SO SETZEN SIE STARKE PASSWORTRICHTLINIEN IN ACTIVE DIRECTORY UM

Ein Leitfaden für die Einführung einer modernen und starken Kennwortrichtlinie in Ihrer Organisation

A SPECOPS WHITEPAPER

SPECOPS
AN OUTPOST24 COMPANY

INHALTSÜBERSICHT

INTRODUCTION

Gründe für die Einführung einer neuen Passwortrichtlinie

DARREN JAMES
Senior Product Manager

Die Erstellung und Einführung einer neuen Kennwortrichtlinie für ein ganzes Unternehmen kann einem wie eine monumentale Aufgabe erscheinen. Und wenn man erst einmal angefangen hat, gibt es überraschend viel zu bedenken. Da stellt sich einem doch ab und zu die Frage: Lohnt sich der Aufwand wirklich? Falls Ihre derzeitige Kennwortrichtlinie Sicherheitslücken und Schwachstellen aufweist oder aktuellen Compliance-Anforderungen nicht genügt, lautet die Antwort mit ziemlicher Sicherheit ja. Denn eine schwache oder wirkungslose Passwortrichtlinie ist einfach zu gefährlich.

Kompromittierte Zugangsdaten sind weiterhin der einfachste Weg für Cyberkriminelle, um in ein Unternehmen einzudringen. Laut dem Data Breach Investigations Report 2024 von Verizon waren gestohlene Zugangsdaten bei 24 % aller Datenschutzverletzungen der erfolgreiche Angriffsvektor. Dieser Anteil steigt bei der Analyse von Angriffen auf SaaS-Anwendungen sogar auf 77 %. Für Cyberkriminelle stehen Passwörter weiterhin ganz klar im Vordergrund, aber dies gilt nicht unbedingt für Ihre Nutzer. Specops' 2024 Breached Password Report fand heraus, dass „123456“ das am häufigsten von Malware gestohlene Passwort war - es ist also klar, dass viele Unternehmen es zulassen, dass Anwender solch schwache Passwörter vergeben.

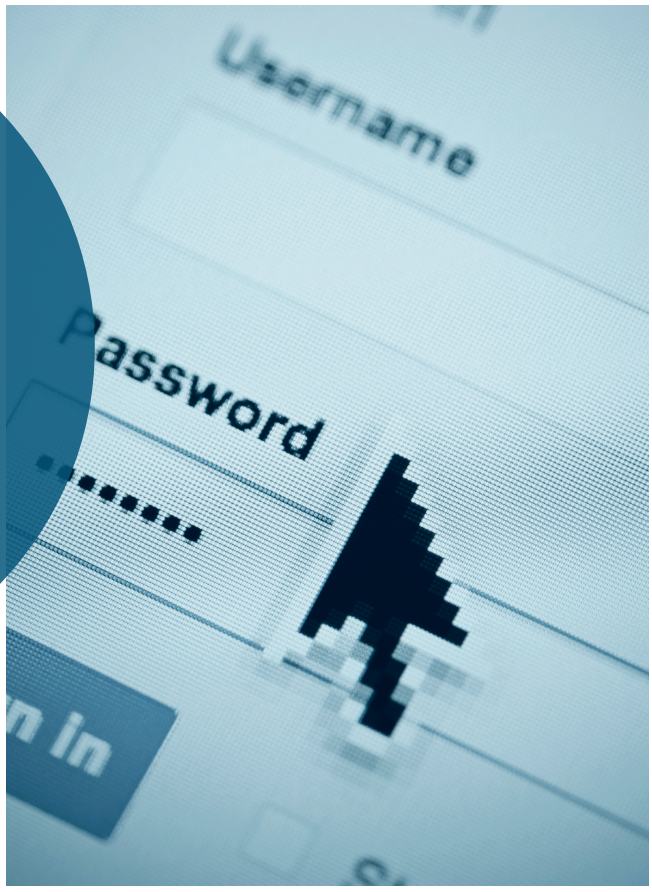
Unsere Analysen haben wiederholt gezeigt, dass Nutzer, wenn sie die Wahl haben, schwache, leicht zu erratende Passwörter erstellen. Auch wenn starke Passwörter gefordert werden, geben 59 % der User zu, dass sie ihre Passwörter auf mehreren Geräten und Konten wiederverwenden, obwohl sie sich des erhöhten Risikos bewusst sind, dass ihr Passwort dadurch kompromittiert werden könnte. Das führt dazu, dass vermeintlich sichere geschäftliche Passwörter durch schwache Sicherheitsvorkehrungen auf den privaten Geräten, Anwendungen oder Websites der Mitarbeiter kompromittiert werden können.

Passwörter sind eine der ersten Verteidigungslinien für Unternehmen, da sie noch ein nahezu universelles Mittel zur Authentifizierung von Benutzern für den Zugriff auf wichtige Konten und Daten darstellen. Ein Active Directory mit starken Passwörtern und einer Möglichkeit, deren Sicherheit zu gewährleisten, sollte daher nicht verhandelbar sein. Mit einer gut definierten Kennwortrichtlinie können Sie Best Practices und Empfehlungen zur Kennwortsicherheit umsetzen und gleichzeitig sicherstellen, dass Ihre Nutzer die Kennwortanforderungen und ihre eigene Verantwortung zum Schutz der Organisation vor Cyberangriffen verstehen.

Dieser Leitfaden soll den Prozess der Erstellung einer neuen und stärkeren Kennwortrichtlinie vereinfachen. Dafür haben wir Tipps von Experten, die auf jahrelanger Erfahrung beruhen, sowie praktische Beispiele zu den technischen Aspekten zusammengestellt. Außerdem erhalten Sie Zugang zu einem kostenlosen Auditing-Tool, das Sie in Ihrem eigenen Active Directory verwenden können, um zu prüfen, wie groß Ihr Handlungsbedarf ist.

Viel Erfolg bei der Umsetzung Ihrer neuen Kennwortrichtlinie!

Starke und sichere Passwörter sollten für ein Unternehmen selbstverständlich sein!



SECTION ONE

Planung der neuen Richtlinie

Jede Organisation ist anders, aber es gibt ein offensichtliches übergreifendes Ziel, das wir von jeder Active Directory Kennwortrichtlinie erwarten: Zugriffe auf das Unternehmensnetzwerk sollen vor schwachen, kompromittierten und leicht zu erratenden Kennwörtern geschützt werden. Daher kann man davon ausgehen, dass es je nach Organisation Unterschiede gibt, was eine „starke“ Richtlinie ausmacht. Die folgenden Fragen können Ihnen dabei helfen, Ihre Richtlinie so einzugrenzen, dass sie den spezifischen Sicherheitsanforderungen Ihrer Organisation gerecht wird.

Welche speziellen Anforderungen hat Ihr Unternehmen?

Leider gibt es keine "One-fits-All"-Richtlinie, weshalb der erste Schritt sein muss, die Ziele der neuen Kennwortrichtlinie festzulegen. Sie sollte zu den allgemeinen Aufgaben, Zielen und Philosophien Ihres Unternehmens in Bezug auf das Informationsrisikomanagement und die Geschäftsabwicklung in Ihrer Branche passen.

Berücksichtigen Sie auch, wozu Sie sich in Bezug auf Kunden- und Geschäftspartnerverträge, Gesetze und Vorschriften usw. bereits verpflichtet haben. Vergewissern Sie sich, dass alle richtlinienbezogenen Formulierungen in Ihrem Mitarbeiterhandbuch oder anderen Geschäftsunterlagen mit Ihren neuen formellen Kennwortrichtlinien übereinstimmen.

Denken Sie auch an Ihre eigenen internen Standards, die für angemessene Passwörter erforderlich sind. Befolgen Sie nicht blindlings Kennwortrichtlinien, wie z. B. die vordefinierten GPO-basierten oder Fine-Grained-Password Policies von Microsoft oder gar die Empfehlungen zum privaten Umgang mit Passwörtern des BSI. Finden Sie stattdessen heraus, was basierend auf den individuellen Anforderungen Ihrer Organisation wirklich erforderlich ist. Wahrscheinlich werden Sie feststellen, dass Sie Ihre Richtlinien feiner definieren müssen als ursprünglich angenommen.

Welche Vorgaben oder Richlinien müssen Sie einhalten?

Je nachdem, wo Ihr Unternehmen geografisch angesiedelt ist und in welcher Branche Sie tätig sind, gibt es möglicherweise spezielle Vorschriften, die Sie in Bezug auf Passwörter einhalten müssen. Wenn Sie sich nicht sicher sind, ist es wichtig, dass Sie sich von Anfang an über sämtlichen passwortbezogenen Vorschriften im Klaren sind. Nachfolgend finden Sie einige hilfreiche Ressourcen zur Einhaltung von Vorschriften, die jedoch nicht erschöpfend sind:

DACH

- **DSGVO:**
  - **“**Unter Berücksichtigung des Stands der Technik…treffen der Verantwortliche…geeignete TOMs, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten…“

- **NIS2:**
  - “…Unter dem Begriff „Cyberhygiene“…werden verschiedene grundlegenden Verfahren… umschrieben, welche…zu einer Verbesserung des Cybersicherheitsniveaus… führen können. Dies beinhaltet beispielsweise ein Patchmanagement, Regelungen für sichere Passwörter…”

- **DORA:**
  - “die Nutzung von Authentifizierungsmethoden ist der gemäß Artikel 8…dem Gesamtrisikoprofil der IKT-Assets angemessen und trägt führenden Praktiken Rechnung…”

- **Grundschutz und ISO2700x:**
  - **“**Passwörter, die leicht zu erraten sind oder in gängigen Passwortlisten geführt werden, DÜRFEN NICHT verwendet werden.“
  - **“**Es MÜSSEN Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen.“
  - IT-Systeme oder Anwendungen SOLLTEN NUR mit einem validen Grund zum Wechsel des Passworts auffordern.

Global

- **PCI DSS V4.0**

Wie dokumentieren Sie Ihre Passwortrichtlinie?

Bei Sicherheitsrichtlinien geht es darum, Erwartungen zu formulieren. Im Idealfall ist Ihre Richtlinie ein eigenständiges Dokument, das nicht in eine allgemeinere IT-Sicherheitsrichtlinie oder eine Richtlinie zur akzeptablen Nutzung eingebettet ist. Sie sollte den Zweck und den Geltungsbereich sowie die spezifischen Rollen und Zuständigkeiten klar darlegen (wenn möglich in einfacher Sprache). Das Dokument sollte auch technische Einzelheiten wie die Länge und Komplexität von Passwörtern und andere Anforderungen enthalten. Es sollte klar sein, für welche Systeme, Anwendungen, Benutzer, Abteilungen und Geräte die Richtlinie gilt und für welche nicht.

Zu den häufigen Versäumnissen gehört es, zu dokumentieren, wie die Einhaltung der Richtlinien überwacht wird, welche Sanktionen bei Verstößen verhängt werden und wie ein Verfahren zur laufenden Überprüfung/Bewertung aussieht. Vergewissern Sie sich, dass Sie jeden dieser Bereiche ansprechen und dass Ihr Sicherheitsausschuss und die betroffenen Benutzer mit den Erwartungen einverstanden sind. Lassen Sie den Entwurf der Richtlinie von Fachleuten überprüfen und aktualisieren Sie die Richtlinie bei Bedarf, bevor Sie sie der Führungsebene zur Genehmigung vorlegen. Es ist hilfreich, die Richtlinie von einem Anwalt, dem Risikomanagement und der Personalabteilung prüfen zu lassen.

