da man sich das Passwort sowieso nicht merken muss, kann es auch komplett zufällig erzeugt werden. Der Generator sollte entsprechend eingestellt sein.

Oft lassen sich unterschiedliche Profile für das Generieren von Passwörtern definieren. Muss man Passwörter gelegentlich abtippen, kann für solche Fälle ein Profil mit tippbaren Zeichen erstellt werden. Bei Admins und Powerusern ist das häufig erforderlich, wenn sie mit virtuellen Maschinen oder remote arbeiten und Copy-and-Paste zum Teil nicht funktioniert.

Die Benutzerinnen und Benutzer müssen jedoch erst gewisse Hürden überspringen, um an die im Manager gespeicherten Passwörter heranzukommen. Dazu gehört mindestens das Log-in am Computer sowie das Masterkennwort des Passwortmanagers. Zudem können weitere Passwörter und PINs hinzukommen, wenn beispielsweise beim Booten des Gerätes die Eingabe der PIN für die Festplattenverschlüsselung BitLocker erforderlich ist.

Eine mögliche Lösung wäre, den Manager auch auf Mobilgeräten einzusetzen, wenn das Unternehmen es erlaubt. Man darf allerdings nicht erwarten, dass jeder Benutzer auf seinem (privaten) Mobiltelefon die entsprechende App nutzt. Um ihn dazu zu bringen, starke Passwörter zu verwenden und sich ein paar davon zu merken, sind Schulungen nötig. Wer nicht versteht, warum Passwörter wichtig sind, wird kein starkes Passwort verwenden. Auch der Umgang mit einem Passwortmanager will gelernt sein.

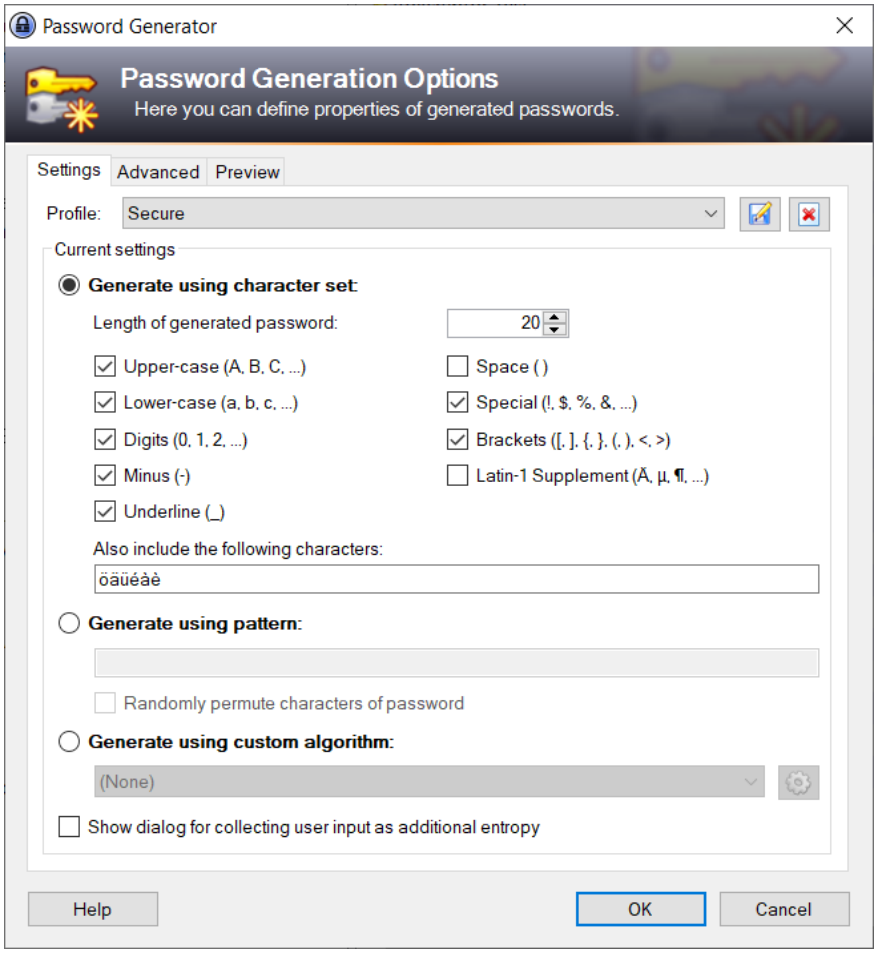
Die Zugangsdaten für Dienstkonten sollten ebenfalls in einem Passwortmanager gespeichert werden, auf den nur die berechtigten Admins Zugriff haben. Zugangsdaten für Dienstkonten werden oft einmal konfiguriert und dann nur in speziellen Fällen wieder benötigt. In der Regel ist ein Abtippen der Zeichen nicht erforderlich. Die Passwörter für Dienste dürfen daher gerne ausreichend lang und komplex sein. Im Normalfall werden keine weiteren Schutzmaßnahmen wie ein zweiter Faktor verwendet – ein weiterer Grund, lange Passwörter zu wählen. Auch bei Dienstkonten gilt: Für jedes Konto ein anderes Passwort.

