Specops Password Policy & Breached Password Protection vs. Microsoft Entra Password Protection (ehemals Azure AD)

Wie Microsoft Entra Password Protection funktioniert

Microsoft Entra (Azure AD) Password Protection ist in den Plänen P1/P2 von Entra ID (Azure AD) enthalten. Der Name vermittelt den Eindruck, dass Benutzer zuverlässig daran gehindert werden, unsichere Passwörter zu verwenden. In der Praxis trifft das jedoch nicht zu. Wenn ein Unternehmen seine Active-Directory-Umgebung ernsthaft absichern möchte, unabhängig davon, ob lokal oder in der Cloud, reichen die integrierten Schutzmechanismen von Entra ID allein nicht aus.

Viele gehen davon aus, dass Entra bereits ausreichenden Schutz bietet und keine zusätzliche Lösung zur Erkennung kompromittierter Passwörter benötigt wird. Diese Annahme entspricht jedoch nicht der Realität. Im Folgenden wird anhand eines praxisnahen Beispiels gezeigt, wie Microsoft Entra Password Protection kompromittierte Passwörter nicht erkennt. Anschließend wird erläutert, warum die beiden verwendeten Passwortlisten aus unterschiedlichen Gründen unzureichend sind.

Neue Studie: Wie gut erkennt Microsoft Entra kompromittierte Passwörter?

Es wurde eine Untersuchung durchgeführt, um die Fähigkeit von Entra ID und Specops Breached Password Protection beim Blockieren von Passwörtern zu vergleichen. Zusätzlich wurde Have I Been Pwned als weiterer Referenzpunkt einbezogen.

Methodik

1. Eine zufällige Stichprobe von 5000 Passwörtern wurde aus den im Mai 2025 veröffentlichten Alien_Txtbase Infostealer Logs entnommen. Diese Auswahl wurde mit Bedacht getroffen, um anderen Leak Datensätzen ausreichend Zeit zur Verarbeitung zu geben.

2. Es wurden Skripte entwickelt, um diese Stichprobe gegen die HIBP-API zu prüfen und gleichzeitig Passwortänderungen auf einem Ziel-Domain-Controller zu simulieren.

3. Eine Entra ID Umgebung wurde mit Entra ID Proxy sowie dem Microsoft Entra Password Protection Agent eingerichtet. Auf dem Domain Controller wurde genau eine Gruppenrichtlinie im Blockmodus angewendet. Es wurden keine weiteren Richtlinien oder benutzerdefinierten Wörterbücher aktiviert. Dadurch konnte sichergestellt werden, dass jede blockierte Passwortänderung eindeutig auf den Passwortfilter zurückzuführen ist.

4. Eine direkte Überprüfung mit Breached Password Protection war nicht notwendig, da der verwendete Datensatz bereits vollständig in BPP enthalten ist und somit alle Einträge blockiert würden. Zu beachten ist, dass die Monate Juni und Juli nicht die aktuellsten Infostealer-Daten im BPP darstellen, da bewusst ältere Daten verwendet wurden. Zur Bewertung der Abdeckung wurde zusätzlich dieselbe zufällige Stichprobe aus einem aktuellen Infostealer-Dump aus einem Darknet-Forum entnommen.

Ergebnisse der Analyse

Die Ergebnisse entsprechen den Erwartungen. Der bewusst ältere Datensatz weist eine bessere Abdeckung bei HIBP auf, da seitdem genügend Zeit vergangen ist, um die Daten über neue Leaks oder Quellen von Strafverfolgungsbehörden zu integrieren. Entra ID schneidet hingegen deutlich schlechter ab. Dies zeigt sich an der hohen Anzahl von Passwortänderungen, die nicht blockiert wurden. Ein Großteil der Passwörter aus dem Mai wird von Entra ID weder erkannt noch blockiert.