Wie werden Sie die Richtlinie in Ihrem bestehenden Netzwerk umsetzen?

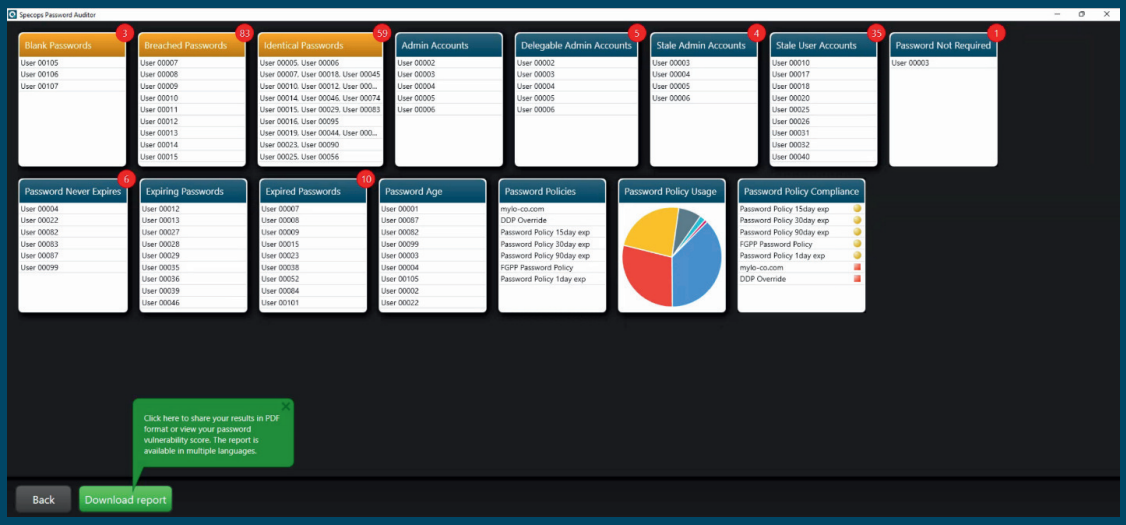
Sie sollten sich nicht der Annahme hingeben, dass Ihre Richtlinie ordnungsgemäß dokumentiert ist und somit auch einfach umzusetzen ist.

Papierkram ohne Plan zur Umsetzung ist lediglich ein guter Ratschlag. Es gibt Unternehmen, in denen eine wirkungsvolle Kennwortrichtlinie theoretisch vorhanden ist, aber die Realität ganz anders aussieht. Kurzum: Eine Passwortrichtlinie ist nutzlos, wenn sie nicht ordnungsgemäß verwaltet und umgesetzt werden kann - denken Sie also darüber nach, wie Sie Ihre geplante Richtlinie in die Tat umsetzen können.

SPECOPS TIPP

Starten Sie mit einer Bestandaufnahme Ihres Active Directories

Sie können nicht einfach beliebige Kennwortrichtlinien erstellen, ohne nicht vorher Ihre spezifischen authentifizierungsbezogenen Sicherheitsrisiken zu kennen. Machen Sie sich ein Bild davon, was in Ihrem Active Directory wirklich vor sich geht, und ermitteln Sie die tatsächlichen kennwortrelevanten Gefahren, denen Sie möglicherweise bereits ausgesetzt sind. Am besten fangen Sie mit einem Active Directory-Audit an.



Specops Password Auditor unterstützt Sie dabei mit einem kostenlosen Read-Only-Scan Ihres Active Directory und liefert Ihnen innerhalb von Minuten einen detaillierten und interaktiven Bericht über Ihre passwortrelevanten Schwachstellen. Darunter fallen Themen wie verwaiste Administratorkonten, inaktive Benutzer, die vergessen wurden, aktuelle Benutzer mit bereits kompromittierten Passwörtern, und vieles mehr.

Laden Sie sich hier den kostenlosen Passwort Auditor herunter.

SECTION TWO

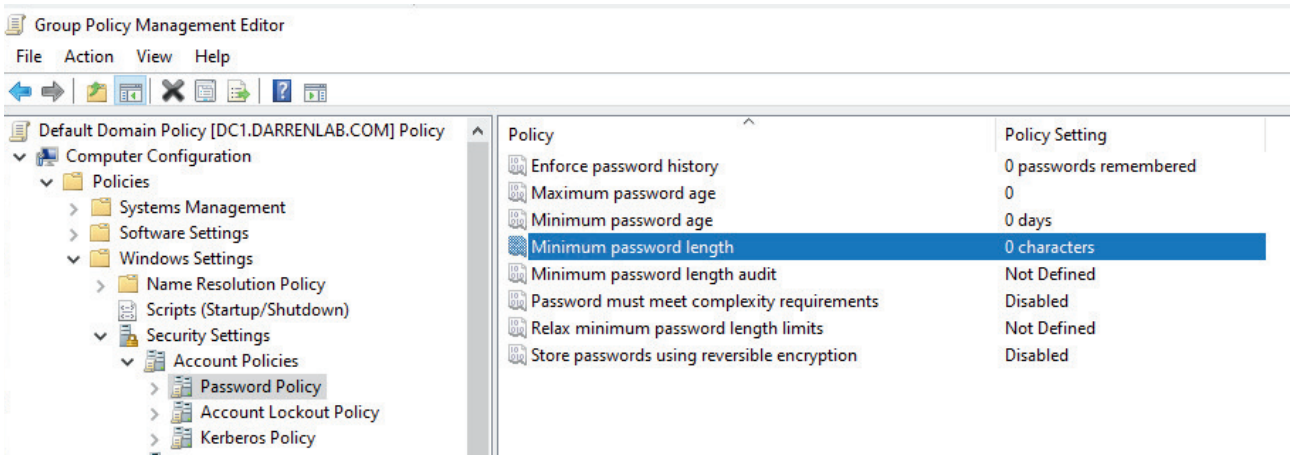
Die wichtigsten Bestandteile einer starken Kennwortrichtlinie

In diesem Abschnitt gehen wir einige der wichtigsten Dinge durch, die Sie in Ihrer Kennwortrichtlinie konfigurieren sollten, und zeigen Ihnen, wo Sie diese in Ihren Active Directory einstellen können. Darüber hinaus werden wir auch die jeweilige Einstellungsmöglichkeit in Specops Password Policy aufzeigen.

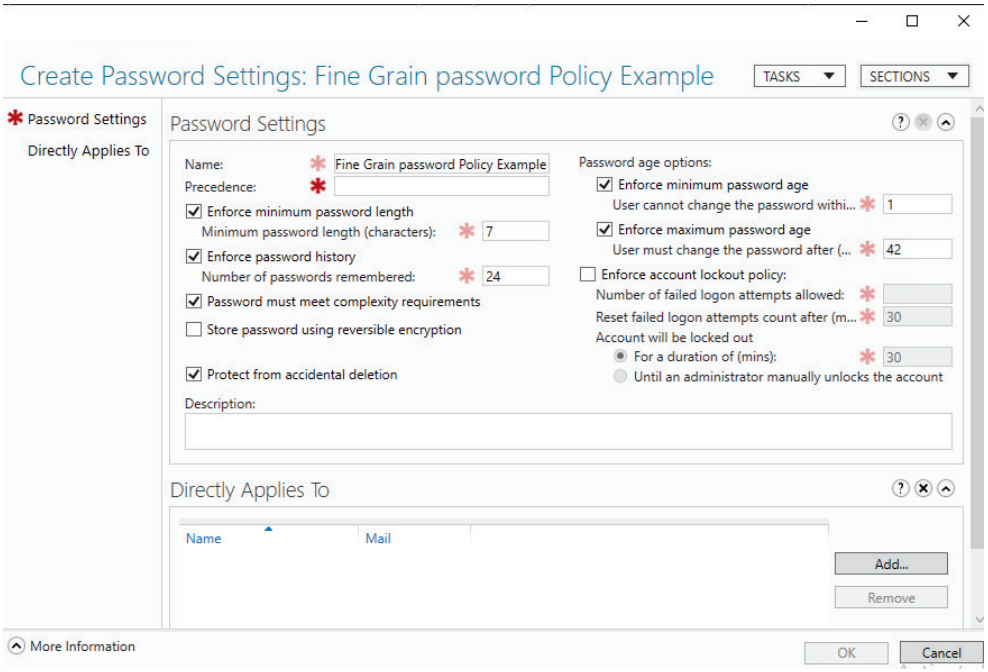
Passwordlänge

Das Erraten von längeren Passwörtern via Brute-Force dauert signifikant länger. Daher empfehlen wir, wo möglich, über die Standardlänge von acht Zeichen hinauszugehen - am besten sind Passwörter mit einer Länge von 15 Zeichen und mehr. Um diese Anforderungen benutzerfreundlicher zu gestalten, sollten Sie Ihre Nutzer zur Erstellung von Passphrasen ermutigen.

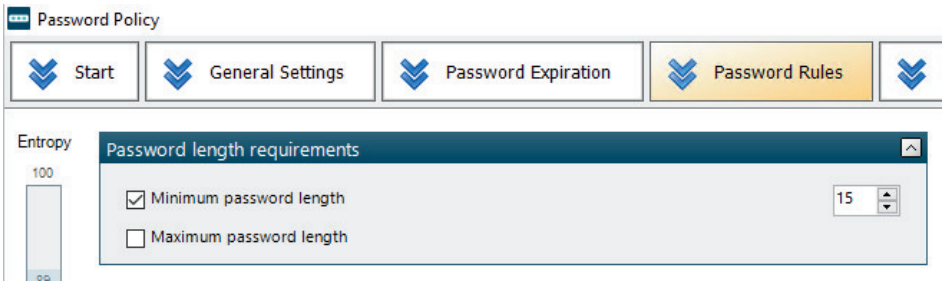
In Active Directory können Sie die Länge der Passwörter für alle Benutzer mithilfe der Gruppenrichtlinie festlegen:



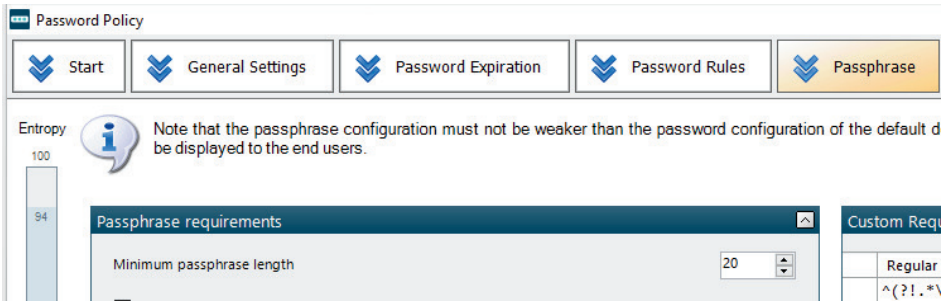
Wenn Sie für Untergruppen von Benutzern (die durch Sicherheitsgruppen definiert sind) unterschiedliche Längen festlegen möchten, können Sie Fine Grain Password Policy (FGPP) verwenden - diese wird über das Active Directory Administrative Center (ADAC) konfiguriert:



