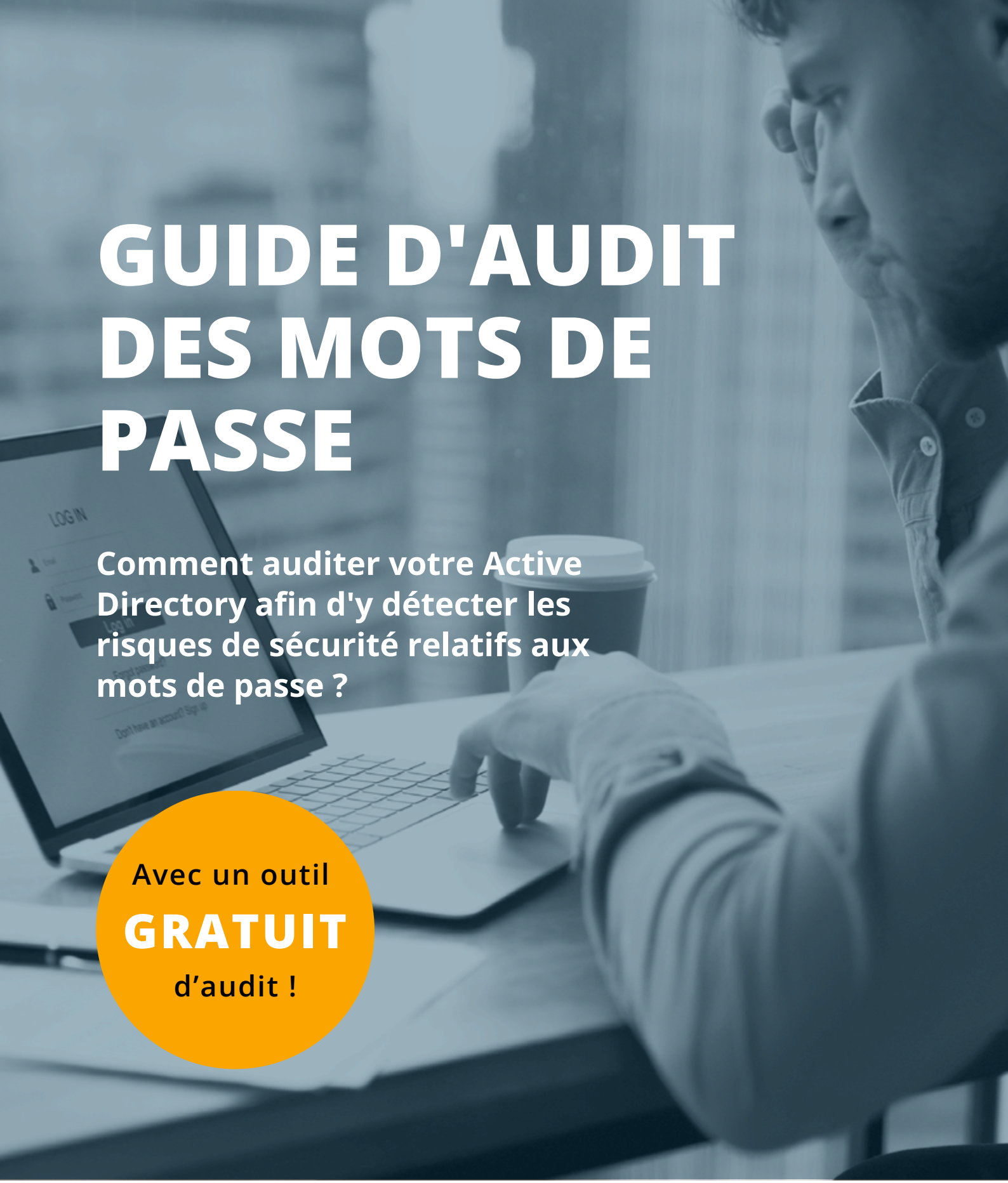


GUIDE D'AUDIT DES MOTS DE PASSE

Comment auditer votre Active Directory afin d'y détecter les risques de sécurité relatifs aux mots de passe ?

Avec un outil
GRATUIT
d'audit !

UN LIVRE BLANC SPECOPS

SPECOPS
AN OUTPOST24 COMPANY

SOMMAIRE

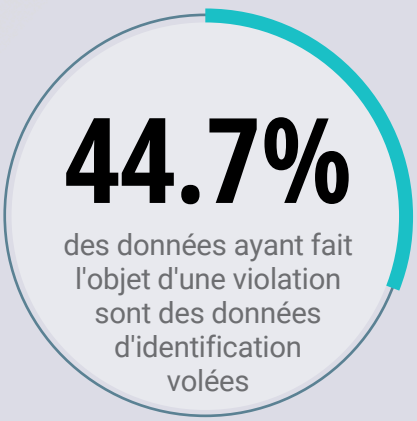
Pourquoi auditer votre environnement Active Directory ?

DARREN JAMES
Chef de produit senior

Selon le rapport 2023 Data Breach Investigation Report de Verizon, les informations d'identification volées sont impliquées dans 44,7 % de toutes les violations de données. Il existe beaucoup de mots de passe faibles et/ou compromis et chacun d'entre eux représente une voie d'attaque potentielle dans votre organisation. Une politique de mots de passe solide est une mesure de cybersécurité efficace, pourtant même les mots de passe les plus forts peuvent être compromis sans que vous en ayez connaissance immédiatement.