Entra ID

Month	May	June	July	October
Missed	4,650	4,644	4,653	4,534
Blocked	348	354	347	466
Blocked %	6.96%	7.08%	6.96%	9.32%

HIBP

Month	May	June	July	October
Missed	338	334	710	2,441
Blocked	4,662	4,666	4,290	2,559
Blocked %	93.24%	93.32%	85.8%	51.18%

Specops

Month	May	June	July	October
Missed	0	0	0	0
Blocked	5,000	5,000	5,000	5,000
Blocked %	100%	100%	100%	100%

Was bedeutet das?

Aufgrund ihrer grundlegenden Designprinzipien unterscheiden sich die Erkenntnisse zwischen HIBP und Entra ID. So ist HIBP ist nicht auf seine öffentliche API beschränkt; sein Datensatz wird auch von mehreren Wettbewerbern als einzige Quelle für kompromittierte Passwörter genutzt (z. B. ManageEngine ADSelfService Plus, und Open Password Filter).

Entra ID

- Entra ID basiert auf einer Liste bereinigter Wörter, ordnet diese einer Sperrliste zu und bewertet Passwörter anhand eines Punktesystems. Dieses Verhalten ist unabhängig vom Datensatz konsistent und führt jedoch dazu, dass kompromittierte Passwörter nicht effektiv blockiert werden. Das System ähnelt eher einer klassischen Passwortrichtlinie mit verbotenen Wörtern als einer umfassenden Datenbank kompromittierter Zugangsdaten.

- Microsoft verwendet ein Punktesystem zur Bewertung der Passwortstärke. Dabei wird auch die interne Liste kompromittierter Passwörter berücksichtigt. Passwörter werden zunächst normalisiert, beispielsweise wird P@ssw0rd zu password umgewandelt. Anschließend wird das Passwort nur dann blockiert, wenn es nicht genügend Entropie erreicht.

- Organisationen, die an Standards wie NIST 800-63B oder CJIS gebunden sind, sollten beachten, dass Entra ID bei der Verhinderung der Verwendung geleakter Passwörter schlecht abschneidet. Diese Lücke ist auf das Design zurückzuführen und nicht auf eine Verzögerung zwischen einem Sicherheitsvorfall und der Abdeckung durch die Datenbasis. Entra ID blockiert kompromittierte Passwörter nicht zuverlässig, und einfache geleakte Passwörter können die Filter weiterhin passieren. Daher sollte es nicht als gleichwertig mit BPP im Hinblick auf die Einhaltung von Standards wie NIST 800-63B oder CJIS betrachtet werden.

- Zusätzlich bietet Entra ID keinen Echtzeitschutz. Passwörter werden ausschließlich bei einer Zurücksetzung oder Änderung überprüft.

HIBP

- HIBP zeigt eine deutlich stärkere Variation zwischen verschiedenen Datensätzen. Mit fortschreitender Zeit und zunehmender Verfügbarkeit von Datenleaks steigt die Wahrscheinlichkeit, dass kompromittierte Passwörter in die HIBP-Datenbank aufgenommen werden. Ältere Leaks weisen daher in der Regel eine geringere Anzahl nicht erkannter Passwörter auf, insbesondere im Vergleich zu Entra ID. Bei neueren Leaks werden hingegen deutlich größere Lücken sichtbar.

- HIBP hat weniger nicht erkannte Passwörter, da es als echte Datenbank für kompromittierte Zugangsdaten eingesetzt wird, ähnlich wie Specops Breached Password Protection. HIBP basiert in erster Linie auf Meldungen von Nutzern sowie von Strafverfolgungsbehörden. Aufgrund dessen kann es zu Verzögerungen bei der Aufnahme oder auch zu Auslassungen kommen.

- Anbieter, die ausschließlich auf HIBP als Quelle für kompromittierte Passwörter setzen, sind daher zeitlich hinter einer vollständig gepflegten und aktiv überwachten Leak-Datenbank zurück. Diese Verzögerung ist jedoch deutlich weniger gravierend als bei Entra ID, da kompromittierte Zugangsdaten zumindest grundsätzlich erkannt und blockiert werden.

