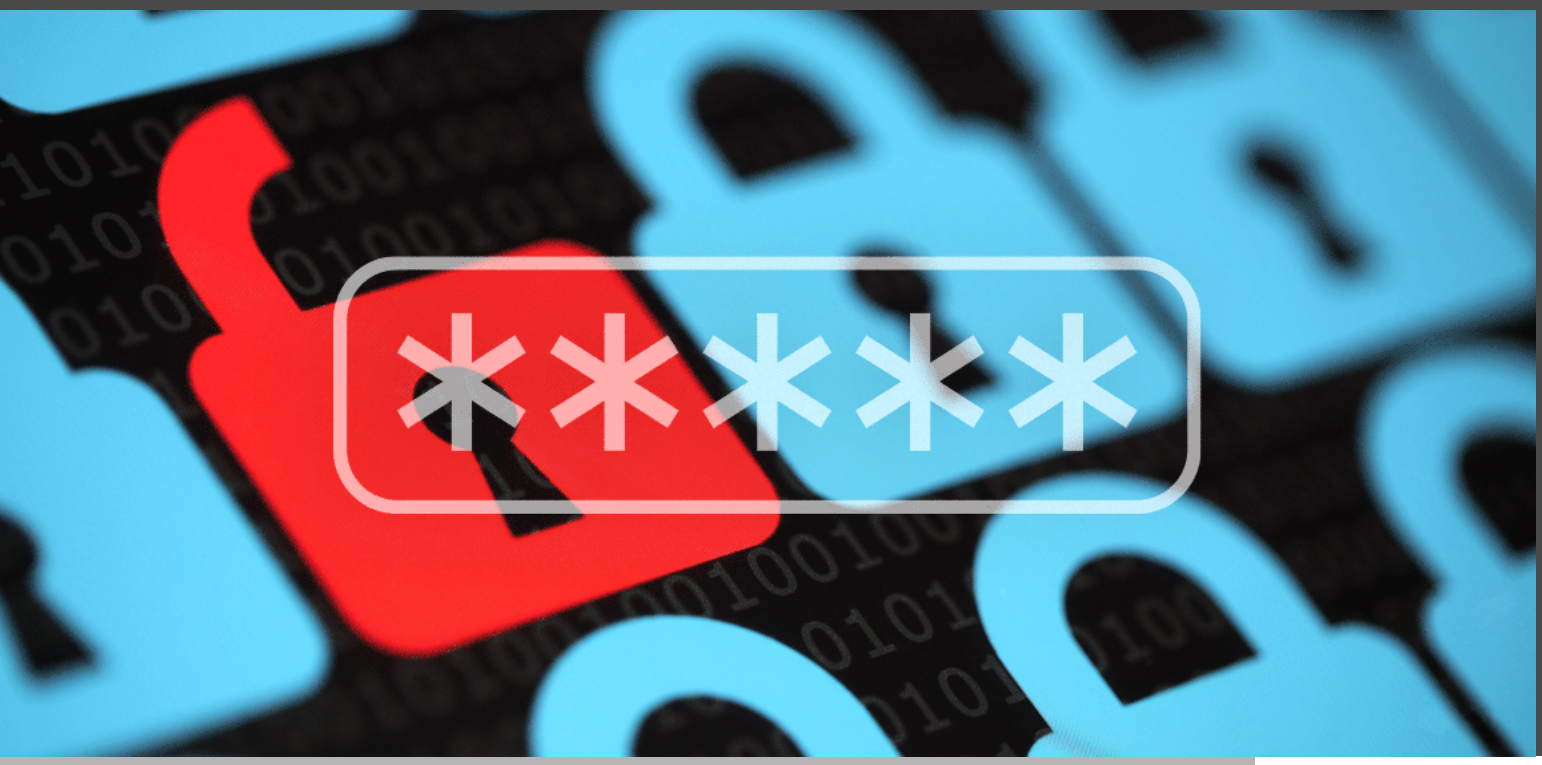
Devolutions

[MISE À JOUR] 10 BONNES PRATIQUES DE GESTION DE MOTS DE PASSE



LA SÉCURITÉ INFORMATIQUE ÉVOLUE RAPIDEMENT

Une bonne mise à jour, ce n'est pas juste sain pour la technologie. Nos pratiques de gestion de mots de passe doivent, elles aussi, être revues régulièrement. La sécurité informatique évolue rapidement et les outils utilisés par les acteurs malveillants sont en constante évolution.

