COMMENT UTILISER « REGEX » POUR IMPLEMENTER DES PASSPHRASES DANS VOTRE ACTIVE DIRECTORY ?

Ce livre blanc pratique vous aidera à comprendre comment utiliser les regex pour mettre en œuvre une politique de phrase de passe dans votre Active Directory.

À PROPOS DE SPECOPS. Specops Software est le principal fournisseur de solutions de gestion des mots de passe et d'authentification. Specops protège les données de votre entreprise en bloquant les mots de passe faibles et en sécurisant l'authentification des utilisateurs.

La CNIL a renouvelé ses recommandations en matière de sécurité des mots de passe en octobre 2022. L'agence suggère l'utilisation de passphrases afin d'atteindre une entropie recommandée de 80 bits ou plus.

Ce document examine les raisons pour lesquelles les passphrases pourraient être une solution à votre problème de mot de passe faible. Il s'intéresse également à la question de savoir pourquoi elles n'ont pas été largement adoptées. Et vous indiquera comment créer une politique de phrase de passe en utilisant Regex.

POURQUOI LES PASSPHRASES CONSTITUENT LE MEILLEUR FORMAT DE MOTS DE PASSE ?

Premièrement, qu'est-ce qu'une phrase de passe ? Une phrase de passe est un moyen beaucoup plus simple pour créer un mot de passe plus fort et plus facilement mémorisable qu'un mot de passe classique. Une phrase de passe est donc un mot de passe qui utilise une technique unique pour sa création. La meilleure façon d'illustrer cela est de prendre un exemple concret de deux mots de passe qui seraient tous deux considérés comme des mots de passe forts.

- Mot de passe traditionnel : l$RhO3M65KJjp
- Phrase de passe : parasolzebralampechocolat

Comme vous pouvez le voir dans les deux exemples ci-dessus, il s'agit dans les deux cas de mots de passe forts. Il est assez peu probable que quelqu'un mémorise facilement le premier mot de passe. La phrase de passe, en revanche, bien que forte, est beaucoup plus lisible et plus facile à mémoriser pour les utilisateurs.

Permettre aux utilisateurs de créer des passphrases en plus des mots de passe, leur offre la possibilité de recourir aux techniques des premières pour créer des mots de passe forts et faciles à mémoriser. Cela encourage également les utilisateurs à rompre le cycle de l'utilisation de mots de passe périmés, faibles et réutilisés sur plusieurs systèmes.

LES DIFFICULTES LIEES A L'UTILISATION DE PASSPHRASES DANS ACTIVE DIRECTORY

La plupart des organisations utilisent aujourd'hui Active Directory Domain Services de Microsoft comme solution d'authentification sur site pour la gestion des identités et des accès, ce qui n'est pas sans poser de problèmes aux administrateurs qui cherchent à renforcer la sécurité de leurs

mots de passe. Il lui manque en effet plusieurs éléments clés nécessaires à la sécurité des mots de passe.

Les limites concernant la sécurité des mots de passe dans Active Directory sont les suivantes :

- Vous ne pouvez pas interdire les mots de passe spécifiques au contexte ;
- Absence de blocage incrémentiel des mots de passe ;
- Pas de système de détection native des mots de passe compromis ;
- Sans un filtre de mot de passe personnalisé .DLL, vous ne pouvez pas facilement bloquer les mots du dictionnaire de mots de passe ;
- Aucun moyen de renforcer la prise en charge des phrases de passe.

Concentrons-nous sur l'impossibilité de bloquer les mots spécifiques, relatif au contexte de votre organisation, qui peuvent être utilisés dans les mots de passe. Qu'est-ce que cela signifie ? Les attaquants utilisent souvent le nom de l'entreprise ou d'autres mots relatifs à l'entreprise visée lorsqu'ils tentent de forcer des mots de passe par force brute ou lors d'attaques par pulvérisation de mots de passe.

UTILISATION EFFICACE DE REQUETES REGEX DANS VOTRE ACTIVE DIRECTORY

Qu'est-ce que Regex ? Regex est l'abréviation de « regular expression » (expression régulière). Un modèle regex est une séquence de caractères qui définit un modèle de recherche utilisé pour faire correspondre des caractères ou des sections d'un texte. Ces motifs regex peuvent être un moyen puissant de trouver et de faire correspondre des motifs spécifiques, comme ceux que l'on trouve souvent dans les mots de passe.

Quelles vérifications peuvent être effectuées avec des requêtes regex par rapport aux mots de passe des utilisateurs dans un environnement ? Avec les requêtes regex, les possibilités sont infinies. Toutefois, à titre d'exemple, Regex peut aider à identifier et à filtrer les éléments de passphrases suivants dans votre environnement Active Directory et peut être utilisé avec des exigences personnalisées pour définir les passphrases dans votre environnement. Voici quelques solutions regex efficaces que vous pouvez déployer dans votre Active Directory :

- Répétition ;
- Vérification des caractères qui précèdent et qui suivent ;

- Blocage des mots du dictionnaire ;
- Blocage des caractères consécutifs ;
- Application d'un formatage spécifique de la phrase de passe.