Hier können Sie die Passwortlänge in Specops Password Policy einstellen:



Oder wenn Sie eine eigene Richtlinie für Passphrasen umsetzen wollen, hier:



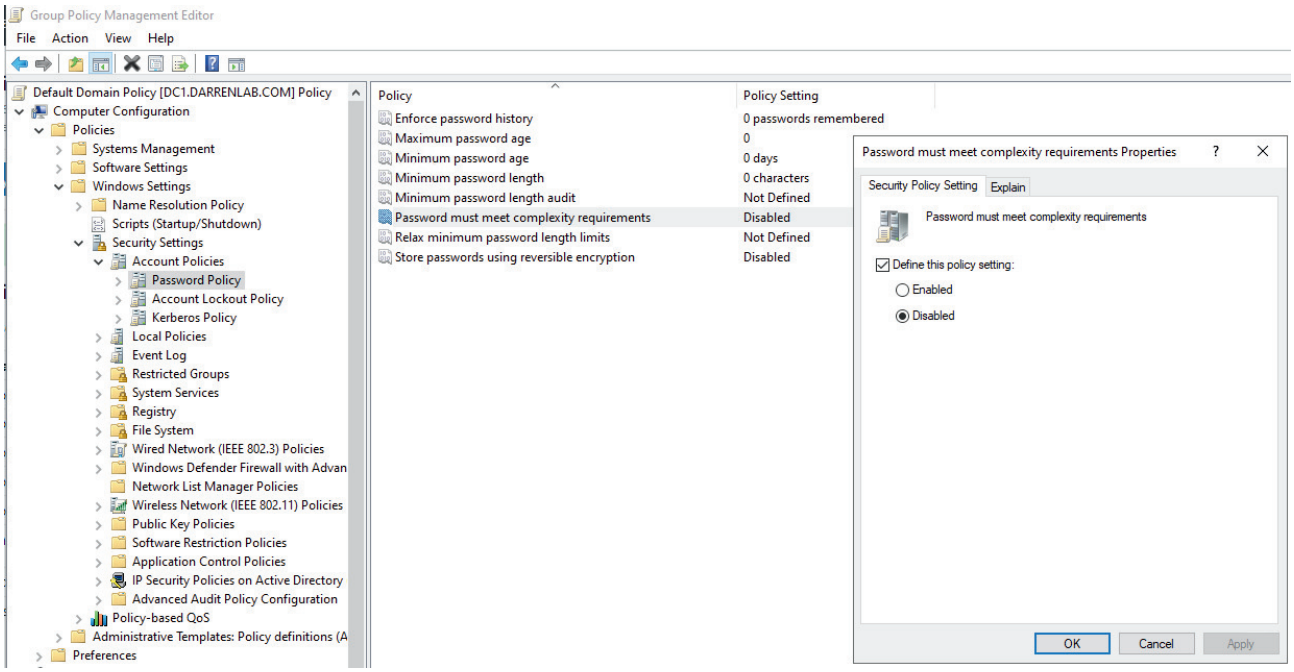
Komplexitätsanforderungen

Durch das Hinzufügen von Komplexitätsanforderungen werden die möglichen Zeichenkombinationen stark erhöht. Ein mit bcrypt-verschlüsseltes Kennwort mit 8 Zeichen, das sich aus Zahlen, Großbuchstaben, Kleinbuchstaben und Symbolen zusammensetzt, würde zu erraten via Brute-Force bis zu 286 Jahre benötigen. Ein ebenso langes Passwort, ohne Zahlen und Symbolen wäre jedoch bereits in 24 Tagen erraten - es kann also entscheidend sein, Länge und Komplexität zu kombinieren.

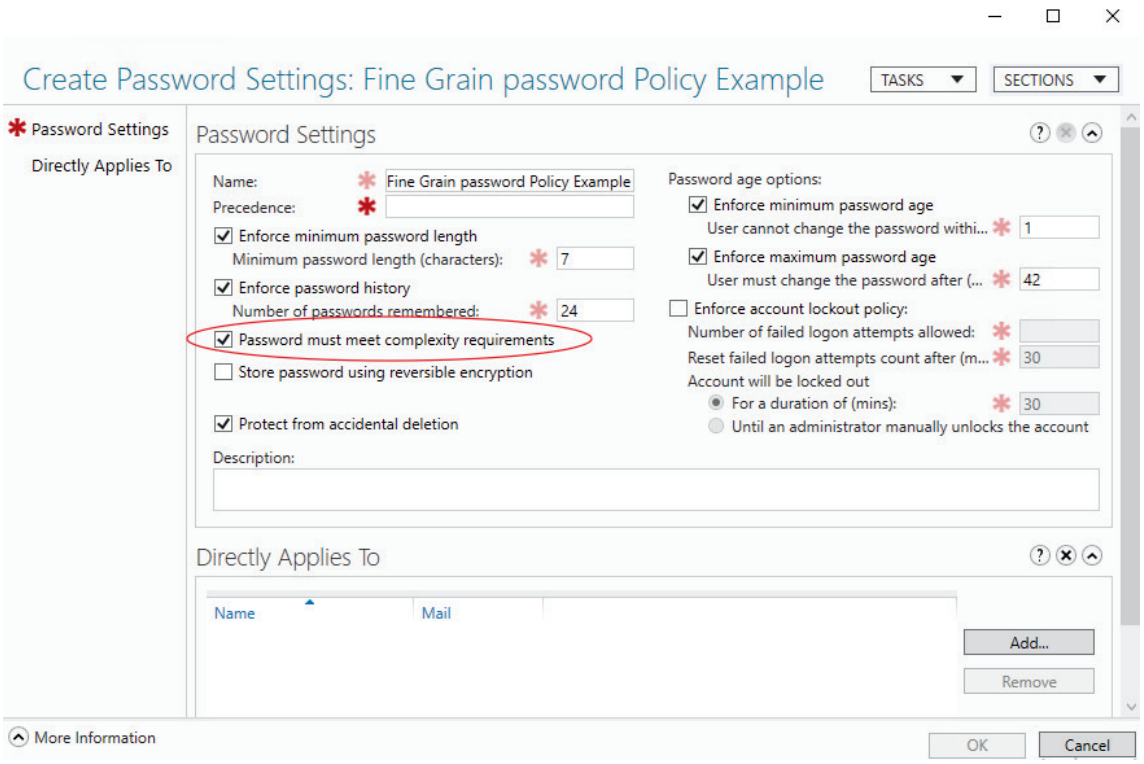
Es gibt leider keine Kontrolle über die „Komplexität“ innerhalb der Microsoft-Gruppenrichtlinien oder der Fine Grain Password Policy-Einstellungen. Sie kann lediglich auf „On“ gesetzt werden, was bedeutet:

- 3 der 5 verschiedenen Zeichentypen (Großbuchstaben, Kleinbuchstaben, Ziffern, Sonderzeichen und Unicode)
- Darf nicht Ihren Benutzernamen enthalten (Vorname, Nachname, Anzeigename oder sAMAccountName)

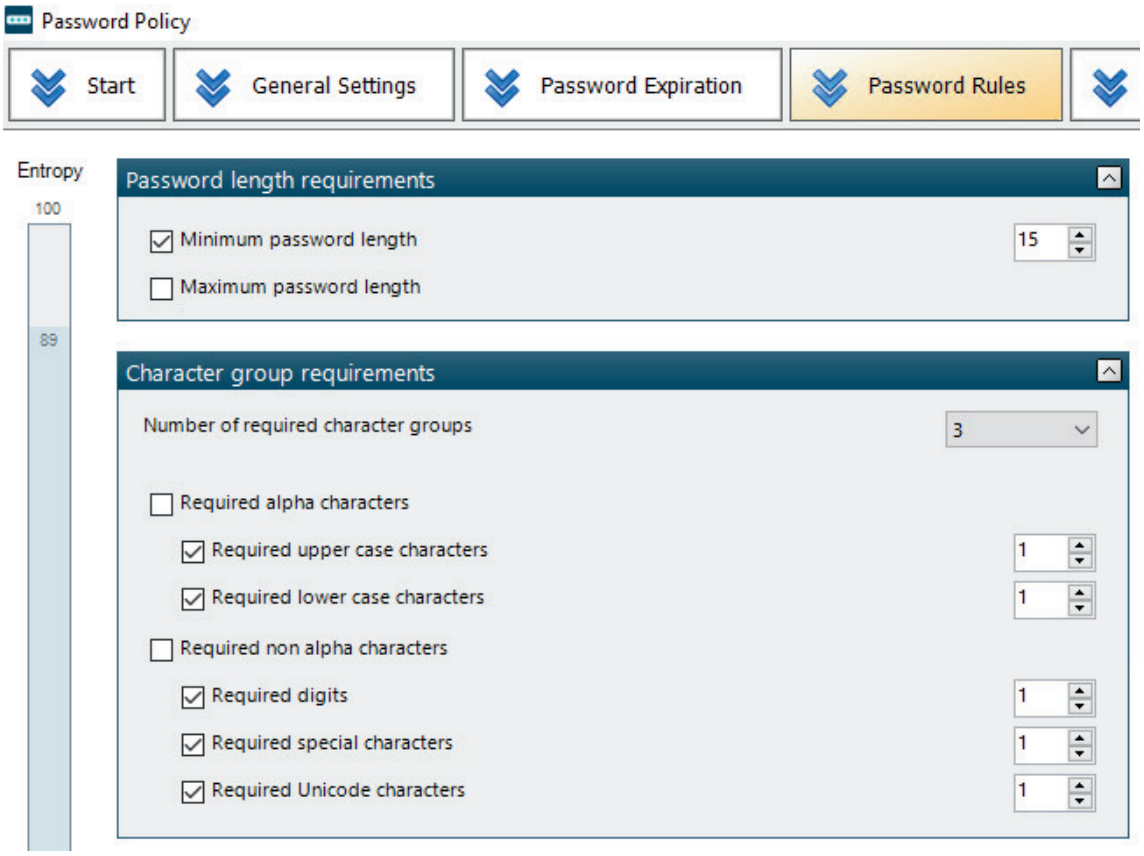
Group Policy:



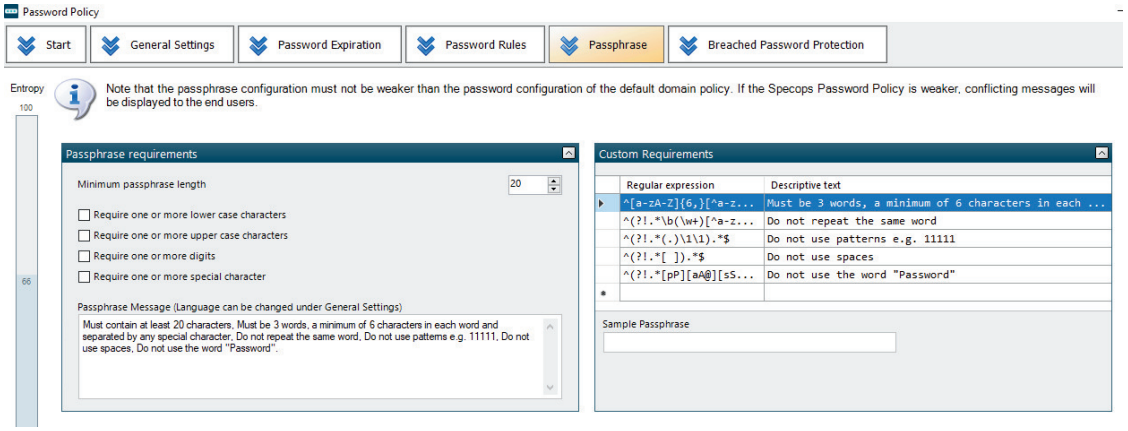
Fine Grain Password Policy:



