Devolutions

RAPPORT

Portrait de la cybersécurité dans les PME en **2020-2021**

TABLE DES MATIÈRES

RÉSUMÉ

Les revenus de la cybercriminalité ont atteint le plateau de 1,5 trillion de dollars par année et chaque incident de violation de données coûte en moyenne 3,9 millions de dollars aux entreprises. Malgré ces coûts astronomiques, les gens continuent de croire que seules les grandes organisations sont ciblées et vulnérables aux cyberattaques. Cependant, les preuves s'accumulent quant à la vulnérabilité croissante des petites et moyennes entreprises (PME), et ne pas prendre conscience de cette réalité peut entraîner de désastreuses conséquences.

Dans le but d'aider les organisations à saisir l'ampleur et l'évolution des cybermenaces, Devolutions a sondé les décideurs dans les PME à travers le monde [1] sur des sujets pertinents en 2020-2021, qui sont d'autant plus d'actualité en raison de la pandémie et des risques accrus reliés au travail à distance. Ces enjeux comprennent notamment la gestion d'accès privilégiés, les pratiques de gestion de mots de passe et les tendances dans le domaine de la cybersécurité. Ainsi, les PME seront en mesure de prendre des décisions éclairées et d'adopter des stratégies qui réduiront les possibilités et la sévérité d'éventuelles cyberattaques.

Voici quelques faits saillants du sondage :

[1] Ce sont les organisations participantes qui se définissent comme PME dans ce présent sondage. Cette approche démontre que la définition d'une PME varie d'une industrie et d'une région à l'autre.

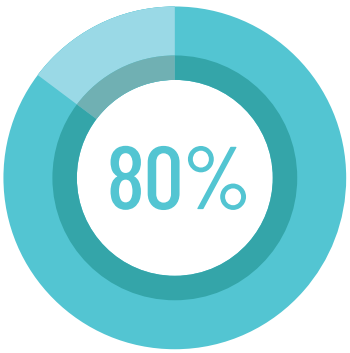
88%

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

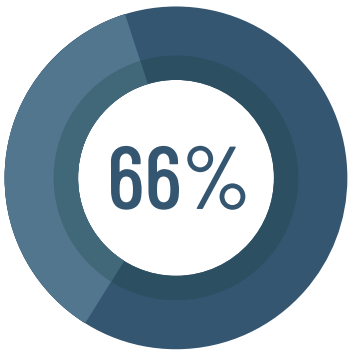
Cette inquiétude est amplement justifiée, puisque les PME sont devenues le « point zéro » de la cybercriminalité. **Par exemple :**

Un courriel sur 323 reçus par les PME est **malicieux.**

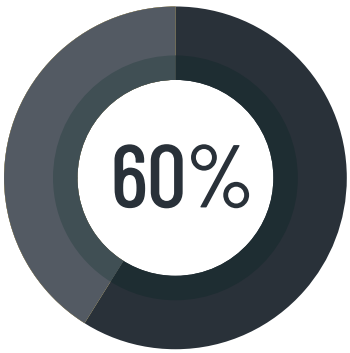
Lors d'une cyberattaque, les PME sont aux prises avec une panne du système qui peut durer au moins huit heures.



80 % des PME admettent qu'un **maliciel a déjoué leur logiciel antivirus.**



66 % des PME ont subi au moins une **cyberattaque** dans les **12 derniers mois.**



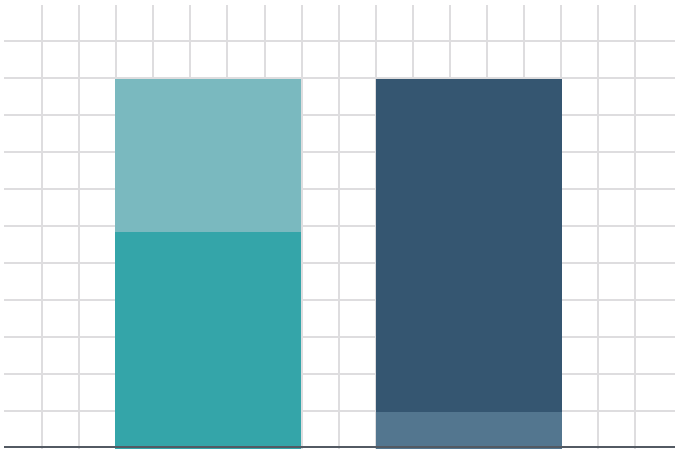
60 % des PME **déclarent faillite dans les six mois** suivant une cyberattaque.

Même si **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.

Les pirates informatiques visent précisément les comptes privilégiés, car 74 % des violations de données proviennent d'une utilisation frauduleuse d'informations privilégiées. Voici les types de comptes que les PME doivent surveiller et vérifier régulièrement :

- Comptes d'administrateurs de domaine
- Comptes d'utilisateurs privilégiés
- Comptes administrateur locaux
- Comptes d'accès d'urgence
- Comptes d'application
- Comptes système
- Comptes de services (domaine)



62% 14%

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.

Les experts recommandent d’effectuer au moins deux audits de sécurité par année, bien que des audits plus fréquents soient vivement encouragés. Un audit de sécurité vérifie les erreurs récurrentes ou anormalités qui peuvent **indiquer la présence de vulnérabilités**. **Un audit spécial de sécurité doit également être mené en cas de :**

- Brèche de sécurité
- Mise à niveau du système
- Changements aux lois de conformité
- Virage numérique
- **Croissance** (ou période intensive d’embauches)
- Fusion

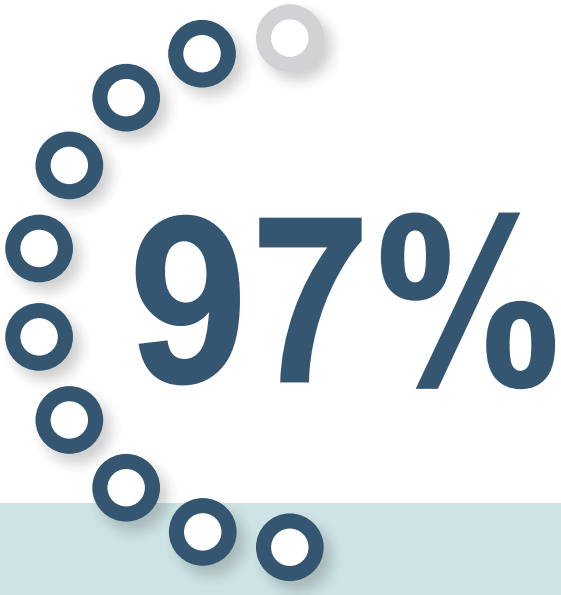
57%

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

Des études ont révélé que **56 % des décideurs en TI** estiment que la **prévention des attaques d'hameçonnage est leur priorité numéro un**. **90 % des attaques et des violations comptent un élément d'hameçonnage et 94 % des logiciels malveillants sont envoyés par courriel.**

De plus, étant donné que **les pirates lancent** des attaques en moyenne toutes les **39 secondes**, il est fort probable que toutes les PME ont subi des attaques plusieurs fois, mais qu'elles ne sont pas conscientes de l'ampleur ou des conséquences. Voici ce que le directeur de la sécurité de Devolutions, Martin Lemay, a à dire sur ce sujet :

> *« Ici même chez Devolutions, lors des 30 derniers jours de la préparation de ce rapport, 21 % des courriels entrants étaient des pourriels ou du contenu malicieux. Une quantité importante de pièces jointes suspectes ont régulièrement déclenché l'alarme de nos systèmes de détection de logiciels malveillants. Tout cela sans compter les multiples campagnes d'hameçonnage par courriel utilisant une provenance forgée, laissant croire que les courriels auraient été envoyés à partir de l'un de nos propres domaines.*
>
> *Nous avons été en mesure d'esquiver ces attaques grâce à une politique robuste d'authentification des messages basée sur le nom de domaine (Domain-based Message Authentication, Reporting and Conformance (DMARC)). L'infrastructure de sécurité fournie par DMARC nous permet d'avoir la visibilité nécessaire pour non seulement détecter les menaces, mais y remédier rapidement. Toutes les PME devraient avoir le même niveau de protection en place. Le problème n'est pas de savoir si une attaque de ce genre va se produire, mais bien à quelle fréquence et avec quelle sévérité elles auront lieu. »*

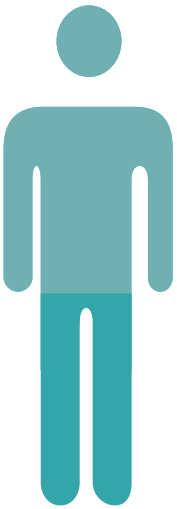


97% des PME croient que les utilisateurs finaux sont responsables en cas de brèche de données.

Ce résultat concorde avec cette recherche levant le voile sur la peur numéro un des professionnels des TI. Selon eux, la menace ne provient pas de pirates à l'extérieur de l'entreprise, mais bien d'utilisateurs finaux incompétents ou négligents. En fait, **79 % des responsables informatiques estiment qu'au cours des 12 derniers mois, leurs propres employés ont accidentellement mis en danger les données de l'entreprise.**

Ce qui est encore plus révélateur, c'est que **55 % des employés qui ont délibérément, mais pas malicieusement, partagé des données contre les règles l'ont fait parce que leur entreprise ne leur a pas fourni les outils nécessaires. En outre, 29 % des employés ne sentaient pas qu'ils avaient enfreint les règles**, car ils croyaient à tort que les données sur lesquelles ils travaillaient leur appartenaient, et non pas à leur employeur.

Selon des recherches, **59 % des utilisateurs finaux réutilisent les mêmes mots de passe pour tous les comptes** pour une raison très humaine : **il est très difficile de se souvenir de plusieurs mots de passe.** En effet, un **utilisateur dans une entreprise a, en moyenne, 191 mots de passe** et doit **saisir ses informations d'identification au moins 154 fois par mois,** toutes applications confondues. Afin de pallier ce problème, les PME devraient implanter un gestionnaire de mots de passe et forcer ses utilisateurs à choisir un mot de passe unique pour chaque compte.



47% des PME permettent aux utilisateurs finaux de réutiliser des mots de passe pour leurs comptes personnels et professionnels.

29% des PME se fient à la mémoire humaine pour stocker les mots de passe.

Cette pratique **dangereuse mène les gens à stocker leurs mots de passe dans des feuilles de calcul ou dans des documents non protégés.** Les gens sont également portés à **réutiliser le même mot de passe**, ce qui est un énorme facteur de risque. Même si un mot de passe est complexe, il peut ouvrir une potentielle porte à tout pirate qui cherche à pénétrer sur le réseau en passant par des terminaux.

À retenir

À la lumière de ces statistiques plutôt éloquentes, deux choses nous apparaissent très claires en 2020-2021 :

1. **Les PME ne peuvent présumer que leur petite taille les protège contre les cyberattaques.** Au contraire, les pirates, les employés et autres acteurs malveillants ciblent de plus en plus les PME puisqu'elles ont des systèmes de défense plus faibles, voire inexistants.

2. **Les PME ne peuvent plus se permettre d'être simplement réactives en cas d'attaque**, car elles pourraient ne pas y survivre. Et même si elles réussissent à passer au travers, cela pourrait leur prendre des années avant de récupérer les coûts, regagner leur clientèle et restaurer leur réputation.

