ManageEngine
ADSelfService Plus

Bessere Passwort-Regeln für das **Active Directory** erschweren Hacker-Angriffe

MicroNova
Software und Systeme

Bessere Passwort-Regeln für das **Active Directory** erschweren Hacker-Angriffe

Das Hacken von Passwörtern ist der einfachste Weg, um Zugang zu einem Anwender-Account im Active Directory zu erhalten. Hackern gelingt es seit vielen Jahren, sich auf einfache Art und Weise die Passwörter von Microsoft Active Directory-Anwendern anzueignen. Das ist kein Wunder, denn die Passwort-Regelungen und die Passwortverwaltung im Active Directory sind seit dem Jahr 2000 unverändert. Vor siebzehn Jahren war die Sicherheitslage noch eine völlig andere und es ist an der Zeit, mit besseren Passwort-Regeln für Active Directory-Umgebungen Hackern das Handwerk zu legen.

Strategien für das Hacken von Passwörtern

Insgesamt haben sich die Strategien, mit denen Hacker an Passwörter gelangen, in den letzten 15 Jahren nicht maßgeblich geändert. Das liegt auch daran, dass sich die entsprechenden Regelungen seitdem nicht verändert haben: Microsoft hat seit der Einführung des Active Directory im Jahr 2000 keine einzige zusätzliche Passwort-Regelungsmöglichkeit integriert. Hacker-Strategien und -Technologien funktionieren bei einem Windows Server 2012 R2 Active Directory-Anwender genauso wie sie auf einer Windows 2000 Mixed Mode Active Directory-Domain funktioniert haben.

Den meisten Werkzeugen für den Passwort-Diebstahl liegt dieselbe Logik zugrunde: Als erstes muss sich der Angreifer Zugriff auf den Hashwert verschaffen. Der Passwort-Hash ist ein mathematischer Algorithmus, der das Passwort in eine alpha-numerische Folge konvertiert, die nicht zurück zum Passwort umgewandelt werden kann. Der Hashwert wird durch das Betriebssystem generiert, in diesem Fall vom Active Directory. Der Hash wird in der Active Directory-Datenbank sowie in der Sicherheitsdatenbank des Client-Computers gespeichert, wenn sich der Anwender einloggt. Er wird für die Authentifizierung des Anwenders in dem Augenblick benötigt, in dem dieser Zugang zu Ressourcen des Netzwerks verlangt. Angreifer können sich den Hash aus der Active Directory-Datenbank, vom lokalen Client-Computer und aus den Authentifizierungspaketen holen.

Als zweiter Schritt wählt der Hacker den Zeichensatz, aus dem der Hashwert errechnet wurde. Dieser Zeichensatz kann aus einem Wörterbuch stammen oder durch bestimmte Parameter wie Buchstaben, Mindest- oder Maximallänge des Passworts definiert werden. Am Ende wird der Hashwert, der im ersten Schritt ermittelt wurde, mit dem verglichen der sich aus dem zweiten Schritt ergeben hat. Wenn die Werte übereinstimmen, wird das Passwort als der Zeichensatz erkannt, der den übereinstimmenden Hashwert generiert hat.

Wörterbuchangriffe

Ein Wörterbuchangriff benutzt als Grundlage des Hacks eine bestimmte Liste von Wörtern aus einer Wörterbuchdatei. In den meisten Fällen werden mehrere Wörterbücher für einen Angriff auf Passwort-Hashs herangezogen. Es kann sich dabei um ganz normale Lexika oder auch um spezielle Hacker-Wörterbücher handeln. Diese basieren auf normalen Wörterbüchern und fügen Wörter hinzu, in denen bestimmte Zeichen ersetzt wurden (Beispiele siehe Abbildung 1).

Language dictionary word	Hacker dictionary words		
password	Pa$$word	P@55w0rd	p@$$w0rD
admin	@dmin	@Dm1n	Adm!N
american	Am3R!c@n	amEr1c@N	@m3r1c@n

Abbildung 1: Beispiele von Wörtern aus Hacker-Wörterbüchern.

Da sich der Aufbau dieser Wörter an existierenden Wörtern orientiert, sind Wörterbuchangriffe schneller als andere Angriffstypen.