Hier können Sie die Komplexitätsanforderungen für Passwörter in Specops Password Policy festlegen:



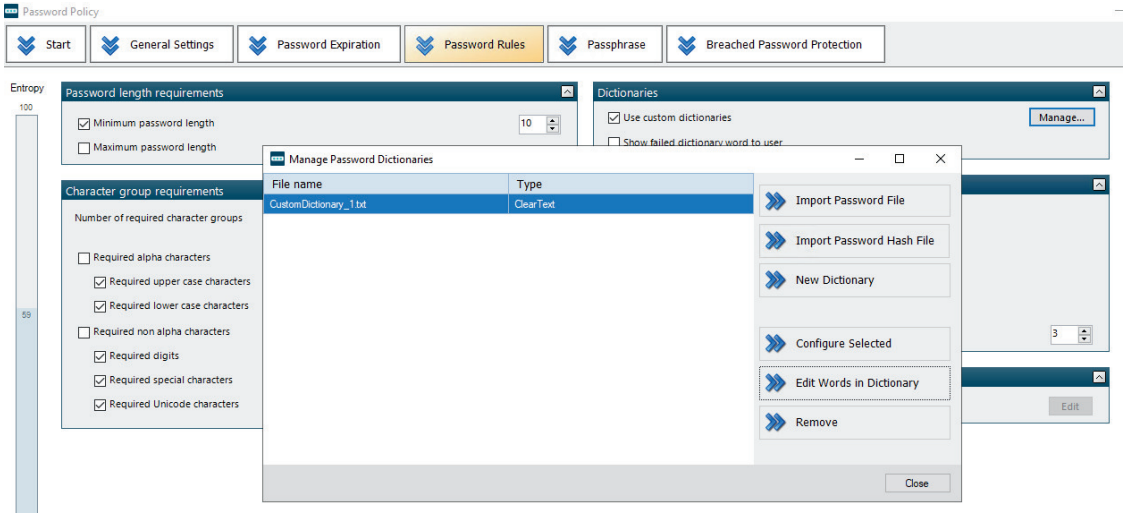
Passphrasen sollten in der Regel nicht zu komplex sein, da die Länge für die Stärke verantwortlich ist. Sie können jedoch mithilfe von RegEx Ihre individuelle Definition von Passphrasen für Ihr Unternehmen erstellen:



Blacklists für Passwörter

Sie können wählen, ob Sie bestimmte Listen mit bereits kompromittierten Kennwörtern ausschließen wollen. Mit einigen Tools ist es auch möglich, benutzerdefinierte Wörterbücher mit Wörtern zu erstellen, die für Ihr Unternehmen oder Ihre Branche spezifisch sind. Beispielsweise Firmen-, Abteilungs- oder Produktnamen, die von Nutzern für die Erstellung von Passwörtern verwendet werden könnten.

Leider gibt es für diese Funktion keine Möglichkeit innerhalb der Standard-Einstellungsmöglichkeiten von Microsoft Active Directory. Hier erfahren Sie, wie Sie mit Specops Password Policy bestimmte Begriffe verbieten können.

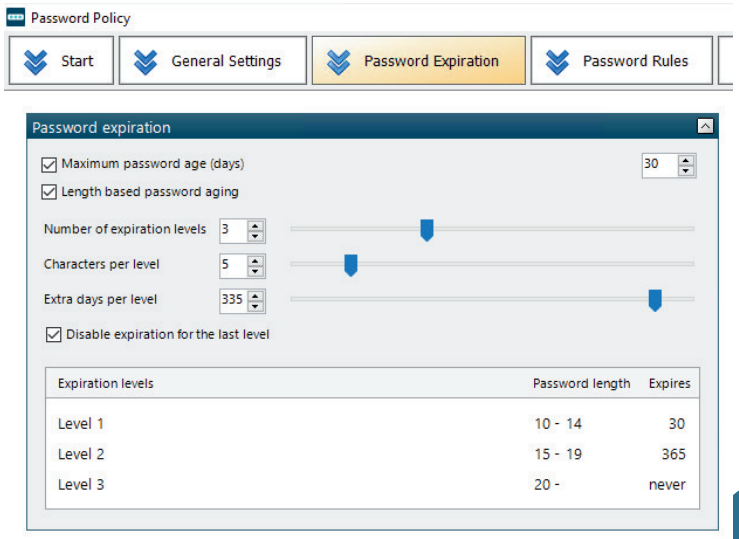


Ablaufdaten für Passwörter

Bis vor einigen Jahren wurde empfohlen, dass Nutzer ihre Passwörter alle 60, 90 oder 120 Tage ändern sollten. Dies führt jedoch häufig dazu, dass Benutzer „Passwort1“ in „Passwort2“ ändern. Überlegen Sie also, welcher Zyklus für Ihr Unternehmen am besten geeignet ist - hier finden Sie weitere Informationen zu Best Practices in Bezug auf den Ablauf von Passwörtern.

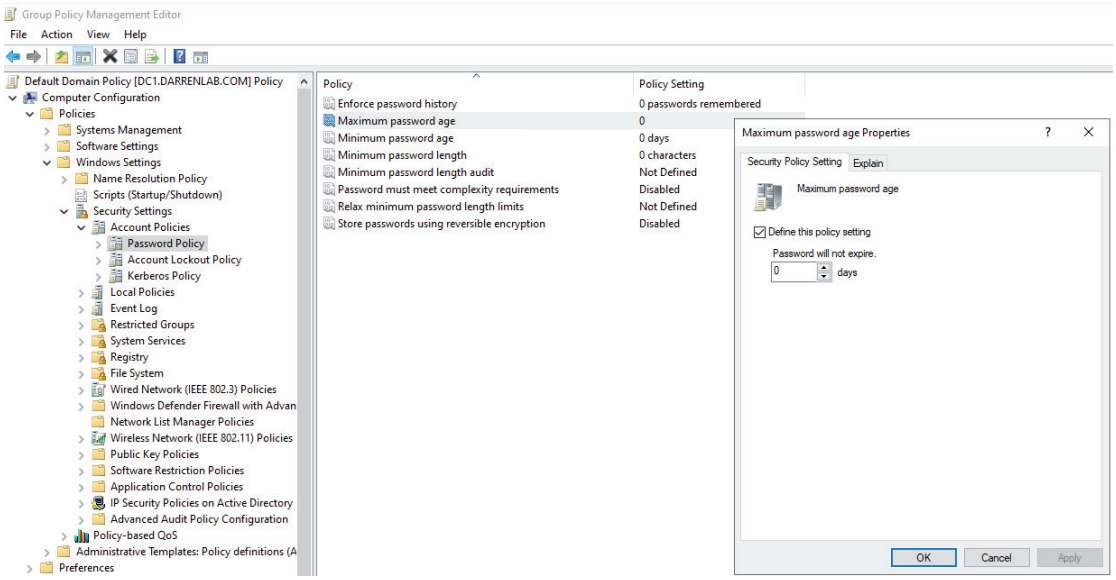
Vergessen Sie nicht, dass Sie mit Specops Password Policy auch die Möglichkeit haben, Benutzer zu belohnen, wenn diese längere Passwörter festlegen, indem Sie längere Ablaufzeiten gewähren. Wir nennen dies längenbasierte Alaufdaten für Passwörter. Im Beispiel unten sehen Sie, dass diese Richtlinie zwar immer noch kürzere Passwörter zulässt, aber längere Passwörter mit 15 bis 19 Zeichen mit einer Verfallszeit von einem Jahr belohnt werden, und wenn ein Benutzer eine Passphrase mit mehr als 20 Zeichen wählt, läuft sie nur ab, wenn wir erkennen, dass das Passwort kompromittiert wurde.

Hier erfahren Sie, wie Sie mit Specops Password Policy den Ablauf von Passwörtern und ein längenbasiertes Ablaufdatum für Passwörter einrichten können:

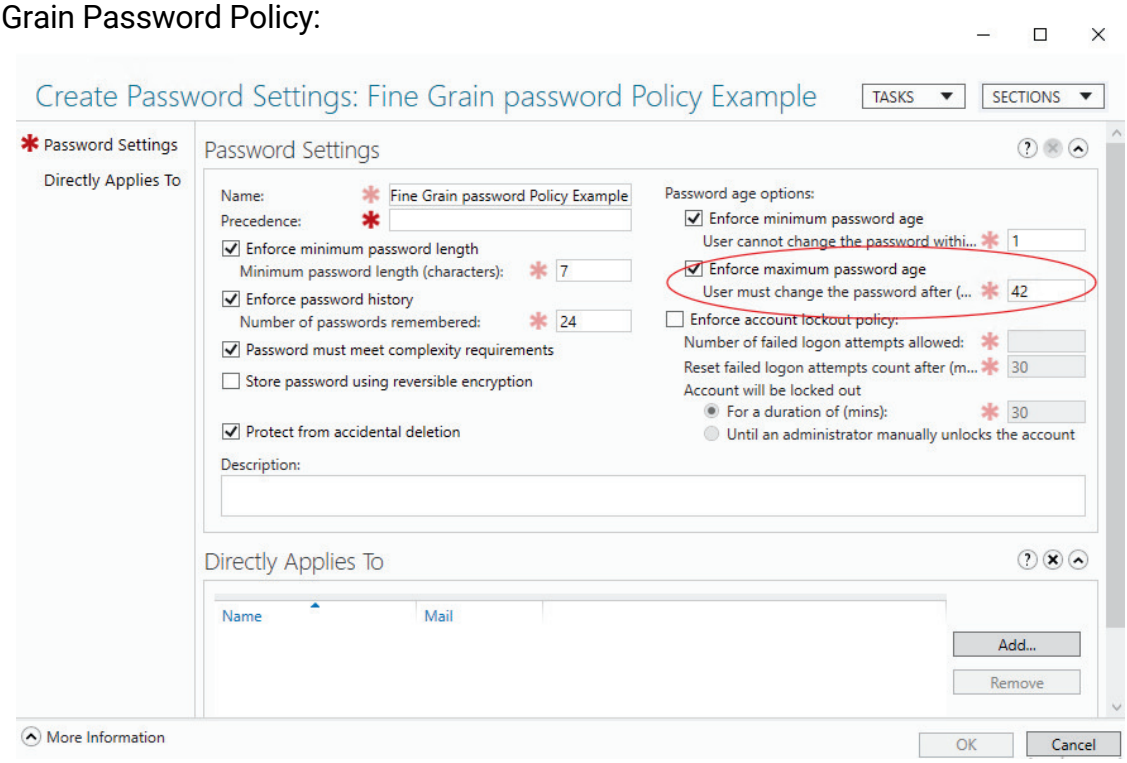


Microsoft hat zwar noch kein Konzept für ein längenbasiertes Ablaufdatum, aber Sie können unterschiedliche Verfallszeiten pro Richtlinie konfigurieren, z. B. wird die Gruppenrichtlinie „Ablauf“ Ihre globalen Einstellungen definieren, und Sie können dann mittels der Fine Grain Password Policy andere Verfallszeiten auf andere Benutzergruppe anwenden.