À PROPOS DE CE RAPPORT

Au total, **182 répondants ont reçu le questionnaire contenant 24 questions**. Toutes les réponses (regroupées par question et par pourcentage), accompagnées de commentaires et de sources d'informations supplémentaires, sont présentées dans les prochaines sections du rapport, divisé en six parties :

Partie 1
Moyens de protection des PME contre les pirates informatiques et vision future du domaine de la cybersécurité

Partie 2
Pratiques et politiques relatives aux mots de passe dans les PME

Partie 3
Connaissance et utilisation de la gestion des accès privilégiés dans les PME

Partie 4
Actions prises par les PME afin d'améliorer la cybersécurité

Partie 5
Recommandations

Partie 6
Profil des répondants

Partie 1

Moyens de protection des PME contre les pirates informatiques et vision future du domaine de la cybersécurité

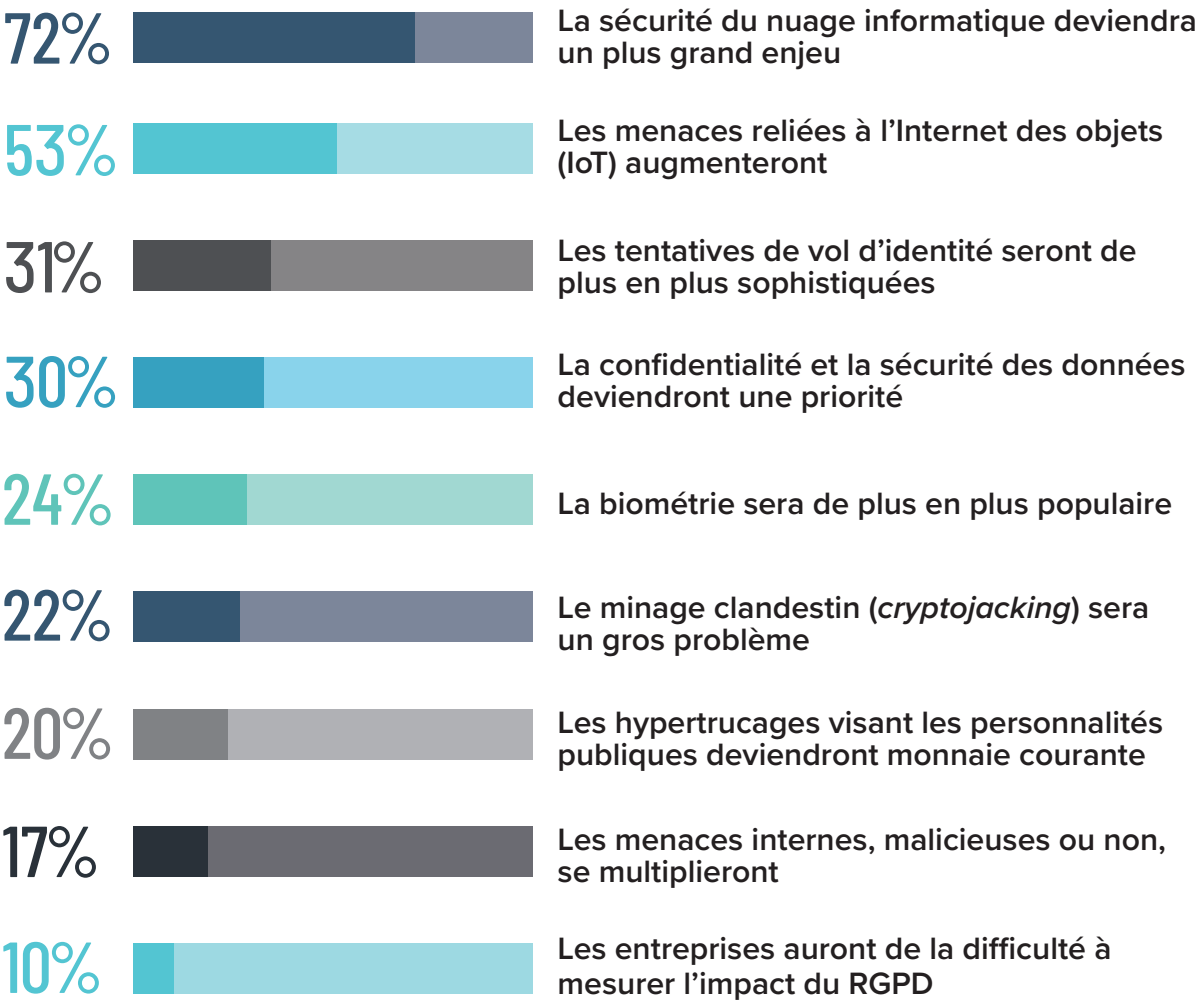
À propos de cette partie

Par le passé, il était tout à fait acceptable pour les PME de se fier aux outils de sécurité visant à protéger le périmètre du réseau : antivirus, pare-feu, portail Web, etc. Cette approche est maintenant insuffisante, puisque les cybercriminels ont considérablement raffiné leurs stratégies d'attaque. Les PME doivent donc s'adapter en conséquence, au risque de devenir la prochaine victime d'une cyberattaque aux conséquences funestes.

La première partie de ce sondage porte **sur la façon dont les PME se protègent contre les cyberattaques en 2020-2021 et sur leur vision du futur de la cybersécurité.**

QUESTION 1

Selon vous, quelles tendances en cybersécurité gagneront en importance au cours des trois prochaines années?
(Veuillez cocher jusqu'à trois éléments)



COMMENTAIRES

Il est intéressant de constater que 72 % des PME croient que la sécurité des services infonuagiques deviendra un plus grand enjeu dans les trois prochaines années. Il y a plusieurs avantages à migrer les données dans le nuage, mais pendant plusieurs années, l'amélioration de la sécurité n'en faisait pas partie. Par contre, ce n'est plus le cas. **De nos jours, le nuage informatique est considéré aussi sécuritaire, et même parfois plus, que les centres de données sur site d'ancienne génération.** Par exemple, les fournisseurs de services infonuagiques :

- Surveillent de près la sécurité en tout temps.
- Mènent des tests d'intrusion et de vulnérabilité en continu.
- Stockent les données à plusieurs endroits, ce qui protège les données contre la corruption et les pannes matérielles.

La plupart des PME ne peuvent maintenir ce niveau de surveillance rigoureuse et continue. De plus, la reprise des activités est quatre fois plus rapide pour les PME qui utilisent des services infonuagiques par rapport à celles qui n'en ont pas.

Il est aussi à noter que **53 % envisagent que les menaces reliées à l'Internet des objets augmenteront dans les prochaines années.** Certains risques comprennent :

- La multiplication des points d'accès vulnérables (p. ex., les imprimantes);
- Le sabotage;
- Les réseaux d'ordinateurs zombies.

En ce qui concerne le dernier point, en 2016, des pirates ont pris le contrôle de plus de 100 000 appareils d'IdO peu sécurisés et ont lancé une attaque massique d'ordinateurs zombies qui ont fait planter l'Internet pour des millions de clients.

Étonnamment, seulement **17 % des PME prévoient que l'augmentation des menaces internes, qu'elles soient malicieuses ou involontaires, sera un enjeu majeur dans les trois prochaines années.** Cette perspective est inquiétante, car **72 % des professionnels en TI croient que leur organisation est vulnérable face à ce type de menace.**

QUESTION 2

Êtes-vous davantage préoccupé par la confidentialité et la sécurité de vos données en ligne maintenant que vous ne l'étiez il y a cinq ans?

OUI

88%

NON

12%

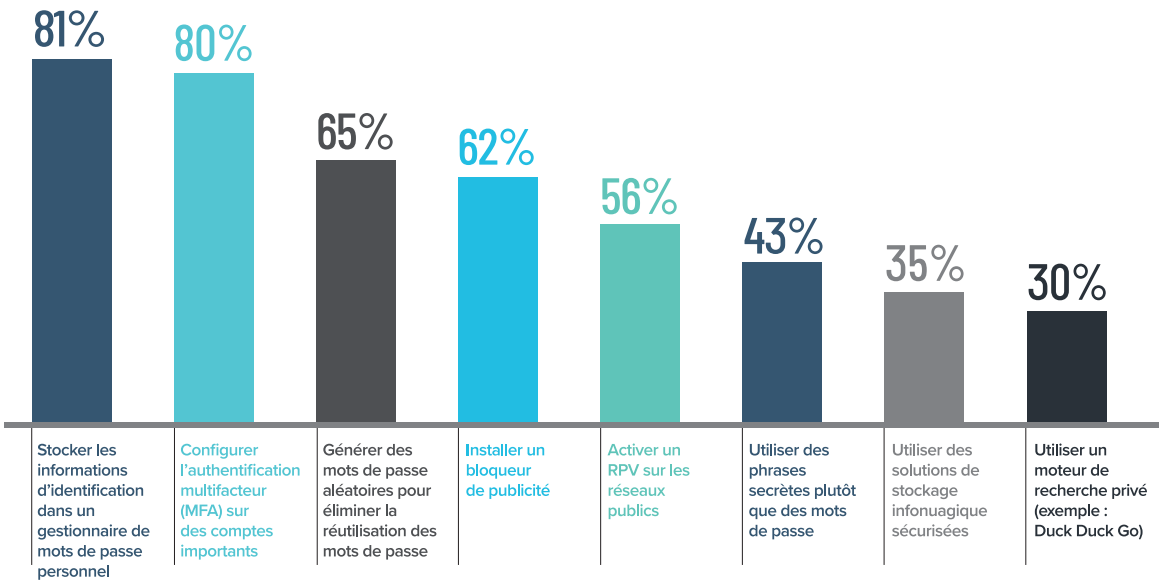
COMMENTAIRES

La popularité émergente des médias sociaux dans le milieu des affaires n'est pas entièrement positive, car elle a conduit à une forte augmentation de la cybercriminalité. Des recherches ont dévoilé que **22 % des utilisateurs de médias sociaux auraient été victimes de piratage au moins une fois, alors que 14 % d'entre eux l'auraient été à plusieurs reprises.** De plus, **les données de plus de 1,3 milliard d'utilisateurs des médias sociaux ont été compromises au courant des cinq dernières années. Sur le Web invisible (*dark web*), il est possible de trouver des outils ou services de piratage clés en main compatibles** avec plus de **40 % de sites de médias sociaux.**

Certes, la sécurité et la transparence dans le traitement des données demeurent des enjeux préoccupants, surtout depuis les derniers scandales. La mauvaise nouvelle, c'est que le nombre d'incidents et scandales impliquant les données ne va que continuer d'augmenter. La bonne nouvelle, c'est qu'on prévoit que le domaine de la sécurité de l'information croîtra considérablement dans le futur.

QUESTION 3

Que faites-vous pour protéger vos données personnelles?
(Veuillez cocher tout ce qui s'applique)



COMMENTAIRES

La popularité grandissante des gestionnaires de mots de passe personnels est une bonne nouvelle, puisque laisser la gestion des mots de passe aux utilisateurs finaux n'est pas une pratique recommandée. En effet, des **recherches** **révèlent que les utilisateurs finaux ont tendance à choisir des mots de passe faibles, à réutiliser les mêmes mots de passe ainsi qu'à stocker et à partager les mots de passe de façon non sécuritaire.**

Heureusement, plus de PME adoptent l'authentification à deux facteurs, une pratique reliée au concept Confiance zéro (*Zero Trust*). Bien que les mots de passe ou phrases secrètes robustes soient importants, **ils ne suffisent pas**. L'accès sécuritaire aux comptes doit être renforcé par l'utilisation d'un appareil physique que l'utilisateur final doit avoir à portée de main : une clé matérielle (sans contact, USB), une carte à puce, un téléphone cellulaire (texto, notification), etc. Même si un deuxième facteur d'authentification n'est pas à toute épreuve, il s'agit d'un pas dans la bonne direction. C'est une protection additionnelle bien peu chère payée lorsqu'on considère la paix d'esprit qu'elle procure.

Partie 2

Pratiques et politiques relatives aux mots de passe dans les PME

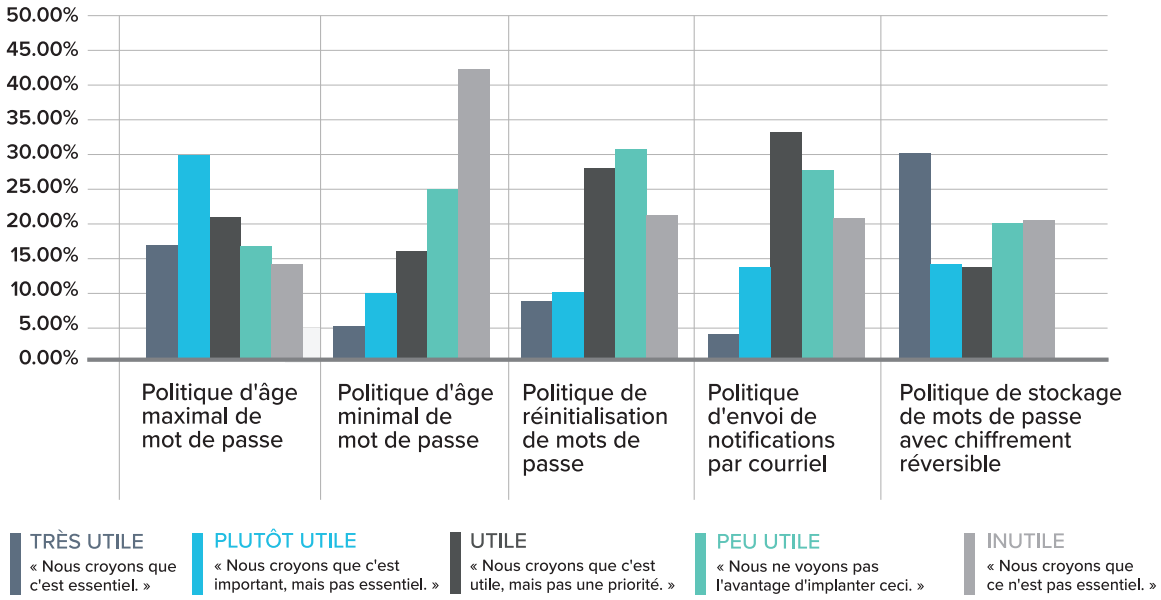
À propos de cette partie

Dans le domaine de la sécurité de l'information, les mots de passe sont perçus comme les « clés du royaume ». Malheureusement, il est plutôt facile pour les pirates de se procurer ces clés — particulièrement celles des PME qui sous-estiment cette menace — et d'ensuite lancer des attaques contre les terminaux et les réseaux. Les recherches montrent d'ailleurs que 81 % des violations de données sont causées par des mots de passe compromis, faibles et réutilisés, tandis que 29 % de toutes les brèches confondues impliquent l'utilisation d'informations d'identification volées.