Brute-Force- oder Exhaustionsmethode

Ein Brute-Force-Angriff nutzt die logische Sequenz der Zeichen, um Hashwerte zu generieren, die dann mit den gehackten Passwort-Hashwerten verglichen werden. Statt einer Liste von Wörtern wie bei einem Wörterbuchangriff, verwendet ein Brute-Force-Angriff jede mögliche Kombination von Zeichen mit einer festgelegten Anzahl. Die für einen Brute-Force-Angriff verwendeten Zeichen können Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen sein (z. B.: a, A, 1, $). Die Länge des Passworts kann von einem einzigen Zeichen aufwärts festgelegt werden (Cain & Abel, ein beliebtes Tool für das Passwort-Recovery hat eine maximale Passwortlänge von 32 Zeichen). Wenn zum Beispiel nur Kleinbuchstaben für einen Brute-Force-Angriff verwendet werden, die minimale Länge des Passworts zwei und die maximale Länge drei Zeichen beträgt, so zeigt Abbildung 2 Beispiele von Passwörtern, aus denen sich Hashwerte für den Vergleich generieren lassen.

aa	ba
ab	bb
ac	bc
...	...
ax	bx
ay	by
az	bz
...	...
aaa	baa
aab	bab

Abbildung 2: Beispiele für Passwörter, die bei einem Brute-Force-Angriff verwendet werden können.

Wie bei jedem Passwort-Angriff werden die aus den Zeichenkombinationen resultierenden Hashwerte mit den entwendeten Werten verglichen. Wenn es eine Übereinstimmung gibt, ist das Passwort gefunden.

Rainbow-Table-Angriffe

Rainbow-Table-Angriffe sind die Weiterentwicklung von Brute-Force-Angriffen. Bei solchen Angriffen muss der Angreifer eine Zeichenfolge (a, A, 1, und/oder $) und die Passwortlänge definieren. Bei jedem Brute-Force-Angriff werden dieselben Zeichenkombinationen und die resultierenden Hashwerte erzeugt. Statt dieselben Werte immer wieder zu erzeugen, speichern sogenannte Rainbow-Tables sie im Cache. Dann wird ein einfacher Vergleich zwischen den Hashwert-Tabellen und den entwendeten Hashwerten vorgenommen, statt jeweils einen neuen Wert zu errechnen. Das erfordert schätzungsweise nur ein Zehntel der für einen Brute-Force-Angriff benötigten Zeit.

Attack Patterns oder Angriffsmuster

Hacker stützen ihre Angriffe auch auf sogenannte Attack Patterns oder Angriffsmuster, also die typischen Merkmale von Anwenderpasswörtern. Beispielsweise bevorzugen Anwender bei Änderungen ihrer Passwörter bestimmte Abfolgen, die sich leichter merken lassen. Konsekutive Passwörter wären zum Beispiel durch ansteigende Zahlen charakterisiert, z.B. Passwort1, Passwort2, Passwort3 usw.

Ein weiteres typisches Muster ist, dass Anwender das Passwort mit einem Großbuchstaben beginnen lassen. Da wir Sätze mit Großbuchstaben beginnen, ist ein solches Passwort leichter zu merken. Anwender, die gezwungen werden drei von vier Zeichentypen (wie a, A, 1, $) zu verwenden, lassen zudem üblicherweise die Sonderzeichen weg.

Auf Grundlage solcher Muster können Hacker Angriffe entwickeln und damit die benötigte Zeit für das Knacken des Passworts reduzieren.

Weitere Information zu den Möglichkeiten, Passwörter über Muster zu hacken können Sie dem „Global Threat Intelligence Report“ der NTT-Group entnehmen (https://www.solutionary.com/_assets/pdf/research/2016-gtir.pdf).

Passwort-Regeln

Die Passwort-Regeln für ein Betriebssystem enthalten bestimmte Vorgaben, die ein Anwender bei der Erzeugung eines Passworts einhalten muss, so sollte es beispielsweise eine Mindest- und eine Maximalanzahl von Zeichen haben. Der Aufbau der Passwort-Regelung sollte gegen die bekannten Passwort-Angriffe schützen und Schwachstellen bei der Passworterzeugung und den entsprechenden Hashwerten vermeiden. Leider ist das in den meisten Fällen nicht gegeben.