Les entreprises se concentrent souvent sur les cyber-attaques les plus sophistiquées, car les mots de passe ne sont pas une nouveauté - nous les utilisons depuis des années. Pourtant, les identifiants volés sont le moyen le plus facile de pénétrer dans un système informatique et les attaquants paient cher pour obtenir des listes d'identifiants piratés. Si les cybercriminels sont si friands de vols d'identifiants, c'est parce qu'ils savent que les mots de passe compromis sont le moyen le plus simple de franchir les défenses de cybersécurité d'une organisation. En d'autres termes, il est bien plus facile de se connecter que de pirater.

Alors comment éradiquer les mots de passe problématiques et sécuriser nos entreprises ?



L'audit de votre Active Directory peut réserver sont lot de surprises (souvent préoccupantes), comme des comptes inactifs avec des mots de passe compromis, des comptes surprivilégiés avec des mots de passe faibles, ou même une politique de mauvaise sécurité d'accès répandue à l'échelle de l'organisation. Le point commun de tous ces éléments est qu'ils offrent aux attaquants des voies d'accès faciles à votre organisation - voies qui peuvent pourtant être bloquées grâce à des solutions relativement simples.

À l'aide de données issues de notre analyse des mots de passe compromis et des mots de passe découverts lors d'attaques en cours sur le réseau de pots de miel de notre équipe, ce rapport vous présente les étapes clés nécessaires pour débarrasser votre organisation des mots de passe à risque. Nous vous proposons également un outil gratuit pour vous aider à mettre tout cela en place.

Bon audit !

Un audit de votre Active Directory peut réserver bien des surprises

PARTIE 1

Le problème des mots de passe faibles

Les attaques par force brute sont l'une des méthodes les plus courantes utilisées par les cybercriminels pour exploiter des mots de passe faibles. Ces attaques sont principalement un moyen de deviner rapidement des mots de passe afin d'accéder à des actifs ou à des systèmes protégés par mot de passe. Les cybercriminels utilisent des outils pour tester toutes les combinaisons de mots de passe possibles au travers d'innombrables tentatives de connexion jusqu'à ce que la bonne

Ces attaques commencent généralement par une liste de dictionnaire de mots de passe courants, probables et même compromis, que l'on confronte de façon systématique au compte de courrier électronique d'un utilisateur afin d'obtenir l'accès à un compte donné. Les attaquants savent que leur chances de réussir sont élevées, car nombreuses sont les personnes qui utilisent et réutilisent les mêmes mots de passe très faibles.

Notre équipe de recherche a analysé un sous-ensemble de plus de 4,6 millions de mots de passe collectés sur plusieurs semaines sur le réseau de pots de miel de notre équipe. Selon vous, quel était le terme de base le plus courant trouvé dans ces mots de passe ? La réponse est à la fois déprimante et peu surprenante pour les professionnels de la sécurité informatique : « Password ».

Le terme de base le plus courant que nous ayons trouvé ? "Password"

Un nombre inquiétant d'entreprises s'appuient encore sur des mots de passe de 8 caractères, conformément au paramètre par défaut d'Active Directory. Ce n'est pas assez long - les mêmes données sur les mots de passe d'octobre 2022 révèlent que 88 % des mots de passe utilisés dans des attaques réelles comportaient 12 caractères ou moins. La longueur de mot de passe la plus courante était de 8 caractères, soit près de 24 % de ces mots de passe. Leur complexité est également un problème. Les mots de passe ne contenant que des lettres minuscules étaient la combinaison de caractères la plus courante, représentant 18,82 % de l'ensemble.

Les attaquants savent que les gens sont aussi souvent inspirés par des événements mondiaux ou culturels. Par exemple, nous avons constaté une forte augmentation des mots de passe liés au football (soccer si vous êtes aux États-Unis) à l'époque de la Coupe du Monde FIFA 2022. Mais cela peut être encore plus simple : un attaquant essayant « septembre » comme mot de passe de base lors d'une attaque par force brute au cours du mois de septembre rencontrerait probablement un certain succès.

Pourquoi les gens créent-ils encore de mauvais mots de passe en 2024 ? C'est dans la nature humaine : personne n'aime être dérangé par une notification « il est temps de changer votre mot de passe ». Les gens ont tendance à éviter ce qu'ils considèrent comme un stress et un effort inutiles, c'est pourquoi ils créent des mots de passe courts, faciles à retenir et les réutilisent. Cependant, cela n'est possible que si une organisation le permet. C'est là qu'interviennent les politiques de mots de passe.

L'ANALYSE DE SPECOPS

Qu'est-ce qui rend un mot de passe fort ?

En augmentant la longueur des mots de passe au-delà des 8 caractères fréquemment exigés, le nombre de mots de passe potentiels monte en flèche, ce qui rend les attaques par force brute exponentiellement plus difficiles, même avec de grandes quantités de puissance de calcul. Nous recommandons toujours une longueur d'un mot de passe supérieure à 15 caractères au minimum, et idéalement supérieure à 20.

