Devolutions

Portrait de la cybersécurité dans les PME en 2021-2022 : Là où les bonnes et mauvaises nouvelles se côtoient

LÀ OÙ LES BONNES ET MAUVAISES NOUVELLES SE CÔTOIENT

Pour une deuxième année consécutive, Devolutions a sondé les décideurs en TI dans les petites et moyennes entreprises (PME) à travers le monde afin de connaître leur profil de sécurité.

Qu'avons-nous découvert?
Qu'il y a de BONNES nouvelles comme des mauvaises!

SAVIEZ-VOUS QUE

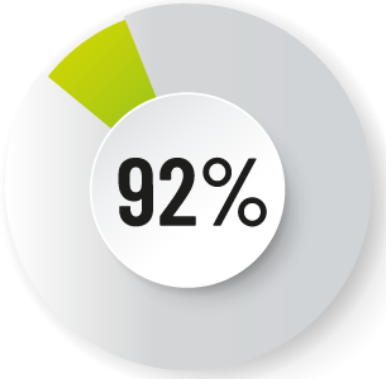
43 % des cyberattaques visent les petites entreprises.

En 2021, le coût moyen d'une brèche de données s'élève à **2,98 millions $ US par incident.**

81 % des violations de données proviennent de mots de passe compromis et **30 % impliquent des employés malveillants.**

LES BONNES NOUVELLES

Il y a quelques statistiques encourageantes qui démontrent que les PME sont plus sensibilisées et protégées contre les cyberattaques. Voici ce que nous avons constaté :



des PME ont un processus en place pour révoquer l'accès aux comptes aux anciens employés.

74% des PME offrent de la formation en cybersécurité à leur personnel.

****

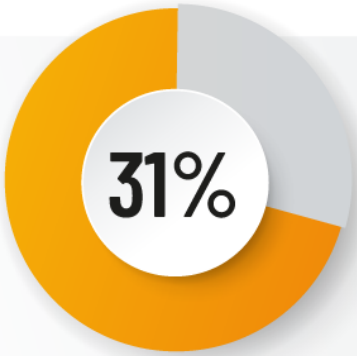
71% des PME stockent leurs mots de passe dans un gestionnaire de mots de passe.

> Les pirates informatiques ont multiplié les attaques contre les PME durant la pandémie et ciblent les télétravailleurs qui sont généralement beaucoup plus vulnérables en dehors de l'environnement du réseau de l'entreprise.

— tiré du rapport sur le portrait de la cybersécurité dans les PME en 2021-2022

LES MAUVAISES NOUVELLES

À l'autre bout du spectre, plusieurs PME demeurent vulnérables aux cyberattaques provenant à la fois de l'externe et de l'interne. Voici quelques exemples :



Seulement **31 % des PME** ont mis en œuvre une politique de gestion de mots de passe couvrant les éléments suivants : la longueur minimale, la complexité, l'historique et l'âge minimal des mots de passe, sans oublier l'authentification multifacteur ou à deux facteurs obligatoire.

Seulement **29 % des PME** surveillent la totalité de leurs comptes privilégiés.

Seulement **13 % des PME** ont déployé une solution de gestion d'accès privilégiés au sein de leur organisation.

> Non seulement les pirates informatiques ciblent les PME, mais ils intensifient leurs attaques pour une raison très simple : en comparaison avec la plupart des grandes organisations et entreprises, leurs moyens de défense sont plus limités ou, dans certains cas, pratiquement inexistants.

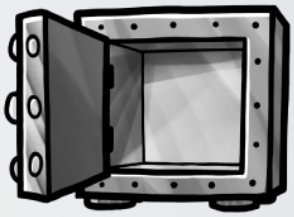
— tiré du rapport sur le portrait de la cybersécurité dans les PME en 2021-2022

AUTRES STATISTIQUES

72% des PME affirment qu'elles sont plus préoccupées par la cybersécurité aujourd'hui qu'il y a un an.

52% des PME ont été victimes d'au moins une cyberattaque dans la dernière année et 10 % en ont subi plus de 10.

32%



des PME ont vécu des violations d'accès privilégiés dans la dernière année.

> Les PME doivent empêcher les acteurs malveillants d'envahir leurs terminaux et leurs réseaux. Toutefois, elles doivent simultanément éviter que les utilisateurs internes (qu'il s'agisse de malfaiteurs ou de personnes commettant des erreurs) accèdent abusivement aux comptes privilégiés et obtiennent ou divulguent des informations sensibles.

— tiré du rapport sur le portrait de la cybersécurité dans les PME en 2021-2022

RECOMMANDATIONS

Le rapport contient 15 recommandations pour aider les PME à améliorer leur profil de cybersécurité et à mitiger les risques d'une brèche de sécurité coûteuse et potentiellement catastrophique :

1. Les PME doivent réaliser qu'elles ne sont pas « trop petites pour être attaquées ».

2. Les PME doivent se prémunir contre les trois principales cybermenaces : les rançongiciels, l'hameçonnage et les attaques de la chaîne d'approvisionnement.

3. Les PME doivent élaborer un plan d'intervention complet et efficace en cas de cyberattaque.

4. Les PME doivent implanter une solution de gestion de mots de passe disposant de fonctionnalités appropriées.

5. Les PME doivent instaurer une politique stricte de mots de passe.

6. Les PME doivent mettre en place un processus efficace de déprovisionnement des accès.

7. Les PME doivent adopter une solution de gestion des accès privilégiés afin de combler le fossé entre l'authentification et l'autorisation.

8. Les PME doivent protéger, surveiller et mettre à jour tous les comptes privilégiés.

9. Les PME doivent mettre en œuvre quatre principes de sécurité primordiaux : le principe du moindre privilège, la séparation des tâches, la Confiance zéro et la défense en profondeur.

10. Les PME doivent sensibiliser davantage leur personnel à la cybersécurité.

11. Les PME doivent éviter que les travailleurs à distance deviennent le maillon faible de la chaîne de défense en matière de cybersécurité.

12. Les PME ont besoin d'un processus complet d'audit de cybersécurité.

13. Les PME ont besoin du soutien des fournisseurs de services gérés pour combler le déficit de défense en cybersécurité.

14. Les PME doivent augmenter la part de leur budget informatique consacrée à la cybersécurité.

15. Les PME doivent se concentrer sur 5 projets de sécurité en 2021-2022 : la gestion sécurisée des accès à distance, un coffre numérique sécurisé, la gestion sécurisée des mots de passe, l'authentification multifacteur et l'automatisation.

Sources :

https://www.ibm.com/security/data-breach

https://www.einnews.com/pr_news/533310673/global-cybercrime-damage-costs-will-reach-11-4-million-per-minute-in-2021

https://www.cybintsolutions.com/cyber-security-facts-stats/

https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Devolutions

SÉCURITÉ ET TI, MAINTENANT RÉUNIES