L'équipe de sécurité de Devolutions vous propose une liste mise à jour des 10 meilleures pratiques dans la gestion de vos mots de passe. Le tout est basé sur diverses sources (y compris les directives d'identité numérique et les directives de politique de mots de passe préconisées par le *National Institute of Standards and Technology* (NIST)). Nous vous encourageons fortement à adopter les mesures et politiques suivantes le plus rapidement possible :

1. Mettre en place une authentification à deux facteurs (2FA) ou à facteurs multiples (MFA)

Même l'utilisateur final le plus prudent peut faire une erreur coûteuse en gestion de mots de passe. Pressé, il peut accidentellement mettre son mot de passe dans le mauvais champ. Il peut aussi ne pas savoir que son ordinateur a été compromis par un enregistreur de frappe (en anglais ***keystroke logger***).

Dans la plupart des cas, les 2FA et MFA empêchent les acteurs malveillants d'accéder aux comptes, même s'ils disposent des informations de connexion correctes. Il existe plusieurs bons outils 2FA et MFA, comme notre Devolutions Authenticator, disponible gratuitement, qui propose également des notifications push.

2. Installer un gestionnaire de mots de passe

Avec un gestionnaire de mots de passe, les utilisateurs n'ont qu'à se souvenir de deux informations de connexion plutôt que des dizaines. La première information de connexion dont ils doivent se souvenir est pour leur propre poste de travail. La deuxième permet d'accéder au gestionnaire de mots de passe. Ce dernier s'assure également que les utilisateurs choisissent des mots de passe très forts (voir la meilleure pratique #3) d'au moins 16 caractères.

De plus, si le gestionnaire de mots de passe est compatible avec l'authentification unique, ***Single Sign-On*** (SSO), de Microsoft, les utilisateurs n'ont à se souvenir que d'une seule information de connexion. Les entreprises qui utilisent le SSO de Microsoft peuvent même aller plus loin et mettre en place une authentification sans mot de passe avec des solutions comme Microsoft Hello (qui utilise la biométrie) ou Yubikey (qui utilise le chiffrement et l'authentification par clé publique). Cliquez ici pour lire notre billet de blogue qui compare les gestionnaires de mots de passe les plus populaires.

3. Utiliser des phrases secrètes

Lorsque les utilisateurs sont obligés de se souvenir de mots de passe (quand l'authentification sans mot de passe est impossible), la longueur doit être privilégiée par rapport à la complexité. De nombreux utilisateurs s'appuient sur des trucs trop simples pour les aider à se souvenir de mots de passe, tels que « Motsdepasse123! ». Certains utilisent aussi le « Leetspeak » et changent des lettres pour des caractères similaires. Ils utiliseront « motdep@55e » au lieu de « mot de passe », par exemple. Ces techniques sont largement connues et exploitées par les acteurs malveillants.

La grande majorité des utilisateurs ne peut se souvenir d'un mot de passe de 16 caractères ou plus sans recourir à ces « trucs ». C'est pourquoi la phrase de passe est une bonne solution. Comme nous l'avons écrit récemment, une phrase de passe est beaucoup plus longue qu'un mot de passe classique (ce qui la rend moins vulnérable à une attaque). Elle contient des lettres, des symboles, des espaces et des chiffres. Par exemple : « Paul, mon chien violet, aime quand je joue au frisbee avec lui ». Comme vous l'aurez peut-être constaté, il est plus sage de choisir une phrase secrète qui n'a pas de sens logique et qui n'est pas associée à l'utilisateur (dans notre exemple Paul n'a pas de chien violet, du moins pas à notre connaissance). Pour une sécurité accrue, les utilisateurs peuvent aussi mélanger les langues.