Examinons ces exemples et voyons comment les requêtes regex peuvent être utilisées pour filtrer chacun de ces éléments :

1. Blocage des caractères répétitifs

Une manière simple de bloquer les caractères répétitifs est d'enfermer n'importe quel caractère entre parenthèses et de le faire correspondre avec la \1 de la manière suivante :

```
(.)\1
```

2. Recherche avant et après

Vous pouvez rechercher un ensemble spécifique de caractères, qui se trouvent fréquemment avant ou après un caractère dans un enchaînement, en utilisant les méthodes suivantes :

```
Ahead: (?=abc)

Behind: (?!abc)
```

3. Bloquer les mots du dictionnaire

Vous pouvez utiliser efficacement Regex pour bloquer des mots ou des chaînes de caractères spécifiques dans les phrases de passe. Dans l'exemple ci-dessus, si nous voulons bloquer et exclure des mots spécifiques des phrases de passe, comme le nom de la société, nous pouvons le faire en utilisant ce qui suit :

```
^(?!.*wackywidgets).*$
```

Si vous souhaitez bloquer plusieurs combinaisons de mots spécifiques, vous pouvez également le faire avec Regex. Par exemple, pour exclure plusieurs combinaisons de mots de passe, nous pouvons utiliser ce qui suit :

```
^(?!.*[pP][aA@][sS$][sS$][wW][oO0][rR][dD]).*$
```

4. Bloquer les caractères consécutifs

Si vous souhaitez bloquer les caractères consécutifs dans les phrases de passe, vous pouvez le faire en utilisant la chaîne regex suivante :

```
^(?!.*(.)\1\1).*$
```

5. Appliquer un formatage spécifique des phrases de passe

Lors de l'utilisation de phrases de passe, de nombreuses organisations voudront imposer des caractéristiques spécifiques aux phrases de passe. Il peut s'agir du nombre de mots devant être utilisés dans une série et du nombre de caractères devant être contenus dans chaque mot. Si nous voulons l'appliquer à chaque mot de six caractères, nous pouvons le faire avec ce qui suit :

```
\w{6,}
```

Les exemples suivants correspondent à un mot de six caractères suivi d'un espace :

```
\w{6,}\s+
```

Si vous souhaitez autoriser les caractères majuscules et minuscules dans trois mots, puis autoriser l'utilisation de chiffres, de caractères spéciaux et de toutes les majuscules dans la phrase de passe, vous pouvez le faire avec les paramètres suivants :

```
^\S{6,}\s+\S{6,}\s+\S{6,}$
```

COMMENT SPECOPS PASSWORD POLICY UTILISE REGEX ?

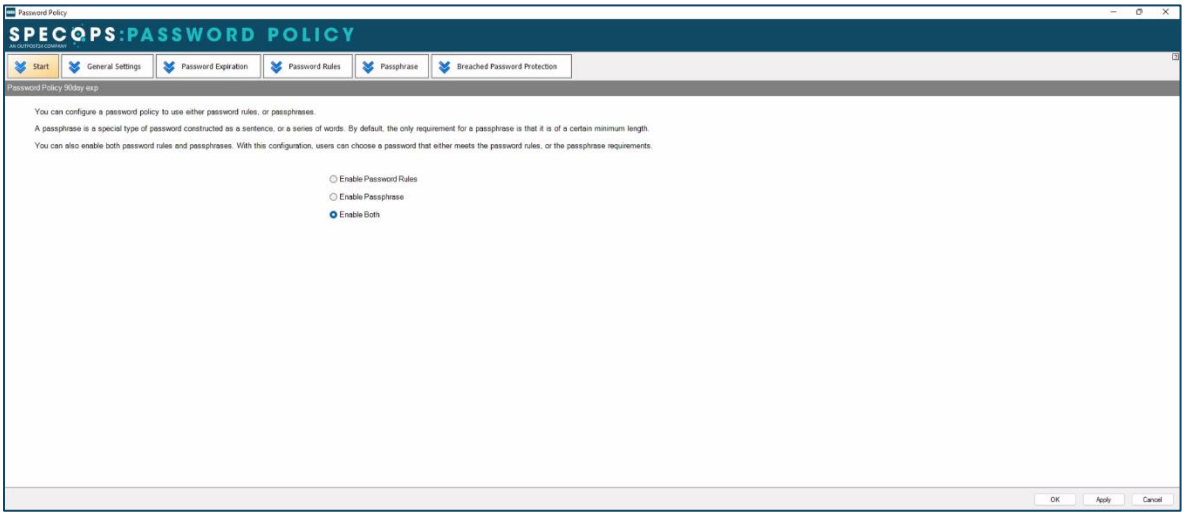
Nous l'avons vu, Active Directory est limité dans ses outils et ses solutions natifs pour empêcher les utilisateurs de recourir à des éléments de mot de passe dangereux. Bien que vous puissiez

utiliser une .dll de filtre de mot de passe personnalisée, cela nécessite de l'expérience en développement et une maintenance constante, nécessaire à l'entretien de la solution.

