Portrait de la sécurité des mots de passe dans les PME en 2020 : Le bon, le mauvais et le pire

Le BON, le MAUVAIS et le PIRE

Devolutions a sondé les décideurs en TI dans les petites et moyennes entreprises (PME) à travers le monde afin de brosser le portrait de la sécurité des mots de passe en 2020 et de connaître leur vision de l'avenir.

SAVIEZ-VOUS QUE

Les revenus de la cyber-criminalité ont atteint le plateau de **1,5 trillion de dollars par année.**

Chaque incident de violation de données coûte en moyenne **3,9 millions de dollars aux entreprises.**

LE BON

des PME offrent de la formation en cybersécurité à leurs utilisateurs finaux.

81% des PME stockent leurs informations d'identification dans un gestionnaire de mots de passe pour protéger leurs données personnelles.

****

77% des PME ont implanté une politique de complexité et de longueur minimale de mot de passe.

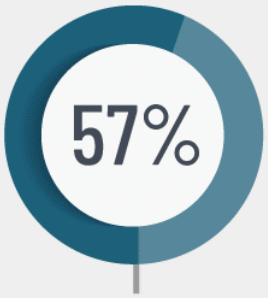
76% des PME croient qu'un gestionnaire de mots de passe est la meilleure solution pour valider et surveiller les bonnes pratiques relatives aux mots de passe.

4 752 PME n'autorisent pas la réutilisation de mots de passe pour tout type de compte.

LE MAUVAIS

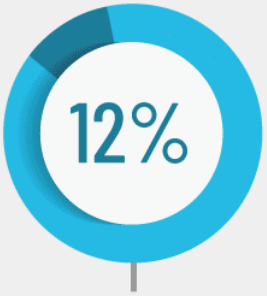
88% des PME **sont davantage préoccupées par la confidentialité et la sécurité** de leurs données en ligne maintenant qu'il y a cinq ans.

72% des PME croient que **la sécurité des services infonuagiques** deviendra un plus grand enjeu dans les trois prochaines années.



des PME ont subi une **attaque d'hameçonnage** dans les trois dernières années.

des PME envisagent que les menaces reliées à l'Internet des objets augmenteront dans les prochaines années.



des PME ne savent pas si elles ont été attaquées dans la dernière année.

LE PIRE

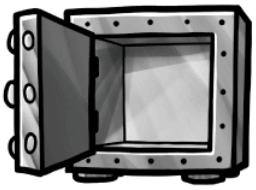
97% des PME croient que les utilisateurs finaux sont responsables en cas de brèche de données.

78% des PME considèrent qu'une solution de gestion d'accès privilégiés occupe une place importante au sein d'un programme de cybersécurité.

76% des PME n'ont pas de solution déployée dans leur organisation.

62% des PME n'effectuent pas d'audit de sécurité au moins une fois par année et **14%** des PME n'ont jamais mené de vérifications.

47%



des PME permettent aux utilisateurs finaux de réutiliser des mots de passe pour leurs comptes personnels et professionnels.

15% des PME n'ont aucun outil en place pour protéger ou gérer les mots de passe.

COMMENT SE PROTÉGER

En matière de sensibilisation à l'importance de la cybersécurité et de protection, les PME sont généralement dans la bonne voie. Cependant, il reste du travail à faire : des vulnérabilités inquiétantes, voire même alarmantes, sont encore présentes. Elles pourraient entraîner des conséquences néfastes et potentiellement catastrophiques si des pirates informatiques arrivaient à les exploiter. De plus, il y a la menace constante que représentent les utilisateurs finaux négligents pouvant accidentellement provoquer des fuites de données. Pour protéger leurs données, leurs clients, leur réputation et leur organisation, les PME devraient adopter les cinq recommandations suivantes :

RECOMMANDATIONS

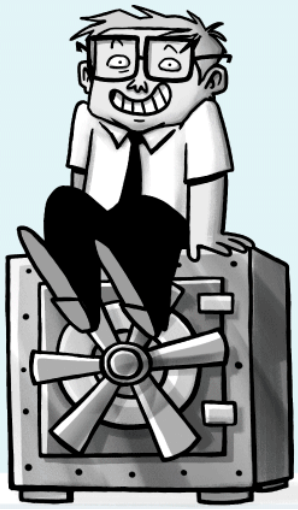
1 - Implanter une solution de gestion d'accès privilégiés

Comme les cybercriminels ont considérablement raffiné leurs stratégies d'attaque, les PME doivent s'adapter en implantant une solution qui offre au moins sept fonctionnalités, comme **un coffre de mots de passe sécurisé, l'injection des informations d'identification et un système de contrôle d'accès basé sur les rôles.**

2 - Mettre en place des politiques strictes de gestion de mots de passe

Les PME sont fortement encouragées à adopter les mesures et politiques suivantes, basées sur diverses sources fiables comme le NIST et le *Center for Internet Security* :

- Configurer l'authentification à deux facteurs
- Installer un gestionnaire de mots de passe
- Utiliser des phrases secrètes
- Modifier les mots de passe après la preuve d'une compromission
- Comparer les mots de passe avec une liste de mots de passe faibles et compromis
- Appliquer l'accès juste-à-temps pour les comptes privilégiés
- Implanter une politique d'historique des mots de passe
- Éliminer la réutilisation des mots de passe



3 - Appliquer le principe de moindre privilège

Le principe du moindre privilège est le principe par lequel les utilisateurs finaux ne bénéficient que de la quantité d'accès dont ils ont réellement besoin pour faire leur travail — ni plus ni moins. Il existe un certain nombre de bonnes pratiques qui devraient être adoptées par les PME, notamment **l'évaluation des niveaux d'accès, l'instauration de mots de passe à usage unique, la mise en place de la séparation de comptes, la surveillance en continu ainsi que la réalisation d'audits à intervalle régulier.**

4 - Implanter la séparation des tâches

Ces dernières années, le concept de séparation des tâches s'est répandu dans le domaine de la cybersécurité afin de prévenir les conflits d'intérêts, les actes illégaux, la fraude, les abus et la création de « silos secrets » au sein des entreprises. Les PME devraient adopter rapidement différentes bonnes pratiques, dont **l'analyse des niveaux d'accès, l'alignement des tâches avec les rôles et la formation des utilisateurs finaux.**

5 - Offrir de la formation en cybersécurité aux utilisateurs finaux

Bien qu'il existe plusieurs façons d'offrir de la formation en cybersécurité, la plus efficace demeure d'inscrire son équipe sur une plateforme de formation en ligne. Il s'agit d'une formation pratique basée sur les compétences et chaque participant apprend à son rythme. Les cours sont offerts sous la forme de simulations réalistes et dynamiques. Le programme de formation peut être personnalisé pour couvrir des sujets spécifiques tels que **l'ingénierie sociale, la sécurité concernant les courriels, la sécurité sur les appareils mobiles, la navigation sur le Web sécuritaire et la sécurité sur les réseaux sociaux.**

Sources

https://www.bromium.com/press-release/hyper-connected-web-of-profit-emerges-as-global-cybercriminal-revenues-hit-1-5-trillion-annually
https://www.ibm.com/security/data-breach

MAÎTRISEZ LE CHAOS RELIÉ AUX TI