4. Modifier les mots de passe après la preuve d'une compromission

Par le passé, les entreprises demandaient aux utilisateurs finaux de changer régulièrement de mots de passe. De nos jours, les conseils du NIST sont très différents: il est préférable que les utilisateurs finaux ne CHANGENT PAS régulièrement de mots de passe. Les recherches ont démontré qu'en les modifiant, les utilisateurs choisissent généralement des informations d'identification plus faibles et plus faciles à identifier (voir SP-800-63B Section 5.1.1.2 paragraphe 9). Aucun changement ne devrait donc être effectué à moins de preuves de compromission.

Pour vérifier si elles ont été compromises, les entreprises peuvent utiliser des services comme Have I Been Pwned? Domain Search qui trouve tous les courriels sur un domaine particulier qui ont été victimes d'une violation de données connue. Il est également possible de recevoir des notifications par courriel en cas de violations futures. Ça aide à empêcher les acteurs malveillants de contourner les doubles facteurs d'authentification, car l'organisation saura quand changer les mots de passe et sur quels services.

5. Comparer les mots de passe avec une liste de mots de passe faibles et compromis

Selon le NIST (voir le paragraphe 5 de la section 5.1.1.2 du SP-800-63B), un mot de passe doit être comparé avec une liste de mots de passe faibles ou compromis connus avant d'être sélectionné. Il est important que cette liste comprenne des mots liés à l'environnement personnel ou professionnel de l'utilisateur, tels que le nom de l'entreprise et le nom d'utilisateur. Il s'agit d'une bonne protection contre une attaque par dictionnaire, qui tentera une liste de mots de passe connus. Les mots de passe courants du dictionnaire incluent des éléments comme « qwerty1! » et « 1122334455667788 », et la liste de mots de passe la plus connue est rockyou.txt.

Pour standardiser ce processus, les entreprises doivent déployer un gestionnaire de mots de passe ou un outil de connexion à distance doté d'une fonctionnalité intégrée de vérification des mots de passe. Par exemple, Remote Desktop Manager propose « Pwned Password Check », qui utilise le système de détection de mots de

passe Pnwed de Troy Hunt et vérifie automatiquement si un mot de passe potentiel a été compromis (pwned) par des pirates. De plus, Azure AD offre une fonctionnalité de protection par mot de passe. Pour leurs comptes personnels, les utilisateurs finaux peuvent utiliser un outil comme Have I Been Pwned? pour voir combien de fois un mot de passe potentiel a été compromis.

6. Appliquer l'accès juste-à-temps pour les comptes privilégiés

Les codes de hachage sont souvent stockés sur un système lorsque des utilisateurs ou des administrateurs se connectent sur un appareil. Cela peut conduire à une attaque « pass-the-hash », dans laquelle les acteurs malveillants volent des informations d'identification hachées et les réutilisent pour inciter un système authentifié à créer une nouvelle session authentifiée sur le même réseau. Surtout, il n'est pas nécessaire de déchiffrer le mot de passe : juste à le capturer, ce qui signifie que la longueur ou la complexité du mot de passe/phrase de passe n'a pas d'importance.

Pour réduire ce risque, les entreprises doivent mettre en place un accès juste-à-temps pour les comptes privilégiés en utilisant une solution robuste de gestion des comptes privilégiés. Une bonne option serait Devolutions Password Server, qui comprend un module PAM qui permet aux administrateurs d'approuver ou de rejeter les demandes d'accès. Il est également possible d'imposer un changement de mot de passe obligatoire après qu'une information d'identification ait été utilisée et/ou à une heure/date programmée.