Dans la deuxième partie du sondage, nous avons demandé aux PME de déterminer quelles politiques et pratiques par rapport aux mots de passe elles ont implantées au sein de leur organisation en 2020-2021 afin de protéger leurs données.

QUESTION 4

Veuillez classer les politiques de mots de passe suivantes du plus utile au moins utile.



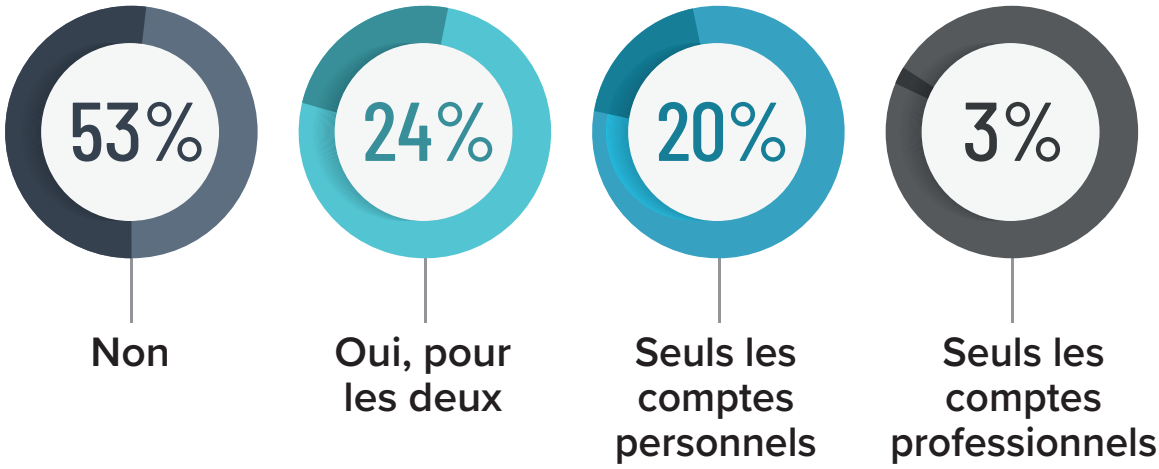
COMMENTAIRES

La perception des PME quant à l'utilité de stocker des mots de passe avec un chiffrement réversible n'a rien d'encourageant : **70 % pensent que c'est plutôt pratique, alors que 21 % pensent que c'est très utile.** Cette façon de faire a été vivement critiquée dans la communauté de la sécurité de l'information, et avec raison : le stockage de mots de passe avec chiffrement réversible équivaut essentiellement à stocker les mots de passe en clair, sans chiffrement. Par défaut, cette politique ne devrait jamais être implantée, sauf pour de rares exceptions, lorsque les avantages surpassent largement les besoins de protection de l'information.

Un autre fait troublant est que **seulement 43 % des PME croient qu'imposer une longueur minimale de mot de passe est une mesure utile**. Non seulement cette politique est essentielle pour toutes les PME, mais elle devrait être obligatoire. Ceci étant dit, bon nombre d'utilisateurs finaux ont de la difficulté à choisir et à mémoriser des mots de passe longs et complexes. Un bon gestionnaire de mots de passe est alors conseillé.

QUESTION 5

Réutilisez-vous les mêmes mots de passe dans vos comptes (professionnels et/ou personnels)?



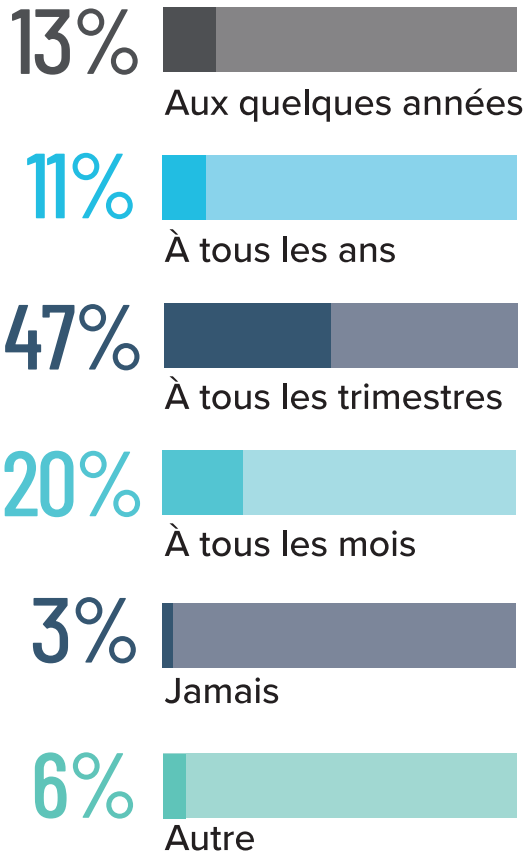
COMMENTAIRES

Selon des recherches, **59 % des utilisateurs finaux réutilisent les mêmes mots de passe pour tous les comptes** pour une raison très humaine : **il est très difficile de se souvenir de plusieurs mots de passe**.

En effet, un utilisateur dans une entreprise a, en moyenne, 191 mots de passe et doit saisir ses informations d'identification au moins 154 fois par mois, toutes applications confondues. Afin de pallier ce problème, les PME devraient implanter un gestionnaire de mots de passe et forcer ses utilisateurs à choisir un mot de passe unique pour chaque compte.

QUESTION 6

À quelle fréquence changez-vous les mots de passe des comptes de l'entreprise?



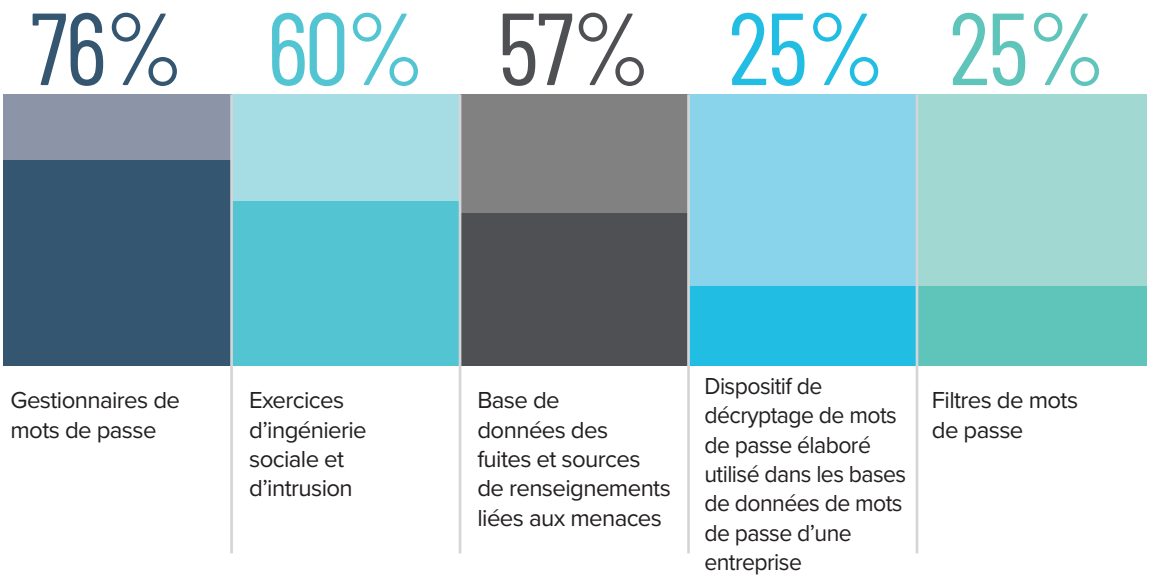
COMMENTAIRES

Par le passé, le *National Institute of Standards and Technology* (NIST) insistait pour que les PME forcent les utilisateurs finaux à changer de mots de passe régulièrement (p. ex., à chaque mois, à tous les trois mois, etc.). Cependant, **le NIST a fait volte-face et recommande maintenant de changer les mots de passe seulement en cas de compromission.**

La raison est simple : **lorsque les utilisateurs finaux choisissent un nouveau mot de passe, ils penchent pour des mots de passe faibles et faciles à décrypter.** La principale cause de ce problème provient de ce qu'on appelle la « fatigue sécuritaire ». Cela se produit lorsque les utilisateurs finaux se sentent dépassés et lassés par l'imposition de plusieurs pratiques et règles quant à la sécurité de l'information.

QUESTION 7

Selon vous, quelles technologies ou mesures de contrôle permettent le mieux de valider et de surveiller les bonnes pratiques relatives aux mots de passe? (Veuillez cocher jusqu'à trois éléments)



COMMENTAIRES

La tendance à adopter un gestionnaire de mots de passe est positive. Toutefois, avant de choisir un (soi-disant) outil gratuit, **il est important de noter qu'ils ont plusieurs limitations**, notamment :

- Aucune assistance par téléphone, et de longs délais de réponse par courriel;
- Difficile à configurer et à déployer;
- Plusieurs contraintes, telles qu'une taille limite de stockage de fichiers chiffrés et pas de copie de sauvegarde en ligne.

C'est également encourageant de découvrir que 60 % des répondants utilisent des tests d'intrusion et des exercices d'ingénierie sociale, qui peuvent aider à détecter des violations de données orchestrées par des personnes à l'interne.

Partie 3

Connaissance et utilisation de la gestion des accès privilégiés dans les PME

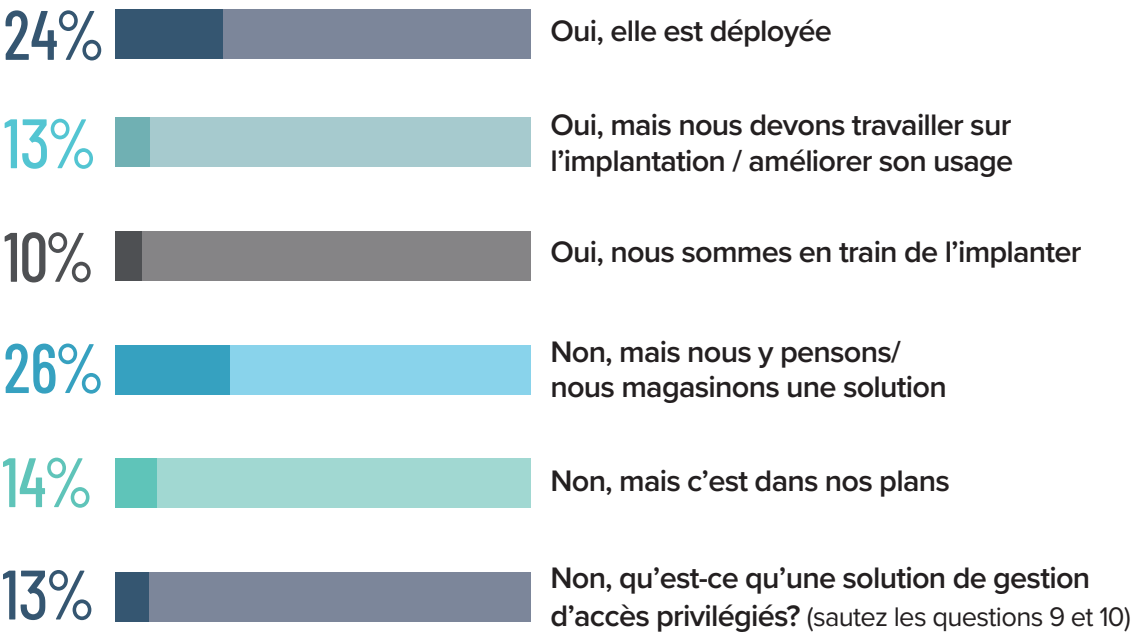
À propos de cette partie

Les solutions de gestion d'accès privilégiés (de l'anglais *Privileged Access Management* (PAM)) permettent aux PME de sécuriser l'accès à des ressources clés, en plus d'instaurer une surveillance des comptes privilégiés avec enregistrement des activités à des fins de conformité. Malgré l'importance de la gestion des accès privilégiés, **88 % des entreprises avec plus d'un million de dossiers n'ont pas de restrictions d'accès appropriées en place, alors que 58 % des entreprises avec plus de 100 000 dossiers donnent un libre accès à tous leurs employés. 55 % des entreprises n'ont aucune idée du nombre de comptes privilégiés qu'elles ont** et comment les trouver. Plus de **50 % des entreprises ont des comptes privilégiés qui n'expirent jamais ou qui sont simplement abandonnés après usage plutôt qu'être supprimés du système. Finalement, 72 % des entreprises ne stockent pas la totalité de leurs comptes privilégiés dans un coffre, que ce soit avec une solution PAM ou un simple gestionnaire de mots de passe. Pour toutes ces raisons, nous avons décidé de nous pencher sur ce sujet.**

Dans la troisième partie du sondage, nous avons donc sondé les PME sur leurs connaissances et leur utilisation de la gestion d'accès privilégiés en général en 2020-2021.