Group Policy:



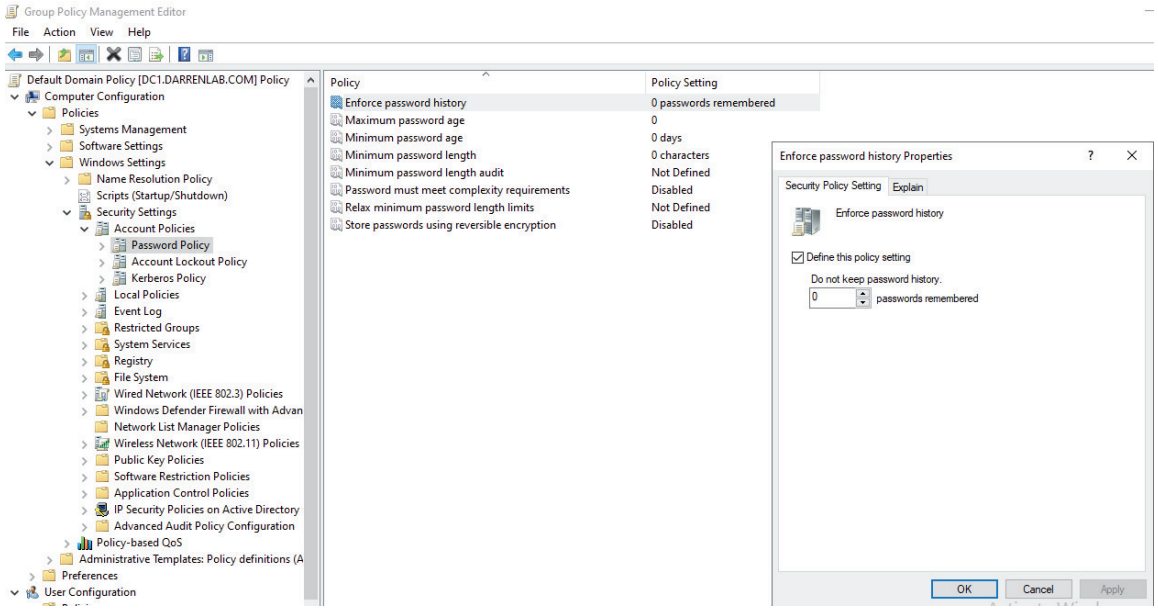
Fine Grain Password Policy:



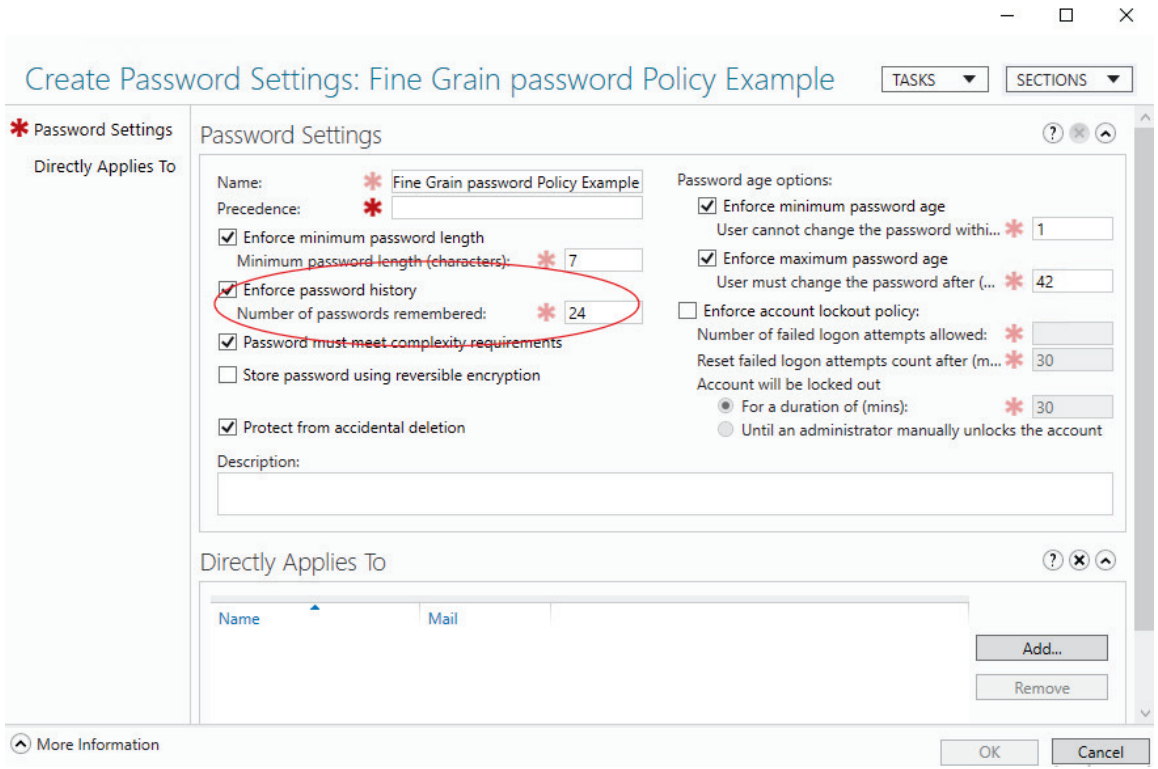
Password History

Der Kennwortverlauf bestimmt die Anzahl der eindeutigen Kennwörter, die ein Benutzer verwenden muss, bevor er ein bereits vergebenes Passwort wieder verwenden kann. Dies ist eine wichtige Einstellung aufgrund der Wiederverwendung von Kennwörtern und den damit verbundenen Risiken.

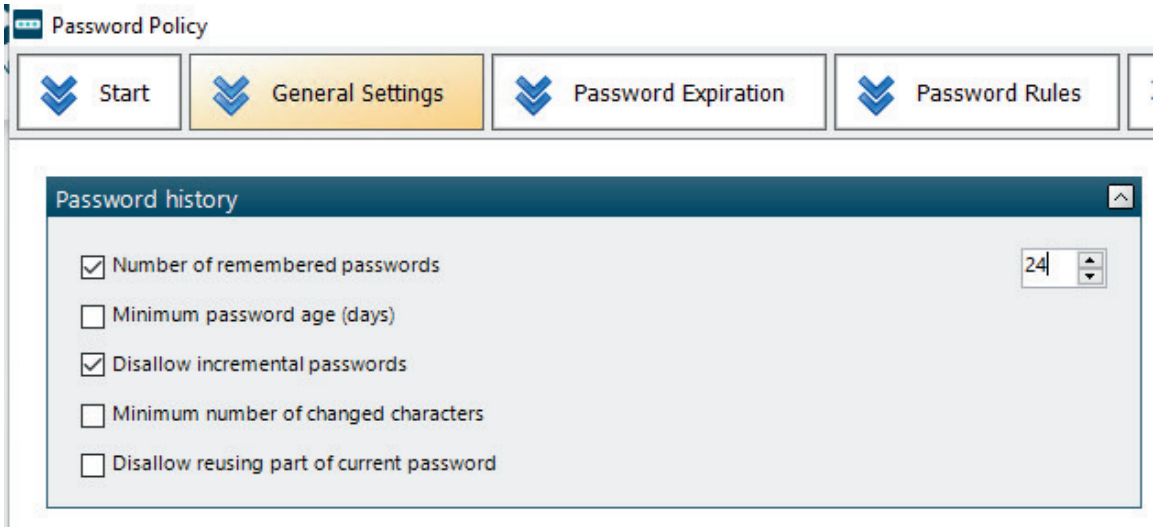
Hier finden Sie die Einstellungen für die Gruppenrichtlinie:



Und hier für Fine Grain Password Policy:



Und hier für Specops Password Policy:

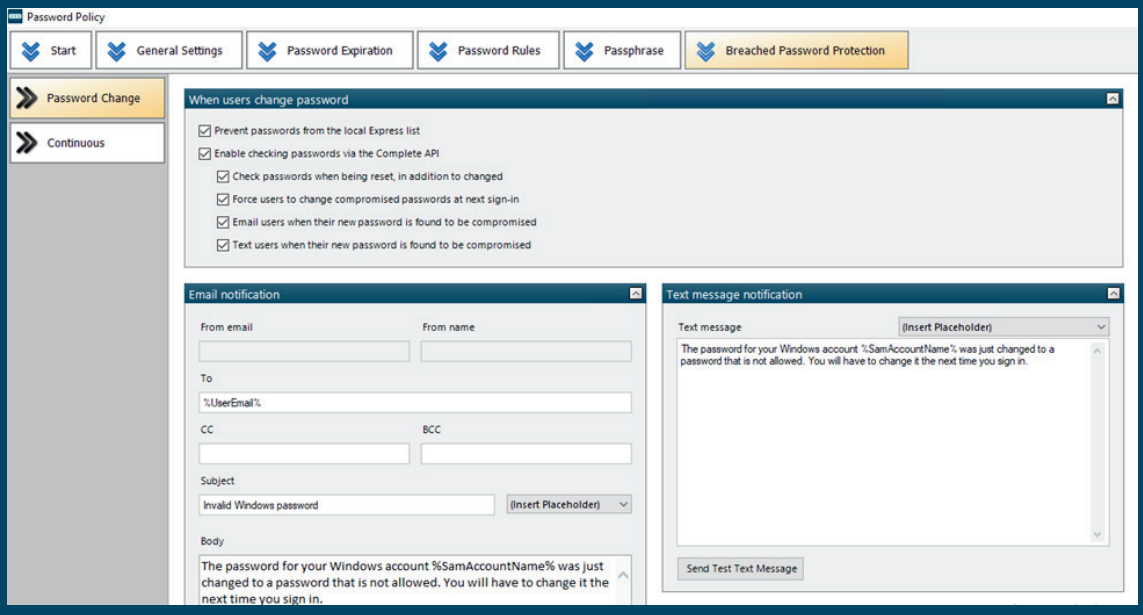


SPECOPS TIPP

Stellen Sie sicher, dass Sie kompromittierte Passwörter im Blick haben!

Passwortrichtlinien können die Erstellung von schwachen Passwörtern verhindern, aber auch starke Passwörter können kompromittiert werden. Unsere Untersuchung ergab, dass 83 % der kompromittierten Passwörter eigentlich bereits die meisten regulatorischen Vorgaben erfüllen. Solche Passwörter können durch Phishing-Angriffe kompromittiert, durch Malware gestohlen oder durch die Wiederverwendung von Passwörtern kompromittiert worden sein (z. B. wenn ein Mitarbeiter sein berufliches Active-Directory-Passwort auf einer fragwürdigen privaten Website wiederverwendet, deren Passwortdatenbank dann geleakt wird). In diesem Fall ist eine kontinuierliche Überprüfung nötig, um sicherzustellen, dass kompromitierte Passwörter sofort aus dem Verkehr gezogen werden.

Tools wie Specops Password Policy mit Breached Password Protection bietet eine kontinuierliche Scan-Funktion, die alle Ihre Active Directory-Passwörter einmal täglich mit unserer Breached Password Protection API auf Kompromittierung überprüft. Dies schützt vor der Verwendung von über 4 Milliarden kompromittierten Kennwörtern.