Specops

- Die Specops Breached Password Protection zeichnet sich durch äußerst kurze Verzögerungszeiten aus. Dies ist auf die Kombination aus Threat-Intelligence-Operationen, Specops-Honeypots sowie manueller Überwachung von Leak- und Angriffsaktivitäten zurückzuführen.

- Specops Password Policy in Verbindung mit Breached Password Protection bietet eine signifikant bessere Abdeckung kompromittierter Zugangsdaten im Vergleich zu Implementierungen, die ausschließlich auf HIBP oder Entra ID basieren.

- Specops Password Policy mit Breached Password Protection blockiert Passwörter unmittelbar nachdem sie neu in das kompromittierte Datenkorpus aufgenommen wurden.

Warum die Liste der weltweit verbotenen Passwörter nicht ausreicht

Die „Liste der weltweit verbotenen Passwörter“ ist keine Liste kompromittierter Passwörter und erfüllt keine Compliance-Anforderungen.

Im Gegensatz zu Specops Breached Password Protection enthält sie keine externen Datenquellen wie Have I Been Pwned oder andere bekannte Leak-Datenbanken. Microsoft nutzt ausschließlich interne Analysen aus Entra-ID-Umgebungen. Der konkrete Inhalt dieser Liste wird nicht veröffentlicht.

Regulatorische Standards wie NIST 800 63B oder NCSC empfehlen ausdrücklich die Verwendung bekannter kompromittierter Passwortlisten. Specops Breached Password Protection erfüllt diese Anforderungen vollständig.

Microsoft gibt nicht an, wie viele Passwörter in der Liste enthalten sind. Es heißt lediglich, dass sie im Vergleich zu anderen Drittanbieterlisten klein ist, durch Fuzzy-Matching jedoch Millionen von Passwortvarianten aus dieser kleineren Liste verbieten kann.

Specops Breached Password Protection Complete ist eine deutlich größere Liste verbotener Passwörter und umfasst derzeit mehr als 5 Milliarden eindeutige kompromittierte Passwörter.

Microsofts Passwort-Bewertungsmodell: „Five wrongs make a right“

Schritt 1: Normalisierung

Zunächst wird der eingegebene Passwortwert in Kleinbuchstaben umgewandelt. Laut Microsoft werden gängige Leetspeak-Zeichenersetzungen ebenfalls rückgängig gemacht, jedoch werden einige häufige Ersetzungen wie €→e und 8→b ignoriert.

Mit aktivierter Zeichenersetzung blockiert Specops Password Policy gängige Leetspeak-Zeichen, einschließlich der folgenden, die von Microsoft nicht berücksichtigt werden:

4 = a; € = e; 6 = g; 7 = t; 8 = b; 9 = g; § = s

Schritt 2: Fuzzy-Match-Prüfung

Der normalisierte Wert wird gegen die Sperrlisten geprüft. Dabei werden exakte Übereinstimmungen sowie Abweichungen von +/- 1 Zeichen berücksichtigt.

Schritt 3: Substring-Prüfung

Der normalisierte Wert wird zusätzlich mit dem Vornamen, dem Nachnamen und dem Tenant-Namen des Benutzers abgeglichen. Teilübereinstimmungen (z. B. „Jeff“ für „Jeffrey“) werden jedoch ignoriert. Specops Password Policy kann hingegen die vollständige oder teilweise Verwendung des Vor- oder Nachnamens eines Benutzers blockieren.

“Selbst wenn ein Benutzerpasswort ein verbotenes Passwort enthält, kann es dennoch akzeptiert werden, sofern das Gesamtpasswort ansonsten stark genug ist.”

Microsoft blockiert die Verwendung von Passwörtern aus der „Liste der weltweit verbotenen Passwörter“ oder einer konfigurierten benutzerdefinierten Sperrliste nicht vollständig. Stattdessen ist die Verwendung eines verbotenen Begriffs nur ein Teil der Bewertungslogik von Microsoft.