Les passphrases composées de trois mots aléatoires sont le meilleur moyen d'y parvenir tout en restant facilement mémorisables. Par exemple : "brocoli-marine-escalier" est plus facile à mémoriser qu'une suite de huit caractères aléatoires. Au lieu d'ajouter de la complexité en ajoutant à cela des caractères spéciaux, il peut être tout aussi efficace de délibérément mal orthographier l'un des mots, créant ainsi une passphrase forte qui n'est pas trop difficile à mémoriser : "brokkolimarine-escalier".

Des mots de passe plus longs ne signifient pas nécessairement une mauvaise expérience utilisateur. Les meilleures solutions guident les utilisateurs grâce à des commentaires dynamiques lors de la création du mot de passe, les aidant ainsi à voir en temps réel les exigences auxquelles ils tentent de répondre. Les organisations peuvent également recourir au vieillissement basé sur la longueur, dans lequel les personnes sont récompensées pour avoir créé des mots de passe forts avec un délai plus long jusqu'à la prochaine réinitialisation du mot de passe.

DARREN JAMES | Chef de produit senior

PARTIE 2

Les mots de passe compromis : un danger caché

Les mots de passe faibles représentent un véritable problème, mais il serait erroné de penser que chaque violation de données liée à un mot de passe est due à la paresse ou à l'ignorance des gens. Les recherches effectuées par Specops montrent que 83 % des mots de passe compromis satisfont les conditions de longueur et de complexité des normes réglementaires en matière de mots de passe, notamment celles des NIST, PCI, HITRUST pour HIPAA, ICO pour RGPD, et Cyber Essentials/ NCSC. Que se passe-t-il donc ?

Si des mots de passe professionnels ont été réutilisés, c'est pour les pirates un moyen facile d'entrer dans l'organisation de l'employé

Imaginons que chaque membre d'une organisation dispose d'un mot de passe long et complexe, cela ne serait pas pour autant synonyme de sécurité. car si un même mot de passe est utilisé pour de nombreux appareils et applications, il suffit d'un lien malveillant pour tout compromettre. Un email d'hameçonnage, un réseau public non sécurisé ou un appareil personnel infecté par un logiciel malveillant peuvent chacun conduire à la compromission d'un mot de passe dans la vie personnelle d'un utilisateur final. S'il a réutilisé son mot de passe professionnel, cet incident cybernétique initialement sans rapport peut entraîner une chaîne d'événements ayant un impact sur votre organisation.

L'un des plus grands risques est que des pirates parviennent à mettre la main sur une base de données de mots de passe provenant d'un site web moins sécurisé ou d'une application SaaS. Supposons par exemple qu'un pirate s'introduise dans une boutique en ligne et s'empare de la totalité d'une base de données de mots de passe. Même si ceux-ci sont hachés, le pirate aura tout le temps d'essayer de les déchiffrer, puis de découvrir qui sont les personnes à qui ils appartiennent et où elles travaillent. Si des mots de passe professionnels ont été réutilisés, cela constitue un moyen facile d'entrer dans l'organisation de l'employé.

Le second problème est que les organisations peuvent ne pas être en mesure de savoir si les informations d'identification d'un employé ont été compromises jusqu'à ce qu'une attaque soit en cours. L'institut Ponemon estime qu'il faut en moyenne 207 jours à une organisation pour découvrir une faille. Un pirate disposant d'un mot de passe compromis pourrait ne pas être découvert pendant une longue période, en particulier si une organisation fait le choix de ne pas scanner son environnement Active Directory en le confrontant à des listes de mots de passe compromis connus.

Le vol d'identifiants est une affaire importante. Les identifiants de connexion capturés lors de violations de données sont régulièrement vendus sur le marché du Crime-as-a-Service pour être utilisés dans d'autres piratages. En février 2022 par exemple, le fabricant de GPU Nvidia a été victime d'une violation massive de données menée par le groupe de ransomware LAPSUS$. L'acteur de la menace s'est introduit dans leur réseau pour voler et divulguer des milliers de mots de passe de leurs employés, obligeant Nvidia à modifier ses mots de passe à l'échelle de l'entreprise.

Specops a pu récupérer 30 000 de ces mots de passe compromis lors de la fuite de données Nvidiaet les a ajoutés à sa base de données de mots de passe compromis connus. Maintenant qu'ils ne sont plus utilisés, nous pouvons dire que bon nombre de ces mots de passe compromis étaient faibles dès l'origine. Nous avons analysé l'ensemble des données pour dégager des modèles de construction de mots de passe et y avons trouvé des mots de base communs utilisés par les employés de Nvidia : 'nvidia', 'welcome', 'password', et 'qwerty'.

Ce scénario n'est pas propre à Nvidia. Sans un audit complet de leur Active Directory, de nombreux responsables informatiques n'ont pas conscience de l'ampleur des risques liés aux mots de passe au sein de leur organisation.

De nombreux responsables informatiques n'ont pas conscience de l'ampleur des risques liés aux mots de passe au sein de leur organisation.

La recherche de mots de passe compromis

De nombreux mots de passe ont été compromis au fil des ans. Cependant, il est tout simplement impossible pour quelqu'un de savoir si son mot de passe a déjà été compromis dans le passé sans utiliser un logiciel pour faire des recoupements avec une liste de mots de masse compromis connus. Et sans scan en temps réel, il est également difficile de repérer les compromissions futures. C'est pourquoi il est essentiel que les équipes informatiques disposent à la fois d'une visibilité en temps réel la plus précise sur les mots de passe compromis dans leur Active Directory ainsi que d'une politique de mots de passe sécurisée, capable de bloquer leur utilisation.