Diese Datenbank enthält Passwortdaten aus bereits bekannten Leaks, unseren eigenen Honeypot-Systemen, die Passwörter sammeln, die in tatsächlichen Passwort-Spray-Angriffen verwendet werden, sowie durch Malware gestohlene Zugangsdaten.

Fordern Sie noch heute einen kostenlosen Test von Specops Password Policy an.

SECTION THREE

Überlegungen bei der Einführung der Richtlinie

Das Ziel bei der Einführung einer neuen Kennwortrichtlinie ist es, dass jeder sein Kennwort auf ein Kennwort ändert, das den Anforderungen der neuen Richtlinie entspricht und bei dem es sich nicht um ein bereits kompromittiertes Passwort handelt. Soweit jedenfalls die Theorie. Allerdings kann es sich in der Praxis etwas schwieriger gestalten, wenn Sie versuchen, die neuen Richtlinien für alle Mitarbeiter gleichzeitig einzuführen.

Um zu verhindern, dass bei der Umstellung auf die neue Richtlinie alle Benutzer gleichzeitig ihre Kennwörter ändern und damit schlimmstenfalls eine Flut von Support-Tickets auslösen, empfiehlt es sich, Ihr Active Directory aufzuteilen und den Rollout zu staffeln. In diesem Abschnitt werden einige weitere Faktoren behandelt, die vor der Einführung einer neuen Passwortrichtlinie berücksichtigt werden sollten.

Wie geht man mit mehreren Richtlinien um?

Es ist kann sein, dass Unternehmen mehrere Kennwortrichtlinien benötigen. Zum Beispiel könnten verschiedene Richtlinien erforderlich sein für:

- Standard-User
- Admins
- Service-Konten
- Benutzer, die unter eine bestimmte Vorschrift wie PCI oder HIPAA fallen.

Nachdem Sie separate Richtlinien erstellt haben, müssen Sie natürlich sicherstellen, dass diese auch für die richtigen Benutzer gelten.

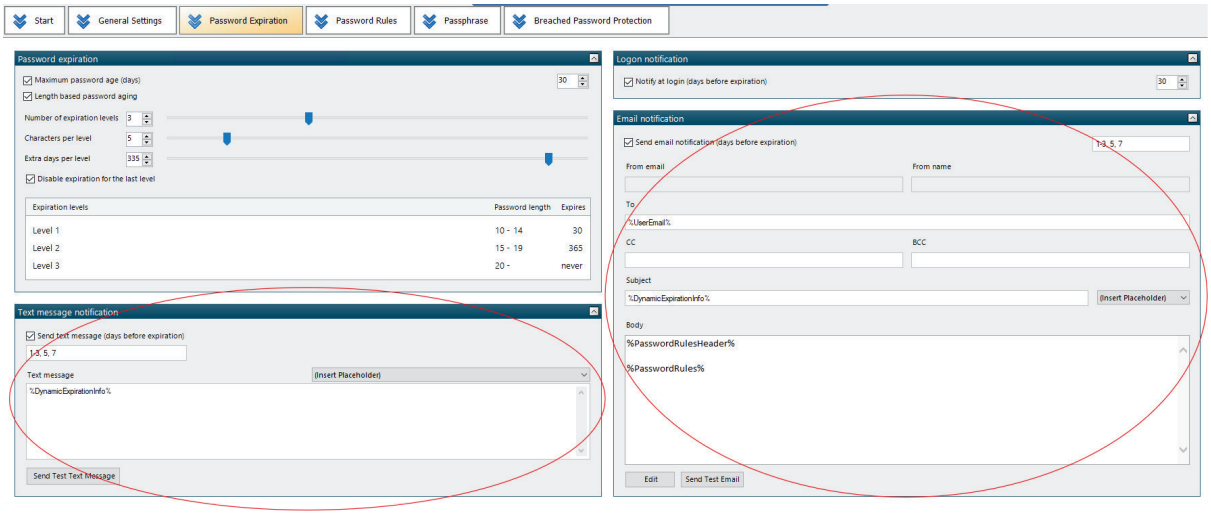
Da wir Gruppenrichtlinien verwenden, können wir dies entweder durch Verknüpfung der Gruppenrichtlinienobjekte (GPOs) mit einer Organisationseinheit (OU) tun. Von dort aus können Sie die Sicherheitsfilter und den Vorrang von GPOs nutzen. Sie können z. B. mehrere Benutzertypen in derselben OU haben, dann aber die Filterung und/oder den Vorrang von GPOs verwenden, um sicherzustellen, dass die richtige Richtlinie auf den richtigen Benutzer angewendet wird. Wenn Sie nicht wollen, dass die Richtlinien sofort greifen, können Sie GPOs erstellen und dann die Verknüpfungen temporär deaktivieren.

Wo befinden sich Ihre Benutzer und welche Geräte sind betroffen?

Ein weiterer wichtiger Punkt ist die Frage, wo sich Ihre Benutzer aufhalten, wenn Sie sie auffordern, ihre Kennwörter zu ändern. Wenn alle Benutzer zu einem bestimmten Zeitpunkt während einer normalen Woche in Ihr Büro kommen, ist es ziemlich einfach. Wenn Sie ein Tool wie den Specops Authentication Client verwenden, haben sie alle „Sichtkontakt“ zu einem Domain Controller (DC) und werden aufgefordert, ihr Passwort bei der nächsten Anmeldung an ihrem domänenverbundenen Windows-Gerät zu ändern.

Was ist mit Remote-Benutzern? Wenn sie kein Windows-Gerät verwenden, das mit der Domäne verbunden ist (z. B. Mac, iOS, Android, Chromebook, Linux oder ein PC oder Laptop, der nur mit Entra ID verbunden ist), haben sie auch keinen Authentication-Client installiert und werden entsprechend nicht aufgefordert, ihr Kennwort zu ändern. Allerdings können Sie E-Mail-Benachrichtigungen zum Ablauf des Passworts konfigurieren, und es gibt auch eine Zusatzoption für SMS-Benachrichtigungen zum Ablauf des Passworts.

Wenn Sie Specops Password Policy verwenden, können diese Benachrichtigungen angepasst werden und an bestimmten Tagen vor Ablauf des Kennworts verschickt werden. Außerdem gibt es ein zusätzliches Modul für Geräte, die nicht an eine Domäne angeschlossen sind oder nicht unter Windows laufen, um eine webbasierte Schnittstelle zur Kennwortänderung zu verwenden.



Vergessen Sie nicht, dass sie auch bei Windows-Geräten, die mit der Domain verbunden sind, nicht zur Änderung aufgefordert werden, wenn Sie kein „Always on VPN“ haben, das die Verbindung zu Ihren DCs herstellt (es sei denn, Sie haben E-Mails/SMS konfiguriert). Diese Benutzer werden auch auf alle möglichen Probleme mit gecacheten Zugangsdaten (Cached Credentials) stoßen - dies macht das Ändern des Passworts bei der nächsten Anmeldung schwierig und verwirrend, um es vorsichtig auszudrücken. In diesem Fall sollte ein Self-Service-Passwort-Reset-System vorhanden sein, um Ihre Helpdeskmitarbeiter zu entlasten.

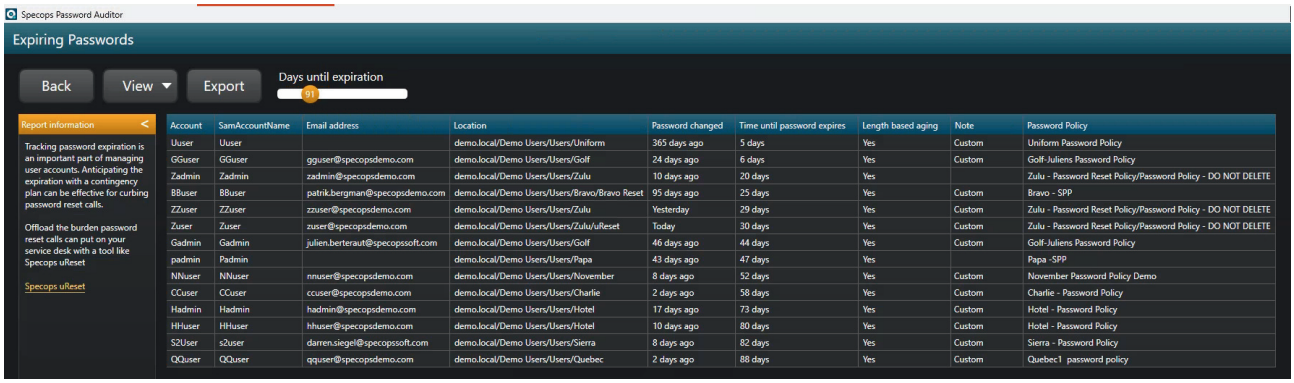
Gibt es bestimmte Nutzergruppen zu berücksichtigen?

- **Neue Mitarbeiter:** Die Einrichtung eines neuen Benutzers mit seinem Passwort ist ein wichtiger Teil des Onboarding. Die Weitergabe per Klartext oder mündlich durch einen Manager kann ein Risiko darstellen, das die Sicherheit Ihrer neuen Passwortrichtlinie untergräbt. Erfahren Sie mehr über die sichere Weitergabe von Passwörtern am ersten Arbeitstag.
- **Service-Konten:** Diese Konten führen in der Regel kritische Dienste und Systeme aus und haben nur sehr selten ein Ablaufdatum für ihre hinterlegten Passwörter. Die Kennwörter für diese Konten werden in der Regel auch nicht regelmäßig manuell eingegeben, sondern aus einem Kennworttresor kopiert und eingefügt. Überlegen Sie, ob Sie die Komplexität und Länge der Passwörter für diese Konten auf sehr hohe Werte einstellen, z. B. 64+ Zeichen, und ob sie anfällig für Denial-of-Service-Angriffe sind, indem Angreifer Ihre Kontosperrungsrichtlinie missbrauchen.
- **Administratoren und leitende Angestellte:** Benutzer mit hoch privilegiertem Zugang zum Netzwerk und/oder Zugriff auf sensible Daten sollten stärker geschützt werden als normale Konten. Die Verwendung längerer Passwörter/Passphrasen sollte in Betracht gezogen werden, sowie möglicherweise feste Ablaufdaten von Kennwörtern, selbst wenn diese nicht kompromittiert sind.
- **Mitarbeiter im Urlaub:** Bei der Planung der Umstellung sollte auch bedacht werden, ob Mitarbeiter für längere Zeit beurlaubt sind. Möglicherweise haben sie keinen Zugang zu den Systemen, die es ihnen ermöglichen würden, ihre Passwörter auf die neuen Vorgaben anzupassen. Besprechen Sie die Bedürfnisse dieser Benutzer mit ihren Managern und der Personalabteilung und treffen Sie mit dem Servicedesk oder durch detaillierte Anweisungen Vorsorge, um diese Benutzer zu unterstützen.

Planen Sie bestimmte Zeiträume?

Vielleicht gibt es ein festes Datum, bis zu dem Sie Ihre Einführung abschließen wollen - vielleicht ein geplantes Audit oder einen Pentest. Dieses Datum stimmt jedoch möglicherweise nicht mit dem Zeitpunkt überein, zu dem einige (oder viele) Anwender ihre Kennwörter ändern müssen. In manchen Unternehmen gibt es sogar Passwörter, die nie ablaufen.