Um den Passwortfilter zu bestehen, muss ein Eintrag 5 Punkte erreichen. Die Verwendung eines verbotenen Wortes zählt dabei nur einen Punkt und ist somit allein nicht ausreichend, um ein Passwort zu blockieren.

Schritt 4: Endgültige Bewertung

Wenn der normalisierte Wert alle vorherigen Prüfungen besteht, vergibt Microsoft eine Punktzahl. Es gibt einen Punkt für jede exakte Übereinstimmung mit einem Wort der globalen Sperrliste, mit einem Wort der benutzerdefinierten Sperrliste oder mit jedem verbleibenden eindeutigen Zeichen.

Ein Eintrag muss alle Prüfungen bestehen und mindestens 5 Punkte erreichen, um akzeptiert zu werden.

Beispielbewertung:

Micr0soft1! [microsoft] + [1] + [!] = 3 → Abgelehnt

Micr0soft124! [microsoft] + [1] + [2] + [4] + [!] = 5 → Akzeptiert

Das bedeutet, dass Microsoft auch Passwörter akzeptiert, die Wörterbuchbegriffe oder bekannte kompromittierte Passwörter enthalten.

Einschränkungen der benutzerdefinierten Sperrliste von Microsoft

Dies ist ein Konkurrenzangebot von Microsoft zu den benutzerdefinierten Wörterbuchlisten von Specops Password Policy.

Die „Custom Banned Password List" ist auf 1.000 Wörter begrenzt, und jeder Eintrag muss mindestens 4 Zeichen lang sein. Dreistellige Kombinationen sind in vielen Unternehmen jedoch sehr verbreitet. Aufgrund der Begrenzung auf 4 Zeichen können folgende Inhalte nicht blockiert werden:

- Kurze Firmennamen oder Akronyme (z. B. IBM, DSW, CBS, FOX, CNN, UPS, CVS, ATT, 3M)
- Kurze Börsensymbole (z. B. GE, BBD, GM, BMY)
- Flughafencodes (z. B. JFK, LHR, LAX, CDG, DXB, ARN, YYZ, FRA)
- Interne Abkürzungen (z. B. Produktkürzel wie SPP, BPP, SSD)

Specops Password Policy kann die Verwendung jedes beliebigen Wortes aus benutzerdefinierten Wörterbüchern auch innerhalb längerer Passwörter blockieren.

Die Wörterbuchlisten von Specops Password Policy sind nicht begrenzt und erlauben Einträge beliebiger Länge.

Microsoft blockiert außerdem nicht immer Wörter aus der „Custom Banned Password List". Aufgrund des „Five Wrongs Make a Right"-Scoring-Modells kann ein verbotener Begriff dennoch Teil eines längeren Passworts sein und akzeptiert werden.

Schwache Passwörter, die in Azure AD akzeptiert werden

Specops124!

[specops] + [1] + [2] + [4] + [!] = 5 → Akzeptiert

Password998!

[password] + [9] + [9] + [8] + [!] = 5 → Akzeptiert

PasswordPasswordPasswordPassword9

[password] + [password] + [password] + [password] + [9] = 5 → Akzeptiert

Kompromittierte Passwörter

Die bekannten Passwort-Leaks „Collections #1–#5“ enthalten mehr als eine Milliarde kompromittierte Passwörter. Microsoft ignoriert diese Daten jedoch zusammen mit weiteren Drittanbieter- und realen Angriffsdatensätzen in seiner „Liste der weltweit verbotenen Passwörter“. Dadurch bleiben Benutzer weiterhin gefährdet.

Nachfolgend einige Beispiele häufig verwendeter komplexer Passwörter aus Collection #2, die den Microsoft Password Protection Filter passieren:

Von Azure AD akzeptierte geleakte Passwörter

- FQRG7CS493
- Sojdlg123aljg
- D1lakiss
- Indya123

Die Denylist von Specops Password Policy enthält diese sowie über 5 Milliarden weitere bekannte kompromittierte Passwörter.