Specops Password Policy propose en option une fonction de Breached Password Protection qui compare votre Active Directory à plus de 4 milliards de mots de passe compromis uniques, offrant ainsi un moyen de vérifier en permanence si un mot de passe a été compromis. La solution vérifie les listes de mots de passe compromis vendues aux cybercriminels ainsi que les attaques en direct capturées par le réseau de pots de miel de notre équipe. Si l'on découvre qu'un utilisateur utilise un mot de passe qui a été compromis à la suite d'une violation de données, il pourra en être informé par SMS ou par email et contraint de changer de mot de passe.

DARREN JAMES | Chef de produit senior

PARTIE 3

Trois étapes pour renforcer la sécurité des mots de passe

Les mots de passe sont un domaine de la cybersécurité qui concerne tous les individus au sein d'une organisation. Trouver les vulnérabilités et mettre en œuvre une refonte à l'échelle de l'entreprise peut sembler une tâche ardue, en particulier lorsque diverses politiques ont été adoptées au fil des ans, certaines peut-être même avant votre arrivée. Nous allons essayer de simplifier les choses en présentant les trois étapes clés que toute organisation devrait suivre.

ÉTAPE 1

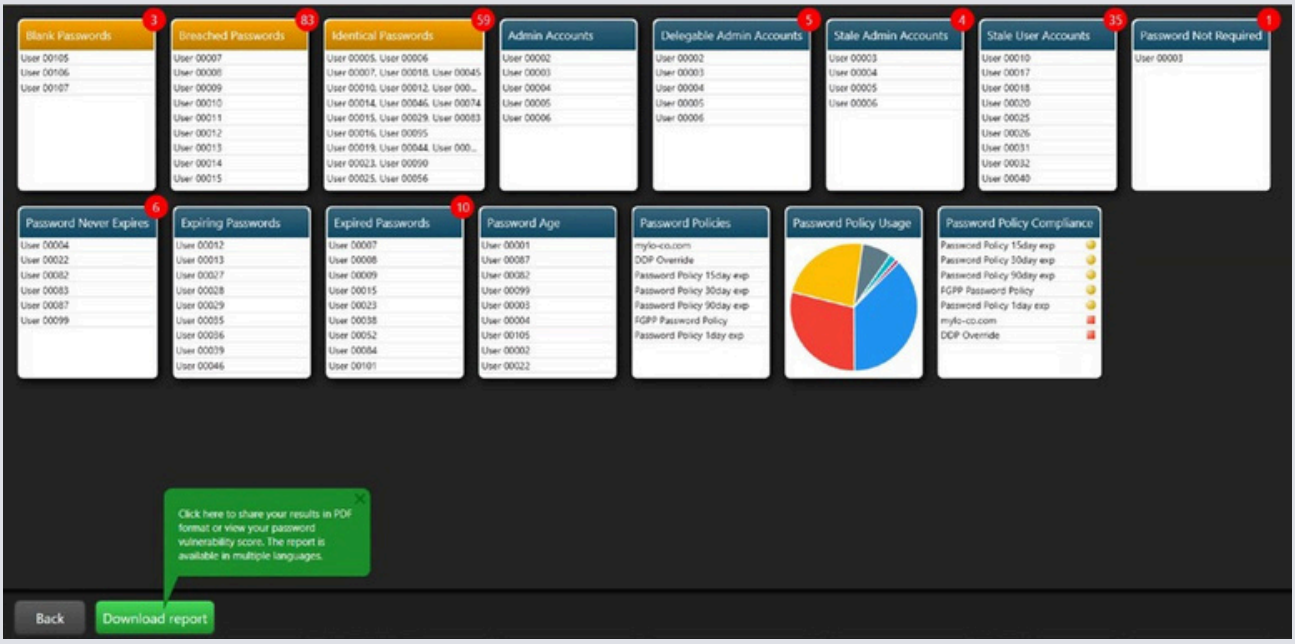
L'audit

Tout d'abord, et c'est le plus important, vous devez avoir une visibilité sur tout problème potentiel de sécurité affectant votre organisation. Au fil des années, le niveau de sécurité des mots de passe a pu se relâcher, et il est presque certain que des risques cachés - dont vous n'avez pas forcément connaissance - sont présents dans votre environnement.

Lorsque vous choisissez un outil pour analyser votre Active Directory à la recherche de vulnérabilités liées aux mots de passe, vous devez vous assurer d'avoir une visibilité sur les éléments suivants :

- Quelqu'un utilise-t-il un **mot de passe issu d'une fuite de données/compromis ?**
- Qui utilise **des mots de passe périmés, identiques ou vierges ?**
- **Dans quelle mesure sommes-nous préparés** à faire face à une attaque par force brute ?
- **Quel est le niveau de sécurité de nos comptes administrateurs clés ?**
- Avons-nous **des comptes administrateurs obsolètes/inactifs ?**
- Des comptes non sécurisés bénéficient-ils **de droits d'accès privilégiés ?**
- **Sommes-nous en conformité** avec les politiques et normes en matière de mots de passe ?