## Konto mit definierten Befugnissen

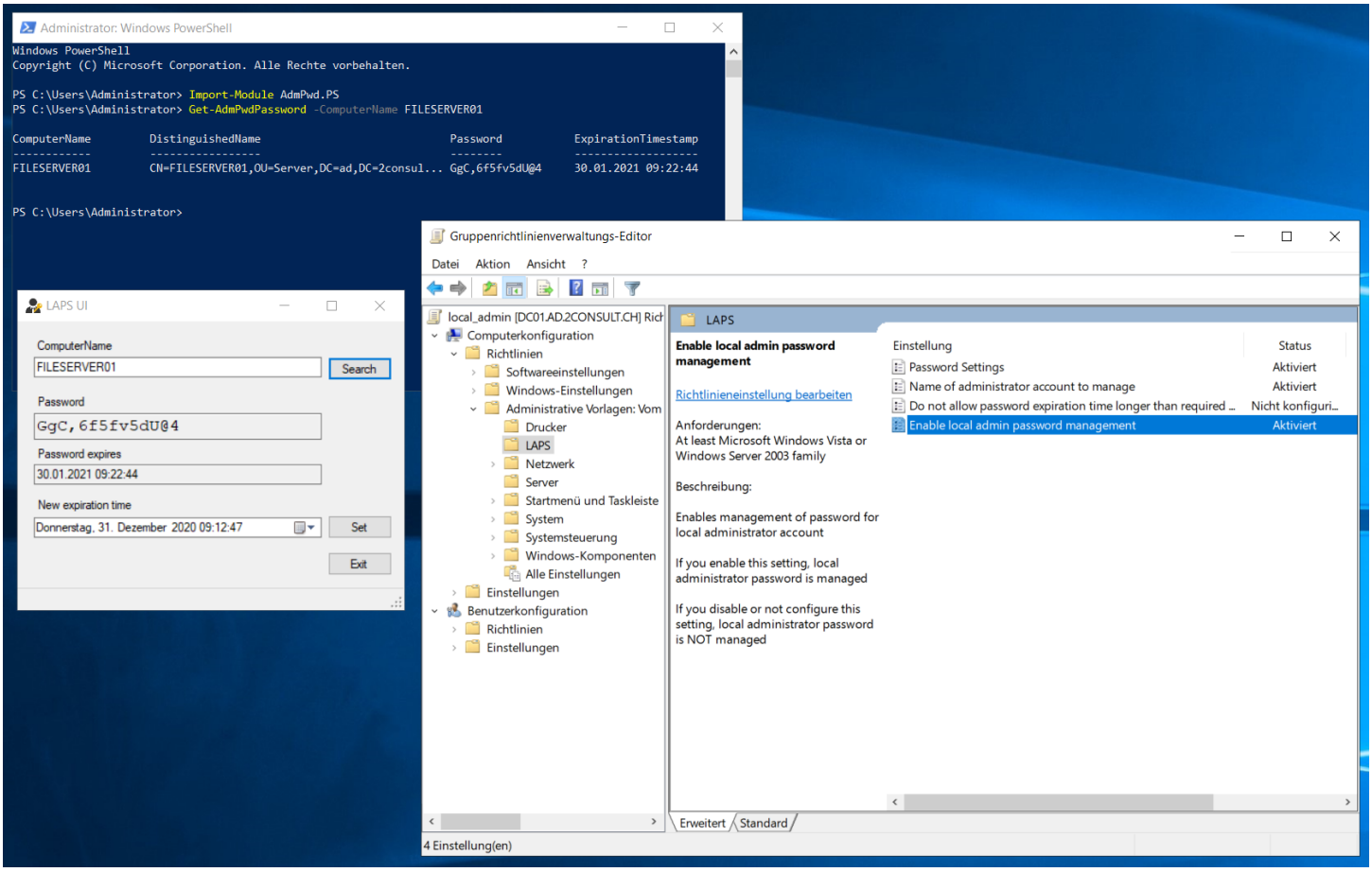
Eine noch bessere Technik sind Group Managed Service Accounts (gMSA, gruppenverwaltete Dienstkonten). Dabei wird das Passwort des Dienstkontos mit dem Domänencontroller ausgehandelt. Daher muss auch kein Admin das Passwort generieren, sehen oder einpflegen. Ein weiterer Vorteil liegt darin, dass gMSA-Konten sich nicht an Systemen anmelden können. Außerdem wird beim Erstellen eines solchen Kontos genau definiert, welche Gruppe oder welcher Account den Dienstbenutzer verwenden darf. Bei Diensten, die auf einem einzelnen Server laufen, wäre dies dann der Computer-Account des Servers.