Die meisten Passwort-Regeln scheitern oder werden mangelhaft umgesetzt, weil die Anwender nicht mitmachen – und bieten damit keinen Schutz vor den bekannten Passwort-Angriffen. Die meisten User wollen oder können im Alltag nicht mit langen, sicheren und komplexen Passwörtern umgehen. Aufgrund dessen erlauben die Unternehmen ihren Mitarbeitern oftmals, kurze, schwache oder nur wenig komplexe Passwörter zu benutzen – und diese sind zumeist leicht zu hacken.

Idealerweise sollte eine Passwort-Regelung auf Vorgaben beruhen, die vor den bekannten Passwort-Angriffen schützen und zugleich flexibel genug sind, um von den Anwendern erinnert werden zu können. Im Folgenden betrachten wir die Microsoft-Lösungen für eine Passwort-Regelung und dann die Lösung von ManageEngine.

Passwort-Richtlinien von Microsoft

Microsoft bietet zwei Lösungen, um eine Passwort-Regelung für Anwender in Active Directory-Domains zu implementieren: Die eine Lösung verfolgt eine Group Policy, die andere eine Fine-grained Password Policy (FGPP). Unabhängig von der Implementierungstechnologie sind hierbei dieselben Regelungen möglich. Die Passwort-Regeln von Microsoft enthalten folgende Kriterien:

- Passwort-Geschichte berücksichtigen
- Maximales Passwortalter
- Minimales Passwortalter
- Minimale Passwortlänge
- Komplexitätsanforderung an das Passwort
- Speicherung des Passworts mittels umkehrbarer Verschlüsselung

Diese Passwort-Regelungen sind seit dem Jahr 2000 und der Einführung von Windows Active Directory vorgegeben. Sie haben sich jedoch als ungenügend erwiesen, um einen wirksamen Schutz gegen Hacker-Technologien zu bieten - der Vorgabewert von mindestens sieben Zeichen für ein Passwort ist zu schwach. Die Anforderungen an die Komplexität sind hinsichtlich Breite und Effektivität ebenso beschränkt. Denn Microsoft definiert die Komplexitätsanforderungen wie folgt:

- Das Passwort darf nicht den Namen des Anwender-Accounts oder Teile des vollen Namens mit mehr als zwei aufeinanderfolgenden Zeichen enthalten.
- Das Passwort muss mindestens sechs Zeichen lang sein.
- Das Passwort muss Zeichen aus drei der folgenden vier Kategorien enthalten:
    - Englische Großbuchstaben (A bis Z)
    - Englische Kleinbuchstaben (a bis z)
    - Ziffern von 0 bis 9
    - Nicht alphabetische Zeichen (z.B. !, $, #, %)

Die Passwort-Regeln von Microsoft schützen somit nicht vor Wörterbuch-, Brute-Force-, Rainbow-Table- und Angriffsmuster-Attacken.

Passwort-Richtlinien über Group Policy

Die Passwort-Regelungsmöglichkeiten des Active Directory beruhen auf Vorgaben, die für alle Passwörter der Anwender-Accounts in einer Domain gelten. Diese Passwort-Strategie ist als Vorgabe in der Default Domain Policy Group Policy Object (GPO) konfiguriert. Das Gruppenrichtlinienobjekt ist mit dem Active Directory Domain Node verlinkt. Wie die Passwort-Regelung für Domain-Anwender über Group Policy implementiert sind, bedarf einiger Erläuterungen:

1. Die Passwort-Richtlinien müssen nicht in der Group Domain Policy konfiguriert werden.
2. Die Passwort-Richtlinien müssen in einem GPP, das mit der Domain verlinkt ist, konfiguriert werden.
3. Die Passwort-Richtlinien werden aus den GPOs entnommen, die mit der Domain verlinkt sind, die die höchste Präferenz für die jeweilige Regel hat.
4. Die GPOs, die die Einstellungen der Passwort-Richtlinien enthalten, mit denen die Organisationseinheiten (OEs) verlinkt sind, betreffen nicht die Domain-Anwender.

Im Ergebnis bedeutet das, dass es bei einer GPO-basierten Passwort-Richtlinie am Ende doch nur eine einzige Regelung für alle Domain-Anwender geben kann. Mit Group Policy lassen sich nicht mehrere Passwort-Regelungen in einer einzigen Active Directory-Domain implementieren.