Wann prüft Entra auf Kompromittierung?

Obwohl Microsoft die Entfernung von Passwortabläufen empfiehlt, prüft Microsoft Entra (Azure AD) Password Protection ausschließlich kompromittierte Passwörter bei einer Zurücksetzung oder Änderung des Passworts.

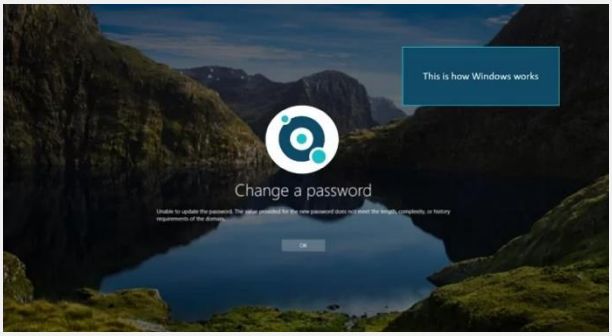
„Wenn Benutzer ihre Passwörter ändern oder zurücksetzen, werden diese Sperrlisten geprüft, um die Verwendung sicherer Passwörter durchzusetzen.“
Microsoft empfiehlt zwar häufig ausdrücklich die Abschaffung von Passwortabläufen, doch viele Organisationen sind dafür noch nicht bereit. Allerdings verfügt Microsoft Entra (Azure AD) Password Protection über keine Methode, um kompromittierte Passwörter außerhalb von Änderungen oder Zurücksetzungen zu überprüfen. Weniger Ablaufereignisse bedeuten daher, dass Passwörter von Entra-geschützten Benutzern nur sehr selten auf Kompromittierung geprüft werden.

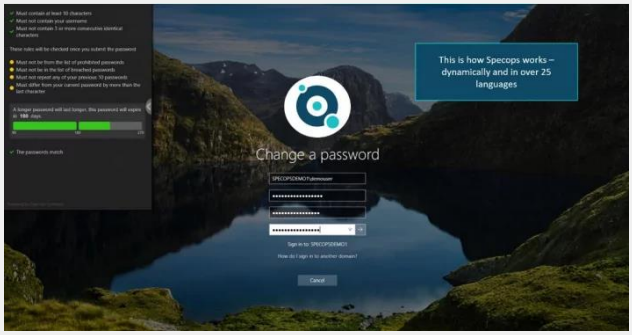
Specops Password Policy bietet hingegen kontinuierlichen Schutz vor der Verwendung kompromittierter Passwörter. Dies wird durch tägliche Prüfungen gegen eine täglich aktualisierte Datenbank sowie zusätzlich bei jeder Passwortänderung sichergestellt.

Benutzererfahrung ist ebenfalls eingeschränkt

Microsoft Entra Password Protection führt wahrscheinlich zu einer erhöhten Anzahl von Anrufen beim IT-Service-Desk.
„Microsoft Entra (Azure AD) Password Protection hat keine Kontrolle über die spezifische Fehlermeldung, die auf dem Client angezeigt wird, wenn ein schwaches Passwort abgelehnt wird."

Microsoft Entra Password Protection führt aus zwei Hauptgründen wahrscheinlich zu mehr Supportanfragen beim IT-Service-Desk.





Die Fehlermeldungen sind unklar und zeigen dem Benutzer nicht eindeutig, welche Änderungen am Passwort erforderlich sind, damit es akzeptiert wird.

Mit Specops Password Policy erhalten Benutzer dagegen bereits während der Eingabe dynamisches Feedback zur Passwortänderung. Zusätzlich können Administratoren die angezeigten Meldungen individuell anpassen, einschließlich der Anzeige des gefundenen Wörterbuchbegriffs.

