Fidelity INVESTMENTS

BUREAU DE LA SÉCURITÉ DE L'INFORMATION

Sécurité des mots de passe

Les pirates informatiques découvrent les mots de passe par différents moyens, notamment à l'aide d'outils gratuits disponibles sur Internet. Aidez vos utilisateurs à sécuriser leurs mots de passe et resserrez ainsi la sécurité de vos systèmes en suivant ces conseils.

Comment les mots de passe sont-ils découverts?

INTERCEPTION
Les mots de passe peuvent être interceptés lorsqu'ils sont transmis sur un réseau.

FORCE BRUTE
Les mots de passe peuvent être découverts à la suite de tentatives répétées et automatisées visant à trouver le bon parmi des milliards.

RECHERCHE
Les infrastructures informatiques peuvent être inspectées afin de découvrir l'endroit où sont stockés les renseignements sur les mots de passe.

VOL DE MOTS DE PASSE
Les mots de passe stockés de façon non sécuritaire (incluant les mots de passe manuscrits cachés près d'un appareil) peuvent être volés.

TENTATIVES MANUELLES
Les renseignements personnels comme le nom et la date de naissance peuvent être utilisés pour trouver des mots de passe courants.

4

Nombre moyen de sites Web pour lequel un utilisateur emploie le même mot de passe

ESPIONNAGE PAR-DESSUS L'ÉPAULE
Un mot de passe peut être découvert en observant quelqu'un entrer son mot de passe.

INGÉNIERIE SOCIALE
Les pirates informatiques se servent de techniques d'ingénierie sociale pour amener les gens à révéler leurs mots de passe.

ENREGISTREMENT DE FRAPPE
Il existe des dispositifs qui permettent d'intercepter des mots de passe lorsqu'ils sont entrés dans un système.

Comment resserrer la sécurité des systèmes?

Aider les utilisateurs à gérer la « surcharge de mots de passe ».

- Utiliser des mots de passe seulement lorsque cela est vraiment nécessaire.
- Utiliser des solutions techniques pour réduire la charge sur les utilisateurs.
- Permettre aux utilisateurs d'enregistrer et de stocker leurs mots de passe de façon sécuritaire.
- Demander aux utilisateurs de modifier un mot de passe seulement si l'on suspecte qu'il a été compromis.
- Permettre aux utilisateurs de réinitialiser un mot de passe rapidement, facilement et à faible coût.

Aider les utilisateurs à générer des mots de passe appropriés.

- Mettre en place des mécanismes de défense afin de permettre l'utilisation de mots de passe plus simples.
- Décourager les utilisateurs d'employer des mots de passe prévisibles et interdire les plus courants.
- Encourager les utilisateurs à ne jamais utiliser un mot de passe personnel au travail et vice versa.
- Former le personnel pour les aider à éviter de créer des mots de passe faciles à deviner.
- Prendre en compte les limitations des indicateurs de sécurité des mots de passe.

Exclure les options de mots de passe les plus courantes.

Surveiller les tentatives de connexion ayant échoué. Former les utilisateurs pour qu'ils signalent toute activité suspecte.

Donner la priorité aux comptes d'administrateur et d'utilisateur à distance.

Ne pas stocker les mots de passe au format texte brut.

Modifier tous les mots de passe par défaut fournis par les fournisseurs avant le déploiement de périphériques ou de logiciels.

Utiliser les fonctionnalités de verrouillage de compte, de régulation et de surveillance afin d'aider à prévenir les attaques par force brute.

FCAN-1014049 09/22