Mit FGPP implementierte Passwort-Richtlinien

Ab Windows Server 2008 hat Microsoft eine weitere Technologie für die Passwort-Regelung, die sogenannte Fine-grained Password Policiy (FGPP), eingeführt. Statt des Group Policy-Ansatzes zur Implementierung von Passwort-Regeln verfolgt Microsoft hier den Ansatz von Active Directory-Objekten. Die Vorgaben für die Regelung sind fast dieselben, doch FGPP bietet einige zusätzliche Möglichkeiten:

- Vorrang einer jeweiligen FGPP-Regelung im Verhältnis zueinander
  (so dass nur eine FGPP für den jeweiligen Anwender zutreffen kann)
- Anwendung der jeweiligen FGPP auf eine oder mehrere Sicherheitsgruppen

Im Ergebnis heißt das, dass es mehr als eine Passwort-Regelung in derselben Active Directory-Domain geben kann. Jedes Mitglied einer Gruppe, die einen Bezug zu einer FGPP hat, erhält die vorrangigste, auf den jeweiligen Anwender zutreffende FGPP. Wenn ein Anwender einer Gruppe, die mit einer FGPP verbunden ist, nicht zugehörig ist, findet auf diesen Anwender die Passwort-Regelung Anwendung, die über die Group Policy implementiert ist.

Über ADSelfService Plus implementierte Passwort-Richtlinien

Da die Passwort-Richtlinien von Microsoft keine sicheren Passwörter bereitstellen, ist eine Lösung erforderlich, die auf Active Directory und Group Policy/FGPP basiert und sichere Passwörter generiert. ADSelfService Plus bietet Schutz vor den neuesten Passwort-Angriffen und kann über Ihr aktuelles Active Directory OE-Design implementiert werden.

ADSelfService Plus verbessert Passwort-Richtlinien von Microsoft, da es in einer einzigen Active Directory-Domain verschiedene Passwort-Richtlinien ermöglicht. Diese Erweiterungen arbeiten nahtlos mit den Einstellungen für Passwort-Richtlinien von Windows zusammen und erlauben es, die Regelungen Ihren Bedürfnissen anzupassen. Folgende Merkmale kennzeichnen ADSelfService Plus im Hinblick auf Active Directory-Passwörter:

- Verschiedene Passwort-Richtlinien in einer Domain
- Implementierung über Gruppenmitgliedschaft oder Anwenderlokation
  in einer OU (Organizational Unit)
- Import von Wörterbüchern, um die Nutzung dieser Wörter in Passwörtern zu verhindern
- Vorgaben für Passwort-Muster (inkrementelle Gestaltung, Weglassen von Sonderzeichen, Palindrome usw.)

- Die Einhaltung der Passwort-Richtlinien wird durch das Web-Portal und die mobile Anwendungen von ADSelfService Plus erzwungen
- Die Einhaltung der Passwort-Richtlinien wird durch den Befehl „Ctrl+Alt+Del Change Password Screen“ erzwungen
- Die Einhaltung der Passwort-Richtlinien wird erzwungen, wenn der Administrator ein Passwort von Anwendern und Rechnern zurücksetzt, die im Active Directory geführt sind.

ADSelfService Plus lässt sich leicht konfigurieren und verwalten. Abbildung 3 zeigt, wie Passwort-Richtlinien für Active Directory definiert werden. Die Passwort-Architektur von ADSelfService stellt eine Verbesserung der Passwort-Regelungen von Microsoft Group Policy und/oder FGPP dar. Auf Anwender, die nicht in diese Regelungen von ADSelfService Plus einbezogen sind (über Gruppenzugehörigkeit oder Organisationseinheit), treffen nur die Vorgaben von entweder FGPP oder Group Policy zu. ADSelfService Plus bietet einen effektiven und einfachen Weg, zusätzliche Passwort-Richtlinien zu implementieren, ohne dass die Architektur der aktuellen Active Directory-Umgebung angepasst werden muss.