Um bei lokalen Administratorenkonten unterschiedliche und starke Passwörter einzusetzen, kann LAPS von Microsoft helfen ([11]; siehe ix.de/z2py). LAPS steht für Local Admin Passwort Solution (Passwortlösung für lokale Administratoren) und unterstützt dabei, auf einfachem, aber sicherem Weg die lokalen Passwörter zu generieren und zu verwalten. Dazu muss man die Verwaltungskomponente sowie die GPO-Erweiterung von LAPS auf dem Domänencontroller installieren und die Clienterweiterung auf den Servern und Geräten.

Per GPO kann jetzt ein auf dem Client lokal bereits vorhandenes Administratorenkonto zur Verwaltung angegeben werden. Entsprechend den gesetzten Regeln wird der Client für dieses Konto ein neues Passwort generieren und in das Feld




**Bei Passwortgeneratoren – hier ein Modell von KeePass – kann man verschiedene Profile anlegen und einstellen, welche Zeichen benutzt werden sollen (Abb. 2).**




**Mit LAPS lassen sich etliche der üblichen Probleme des Passwortmanagements vermeiden (Abb. 3).**

`ms-Mcs-AdmPwd` des Computerobjekts im Active Directory schreiben. Das Spezielle daran ist, dass der Client dieses Feld nur schreiben darf, nicht lesen. Nur Domänenadmins sind dazu berechtigt, es auszulesen. Das geht am einfachsten mit PowerShell.

Mit LAPS lassen sich die lokalen Passwörter regelmäßig oder auf Befehl hin ändern. Daher eignen sich die lokalen Konten auch für den Support. Ein solches Kennwort kann sogar an versierte Nutzer abgegeben werden. Sind sie mit der Aufgabe fertig, kann auf dem Domänencontroller per PowerShell der Befehl zum Ändern des entsprechenden Passworts gegeben werden, woraufhin der Client bei der nächsten Gruppenrichtliniensynchronisation ein neues Passwort generiert und in das Feld in seinem Objekt auf dem DC schreibt.