QUESTION 8

Est-ce que votre organisation a implanté une solution de gestion d'accès privilégiés?



COMMENTAIRES

Plusieurs raisons expliquent pourquoi l'adoption d'une solution PAM par les PME se fait souvent à contrecoeur, à pas de tortue ou sans intérêt réel. **Les solutions PAM visent souvent les grandes entreprises** avec un prix hors de portée de ceux qui n'ont pas le même budget. De plus, **le manque d'expertise à l'interne** rend difficile l'implantation et la gestion d'une solution PAM, **sans compter la confusion et la difficulté à bien évaluer les différents produits**. Pour aider à surmonter cet obstacle, il est recommandé aux PME d'effectuer leur comparaison selon les six fonctionnalités essentielles suivantes : la facilité de déploiement et de gestion, un coffre sécurisé de mots de passe, de la journalisation et génération de rapports, l'authentification à deux facteurs, l'injection des informations d'identification et le contrôle d'accès basé sur les rôles.

QUESTION 9

Quelle place la gestion d'accès privilégiés occupe-t-elle dans le plan de cybersécurité de votre organisation?

18%	ESSENTIELLE
20%	TRÈS IMPORTANTE
22%	IMPORTANTE
18%	UN PEU IMPORTANTE
8%	PAS IMPORTANTE
14%	JE NE SAIS PAS

COMMENTAIRES

Plusieurs mythes persistent au sujet des solutions PAM et freinent les PME d'en implanter une dans leur organisation. **En voici quelques-uns :**

MYTHE	RÉALITÉ
Nous n'avons pas besoin d'une solution PAM si nous utilisons un réseau de type avancé.	Plus de 81 % des piratages impliquent des mots de passe volés ou faibles. Les pirates affectionnent particulièrement les comptes d'administrateur de domaine Windows ou le compte root sur UNIX. Une fois qu'ils mettent la main sur le bon mot de passe, ils n'hésitent pas à voler des données, commettre des vols d'identité et ternir des réputations.
Une solution PAM n'est pas nécessaire si les mots de passe sont régulièrement changés.	En théorie, la rotation de mots de passe est une bonne pratique. Cependant, plutôt que de choisir des mots de passe robustes, les utilisateurs finaux ont tendance à choisir des mots de passe faibles.
Une PME qui n'a pas de solution PAM et qui n'a pas été piratée doit donc avoir suffisamment de contrôles de sécurité mis en place.	Les PME n'ayant pas une solution PAM en place devraient se trouver chanceuses plutôt qu'être protégées. Tôt ou tard, une attaque aura lieu et les coûts seront faramineux, voire catastrophiques.
L'implantation d'une solution PAM signifie qu'il faut aussi implanter le principe de moindre privilège, la séparation des tâches et une architecture Confiance zéro. Tous ces beaux principes nuisent à l'efficacité et à la productivité des utilisateurs finaux.	Certes, implanter une solution PAM n'est pas un jeu d'enfant : cela nécessite des ajustements au flux de travail quotidien. Toutefois, ce sont des efforts qui porteront fruit. La clé du succès est de former les utilisateurs finaux et de les responsabiliser afin qu'ils participent activement au programme de sécurité.

QUESTION 10

Selon vous, quels aspects d'une solution PAM encouragent le plus son adoption?
(Veuillez cocher jusqu'à trois éléments)

49%
Séparation des tâches et le principe de moindre privilège

43%
Authentification multifacteur exigée

46%
Audit et conformité

46%
Application de politiques de gestion de mots de passe

42%
Stockage et gestion sécuritaire des informations d'identification

COMMENTAIRES

Les PME dépendent des comptes privilégiés pour accroître l'efficacité et la productivité de leurs employés. Toutefois, elles doivent garder en tête que **les pirates se servent également des comptes privilégiés vulnérables pour compromettre des réseaux, accéder aux systèmes clés et voler des données confidentielles**. Étant donné l'existence de cette dualité, il n'est pas surprenant que Gartner ait présenté **les solutions PAM comme l'un des 10 projets de sécurité de 2019 .**

En outre, la gestion d'accès privilégiés aide les PME à prévenir les menaces internes, en plus de détecter et corriger des erreurs. Des études ont démontré que **15 % de toutes les menaces proviennent de personnes non malicieuses** (p. ex., des employés qui commettent des erreurs graves sans de mauvaises intentions), alors que **13 % proviennent d'initiés malveillants.**

Partie 4

Actions prises par les PME afin d'améliorer la cybersécurité

À propos de cette partie

Avant, la plupart des pirates ne cherchaient qu'à détruire des machines et semer le chaos. Même si ces attaques avaient un impact financier majeur sur l'entreprise visée, ce n'était pas l'objectif principal. Or, les pirates d'aujourd'hui diffèrent de leurs prédécesseurs. **Ils carburent à l'argent et misent sur le vol de données soit pour commettre un vol d'identité, soit pour les vendre sur le Web invisible (*dark web*).**

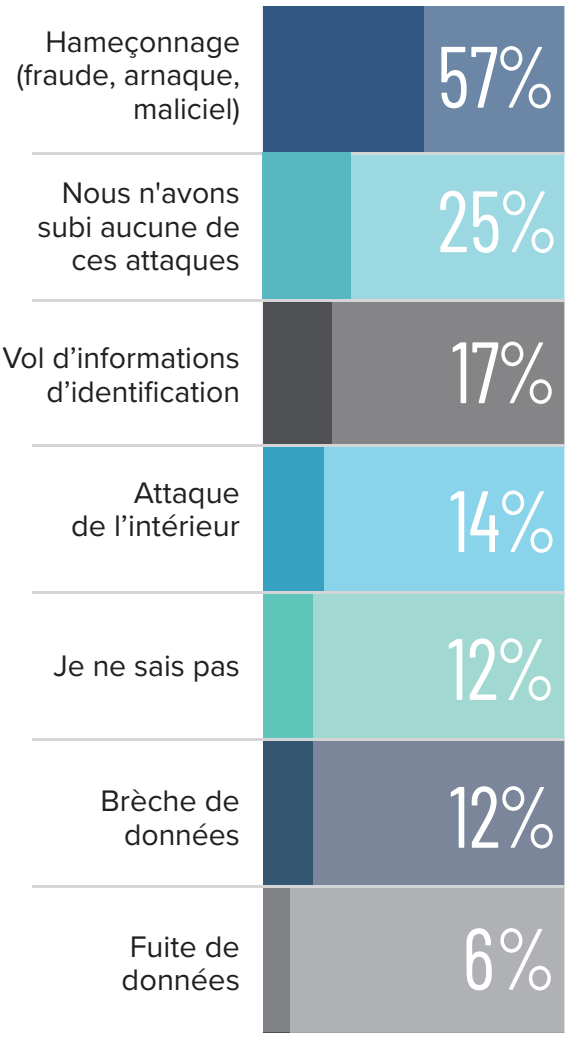
De plus, il y a plusieurs coûts associés à une brèche de données, notamment l'enquête sur l'incident, les mesures de réparation ou de restauration, l'avis aux clients, la gestion de la crise, les amendes ou les pénalités, et, possiblement, des poursuites judiciaires. **Le coût moyen d'une violation de données est maintenant de 117 000 $ par incident**. Il s'agit d'une moyenne : pour plusieurs PME, cela représente beaucoup plus. Pire encore, parlons des dommages causés à la réputation de l'entreprise.

En effet, les dommages causés à la réputation peuvent être plus dévastateurs que les conséquences financières. Ironiquement, plus c'est une grosse compagnie établie, mieux c'est. Par exemple, même si la réputation de Target et de Sony en a pris un coup à la suite de leurs brèches de données respectives, **aucune des deux compagnies n'est passée proche de disparaître de la carte**. Toutefois, plusieurs PME ne peuvent compter là-dessus. Si leur marque s'avère associée à une brèche, il sera difficile, voire impossible, de regagner la confiance des gens dans l'industrie. Selon des études, dans les six mois suivant une cyberattaque, **60 % des petites entreprises mettent la clé dans la porte.**

Dans la quatrième partie de ce sondage, nous avons posé des questions aux PME à propos des actions prises pour augmenter la cybersécurité et pour réduire les risques de cyberattaques en 2020-2021 et dans le futur.

QUESTION 11

Est-ce que votre organisation a subi l'une des attaques suivantes dans les trois dernières années?
(Veuillez cocher tout ce qui s'applique)



COMMENTAIRES

Bien que l'hameçonnage fasse partie du paysage des cybermenaces depuis longtemps, cette stratégie n'est pas près de disparaître. **90 % des brèches de sécurité comprennent un élément d'hameçonnage, 94 % des maliciels sont envoyés par courriel et 56 % des décideurs en informatique croient que la protection contre ces attaques constitue la priorité numéro un de leur organisation en matière de cybersécurité.**

Dans le présent sondage, **14 % des répondants affirment qu'ils ont été victimes d'une attaque de l'interne dans les trois dernières années** — probablement plus puisque **12 % des PME ne savent pas si elles ont été attaquées pendant cette période.** Selon des recherches, **72 % des professionnels des TI admettent que leur organisation est vulnérable face aux menaces internes.** Leur plus grande peur est une erreur commise par un membre du personnel (40 %), suivie d'une attaque d'un employé malveillant (35 %). D'ailleurs, **74 % des professionnels des TI ne peuvent détecter une attaque avant l'exfiltration des données, et 64 % d'entre eux n'ont pas les ressources pour détecter une attaque en temps réel.**

QUESTION 12

Si vous avez répondu « Oui » à la question 11, racontez-nous plus en détail ce qui s'est produit.

Voici quelques réponses de la part des répondants :

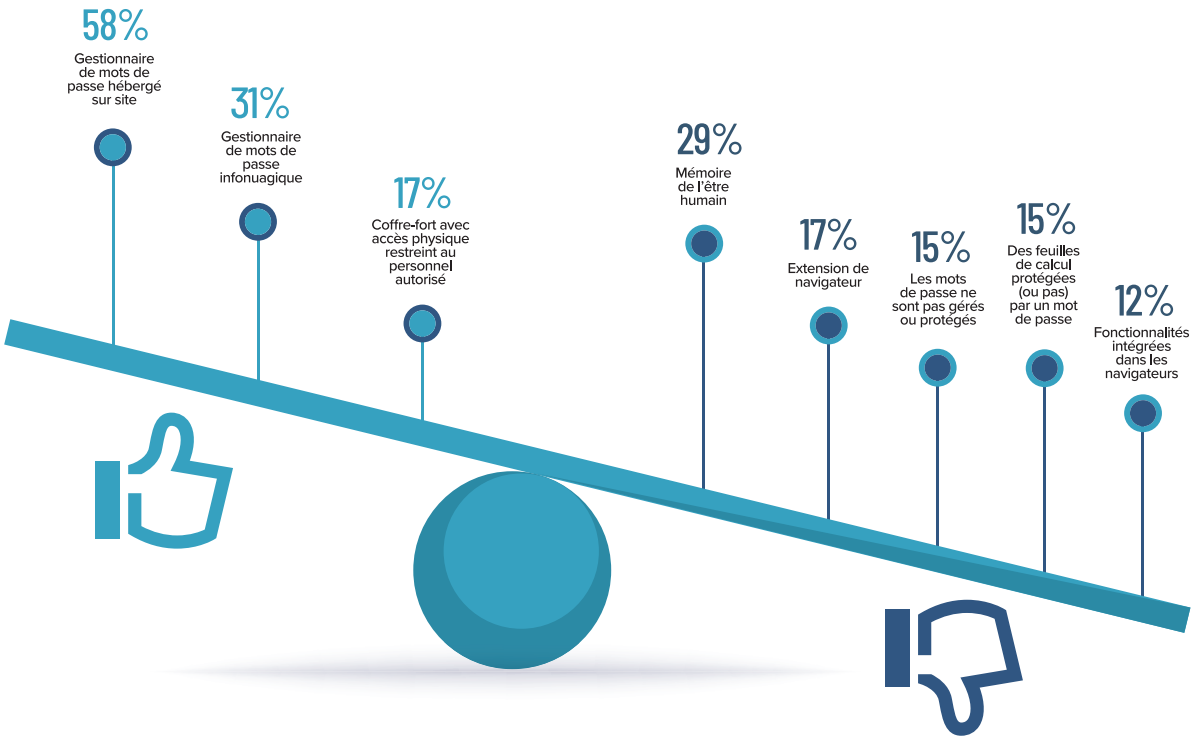
« Les tests d'hameçonnage révèlent qu'un grand nombre d'utilisateurs cliquent sur les liens. Par exemple, un client est tombé dans le panneau en envoyant un paiement préautorisé. Les courriels provenaient d'un compte de messagerie externe contenant une faute dans le nom du domaine. »