Wenn eine Gruppe von Kennwörtern ohnehin in den nächsten Tagen oder Wochen abläuft, warum nicht die neue Richtlinie zuerst auf diese Benutzer anwenden? Für Benutzer, deren Kennwörter noch lange nicht ablaufen, weil sie sie erst kürzlich geändert haben, könnte es frustrierend sein, sie so bald wieder ändern zu müssen - Sie könnten ihnen Zeit lassen, bis die Einführungsfrist näher rückt.



Account	SamAccountName	Email address	Location	Password changed	Time until password expires	Length based aging	Note	Password Policy
Uuser	Uuser		demo.local/Demo Users/Users/Uniform	365 days ago	5 days	Yes	Custom	Uniform Password Policy
GGuser	GGuser	gguser@specopsdemo.com	demo.local/Demo Users/Users/Golf	24 days ago	6 days	Yes	Custom	Golf-Juliens Password Policy
Zadmin	Zadmin	zadmin@specopsdemo.com	demo.local/Demo Users/Users/Zulu	10 days ago	20 days	Yes		Zulu - Password Reset Policy/Password Policy - DO NOT DELETE
BBuser	BBuser	patrik.bergman@specopsdemo.com	demo.local/Demo Users/Users/Bravo/Bravo Reset	95 days ago	25 days	Yes	Custom	Bravo - SPP
ZZuser	ZZuser	zzuser@specopsdemo.com	demo.local/Demo Users/Users/Zulu	Yesterday	29 days	Yes	Custom	Zulu - Password Reset Policy/Password Policy - DO NOT DELETE
Zuser	Zuser	zuser@specopsdemo.com	demo.local/Demo Users/Users/Zulu/uReset	Today	30 days	Yes	Custom	Zulu - Password Reset Policy/Password Policy - DO NOT DELETE
Gadmin	Gadmin	julien.berteraut@specopssoft.com	demo.local/Demo Users/Users/Golf	46 days ago	44 days	Yes	Custom	Golf-Juliens Password Policy
padmin	Padmin		demo.local/Demo Users/Users/Papa	43 days ago	47 days	Yes		Papa -SPP
NNuser	NNuser	nnuser@specopsdemo.com	demo.local/Demo Users/Users/November	8 days ago	52 days	Yes	Custom	November Password Policy Demo
CCuser	CCuser	ccuser@specopsdemo.com	demo.local/Demo Users/Users/Charlie	2 days ago	58 days	Yes	Custom	Charlie - Password Policy
Hadmin	Hadmin	hadmin@specopsdemo.com	demo.local/Demo Users/Users/Hotel	17 days ago	73 days	Yes	Custom	Hotel - Password Policy
HHuser	HHuser	hhuser@specopsdemo.com	demo.local/Demo Users/Users/Hotel	10 days ago	80 days	Yes	Custom	Hotel - Password Policy
S2User	s2user	darren.siegel@specopssoft.com	demo.local/Demo Users/Users/Sierra	8 days ago	82 days	Yes	Custom	Sierra - Password Policy
QQuser	QQuser	qquser@specopsdemo.com	demo.local/Demo Users/Users/Quebec	2 days ago	88 days	Yes	Custom	Quebec1 password policy

Es gibt ein paar Taktiken, die Ihnen bei der Planung von Ablauffristen helfen können:

- Wenn Sie Hilfe beim Ablauf von Passwörtern benötigen, finden Sie im pwdlastset-Attribut eine nützliche Einstellung
- Wir haben auch einen Blog-Beitrag darüber, wie Sie Passwörter an einem bestimmten Tag in der Zukunft für einige oder alle Ihre Benutzer ablaufen lassen können

Self-service-Passwort-Reset-Lösungen

Der einfachste Weg, Kennwörter im großen Stil zurückzusetzen, besteht darin, die Benutzer zu ermutigen, ihre Kennwörter selbst zurückzusetzen oder zu ändern, bevor Sie eine Änderung erzwingen. Durch die Förderung der Nutzung einer Self-Service-Lösung für das Zurücksetzen von Kennwörtern vor dem Stichtag kann Ihr IT-Service Desk entlastet werden.

Wenn Sie eine externe Self-Service-Passwort-Reset-Lösung (SSPR) einsetzen, kann diese möglicherweise bei den im vorigen Abschnitt erwähnten Cached-Credential und nicht mit der Domäne verbundenen Geräten helfen. SSPR-Lösungen wie Specops uReset können Ihren Benutzern hilfreiches Feedback zu den Richtlinien geben und die im Zwischenspeicher befindlichen Zugangsdaten auf einem Remote-Laptop aktualisieren. Wir empfehlen, einen Hinweis in Ihre E-Mail-Benachrichtigungen über das Auslaufen von Passwörtern aufzunehmen, dass der Benutzer das SSPR-System verwenden sollte, um seine Passwörter zu ändern, oder dass er warten sollte, bis er das nächste Mal vor Ort ist, bevor er versucht, sie zu ändern.

Müssen Sie Nutzer dazu zwingen, ihr Kennwort zurückzusetzen?

Um tatsächlich alle Kennwörter ablaufen zu lassen und eine Rücksetzung bei der nächsten Anmeldung für Benutzer zu erzwingen, die ihre Kennwörter nicht innerhalb der von Ihnen gesetzten Frist selbst zurückgesetzt haben, benötigen Sie einige Informationen darüber, wer sein Kennwort seit Ihrer Aufforderung geändert hat. Mithilfe von PowerShell-Skripten, können Sie die Kennwortänderung erzwingen.

Bevor Sie das Skript ausführen, sollten Sie den Benutzern mitteilen, dass sie ihre Kennwörter bei der Anmeldung am nächsten Tag ändern müssen, und sie an die Anforderungen für das neue Kennwort erinnern sowie daran, wo sie ihre Kennwörter sonst noch aktualisieren müssen - sei es auf ihrem Mobilgerät oder in anderen Anwendungen, die Zugangsdaten zwischenspeichern (mehr zur Kommunikation an betroffene Benutzer im nächsten Abschnitt).

Wenn Sie eine Self-Service-Lösung zum Zurücksetzen von Passwörtern haben, sollten Sie sicherstellen, dass Ihr IT-Service-Desk darin geschult ist, Anrufer zur Nutzung dieser Lösung anzuleiten, vor allem, wenn das Call-Volumen hoch ist. Bewährte Service-Desk-Praktiken wie das Erzwingen einer Identitätsüberprüfung vor dem Zurücksetzen von Kennwörtern und mehr sind ebenfalls eine gute Idee. Wenn die Endbenutzer eingerichtet sind, sollten Sie sicherstellen, dass Sie auch die Kennwörter für Servicekonten zurückgesetzt haben, für die häufig keine MFA konfiguriert ist.

SPECOPS TIPPS

So gehen Sie mit Usern um, die kompromittierte Kennwörter verwenden

Sie haben vielleicht eine Gruppe von Nutzern mit dem Specops Password Auditor oder einem anderen Tool isoliert, deren Kennwörter kompromittiert wurden? Eine Ihnen bekannte Gruppe mit kompromittierten Passwörtern bietet Ihnen die Möglichkeit für einen ersten Test Ihrer neuen Passwortrichtlinien. Sie können diese Konten als Pilotgruppe für Ihren Rollout verwenden, d.h. Sie kümmern sich zuerst um die Benutzer mit dem höchsten Risiko und erhalten zudem Feedback darüber, ob der Rollout reibungslos verläuft.

Wenn Sie sich für den Einsatz von Specops Password Auditor entscheiden, sollten Sie bedenken, dass dieser nur einen Bruchteil (1 Milliarde kompromittierter Passwörter) der gesamten Specops-Datenbank (über 4 Milliarden kompromittierter Passwörter) nutzt. Alternativ können Sie auch die Continuous Scanning-Funktion von Specops Password Policy mit Breached Password Protection verwenden, die die bestehenden Active Directory-Passwörter Ihrer Benutzer täglich mit unserer kompletten Datenbank abgleicht und einen ausführlicheren Bericht erstellen kann. Dies wird wahrscheinlich weitere gefährdete Benutzer hervorheben, allerdings nimmt dieser Scan mehr Zeit in Anspruch.

Erfahren Sie mehr in einer kostenlosen Demo!

SECTION FOUR

Effektive Kommunikation der Änderungen an betroffene Nutzer

Die Einführung einer neuen Kennwortrichtlinie ohne einen Kommunikationsplan kann für Unruhe im Unternehmen sorgen. Besonders wenn Sie alle Nutzer dazu auffordern, ihre Passwörter zu ändern, ohne dass diese verstehen, was sie da tun oder warum - das würde bei Ihrem Helpdesk oder IT-Team Chaos auslösen und Gerüchte schüren.

Kommunikation an die Nutzer

Wenn Sie Ihre Anwender vor der offiziellen Aufforderung zum Zurücksetzen der Passwörter via E-Mail benachrichtigen, kann der Rollout reibungsloser verlaufen. In solch einer Mitteilung sollte erklärt werden:

1. Warum dies geschieht
2. Die neuen Anforderungen der Kennwortrichtlinie
3. Erinnerung an Best Practices und Aufforderung Passwörter nicht weiterzugeben, aufzuschreiben oder wiederzuverwenden
4. An wen man sich mit Fragen wenden kann

Außerdem sollten Sie erwägen, die Anleitung für den Nutzer zu testen. Achten Sie darauf, dass die Dinge einfach und leicht verständlich sind. Wenn sie von einer Passwortrichtlinie, bei der sie ein kurzes, komplexes Passwort (z. B. acht Zeichen mit einer Mischung aus Zahlen, Kleinbuchstaben, Großbuchstaben und einem Sonderzeichen) erstellen mussten, auf eine einfachere, aber längere Passphrase umsteigen, kann sich dies von den Richtlinien unterscheiden, die sie bislang gewohnt waren. Nutzen Sie auch dafür die Chance mögliche Datenschutzrechtliche Bedenken zu beschwichtigen, sollten die Nutzer Angst haben, dass Sie ihre Passwörter beispielsweise im Klartext mitlesen.

Vorlage für die Kommunikation an Kollegen und Mitarbeiter

Hier eine grobe Vorlage, die Sie auf Ihre Bedürfnisse anpassen können:

Liebe Kollegen,

Zwischen X/X/X und X/X/X werden wir in der gesamten Organisation eine neue Passwortrichtlinie einführen. Dies wird sowohl Sie als auch das Unternehmen davor schützen, dass Passwörter gehackt oder von Cyberkriminellen einfach erraten werden. Sie werden irgendwann innerhalb des oben genannten Zeitraums eine Benachrichtigung erhalten, dass Sie dazu auffordert, ein neues Active Directory-Benutzerpasswort zu vergeben.

Die Anforderungen der neuen Kennwortrichtlinie lauten wie folgt:

Länge :	*Neue Kennwörter müssen mindestens 15 Zeichen lang sein.*
Komplexität:	*Neue Passwörter müssen mindestens einen Großbuchstaben, eine Zahl und ein Sonderzeichen enthalten.*
Wiederverwendung:	*Wiederverwendete oder leicht veränderte Passwörter werden automatisch abgelehnt.*
Prüfung auf kompromittierte Kennwörter:	*Bereits bekannte kompromittierte Passwörter werden ebenfalls automatisch abgelehnt. Keine Sorge, kein IT-Mitarbeiter wird dazu Zugriff auf Ihre Passwörter im Klartext erhalten.*

Wir empfehlen, eine „Passphrase“ zu erstellen, da dies der einfachste Weg ist, ein langes, sicheres und leicht zu merkendes Passwort zu erstellen.