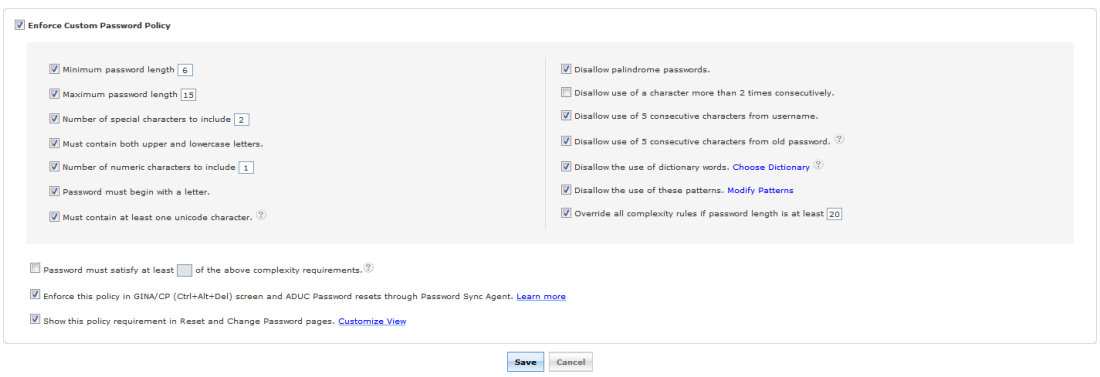

Abbildung 3: Implementierung von Passwort-Regeln mit ADSelfService Plus

Durch die Möglichkeit, eines oder mehrere Wörterbücher in die Passwort-Richtlinien einzubinden, können Sie sich besser gegen Wörterbuchangriffe verteidigen. Die von ADSelfService Plus bereitgestellten Regeln zur Vermeidung von Passwort-Mustern verhindern, dass Anwender beim Anlegen von Passwörter die gängigen Musterfehler begehen. So können Sie mit ADSelfService Plus den Schutz von Anwenderpasswörtern im Active Directory gegen verbreitete Passwort-Angriffe optimieren.

Zusammenfassung

Wir werden angegriffen! Dennoch hat es Microsoft unterlassen, zusätzliche Passwort-Richtlinien bereitzustellen, um die Passwörter von Active Directory-Anwendern besser zu schützen. Ohne entsprechende zusätzliche Schutzmaßnahmen und -technologien werden Passwörter nur unzureichend geschützt. Die Passwort-Regeln von Group Policy und FGPP reichen nicht aus. Zwar bietet FGPP mehr als nur eine Passwort-Regelung für eine einzelne Domain, doch die Regeln werden über Gruppenzugehörigkeit oder OU-Lokation zugewiesen. Das stellt eine erhebliche Einschränkung dar und hindert Sie daran, für einen effektiven Passwort-Schutz zu sorgen.

ADSelfService Plus ist die intelligente Lösung, die Ihren Anwendern in einer Active Directory-Domain den nötigen Schutz bietet. Die meisten Active Directory-Installationen profitieren von der Möglichkeit, mehrere Passwort-Regelungen in einer einzelnen Domain, distribuiert über Gruppenzugehörigkeit oder OU-Lokation, implementieren zu können. Durch die Einführung von Passwort-Regelungen, die gegen Wörterbuchangriffe und Angriffe über vermeidbare Passwort-Muster schützen, erhöht sich die Schutzwirkung von ADSelfService Plus zusätzlich. ADSelfService Plus ist die sichere Lösung für jede Active Directory-Domain und dabei einfach zu implementieren, zu konfigurieren und zu verwalten.

Weitere Informationen
https://www.manageengine.de/produkte-loesungen/active-directory/adselfservice-plus.html

MicroNova AG | Unterfeldring 17 | D-85256 Vierkirchen
Tel.: +49 81 39 / 93 00-456 | Fax: +49 81 39 / 93 00-80
E-Mail: sales-ManageEngine@micronova.de

ADSelfService Plus

ManageEngine ADSelfService Plus ist eine sichere webbasierte Software, mit der Benutzer ihr Passwort in Microsoft Active Directory selbst zurücksetzen können. Die Software ermöglicht es den Anwendern zudem, das eigene Konto zu entsperren und persönliche Kontaktinformationen wie Telefonnummern im Active Directory zu pflegen. Für das Zurücksetzen der Passwörter können – alternativ oder zusätzlich zu personalisierten Fragen – Einmal-Token per SMS oder E-Mail genutzt werden.

Für Administratoren bietet ADSelfService Plus detaillierte Audit-Reports und Administrationsfunktionen, die sichere Passwörter und ein ebenso sicheres Passwort-Reset garantieren.

30 Tage gratis testen: https://www.manageengine.de/produkte-loesungen/active-directory/adselfservice-plus/download.html