« Un pirate, ayant réussi à s'infiltrer dans le réseau d'un vendeur, s'est inséré dans une conversation par courriel entre l'équipe d'AP et le vendeur. Le pirate a alors demandé de changer les informations bancaires pour les paiements. Il a même confirmé le changement par le biais d'un fil de courriels piraté quand l'équipe d'AP a demandé une confirmation. »

« Un utilisateur a cliqué sur un courriel douteux. Un pirate a alors pu prendre le contrôle du compte de courriels de l'entreprise et envoyer massivement des courriels malicieux. Nous avons donc été placés sur la liste noire de plusieurs listes d'envoi. »

QUESTION 13

Qu'est-ce que votre organisation utilise pour gérer et protéger les mots de passe?
(Veuillez cocher tout ce qui s'applique)



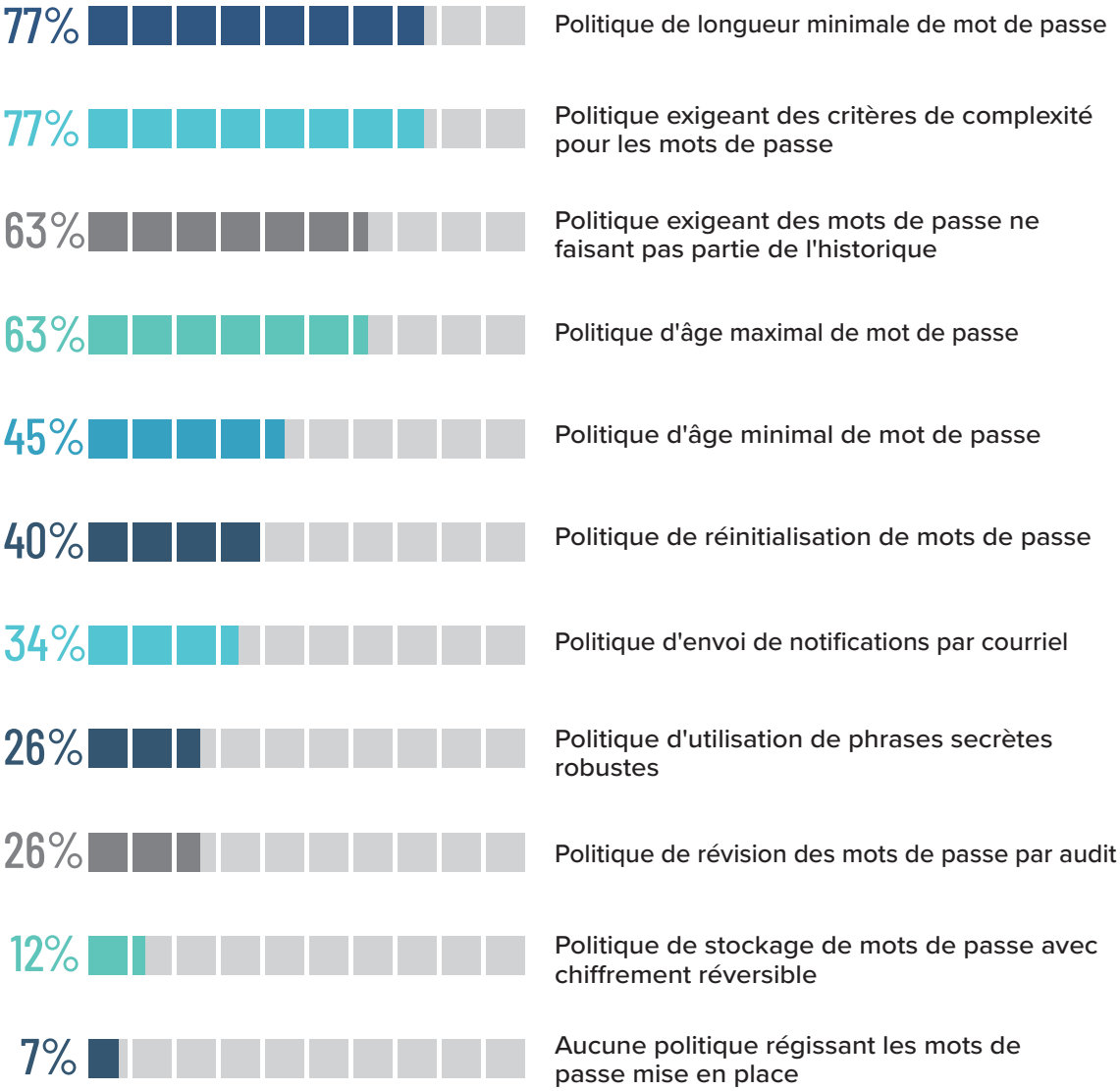
COMMENTAIRES

Il est encourageant de constater que la **majorité des PME utilisent un gestionnaire de mots de passe**. Grâce à cet outil, les utilisateurs n'ont qu'à se souvenir de deux informations de connexion plutôt que des dizaines (ou d'une seule si le gestionnaire de mots de passe intègre l'authentification unique (SSO)). Les entreprises pourraient même aller plus loin en implantant l'authentification biométrique ou matérielle.

Pourtant, l'implantation de gestionnaire de mots de passe n'est pas une pratique adoptée par tous, puisque **29 % des répondants se fient à la mémoire humaine pour certains comptes, et 15 % d'entre eux utilisent des feuilles de calcul.** Cette approche mène presque systématiquement à la réutilisation de mots de passe, ce qui représente un énorme facteur de risque. Même si un mot de passe est complexe, il peut facilement devenir une clé maîtresse pour les acteurs malveillants.

QUESTION 14

Quelles politiques de mots de passe avez-vous mises en place, documentées et communiquées dans votre organisation? (Veuillez cocher tout ce qui s'applique)



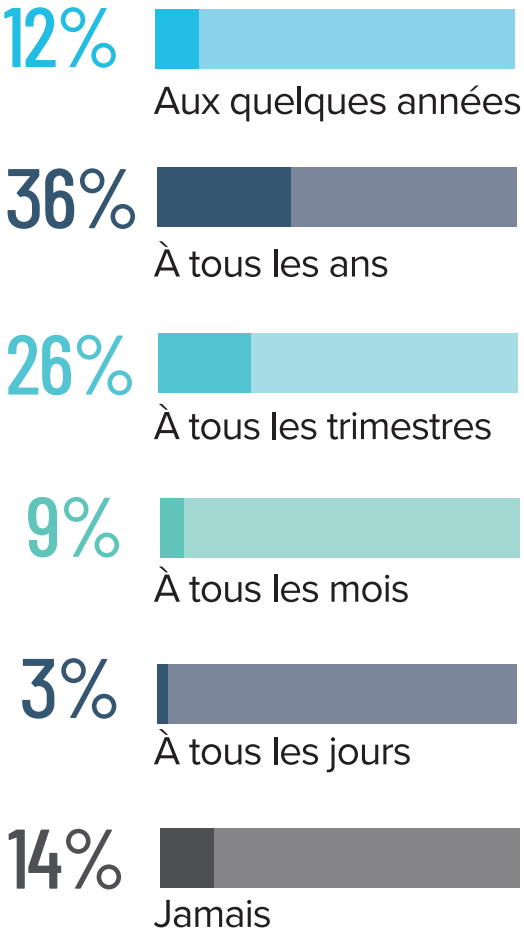
COMMENTAIRES

Auparavant, la longueur minimale de mot de passe requise était d'au moins huit caractères. Toutefois, le *Center for Internet Security* (CIS) recommande maintenant de définir cette valeur à **24 ou plus**. Une recommandation supplémentaire serait de mettre en place une politique reliée à l'âge minimal de mot de passe afin d'empêcher les utilisateurs de changer de mot de passe plusieurs fois en quelques minutes dans le but de réutiliser leur mot de passe préféré.

Considérant la difficulté de choisir un mot de passe à 24 caractères, les PME devraient plutôt inciter les utilisateurs à adopter les **phrases secrètes** **comme autre solution**. Une phrase secrète est beaucoup plus longue qu'un mot de passe classique et peut contenir des lettres, des symboles et des chiffres. Ce peut être une phrase mal écrite ou grammaticalement incorrecte.

QUESTION 15

À quelle fréquence effectuez-vous un audit de sécurité dans votre organisation?



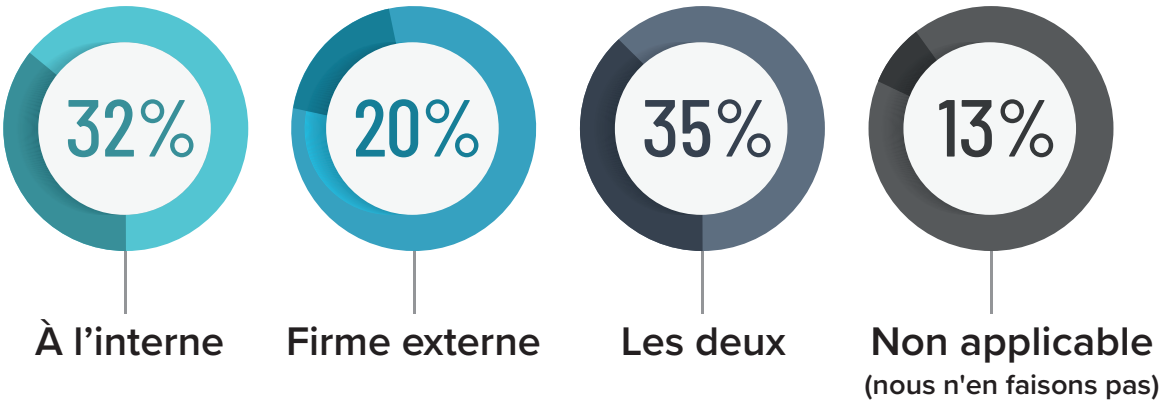
COMMENTAIRES

Même si les experts recommandent d'effectuer au moins deux audits de sécurité par année, le sondage révèle que **62 % des répondants ne satisfont pas ces normes, incluant 14 % des PME qui n'ont jamais mené d'audit.** Il y a généralement deux raisons qui expliquent cette omission. La première : les PME pensent qu'elles sont trop petites pour être ciblées par les cyberpirates. La deuxième consiste en la croyance qu'un audit (et toute autre procédure essentielle de sécurité de l'information) coûte trop cher.

Comme abordé dans ce sondage, **ces deux perceptions sont erronées.** Les PME sont en effet ciblées par les pirates informatiques qui comptent exploiter leurs systèmes vulnérables. En général, le coût d'une brèche de données sera plus grand que le coût de la mise en place de bonnes stratégies de sécurité des données.

QUESTION 16

Est-ce que vos audits de sécurité sont gérés à l'interne ou par une compagnie externe?