7. Mettre en place une politique d'historique des mots de passe

Les entreprises doivent se doter d'une politique d'historique des mots de passe pour garantir que les utilisateurs finaux ne sélectionnent pas les anciens mots de passe. Le Center for Internet Security (CIS) recommande de définir cette valeur sur 24 ou plus (section 1.1.1). En outre, la politique doit également appliquer un âge minimum pour les mots de passe. Sinon, les utilisateurs finaux pourraient changer leur mot de passe plusieurs fois en quelques minutes afin de réutiliser le mot de passe préféré.

8. Éliminer la réutilisation des mots de passe

En parlant de réutilisation de mots de passe: une pratique étonnamment courante pour les utilisateurs et même certains administrateurs consiste à réutiliser les mêmes mots de passe partout. Même si c'est très pratique, c'est également très risqué. Il existe cependant des scénarios où la réutilisation du mot de passe n'est pas intentionnelle.

Par exemple, une image de système d'exploitation générique est utilisée pour configurer rapidement les systèmes et elle contient le même compte administratif local par défaut (a.k.a. comptes de porte dérobée pour les administrateurs). Malheureusement, ça signifie que la compromission d'un appareil les déverrouille tous.

Une excellente solution à ce problème consiste à installer Local Administrator Password (LAPS) pour Windows ou à s'appuyer sur une solution tierce. Cela permet à différents mots de passe d'être utilisés par tous les ordinateurs et serveurs et contribue à atténuer le risque et la gravité des attaques à grande échelle.

9. Activer le copier/coller des mots de passe

En théorie, les utilisateurs ne devraient pas être autorisés à copier/coller des mots de passe. Dans la réalité, c'est toutefois conseillé, car ça empêche les utilisateurs de choisir des mots de passe simples et faciles à retenir.

Si vous pensez que nous sommes tombés sur la tête, nous ne sommes pas les seuls à le recommander. Voici ce que dit le NIST (SP 800-63b paragraphe section 5.1.1.2): « Les vérificateurs DEVRAIENT permettre aux demandeurs d'utiliser la fonctionnalité «coller» lors de la saisie d'un mot de passe. Ça facilite l'utilisation de gestionnaires de mots de passe, qui sont largement utilisés et, dans de nombreux cas, augmentent la probabilité que les utilisateurs choisissent des mots de passe plus forts. »

10. Inscrire les utilisateurs finaux à une plateforme de formation sur la cybersécurité

Bien que ça ne fasse pas partie d'un processus de gestion des mots de passe en soi, il est vital de s'assurer que les utilisateurs finaux — qui sont et seront toujours les plus grandes menaces à votre cybersécurité — fassent partie de la solution. Pour ce faire, les entreprises devraient inscrire leurs utilisateurs finaux sur une plateforme de formation sur la cybersécurité qui couvre des sujets tels que l'ingénierie sociale, la sécurité des courriels, la sécurité des appareils mobiles, la navigation Web sécurisée, les réseaux sociaux sécurisés, la protection des informations sur la santé, etc. Les gestionnaires peuvent également suivre les progrès de l'utilisateur final pour identifier les lacunes dans les connaissances et les besoins de formation. Pour en savoir plus, veuillez lire notre article ici.

Penser au futur

Il est important d'implanter une solide politique de gestion des mots de passe à l'interne. Toutefois, les entreprises

ont également besoin de bons outils technologiques et elles doivent assurer une cohérence entre les pratiques de tous les utilisateurs finaux — en particulier les utilisateurs professionnels non techniques qui peuvent faire passer la commodité avant la sécurité. Un gestionnaire de mots de passe, comme Devolutions Password Hub, ou une solution PAM, comme Devolutions Password Server, est un must pour toute entreprise. En utilisant les outils appropriés, on travaille tous à créer un futur plus sécuritaire.

Nous espérons que ces informations mises à jour vous seront utiles et qu'elles aideront à protéger votre entreprise, vos utilisateurs finaux, vos données et votre réputation!