RESOURCE CENTER

Five Best Practices for Enterprise Password Management

Learn the best practices for enterprise password management in this white paper.

Get the full interactive view at https://bitwarden.com/fr-fr/resources/five-best-practices-for-password-management-white-paper/

bitwarden

Alors que les organisations continuent à faire de la sécurité une priorité, une partie importante de cet effort consiste à éduquer et à responsabiliser les utilisateurs généraux sur les meilleures pratiques. Voici quelques statistiques tirées du rapport Yubico 2019 State of Password and Security Authentication Security Behaviors Report (Rapport sur l'état des comportements en matière de mots de passe et d'authentification) :

- 2 personnes interrogées sur 3 partagent leurs mots de passe avec leurs collègues
- 51% des participants déclarent réutiliser les mots de passe sur leurs comptes personnels et professionnels.
- 57% ont déclaré ne pas avoir modifié leurs mots de passe après avoir subi une tentative d'hameçonnage.

Pour faire évoluer une entreprise, les équipes chargées de la sécurité et de l'informatique doivent former les employés aux meilleures pratiques. En ce qui concerne la gestion des mots de passe, l'un des moyens les plus simples d'encourager une bonne hygiène des mots de passe est de déployer une solution de gestion des mots de passe sur votre lieu de travail. Voici quelques bonnes pratiques à adopter.

1. Utiliser une solution de gestion des mots de passe

Tout au long de la journée, la plupart des gens visitent de nombreux sites différents qui nécessitent des mots de passe. Il est pratiquement impossible de mémoriser un grand nombre de mots de passe (ou phrases de passe) uniques et suffisamment forts. Un gestionnaire de mots de passe simplifie l'utilisation des mots de passe sur différents sites afin de renforcer la sécurité des utilisateurs. Il existe un certain nombre de gestionnaires de mots de passe efficaces. Donnez la priorité à ceux qui fonctionnent sur plusieurs plates-formes et qui offrent des services aux particuliers gratuitement ou à un prix très bas. La plupart des fonctionnalités des gestionnaires de mots de passe se sont également développées au fil des ans.

2. Choisissez un outil que vous pouvez facilement déployer au sein de votre organisation

Les gestionnaires de mots de passe doivent être faciles à utiliser pour tous les niveaux d'utilisateurs, du débutant au plus expérimenté. Si l'on considère une base d'employés importante ou distribuée, les applications doivent être intuitives pour l'utilisateur et faciles à déployer. Par exemple, que vous choisissiez le Bitwarden Cloud ou que vous déployiez votre propre instance hébergée, il est facile de mettre Bitwarden en place et de le faire fonctionner. Bitwarden Directory Connector fonctionne avec les services d'annuaire les plus utilisés aujourd'hui, tels qu'Azure, Active Directory, Google, Okta et d'autres, pour que les utilisateurs de Bitwarden restent en phase avec vos équipes et vos employés.

3. Ne changez vos mots de passe que lorsque vous risquez d'avoir été compromis

L'époque où l'on changeait son mot de passe tous les trois mois est révolue. Vous ne devez désormais les modifier que si vous pensez avoir été compromis. Le National Institute of Standards and Technology (NIST) ne recommande pas aux utilisateurs de modifier fréquemment leurs mots de passe. Cela conduit en fait à un comportement qui peut aboutir à des mots de passe plus faibles au fil du temps. Vous pouvez déterminer si un mot de passe a été compromis en vous référant à des preuves tangibles, telles qu'une fraude à la carte de crédit, ou en utilisant un outil (comme votre gestionnaire de mots de passe) qui peut déterminer si votre mot de passe a été exposé lors d'une violation.

4. Utiliser des mots de passe forts et uniques

L'utilisation de mots de passe forts et uniques pour chaque service que vous utilisez en ligne permet de minimiser l'impact des violations de données. Un mot de passe fort ne signifie pas nécessairement qu'il suffit d'ajouter des caractères spéciaux ou des chiffres à un mot ou à un nom courant, mais qu'il faut augmenter l'entropie du mot de passe, c'est-à-dire son caractère aléatoire. Une tactique simple pour créer un mot de passe fort consiste à utiliser une phrase de passe. Une phrase de passe combine des mots ou des phrases apparemment sans rapport qui sont facilement mémorisables par l'utilisateur, mais qui seraient autrement difficiles à deviner par un pirate. Les phrases de passe ont un degré élevé d'entropie tout en étant faciles à mémoriser.

5. Activer l'authentification à deux facteurs chaque fois que cela est possible

L'authentification à deux facteurs (2FA) étant de plus en plus répandue sur les sites web grand public et professionnels, un bon gestionnaire de mots de passe comprendra des moyens d'étendre cette fonction. L'utilisation de 2FA augmente la sécurité de votre compte en vous demandant d'entrer un autre jeton en plus de votre mot de passe principal. Même si quelqu'un découvrait votre mot de

passe principal, il ne pourrait pas se connecter à votre gestionnaire de mots de passe sans avoir accès au jeton supplémentaire. Si vous souhaitez commencer à utiliser un gestionnaire de mots de passe, vous pouvez ouvrir un compte Bitwarden gratuit ici.