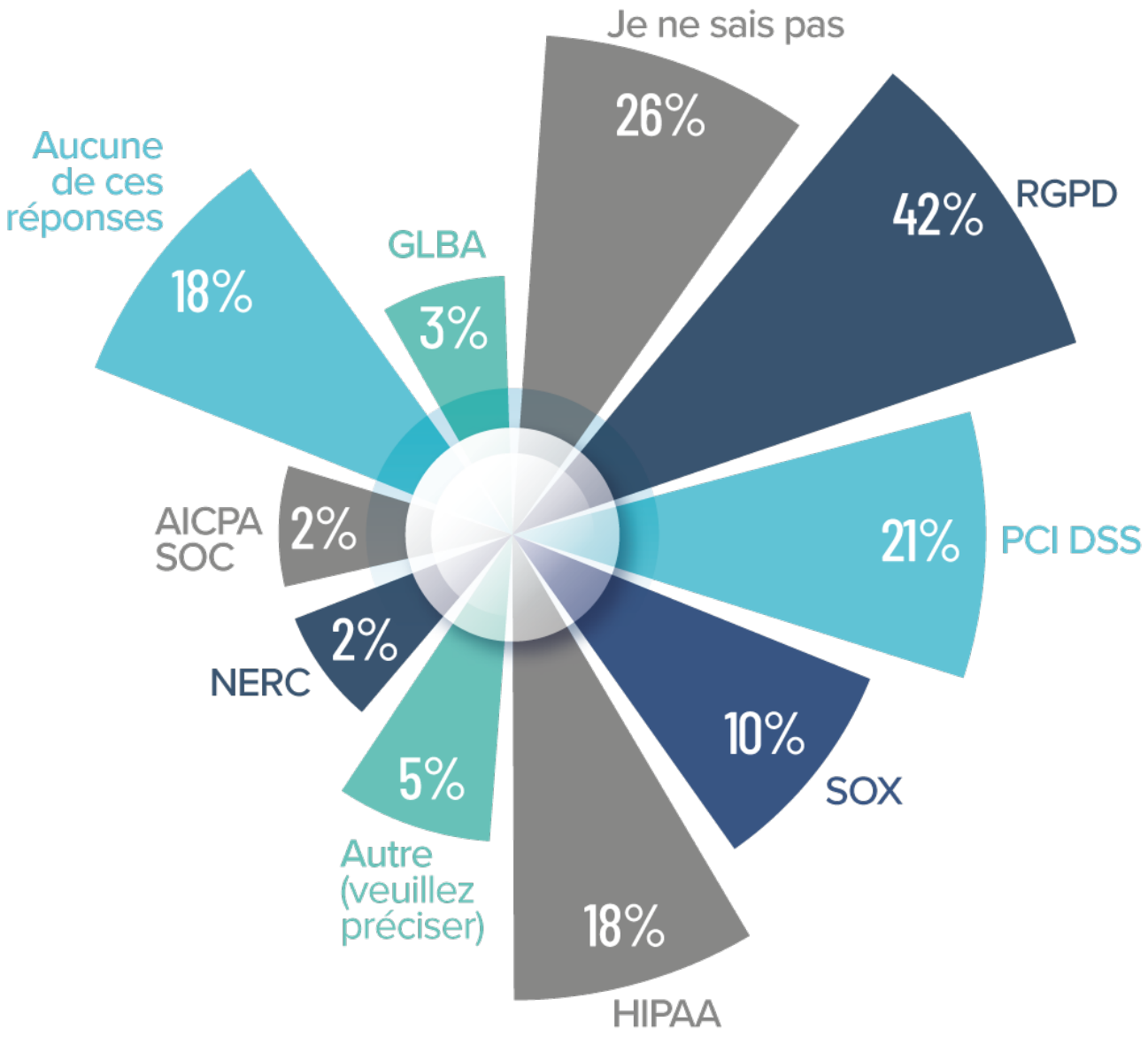
COMMENTAIRES

Idéalement, les PME feraient appel à des auditeurs externes qui ont les compétences et les outils spécialisés. Dans ce cas, il est essentiel de fournir toutes les données pertinentes, de déterminer des buts ou des attentes et de mettre en place toutes les recommandations approuvées.

Or, plusieurs PME mènent leurs audits à l'interne, car ils sont normalement plus abordables, plus rapides et plus pratiques que ceux effectués par des firmes ou des consultants à l'externe. Il est donc important de s'assurer qu'il n'y a pas de conflit d'intérêts, et que l'auditeur ne manipule ou ne dissimule pas de données.

QUESTION 17

À quels programmes de conformité votre organisation se conforme-t-elle?
(Veuillez cocher tout ce qui s'applique)



COMMENTAIRES

Les deux programmes de conformité les plus populaires sont le **RGPD** et **PCI DSS**.

Le Règlement général de la protection des données (RGPD) a été adopté par l'Union européenne et par l'Espace économique européen. Il s'applique à toutes les organisations qui collectent, stockent et utilisent des données personnelles des consommateurs européens, peu importe l'emplacement du siège social de l'organisation dans le monde. Le RGPD régit également le transfert de données à caractère personnel vers d'autres pays à l'extérieur de l'Europe. Il couvre un grand éventail de types de données privées, dont :

- les informations de base (p. ex., nom, adresse, numéro d'identification, etc.)
- les données Web (p. ex., adresse IP, balises RFID, témoins, etc.)
- les informations bancaires
- les informations médicales
- les photos
- les mises à jour sur les réseaux sociaux
- les données biométriques
- les données raciales et ethniques
- les allégeances politiques
- l'orientation sexuelle

PCI DSS est l'acronyme de *Payment Card Industry Data Security Standard*. Il s'agit d'un ensemble de standards international concernant la sécurité des données créé par les principales compagnies de cartes de crédit. Toute entreprise qui stocke, traite ou transmet des données de carte de paiement doit respecter cette norme établie dans le but de protéger à la fois les consommateurs et les entreprises. De l'accompagnement est aussi offert aux créateurs de dispositifs, d'applications et de logiciels qui facilitent les transactions de paiement par carte de crédit.

Dans un rapport, **72 % des clients ont mentionné qu'ils boycotteraient une entreprise qui ne respecte pas la protection de leurs données, et 50 % d'entre eux ont affirmé qu'ils encourageraient une compagnie qui prend la protection des données au sérieux.**

En se conformant à ces règlements, les PME incitent les dirigeants et les employés à comprendre que la sécurité de l'information est au coeur de tout processus ou décision. Il s'agit d'un changement majeur dans la culture de l'entreprise.

QUESTION 18

Formez-vous vos employés sur la cybersécurité?

OUI
88%

NON
12%

COMMENTAIRES

Le fait que **88 % des PME offrent de la formation en cybersécurité à leurs utilisateurs finaux est un bon signe.** Toutefois, étant donné les risques et les conséquences potentielles, le pourcentage devrait être 100 %. Autrement dit, l'éducation devrait être essentielle plutôt qu'optionnelle.

Alors que les PME doivent établir leur plan de formation en fonction de facteurs de risque et d'exigences de conformité qui leur sont propres, **l'approche devrait inclure des contrôles techniques et non techniques :**

- Inscrire les utilisateurs à une formation en cybersécurité sur l'une des plateformes de formation en ligne.
- Déterminer et analyser tous les comptes privilégiés.
- Auditer et analyser les pratiques concernant les départs.
- Simplifier le message.
- Implanter la séparation des tâches.
- Appliquer le principe de moindre privilège.

QUESTION 19

Quelle est la meilleure façon de former les utilisateurs finaux en cybersécurité?
(Veuillez cocher jusqu'à trois éléments)

66% **Fournir de l'information et des conseils pratiques** (vidéos, articles, etc.)

46% **Utiliser les bons outils** (faciles à utiliser, etc.)

37% **Rédiger des politiques, standards et lignes directrices internes**

28% **Utiliser une plateforme de formation en cybersécurité**

23% **Offrir des formations en format *lunch and learn***

21% **Élaborer des simulations**

18% **Créer un canal de communication dédié aux enjeux de la sécurité**

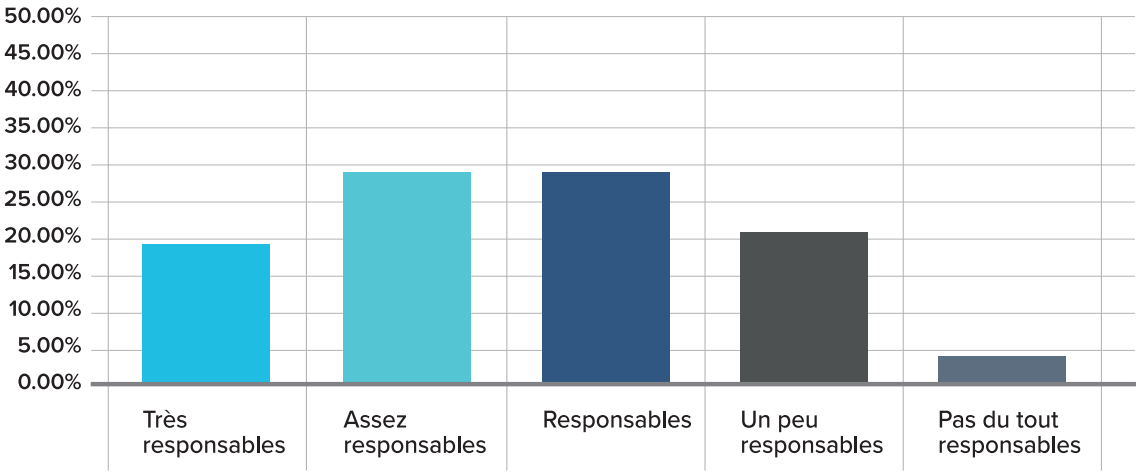
18% **Rendre la formation en sécurité ludique**

COMMENTAIRES

Tel que mentionné plus tôt dans ce rapport, **43 % des cyberattaques ciblent les PME et 60 % des PME font faillite dans les six mois suivant une cyberattaque.** À la lumière de ces statistiques alarmantes, les PME devraient sérieusement envisager d'investir dans une plateforme de formation en cybersécurité, afin que leurs employés puissent servir de dernière ligne de défense au lieu d'ouvrir involontairement la porte aux pirates. Naturellement, il y a des frais à payer (généralement un abonnement annuel basé sur le nombre d'employés). Toutefois, compte tenu des coûts et des conséquences énormes d'un vol de données, y compris une atteinte à la réputation de l'entreprise, le jeu en vaut vraiment la chandelle.

QUESTION 20

À quel degré pensez-vous que les utilisateurs finaux sont responsables en cas de violation de données?



TRÈS RESPONSABLES
« Les utilisateurs finaux sont les premiers responsables lors d'une brèche de données. »

ASSEZ RESPONSABLES
« Les utilisateurs finaux sont assez responsables lors d'une brèche de données. »

RESPONSABLES
« Les utilisateurs finaux sont responsables lors d'une brèche de données. »

UN PEU RESPONSABLES
« Les utilisateurs finaux sont un peu responsables lors d'une brèche de données. »

PAS DU TOUT RESPONSABLES
« Les utilisateurs finaux ne sont pas responsables lors d'une brèche de données. »

COMMENTAIRES

Presque toutes les PME (97 %) s'entendent pour dire que les utilisateurs finaux sont responsables en cas de brèche de données. Par contre, le degré de culpabilité varie : **alors que la moitié des répondants disent que les utilisateurs sont assez ou peu responsables, l'autre moitié (48 %) croit que les utilisateurs sont responsables ou très responsables.**

Partie 5

RECOMMANDATIONS

En matière de sensibilisation à l'importance de la cybersécurité et de protection, les PME sont généralement dans la bonne voie. Or, il reste du travail à faire : des vulnérabilités inquiétantes, 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.

Nous encourageons fortement toutes les PME à analyser et à auditer de façon proactive leur profil de cybersécurité actuel et de suivre les recommandations suivantes :

Les recommandations suivantes demeureront tout aussi pertinentes en 2020-2021 que dans le futur. La pandémie a transformé la façon de travailler partout dans le monde, puisque le télétravail est devenu la norme. Qui dit travail à distance, dit augmentation des risques reliés à cette façon de travailler.

Nous encourageons fortement les PME à mettre en place ces éléments clés afin de renforcer leur profil de cybersécurité.

1. Implanter une solution de gestion d'accès privilégiés
2. Mettre en place des politiques strictes de gestion de mots de passe
3. Appliquer le principe de moindre privilège
4. Implanter la séparation des tâches
5. Offrir de la formation en cybersécurité aux utilisateurs finaux

RECOMMANDATION

1 IMPLANTER UNE SOLUTION DE GESTION D'ACCÈS PRIVILÉGIÉS

Il y a quelques années, pour contrer les pirates, il était tout à fait acceptable pour les PME de se fier aux outils de sécurité visant à protéger le périmètre du réseau : antivirus, pare-feu, portail Web, etc. Cette approche est maintenant insuffisante, puisque les cybercriminels ont considérablement raffiné leurs stratégies d'attaque. Les PME doivent donc s'adapter en implantant une solution PAM qui offre **au moins les sept fonctionnalités suivantes :**

1- FACILITÉ D'IMPLANTATION ET DE GESTION

Pour éviter des problèmes coûteux d'installation et de gestion, voire des maux de tête, les **PME devraient rechercher une solution PAM qui :**

- Offre une implantation simple pilotée par un assistant.
- Dispose d'une console de gestion intuitive.
- Ne nécessite aucune modification à une infrastructure existante d'Active Directory.
- S'intègre avec Azure AD (si Office 365 est utilisé).