Dans la section suivante, nous allons vous montrer comment implémenter cette première étape essentielle et répondre aux questions ci-dessus en quelques minutes grâce à un outil gratuit : Specops Password Auditor.



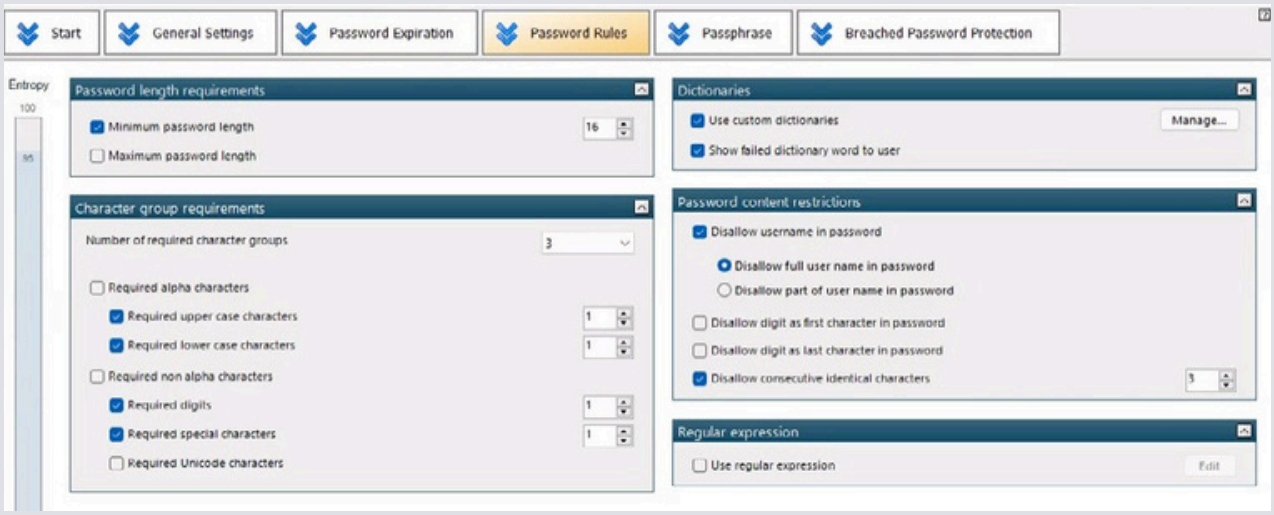
Specops Password Auditor : Tableau de bord des résultats

ÉTAPE 2

Remédier

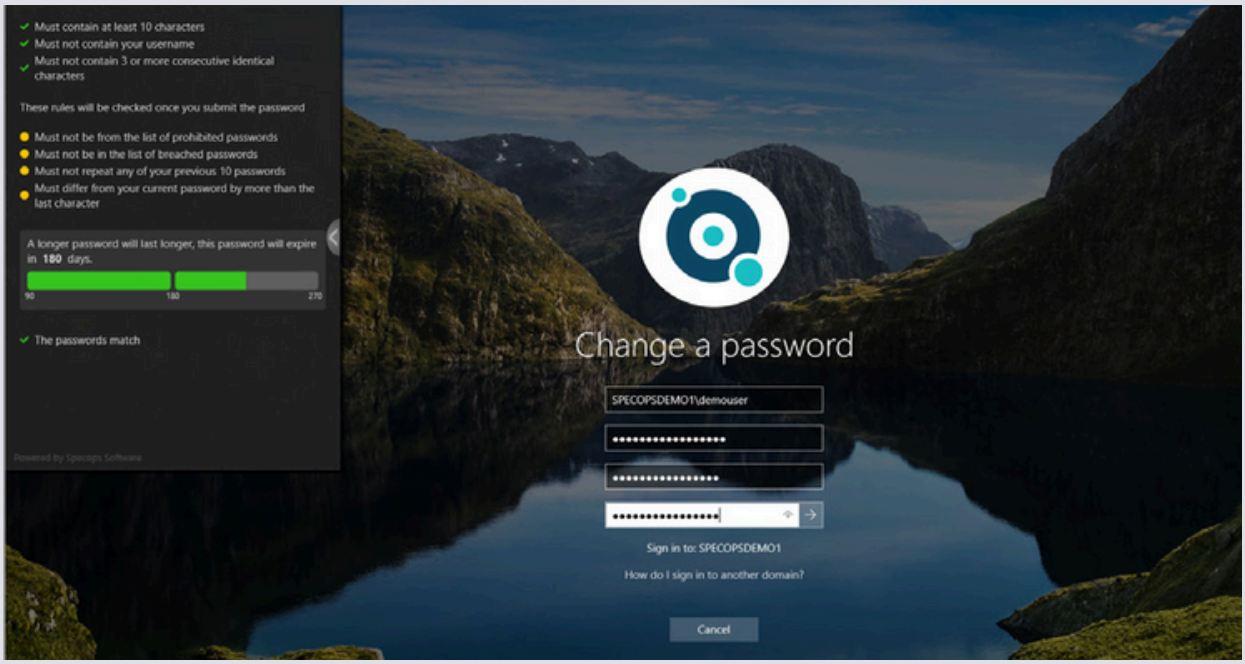
Une fois que vous disposez d'un panorama précis des vulnérabilités liées aux mots de passe, vient le temps de la remédiation des risques avec la création de politiques de mots de passe plus strictes dans votre Active Directory. Il vous faut en premier lieu définir une nouvelle politique de mots de passe qui réponde aux vulnérabilités détectées lors de votre audit. Par exemple, vous pourriez choisir d'imposer une passphrase de 20 caractères, composée de 3 mots aléatoires sans rapport entre eux.