## Vorsicht beim Erzeugen von Passwörtern

Gruppenrichtlinieneinstellungen (Group Policy Preferences, GPP) wurden ausführlich in [3] behandelt. Oft werden über sie lokale Administratorenkonten angelegt. Das hat zwei Nachteile: Erstens können Angreifer alle Passwörter, die in den GPO oder GPP vorhanden sind, auslesen. Zweitens haben mit dieser Methode zwangsläufig mehrere, wenn nicht alle Clients und Server den gleichen Benutzer mit gleichem Passwort installiert. LAPS kann dies einfach und effektiv verhindern. 2014 hat Microsoft das Speichern von Passwörtern in den Gruppenrichtlinieneinstellungen mit einem Update deaktiviert. Bestehende GPP-Einstellungen inklusive der Passwörter blieben aber funktionstüchtig, um die jeweiligen Organisationen nicht lahmzulegen.

Bei Skripten gilt dasselbe: Soll ein Skript als Beispiel mit Adminrechten auf allen Clients eine Operation vornehmen, ist es eine schlechte Idee, in diesem Skript Benutzername und Passwort eines Domänenadmins zu hinterlegen und es für alle lesbar auf einer Dateifreigabe abzulegen. Ein Angreifer dürfte diese Zugangsdaten finden und zu verwenden wissen. Besser wäre, das Skript mithilfe einer geplanten Aufgabe als LOCAL\System ausführen zu lassen. Per GPP konfiguriert, benötigt es kein Passwort und wird nur mit lokalen Berechtigungen ausgeführt.

Um vor Passwortverlust, Anwenderfehlern und schwachen Passwörtern sicher zu sein, kann der Einsatz eines weiteren Faktors zusätzlich zum Passwort sinnvoll sein.

## Authentifizierung: Mehr ist mehr

Für Log-ins kann man heute relativ einfach mehrere, mindestens aber zwei Faktoren einbeziehen (MFA, Multi Factor Authentication, beziehungsweise 2FA). Üblicherweise unterscheidet man die Faktoren nach Wissen (Passwort, PIN), Besitz (Token, Handy, Einmalpasswortgenerator) und Biometrie (Merkmale des Benutzers wie Fingerabdrücke). Anbieter solcher Produkte gibt es viele. Naheliegend ist das Nutzen von Microsofts Mehr-Faktor-Authentifizierung, gerade wenn Cloud-Produkte des Anbieters in einem Unternehmen zumindest stellenweise zum Einsatz kommen. Aber auch andere Produkte, etwa Cisco DUO, lassen sich mit den unterschiedlichsten Diensten einrichten und unterstützen ebenfalls Cloud-Anwendungen.

Einen zweiten Faktor für externe Zugriffe einzusetzen, beispielsweise für das VPN, ist sinnvoll, da auch die stärksten

Passwörter verloren gehen können – sei es durch einen menschlichen Fehler oder durch technisches Versagen. Außerdem kann man sich nicht darauf verlassen, dass alle Benutzer einen guten Umgang mit Passwörtern pflegen. Ein zweiter Faktor schafft da Abhilfe. Ein Angreifer müsste, wenn er ein Passwort ergattert hat, auch den zweiten Faktor kontrollieren oder herausfinden. Er ist durchaus auch angreifbar – SMS können abgefangen, Benutzer per Phishing zur Eingabe gebracht oder Handys gehackt werden. Es ist jedoch um einiges aufwendiger, als lediglich ein gestohlenes Passwort einzutippen.

Ein zweiter Faktor macht neben externen Zugängen auch bei hoch privilegierten Benutzerkonten oder schützenswerten Systemen eine gute Figur. So können zum Beispiel die Domänenadmins bei jedem Verbindungsaufbau einen zweiten Faktor verwenden oder alle Benutzer beim Zugriff auf sensible Systeme. Allerdings lassen einige Protokolle keinen zweiten Faktor zu, etwa PowerShell Remoting oder SMB (Server Message Block). Während RDP nach einem zweiten Faktor fragt, benötigt man für die genannten Protokolle nur das Passwort oder wird per Single Sign-on angemeldet. Zudem kennen MFA-Produkte selbst eine unterschiedliche Anzahl an Protokollen.