#2 – Komplexität des Microsoft Entra (Azure AD)Passwort-Scorings

Das in Microsoft Entra Password Protection verwendete Scoring-Modell ist komplex. Die Protokolle für IT-Administratoren zeigen lediglich, dass ein Passwort abgelehnt wurde, weil es auf der globalen oder benutzerdefinierten Sperrliste gefunden wurde. Sie geben jedoch nicht an, welche Liste oder welcher Eintrag betroffen war.

Diese mangelnde Transparenz über die zugrunde liegenden Regeln erschwert es dem IT-Service-Desk erheblich, Probleme beim Setzen von Passwörtern korrekt zu identifizieren.

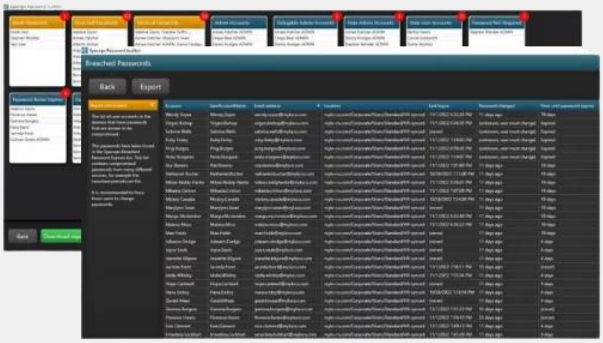
Mit Specops Password Policy hingegen zeigen Administrator-Logs exakt an, in welcher Passwortliste der abgelehnte Eintrag gefunden wurde.

Was empfehlen wir?

Sie müssen Entra ID nicht ersetzen, um stärkere Passwortrichtlinien zu implementieren oder die Nutzung kompromittierter Passwörter zu verhindern.
Stattdessen können Sie Specops Password Policy und Breached Password Protection einsetzen, um diese Richtlinien in Ihrer On-Premises-Umgebung durchzusetzen. Zusätzlich können Sie eine Federation-Lösung oder Microsoft Entra (Azure AD) Password Writeback verwenden, um diese Richtlinien auch in hybriden Umgebungen anzuwenden.

Prüfen Sie, wie viele Ihrer Entra-ID-Benutzer noch kompromittierte Passwörter verwenden

Specops Password Auditor ist ein kostenloses, schreibgeschütztes Tool, das Active-Directory-Benutzerkonten analysiert und deren Passwörter gegen eine Liste kompromittierter Passwörter überprüft.



Viele unserer Kunden, die sich ausschließlich auf Microsoft Entra (Azure AD) Password Protection verlassen haben, waren überrascht, wie viele kompromittierte Passwörter tatsächlich noch im Einsatz waren, nachdem sie einen Scan mit dem Password Auditor durchgeführt hatten.

Denn bereits ein einziges kompromittiertes Passwort reicht aus, um ein erhebliches Sicherheitsrisiko zu erzeugen. Laden Sie hier Ihre kostenlose Version von Specops Password Auditor herunter.

Demo von Specops Password Policy anfordern

Specops Password Policy verbessert die Passwortsicherheit in On-Prem-Microsoft-Active-Directory- oder hybriden Entra-ID-(Azure-AD-)Umgebungen. Die Lösung kann auf jeder GPO-Ebene sowie für Gruppen, Benutzer oder Computer angewendet werden und unterstützt Passwortkomplexität, Wörterbücher und Passphrasen. Mithilfe von Specops Breached Password Protection können IT-Teams über 4,5 Milliarden eindeutige kompromittierte Passwörter blockieren. Diese stammen aus realen Angriffen und bekannten Leak-Datenbanken und erleichtern die Einhaltung von Standards wie NIST oder NCSC.

Wenn Sie erfahren möchten, wie Specops Password Policy und Breached Password Protection in Ihrer Umgebung eingesetzt werden können, können Sie hier eine kostenlose Demo- oder Testversion des Tools „Active Directory Password Policy Protection„ anfordern.