Vous devrez ensuite imposer la réinitialisation des mots de passe à tous les utilisateurs dont les mots de passe sont faibles ou compromis. Un outil comme Specops Password Policy peut bloquer des modèles de mots de passe courants et personnaliser des dictionnaires de mots pertinents pour votre entreprise. Par exemple, vous pouvez bloquer le nom de votre entreprise, les noms de produits ou même celui des équipes sportives locales. Tout nouveau mot de passe créé sera conforme à votre politique de mots de passe mise à jour et renforcée. N'oubliez pas d'accorder une attention particulière aux comptes administrateur ou aux comptes sur-privilégiés, car ils représenteraient un préjudice majeur pour votre organisation si des pirates parvenaient à s'en emparer.



Specops Password Policy : les paramètres de la politique de mots de passe

L'expérience utilisateur est un facteur important dans cette étape, privilégiez le recours à une solution qui vous permet de personnaliser vos notifications à l'intention de l'utilisateur final. Un retour d'information dynamique au moment du changement de mot de passe peut aider à guider vos utilisateurs lorsqu'ils sont forcés de réinitialiser leur mot de passe, en les aidant à construire un mot de passe fort et facile à mémoriser. En leur proposant un vieillissement basé sur la longueur, vous montrez également aux utilisateurs que plus leur mot de passe est fort, plus longtemps ils peuvent se passer d'une nouvelle réinitialisation.



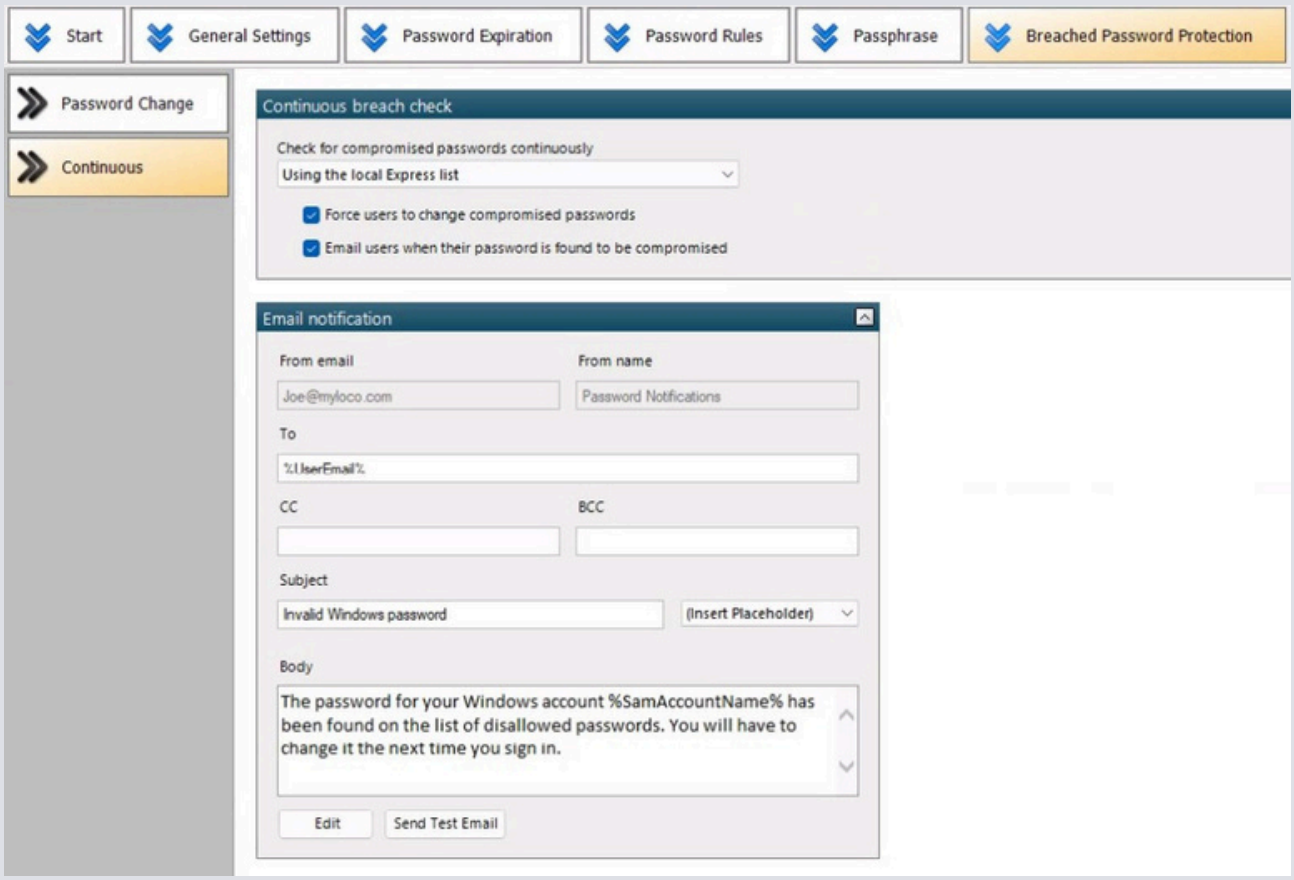
Specops Password Policy : un retour d'information dynamique pour l'utilisateur final