Bitte beachten Sie auch Best Practices im Umgang mit Passwörtern, die Sie im Rahmen Ihrer Cybersicherheitsschulung kennengelernt haben:

- *Geben Sie Ihr Passwort nicht weiter*
- *Schreiben Sie Ihr Passwort niemals auf (es sei denn, Sie bewahren es an einem sicheren Ort auf)*
- *Verwenden Sie Ihr Passwort nicht auf privaten Geräten, Anwendungen, Accounts und Websites wieder.*

Wenn Sie Fragen haben, wenden Sie sich bitte an [email]

Viele Grüße,
X

Kommunikation an weitere Stakeholder

Es gibt noch weitere Benutzergruppen innerhalb einer Organisation, für die Sie die oben beschriebene Kommunikation möglicherweise anpassen wollen. Nachfolgend sind einige der wichtigsten Gruppen aufgeführt.

Service Desk/IT-Helpdesk/Security-Teams

Diese Teams müssen wissen, wann sie mit einem höheren Aufkommen an Tickets und potenziellen Problemen im Zusammenhang mit Passwörtern rechnen müssen. Hoffentlich verläuft die Einführung reibungslos und die transparente Kommunikation mit den Nutzern ist von Nutzen, aber es kann immer zu Anlaufschwierigkeiten kommen. Auch diese Teams sollten sich über die neuen Anforderungen der Richtlinien im Klaren sein. Und denken Sie daran, dass alle Anrufe zum Zurücksetzen von Kennwörtern durch eine erzwungene Identitätsüberprüfung geschützt werden sollten (Erfahren Sie mehr über die sichere Authentifizierung am Servicedesk in diesem Webinar on Demand).

Geschäftsführung und Teamleiter:

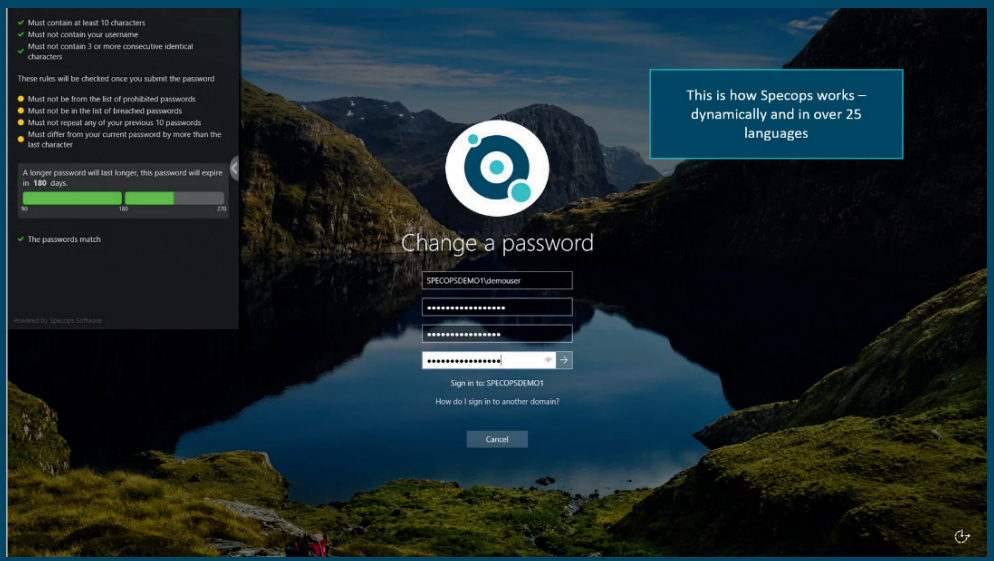
Für diese Gruppe ist es besonders wichtig, die Gründe für die neue Passwortrichtlinie zu verstehen, damit sie die Einführung befürwortet und unterstützen. Es kann sich auch lohnen, Statistiken oder Daten über die Risiken kompromittierter Passwörter mitzuteilen, um die Akzeptanz der Richtlinien zu fördern.

SPECOPS TIPP

Wie lässt sich die Benutzerfreundlichkeit einer Passwortrichtlinie verbessern?

Es gibt verschiedene Möglichkeiten, wie Sie den Umgang mit Passwörtern für die Endbenutzer einfacher gestalten können. Dinge wie Single Sign-On (SSO), Passwortmanager und Authentifizierungshardware wie YubiKeys gehören dazu, sind aber meist mit zusätzlichen Investitionen verbunden. Eine Möglichkeit, Passwortrichtlinien benutzerfreundlicher zu gestalten ist Feedback bei der Vergabe des Passwortes.

Specops Authentication Client bietet hierfür ein dynamisches Feedback bei der Vergabe des Passwortes und zeigt dem Nutzer in Echtzeit, welche Kriterien der Richtlinie er bereits erfüllt und noch erfüllen muss. Zur Förderungen längerer Passwörter wird auch (falls aktiviert) die Schwellenwerte für die längenbasierten Ablaufdaten der Passwörter eingeblendet werden. Erfahren Sie hier mehr über die Verbesserung der Benutzerfreundlichkeit von Passwörtern.



SECTION FIVE

Checkliste zur Umsetzung einer Passwortrichtlinie

PLANUNG DER PASSWORTRICHTLINIE

- ☐ Definieren Sie, was das Ziel Ihrer Kennwortrichtlinie ist und wie sie sich auf die Schutzziele der Organisation auswirkt.
- ☐ Listen Sie alle besonderen Anforderungen auf, die Ihr Unternehmen in seiner Passwortrichtlinie berücksichtigen muss (z. B. bestehende Verträge, Gesetze, Vorgaben und Branchenstandards).
- ☐ Informieren Sie sich über alle Vorschriften/Richtlinien, die für Ihren Standort/Ihre Branche gelten.
- ☐ Dokumentieren Sie Ihre neue Richtlinie und lassen Sie sie von relevanten Stakeholdern prüfen.
- ☐ Stellen Sie sicher, dass Sie eine Möglichkeit haben, die Passwortrichtlinie umzusetzen.

UMSETZUNG DER PASSWORTRICHTLINIE

- ☐ Vergewissern Sie sich, dass Sie die folgenden Komponenten korrekt eingestellt haben, damit sie mit Ihrem dokumentierten Entwurf übereinstimmen
  - ☐ Länge der Passwörter
  - ☐ Komplexitätsanforderungen
  - ☐ Blacklists und gesperrte Begriffe
  - ☐ Gültigkeitsdauer der Passwörter
  - ☐ Passwortverlauf
  - ☐ Überwachung kompromittierter Kennwörter

PLANUNG DES ROLLOUTS

- ☐ Erstellen Sie einen Plan, um die Umsetzung zu staffeln, anstatt alle Anwender gleichzeitig zu zwingen, ihre Passwörter zu ändern.
- ☐ Achten Sie auf folgende Themen:
  - ☐ Wie werden mehrere Passwortrichtlinien behandelt?
  - ☐ Wie werden Remote-Nutzer und unterschiedliche Geräte einbezogen?
  - ☐ Wie geht man mit unterschiedlichen Benutzergruppen um?
  - ☐ Gibt es eine feste Deadline?
  - ☐ Self-Service-Passwort-Resets
  - ☐ Wie erzwingt man eine Änderung des Passwortes?

KOMMUNIKATION DER NEUEN RICHTLINIEN

- ☐ Kommunizieren Sie den Plan klar und deutlich an betroffene Nutzer. Möglicherweise muss die Kommunikation für die folgenden Benutzergruppen angepaßt werden:
  - ☐ Anwender
  - ☐ Service-Desk/IT-Teams
  - ☐ Geschäftsführung und leitende Positionen

Benötigen Sie Unterstützung bei der Einführung einer starken und benutzerfreundlichen Passwortrichtlinie?

In diesem Beitrag haben wir vor allem allgemeine Best Practices vorgestellt, die für möglichst viele Unternehmen gelten sollen. Wenn Sie jedoch spezielle Fragen zu Ihrem eigenen Unternehmen oder Ihrer Branche haben, helfen wir Ihnen gerne weiter. Gerne beraten wir Sie, wie Sie Specops Password Policy oder uReset in Ihre Organisation integrieren können, um die Einführung neuer Passwortrichtlinien einfacher und sicherer zu gestalten. Bitte zögern Sie nicht, uns zu kontaktieren und einen Termin zu vereinbaren, um Ihre spezifischen Anforderungen zu besprechen.

ÜBER SPECOPS SOFTWARE GMBH

Specops Software, ein Outpost24 Unternehmen, ist der führende Anbieter von Passwort-Management- und Authentifizierungslösungen. Specops Software schützt Ihre Geschäftsdaten, indem es schwache Passwörter blockiert und die Benutzerauthentifizierung sichert. Mit einem kompletten Portfolio von Lösungen, die nativ in Active Directory integriert sind, stellt Specops sicher, dass sensible Daten vor Ort und unter Ihrer Kontrolle gespeichert werden. Specops Software wurde 2001 gegründet und hat seinen Hauptsitz in Stockholm, Schweden, sowie weitere Niederlassungen in den USA, in Kanada, Großbritannien, Frankreich und Deutschland. Mehr Informationen unter: https://specopssoft.com/de/

JETZT DEMOTERMIN VEREINBAREN>> **PREISINFORMATION >>**

KONTAKT

Global HQ
Karlskrona, Sweden
Blekingegatan 1,
371 57 Karlskrona, Sweden
info@outpost24.com

US HQ
Philadelphia, United States
123 S Broad St Suite 2530,
Philadelphia, PA 19109,
United States
Phone +1 877 773 2677

Stockholm, Sweden
Vasagatan 7A,
111 20 Stockholm, Sweden
info@outpost24.com

Copenhagen, Denmark
Axel Towers 2F, 4th floor,
1609 Copenhagen V,
Denmark
+45 53 73 05 67

Sophia Antipolis, France
950 Route Des Colles Les Templiers
CS30505
06410 Biot, France

London, United Kingdom
2 Stephen St, London W1T 1AN, United Kingdom

Plymouth, United Kingdom
Poseidon House, Neptune Park, Plymouth PL4 0SJ, United Kingdom

Reading, United Kingdom
Thames Tower, Station Rd, Reading RG1 1LX, United Kingdom

Amsterdam, Netherlands
Strawinskylaan 257
1077 XX Amsterdam,
Netherlands
+31 20 420 9560

Leuven, Belgium
Kapeldreef 60,
3001 Leuven, Belgium
+32 16 22 76 60

Barcelona, Spain
Plaça de Gal·la Placídia,
1-3, Oficina 303,
08006 Barcelona, Spain

Chicago, United States
35 S Washington St., Suite 308, Naperville, IL 60540

Toronto, Canada
517 Wellington Street West, Suite 400
Toronto, ON M5V 1G1
+1 877 773 2677

Berlin, Germany
Gierkezeile 12, 10585 Berlin
+49 30166 37218

Hanoi, Vietnam
15th Floor, Peakview Tower Building, 36 Hoang Cau,
Dong Da, Hanoi, Vietnam

SPECOPS
AN OUTPOST24 COMPANY