En outre, l'option de déployer les composants sur plusieurs serveurs pour améliorer la performance devrait être de mise. Pour assurer la continuité des services, des fonctionnalités de copie de sauvegarde et de restauration doivent être complètes, mais faciles à configurer et à utiliser.

2- COFFRE DE MOTS DE PASSE SÉCURISÉ

Un fait effarant : plus de **81 % des piratages impliquent des mots de passe volés ou faibles. Un coffre sécurisé donne aux PME l'assurance que les mots de passe sont en sécurité et qu'ils peuvent être récupérés si nécessaire par des utilisateurs autorisés**. Cela permet également aux utilisateurs finaux de partager sécuritairement des mots de passe plutôt qu'à les transmettre par courriel, dans des feuilles de calcul, des documents, des *post-it* ou toute autre méthode non sécurisée et non conforme aux standards de l'industrie.

3- JOURNALISATION ET RAPPORTS

Tout comme les grandes entreprises, les PME nécessitent des fonctionnalités complètes de journalisation et de création de rapports afin de savoir qui utilise quel compte privilégié, quand, comment et pourquoi. Toute activité reliée aux mots de passe doit être documentée, incluant les tentatives et l'historique de connexions. Pour ce faire, les PME doivent choisir une solution PAM qui :

- Génère des rapports prêts à l'emploi.
- Offre des options de recherche avancée.
- Produit des rapports personnalisés.
- Prend en charge l'exportation de données en plusieurs formats.

4- AUTHENTIFICATION À DEUX FACTEURS

La prise en charge intégrée de différentes technologies **d'authentification à deux facteurs** est primordiale. Il s'agit un niveau de sécurité supplémentaire qui exige des utilisateurs finaux de saisir leurs informations d'identification en plus d'un autre type d'information. **Cette information peut être :**

- Quelque chose qu'ils savent, comme une réponse à une question secrète ou un NIP.
- Quelque chose qu'ils possèdent, tels un téléphone intelligent ou un jeton.
- Une donnée biométrique (empreinte digitale, visage ou voix).

5- INJECTION DES INFORMATIONS D'IDENTIFICATION

L'injection d'informations d'identification permet aux utilisateurs finaux d'accéder aux comptes privilégiés sans connaître (ni de voir) les informations de connexion. Non seulement **cette fonctionnalité renforce la sécurité, mais elle élimine le besoin d'effectuer constamment des rotations de mots de passe** (c'est-à-dire réinitialiser automatiquement le mot de passe à chaque utilisation). L'injection des informations d'identification empêche également les utilisateurs d'accéder aux ressources en dehors d'un flux de travail, ce qui réduit potentiellement le risque d'abus.

6- CONTRÔLE D'ACCÈS BASÉ SUR LES RÔLES

Les solutions PAM incluant un système de contrôle d'accès basé sur les rôles (RBAC) permettent aux PME de définir plusieurs rôles et d'y associer des niveaux d'accès, pour ensuite les assigner à différents types d'utilisateurs finaux (p. ex., le personnel des TI, le personnel administratif, etc.). Ainsi, **ces utilisateurs n'auront accès qu'aux comptes privilégiés associés à leur rôle, pas plus, ni moins.** Les PME devraient également choisir une solution PAM qui s'intègre avec Active Directory afin d'utiliser des groupes et des utilisateurs déjà existants et définis.

7- ABORDABILITÉ

Dernier point mais non le moindre, les PME doivent considérer **l'abordabilité de la solution.** Heureusement, plusieurs produits offerts sur le marché correspondent au budget des PME. Ce n'était pas le cas avant, alors que seules les grandes organisations pouvaient se permettre d'acheter des licences et des abonnements à un prix exorbitant.

RECOMMANDATION

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* :

1- CONFIGURER L'AUTHENTIFICATION À DEUX FACTEURS

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, l'authentification à deux facteurs empêche les pirates d'accéder aux comptes, même s'ils disposent des informations de connexion correctes.

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 **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).

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, comme « 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 pirates.

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 secrète est une bonne solution. Une phrase secrète 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 grand chien brun, aime quand je joue au frisbee avec lui. » 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 mots de passe plus faibles et plus faciles à décrypter. 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 la recherche sur le domaine *Have I Been Pwned?* 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 pirates de contourner l'authentification à deux facteurs, 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

Un mot de passe doit être comparé avec **une liste de mots de passe faibles ou compromis connus avant d'être choisi.** Il est important que cette liste comprenne des mots liés à l'environnement personnel ou professionnel de l'utilisateur, dont 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 PME devraient 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. 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 lancer 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 ou de la phrase secrète 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 d'accès privilégiés, qui permet aux administrateurs d'autoriser ou de refuser des demandes d'accès. Les administrateurs devraient également imposer un changement de mot de passe obligatoire après que des informations d'identification aient été utilisées et/ou à une heure/date programmée.

7- IMPLANTER UNE POLITIQUE D'HISTORIQUE DES MOTS DE PASSE

Les PME doivent se doter d'une politique d'historique des mots de passe pour garantir que les utilisateurs finaux ne choisissent pas les anciens mots de passe. **Les spécialistes recommandent de définir cette valeur à 24 ou plus** (ce qui signifie que les utilisateurs ne peuvent pas choisir un mot de passe qui a déjà été utilisé parmi les 24 derniers mots de passe). 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 leur mot de passe préféré.

8- ÉLIMINER LA RÉUTILISATION DES 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 (autrement appelé 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.

RECOMMANDATION

3 APPLIQUER LE PRINCIPE DE MOINDRE PRIVILÈGE

Le principe du moindre privilège, *Principle of Least Privilege* (POLP) en anglais, 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. En plus de réduire la taille de la surface d'attaque, ce principe offre d'autres avantages en matière de sécurité, **comme :**

• **Une sécurité renforcée :** Avant de mettre en place le POLP, les PME doivent analyser les niveaux d'accès actuels de chaque utilisateur final. Ce processus révèle souvent que de nombreux utilisateurs finaux – et dans certains cas, la plupart – ont trop d'accès et que cet accès peut facilement être limité sans nuire à leur travail.

• **Lutte contre les logiciels malveillants :** le POLP peut aider à contenir les maliciels sur un nombre limité d'appareils, ce qui peut donner aux PME le temps dont elles ont besoin pour enquêter, contenir et corriger la situation.

• **Une meilleure stabilité :** le POLP empêche les utilisateurs finaux avec des comptes de niveau relativement bas d'exécuter des changements qui affecteraient l'ensemble du système.

• **Classification des données :** le POLP aide les entreprises à déterminer les données dont elles disposent dans leur écosystème, où elles se trouvent et qui y a accès.

• **Préparation aux audits :** le POLP simplifie considérablement le processus d'audit.

Tout dépendant du système d'exploitation, le POLP peut être instauré en se basant sur un ou plusieurs critères **tels que :**

• Rôle (par exemple chefs de projet, gestionnaires de ressources, etc.)
• Ancienneté (par exemple superviseurs, gestionnaires, cadres, etc.)
• Département (par exemple développement, marketing, RH, etc.)
• Emplacement (par exemple le siège social, les bureaux satellites, etc.)
• Heure (par exemple les heures de bureau, après les heures de bureau, etc.)

Règle générale, les administrateurs système personnalisent le POLP en fonction des besoins spécifiques de leur entreprise et cherchent à trouver un équilibre entre la sécurité et la productivité des utilisateurs finaux. Il existe un certain **nombre de bonnes pratiques du POLP qui devraient être adoptées par les PME :**

ÉVALUATION DES NIVEAUX D'ACCÈS

En consultation avec les utilisateurs finaux (ou chefs d'entreprise), **les PME devraient évaluer chaque rôle pour déterminer le niveau d'accès approprié.** L'accès par défaut devrait être défini au « moindre privilège », puis des niveaux d'accès supérieurs devraient être accordés seulement si nécessaire.

COMMUNICATION EFFICACE

Les PME devraient communiquer l'objectif du POLP à tous les utilisateurs finaux afin qu'ils comprennent que l'approche ne vise pas à diminuer leur productivité, mais plutôt à protéger l'organisation. Un petit rappel aux utilisateurs mécontents que la majorité des PME font faillite six mois suivant une cyberattaque peut leur faire changer d'attitude.

INSTAURATION DE MOTS DE PASSE À USAGE UNIQUE

Lorsqu'un accès privilégié temporaire est requis, **les PME devraient utiliser des informations d'identification à usage unique qui sont accordées au dernier moment et qui sont révoquées immédiatement après l'utilisation.** Cette approche, appelée bracketing de privilèges, peut être utilisée pour des utilisateurs finaux individuels ainsi que pour des processus ou des systèmes.

MISE EN PLACE DE LA SÉPARATION DE COMPTES

Les PME devraient séparer les comptes administrateur des comptes standards, puis les fonctions des systèmes de niveau supérieur de celles de niveau inférieur. Cette pratique est expliquée plus en détail dans la prochaine recommandation sur l'implantation de la séparation des tâches.

SURVEILLANCE EN CONTINU ET AUDITS À INTERVALLE RÉGULIER

Il est très important pour les **PME de voir exactement ce que font les utilisateurs finaux et quand ils le font.** De plus, **les PME devraient mener régulièrement des audits auprès des utilisateurs finaux pour s'assurer que leur accès est approprié.** Ceci inclut de supprimer l'accès aux employés qui quittent l'entreprise et de disposer d'un moyen de révoquer automatiquement l'accès privilégié en cas d'urgence.

RECOMMANDATION

4 IMPLANTER LA SÉPARATION DES TÂCHES

Les mêmes facteurs qui rendent les PME particulièrement vulnérables aux pirates externes les rendent également sensibles aux attaques d'employés ou ex-employés mécontents, de fournisseurs, de sous-traitants et autres personnes qui gravitent autour de l'entreprise. Évidemment, les violations de données sont parfois le résultat d'une négligence, d'une incompétence ou d'une erreur humaine. Et c'est là que la séparation des tâches (appelée *Segregation of Duties* (SoD) en anglais) entre en scène.

La séparation des tâches est une politique qui interdit à une seule personne d'être responsable de l'exécution de tâches conflictuelles. L'objectif, comme indiqué dans la norme ISO/IEC 27001, est de réduire les possibilités de manipulation ou d'utilisation abusive ou non autorisée des actifs organisationnels. Autrement dit, lorsque plusieurs personnes sont impliquées dans des tâches à caractère sensible, il y a moins de chances qu'une personne essaie d'enfreindre les règles ou que les erreurs ne soient pas détectées.

SoD est utilisé depuis plusieurs décennies dans la comptabilité, la gestion de risques et l'administration financière. **Cependant, ces dernières années, le concept est entré dans l'espace de la cybersécurité afin de :**

• Prévenir les conflits d'intérêts (réels ou apparents), les actes fautifs, la fraude, les abus et la construction de « silos secrets ».

• Détecter les défaillances de contrôle, telles que les failles de sécurité, le vol d'informations et le contournement des contrôles de sécurité.

• Empêcher les erreurs de se produire parce que les employés portent plusieurs chapeaux.

Les PME doivent adopter rapidement les bonnes pratiques suivantes :

ANALYSER LES NIVEAUX D'ACCÈS

Les PME devraient s'assurer qu'aucune personne n'a accès à un système sans contrôle et sans surveillance. L'exception à cette règle dans de nombreuses PME sera les administrateurs système, qui ont légitimement besoin d'accéder à toutes les applications, bases de données, etc.

ALIGNER LES TÂCHES AVEC LES RÔLES

Les PME devraient configurer les bases de données en respectant le principe de séparation de tâches et de rôles, basé sur le principe du moindre privilège (POLP) expliqué précédemment.

MENER DES AUDITS RÉGULIÈREMENT

Les PME devraient mener des audits de sécurité et porter une attention particulière aux activités potentiellement frauduleuses. Il est conseillé aux PME qui ne disposent pas d'une expertise interne dans ce domaine de travailler avec une firme ou un consultant externe, parce que les activités malveillantes sont presque toujours cachées et difficiles à détecter. De plus, **les PME devraient expliquer clairement aux utilisateurs finaux que des audits et des vérifications sont en cours**. Le simple fait que ces vérifications aient lieu aura un effet dissuasif sur les employés mal intentionnés.