ÉTAPE 3

Contrôler et gérer

La sécurité des mots de passe n'est pas une tâche ponctuelle, c'est pourquoi vous devez mettre en place des processus qui vous permettront de maintenir tout le travail accompli lors de la deuxième étape. Comme nous l'avons vu, les mots de passe forts peuvent toujours être compromis, de sorte que l'élimination des mots de passe faibles et compromis découverts lors de votre audit ne vous protégera pas éternellement. C'est pourquoi Specops Password Policy est livré avec une option permettant d'inclure une fonction de protection contre les compromissions de mots de passe qui vous permet de vérifier en permanence si un mot de passe a été compromis.

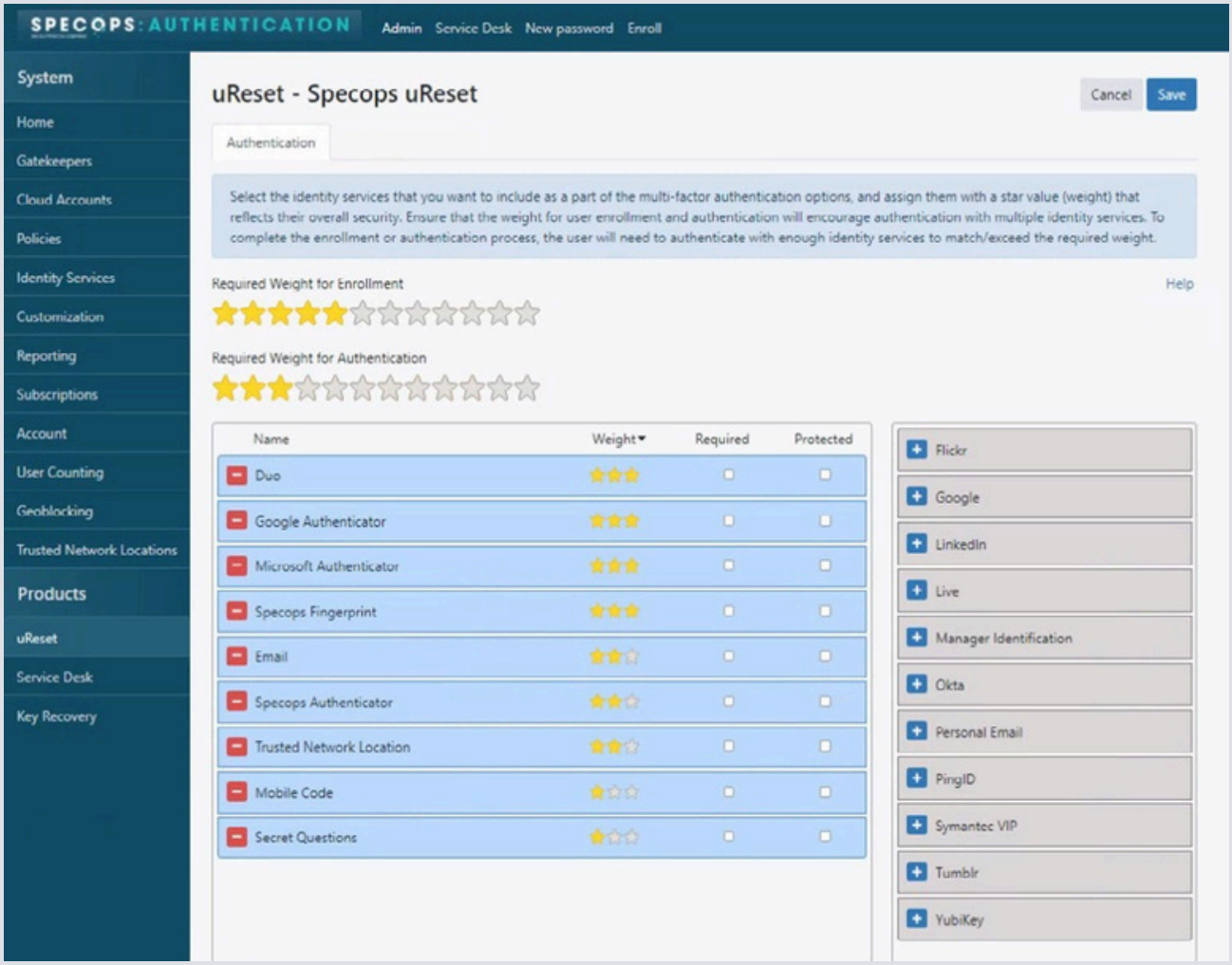
Si l'on découvre qu'un utilisateur a recours à un mot de passe compromis à la suite d'une fuite de données, il peut être contraint de changer de mot de passe. La fonction Breached Password Protection renvoie à une liste de plus de 4 milliards de mots de passe compromis, y compris ceux qui sont actuellement détectés par les comptes Honeypot de Specops.