Schützenswerte Systeme sollten daher mit einer Firewall gesichert werden, damit Protokolle ohne zweiten Faktor nicht generell, sondern nur von den erforderlichen Orten aus erreichbar sind. Wie der kommende Artikel zeigt, kommt es dabei auf die Netzwerksegmentierung sowie auf die Beschränkung der Berechtigungen an. Sind Admins an ihren Arbeitsgeräten mit dem Domänenadmin-Konto angemeldet und erreichen von dort aus alle Server auf allen Ports, ist es für einen Angreifer viel einfacher, Beschränkungen wie einen zweiten Faktor zu umgehen.

## Altbekannte Gegenmaßnahmen

Die bei der Absicherung eines Systems relevanten Themen sind bekannt: magische GPO-Einstellungen, Updates und Passwörter. Doch die Erfahrung zeigt, dass sie immer noch zu wenig berücksichtigt werden. Viele Angriffe, vor allem die Rechteausweitung, machen sich diesen Umstand zunutze. Passwörter werden gestohlen, ausgespäht, erraten, geknackt oder umgangen, Sicherheitslücken ausgenutzt, und fehlende Härtung per Richtlinie erlaubt unter anderem das einfachere Einnehmen anderer Ziele im Netzwerk. Dabei kann man mit den beschriebenen Maßnahmen den Missbrauch eindämmen oder gar verhindern. Der kommende Artikel stellt weitere Maßnahmen vor und beschreibt, wie mit einem Angriff auf die eigene Infrastruktur Lücken aufgedeckt werden können. (ur@ix.de)

### Quellen


[1] Frank Ully; Himmelsgeschenk; Active Directory: Komfortable IT-Schaltzentrale mit Schwachpunkten; *iX* 10/2020, S. 40

[2] Frank Ully; Allgegenwärtig; Der Verzeichnisdienst Active Directory: einer für alle(s); *iX* 10/2020, S. 48

[3] Frank Ully; Nach oben gehangelt; Informationsbeschaffung – was jeder Domänenbenutzer alles sieht; *iX* 10/2020, S. 58

[4] Frank Ully; Fette Beute; Passwörter und Hashes – wie Angreifer die Domäne kompromittieren; *iX* 11/2020, S. 94

[5] Frank Ully; Frisch geröstet; Roasting, Rechte, Richtlinien: Wie Angreifer sich im Active Directory Zugriff verschaffen; *iX* 12/2020, S. 92

[6] Frank Ully; Vertrauensfrage; Active Directory: Wie Angreifer Tickets, Delegierung und Trusts missbrauchen; *iX* 2/2021, S. 116

[7] Yves Kraft, Frank Ully; Zwischen den Wäldern; Inter-Forest und Persistenz: Wie Angreifer sich über einen AD-Forest hinaus ausbreiten und festsetzen; *iX* 4/2021, S. 102

[8] Lukas Grunwald; Profi-Attacke; Die schleichende Gefahr: Advanced Persistent Threats; *iX* 7/2012, S. 42

[9] Martin Wundram, Alexander Sigel; Aus Fehlern lernen; Organisatorische und technische Maßnahmen zum IT-Selbstschutz; *iX* 2/2021, S. 48

[10] Sascha Herzog; Seitwärtsbewegungen; Red Teaming: Post Exploitation und Lateral Movement; *iX* 12/2018, S. 82

[11] Jan Mahn; Passwort-Auswürfler; Lokale Admin-Passwörter in der Windows-Domäne verwalten; c't 14/2019, S. 158

[12] Details zu den hier vorgestellten Maßnahmen, Blogartikel und Hilfestellungen sind über ix.de/z2py zu finden.



**Marco Wohler**

ist System Engineer bei der Oneconsult AG. Als Gegenpart zu den Penetration-Testing-Teams ist er spezialisiert auf die Absicherung von IT-Systemen.