Specops Password Policy est une solution robuste de sécurité concernant les mots de passe, capable de renforcer les capacités natives d'Active Directory et permettant aux organisations de mettre en application les toutes dernières recommandations en matière de sécurité des mots de passe.

Specops Password Policy permet, non seulement aux organisations de mettre en œuvre efficacement et d'encourager l'utilisation de passphrases dans leur environnement, mais il leur permet également d'utiliser la puissance de Regex pour créer un filtrage efficace des mots de passe dans Active Directory, basé sur des modèles ou des phrases réputés faibles ou vulnérables, de façon automatisée.

Specops Password Policy permet aux utilisateurs de recourir à des mots de passe forts, des phrases de passe, ou aux deux.

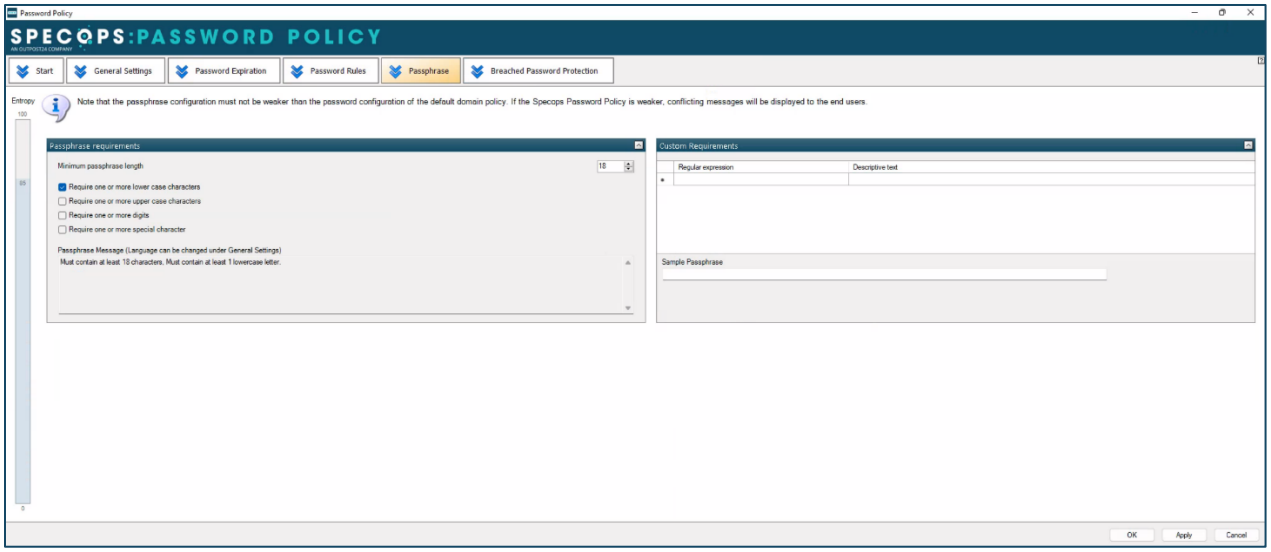


Specops Password Policy permet de créer des politiques avec des mots de passe et des phrases de passe.

(Source : Specops)

Lorsqu'ils utilisent des passphrases dans leur environnement, les administrateurs peuvent vouloir exclure certains éléments de l'utilisation des passphrases créées par les utilisateurs.

Par exemple, les administrateurs peuvent utiliser des expressions régulières pour exclure des composants spécifiques des passphrases et appliquer certaines caractéristiques dans l'onglet de configuration des phrases de passe.



Utilisation de regex avec Specops Password Policy pour renforcer les phrases de passe.

(Source : Specops)

La section des exigences personnalisées peut contenir diverses requêtes regex pour imposer et exclure l'utilisation d'éléments de phrase de passe dans l'organisation.

UTILISATION DE PASSPHRASES ET DE REGEX DANS VOTRE AD A L'AVENIR

Les passphrases représentent une technique plus avancée pour créer des mots de passe forts au sein d'un environnement. Leur force provient de la longueur et de l'identité unique de la phrase de passe. Cependant, les administrateurs souhaitent toujours être en mesure de contrôler et d'exclure certains termes ou mots des passphrases pour une sécurité accrue.

Ces paramètres personnalisés autour des passphrases peuvent mis en place en utilisant des requêtes regex. Specops Password Policy fournit des outils et des solutions robustes pour encourager l'utilisation de mots de passe forts et de passphrases dans un environnement, y compris l'utilisation de Regex pour exiger ou exclure certains éléments de phrase de passe.

Découvrez-en davantage à propos de Specops Password Policy, ou essayez-le gratuitement à tout moment dans votre Active Directory avec un compte d'essai.