Specops Password Policy : la fonctionnalité Breached Password Protection

Il est également utile de disposer d'un moyen simple et efficace de réinitialiser les mots de passe lorsque des compromissions sont découvertes. Dans les cas où il est nécessaire de réinitialiser les mots de passe, il est bon de disposer d'un moyen permettant aux utilisateurs de s'authentifier en toute sécurité et de réinitialiser leurs mots de passe sans faire peser une charge de travail sur le service informatique. Selon Gartner, entre 20 et 50 % des appels auprès du helpdesk concernent les réinitialisations de mots de passe. Les données de Forrester Research estiment que le coût de la main-d'œuvre pour chaque réinitialisation de mot de passe serait d'environ 70 $ - dépenses qui s'accumulent lorsque les gens continuent d'oublier leurs mots de passe après avoir été forcés d'en choisir un nouveau, unique. Et bien sûr, une fois le mot de passe réinitialisé, le cycle recommence, l'utilisateur devant créer un nouveau mot de passe.

Specops uReset peut être configuré pour fonctionner avec une gamme d'options d'authentification multi-facteurs répandues, améliorant l'expérience de l'utilisateur final lors des réinitialisations de mots de passe, réduisant par la même la charge de travail des administrateurs informatiques.



Specops uReset : options d'enrôlement et d'authentification

L'importance de l'audit

L'audit est une première étape essentielle vers la sécurité des mots de passe. Les étapes de remédiation et de gestion ne sont tout simplement pas possibles à mettre en place sans connaître au préalable l'ampleur du problème auquel vous êtes confronté. Nous avons développé Specops Password Auditor pour aider les organisations à obtenir cette visibilité initiale et à comprendre l'ampleur du problème qu'elles rencontrent. Cela peut ensuite éclairer les politiques de mot de passe qu'ils souhaitent implémenter et la façon dont ils veulent gérer les réinitialisations et la surveillance des risques à l'avenir.

DARREN JAMES | Chef de produit senior

La priorité absolue est d'avoir une visibilité sur les problèmes potentiels affectant votre organisation

PARTIE 4

Lancez votre audit dès aujourd'hui

L'audit est le point de départ de la mise en place d'une meilleure sécurité des mots de passe. Specops Password Auditor est totalement gratuit et capable d'identifier plusieurs types de vulnérabilités en seulement quelques minutes. SPA effectue une vérification en lecture seule de votre Active Directory et le confronte à 1 milliard de mots de passe compromis connus, ainsi qu'une analyse de vos politiques de mots de passe de domaine et de vos politiques de mot de passe à granularité fine.

Votre rapport exportable vous donnera une visibilité sur les vulnérabilités liées aux mots de passe suivantes :

- **Mots de passe vides**
- **Mots de passe compromis**
- **Mots de passe identiques**
- **Comptes administrateurs**
- **Comptes administrateurs déléguables**
- **Comptes administrateurs obsolète**
- **Comptes "Mot de passe non requis"**
- **Mots de passe obsolète**
- **Comptes avec mot de passe qui n'expire pas**
- **Mots de passe expirés**
- **Politiques de mots de passe + utilisation**
- **Conformité de la politique de mots de passe**

★★★★★

"À la fois puissant et facile à utiliser. La richesse des informations fournies par l'outil a été un atout majeur, en particulier la comparaison de la politique actuelle avec les meilleures pratiques du secteur."

Jesse F. (Source : Captera.com)

TELECHARGEZ Specops Password Auditor

Prêt à commencer ?

LES CARACTÉRISTIQUES DE SPECOPS PASSWORD AUDITOR

Aperçu des politiques de mots de passe y compris l'intervalle de changement, l'application du dictionnaire, ainsi que la force relative

Identifier les comptes qui utilisent **l'un des plus d'un milliard de mots de passe compromis connus**

Identifier les comptes d'utilisateurs sans **longueur minimale du mot de passe**

Identifier **les comptes utilisateurs dormants**

Rapports sur l'expiration des mots de passe pour **réduire les appels au helpdesk relatifs aux mots de passe**

Utilisation autonome ou intégration avec Specops Password Policy

Exporter les données du rapport au format CSV pour un traitement ultérieur

Générer un rapport de synthèse PDF afin de partager vos résultats avec les décideurs (disponible en anglais, français ou allemand)

Auditer la mise en œuvre du principe du moindre privilège grâce à un **examen des comptes disposant de droits administrateurs**

Identifier les **utilisateurs qui n'ont pas modifié leur mot de passe depuis une date X** afin de faciliter une directive de réinitialisation de tous les mots de passe ou le déploiement d'une nouvelle politique de mots de passe

Téléchargez Specops Password Auditor **aujourd'hui**

Obtenir l'outil d'audit GRATUIT

L'HISTOIRE DE SPECOPS

Specops Software, filiale d'Outpost24, est le leader des solutions de gestion des mots de passe et d'authentification. Elle protège les données de votre entreprise en bloquant les mots de passe faibles et en sécurisant l'authentification. Ses solutions, intégrées à Active Directory, garantissent que les données sensibles restent sous votre contrôle. Fondée en 2001, Specops est basée à Stockholm et dispose de bureaux aux États-Unis, au Canada, au Royaume-Uni, en France et en Allemagne.

RÉSERVER UNE DEMO >> **DEMANDER UN TARIF PERSONNALISÉ >>**

CONTACTEZ-NOUS

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