METTRE EN PLACE DES TECHNOLOGIES APPROPRIÉES

Les fonctionnalités clés des outils à implanter sont le contrôle d'accès basé sur les rôles, **l'authentification à deux facteurs et celles des solutions de gestion d'accès privilégiés.**

INTÉGRER DES POLITIQUES DE RESSOURCES HUMAINES

Les PME devraient mettre en place des politiques de ressources humaines qui soutiennent un programme SoD complet. **Elles comprennent les éléments suivants :**

• Procéder à un filtrage préemployé et poursuivre le filtrage continu après l'embauche. L'existence même de cette politique découragera les candidats qui ont une intention malveillante de travailler pour l'entreprise. Elle empêchera probablement aussi les employés actuels d'avoir des activités illicites.

• Former les superviseurs et les gestionnaires à reconnaître, documenter et (au besoin) communiquer tout changement dans les comportements et les habitudes de leurs employés, comme une apparente nervosité lorsqu'on leur pose des questions banales.

• Si possible, forcer les employés à prendre au moins deux semaines de vacances par année. L'ironie est que dans de rares cas, un employé qui semble très travaillant et qui prend rarement du temps pour lui n'est peut-être pas aussi dévoué qu'on le pense. Il est plutôt terrifié à l'idée de voir ses actes illégaux exposés au grand jour. Jonathan Middup, associé chez *Ernst & Young's Fraud Investigation and Dispute Services Practice*, affirme d'ailleurs que « le profil d'un fraudeur typique est un employé de longue date et de confiance, qui travaille de longues heures et hésite à prendre son congé annuel ».

FORMER LES UTILISATEURS FINAUX

Les PME devraient offrir de la formation en cybersécurité aux utilisateurs finaux, idéalement sur une plateforme en ligne. En plus de réduire le risque d'erreurs, la formation sensibilise les employés et favorise une culture de vigilance en matière de cybersécurité, ce qui est dissuasif en soi. La formation en cybersécurité est abordée plus en profondeur dans la prochaine recommandation.

RECOMMANDATION

5 OFFRIR DE LA FORMATION EN CYBERSÉCURITÉ AUX UTILISATEURS FINAUX

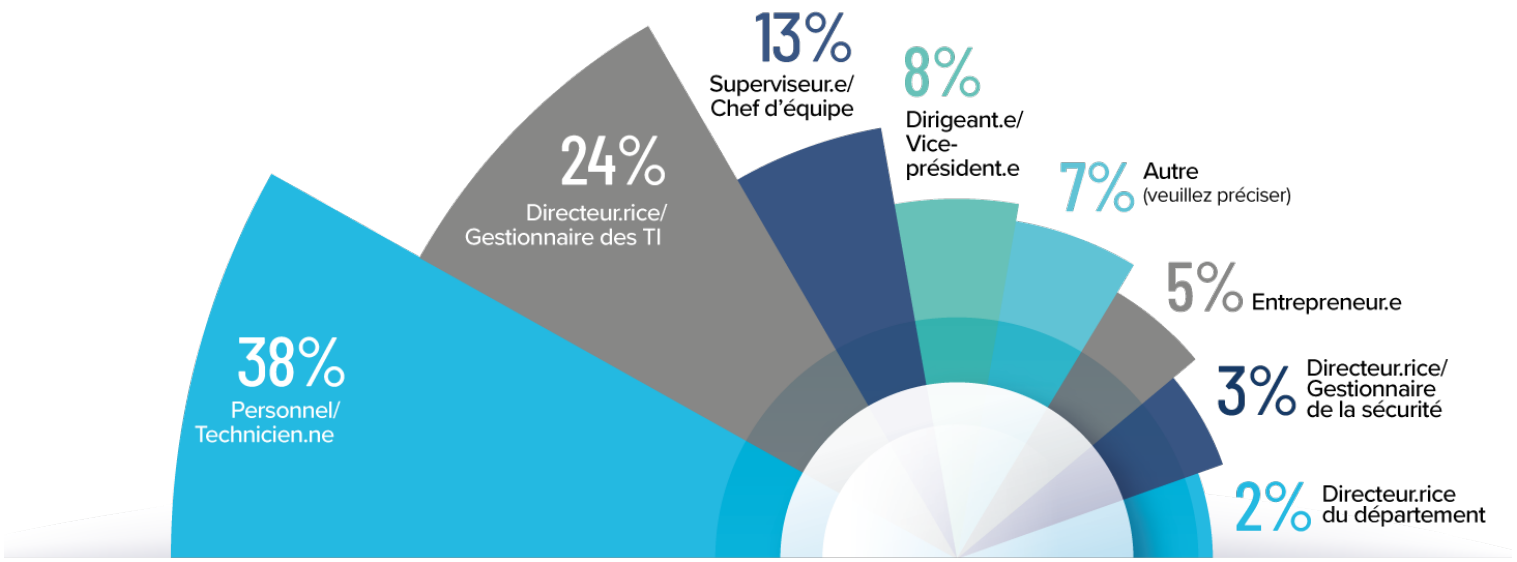
Bien qu'il existe plusieurs façons d'offrir de la formation en cybersécurité, **la plus efficace demeure d'inscrire son équipe sur une plateforme de formation en ligne.** Il s'agit d'une formation pratique basée sur les compétences et chaque participant apprend à son rythme. Les cours sont offerts sous la forme de simulations réalistes et dynamiques. On y traite par exemple des rançongiciels, de l'hameçonnage, d'attaques par déni de service distribué (DDoS), etc. Le programme de formation peut être personnalisé pour couvrir des sujets spécifiques tels que l'ingénierie sociale, la sécurité concernant les courriels, la sécurité des appareils mobiles, la navigation Web sécuritaire, la sécurité sur les réseaux sociaux, la protection des informations relatives à la santé et bien plus.

Les utilisateurs obtiennent un retour immédiat après chaque décision et progressent dans la formation en fonction de leur performance. Les responsables peuvent également se connecter à un tableau de bord et suivre les progrès de chaque employé, puis identifier les forces et les faiblesses de chacun. Par exemple, un employé peut être compétent pour naviguer sur le Web en toute sécurité, mais avoir besoin d'une formation supplémentaire en matière de sécurité des appareils mobiles.

Partie 6

Profil des répondants

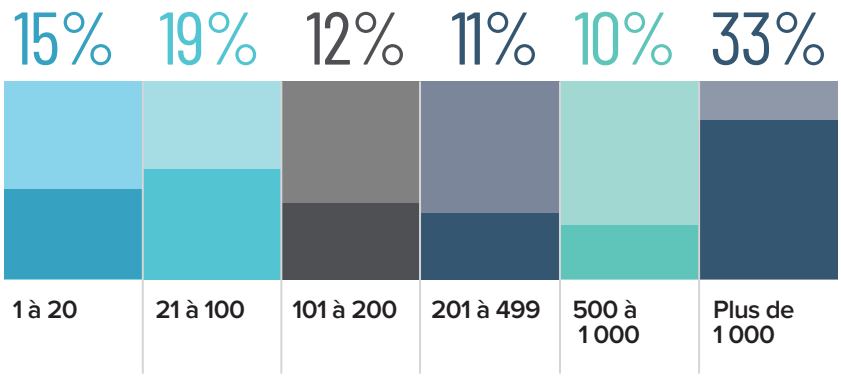
Quel nom de poste correspond le mieux à votre rôle dans l'organisation?



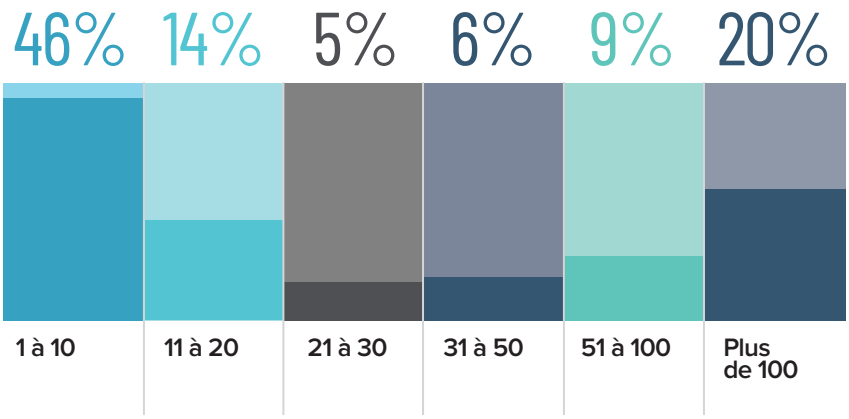
Qu’est-ce qui décrit le mieux le secteur d'activité de votre organisation?

27%	Services de TI
9%	Santé
8%	Éducation
8%	Technologies
8%	Finances et assurances
8%	Industrie manufacturière
4%	Commerce de détail
3%	Organismes à but non lucratif
3%	Services aux consommateurs
3%	Gouvernement
3%	Sécurité informatique et des réseaux
3%	Services généraux aux entreprises
2%	Communications
2%	Divertissement
2%	Transport
2%	Autre (veuillez préciser)
1%	Pharmaceutique
1%	Services publics
0.5%	Mode et vêtement
0.5%	Droit
0.5%	Pétrole et énergie
0.5%	Sécurité, technologies défensives et infrastructure

Combien avez-vous d'employés dans votre organisation?



Combien d'employés travaillent dans le département des TI?



Devolutions aide les PME à prospérer en toute sécurité

Sur le marché mondial, 99% des entreprises sont des petites et moyennes entreprises (PME). Malgré cette statistique plutôt éloquente, toutes les solutions offertes de gestion d'accès privilégiés, de gestion de mots de passe et de gestion de connexions à distance sont très onéreuses et excessivement trop complexes pour la plupart des PME. Ainsi, ces PME sont laissées à elles-mêmes devant les cyberattaques en présentant des failles en matière de sécurité et de conformité, ce qui peut, entre autres, nuire à leur productivité et à leur compétitivité.

Chez Devolutions, nous avons à cœur les intérêts de toutes les entreprises, sans exception. Nous croyons donc qu'il est inconcevable de traiter les PME comme des « citoyens de deuxième classe ». C'est pourquoi nous avons décidé de combler leurs besoins et leurs attentes en conceptualisant des solutions de gestion universelle de connexions à distance et de mots de passe qui sont :

- **Abordables, avec des modèles de licences flexibles correspondant à tous les budgets.**
- **Sécurisées par une protection à toute épreuve, incluant de la journalisation et de la surveillance.**
- **Faciles à déployer autant dans le nuage informatique que dans sa propre infrastructure.**
- **Intuitives et conviviales pour tous les types d'utilisateurs.**
- **Accessibles depuis des applications mobiles afin de travailler à distance en tout temps.**
- **Soutenues par une équipe des ventes et d'assistance technique mondialement réputée.**

Nous créons les meilleures solutions de gestion d'accès privilégiés, de mots de passe et de connexions à distance dans le but d'aider TOUTES les organisations, incluant les PME. De nos jours, peu importe la taille de l'entreprise, tout le monde doit gérer le chaos relié aux TI, renforcer la sécurité et augmenter la productivité afin d'obtenir du succès.

NOTRE GAMME DE PRODUITS

Nous vous présentons nos différentes solutions ci-dessous.

Des essais gratuits sont offerts.

Devolutions Server

Devolutions Server (DVLS) est une solution de gestion de mots de passe et de comptes partagés, qui inclut des composants de gestion d'accès privilégiés répondant aux exigences toujours croissantes en matière de sécurité des PME. Grâce à ce module de gestion d'accès privilégiés, Devolutions Server offre la détection de comptes sur le réseau, un système d'approbation de réservations de comptes et une rotation automatique de mots de passe.

En savoir plus.

Password Hub Business

Password Hub Business (PHB), anciennement connu sous le nom de Devolutions Password Hub, est une solution infonuagique et sécurisée de gestion de mots de passe conçue pour les équipes. Grâce à son interface Web conviviale, les PME peuvent stocker et gérer des informations confidentielles, dont les mots de passe de l'entreprise, en toute tranquillité d'esprit. PHB dispose également d'un système de contrôle d'accès basé sur les rôles, d'un coffre sécurisé de mots de passe, d'un générateur de mots de passe robustes et bien plus.

En savoir plus.

Remote Desktop Manager

Remote Desktop Manager (RDM) vous permet de centraliser toutes vos connexions à distance dans une seule plateforme et de les partager avec tous les membres de l'équipe. Grâce à la prise en charge de centaines de technologies intégrées, dont de multiples protocoles et réseaux privés virtuels, aux gestionnaires de mots de passe complets, aux contrôles d'accès généraux ou granulaires ainsi qu'aux applications clientes et mobiles, RDM est un couteau suisse en matière d'accès à distance. RDM comprend un système de contrôle d'accès basé sur les rôles, l'injection d'identifiants, le partage de mots de passe administratifs, l'enregistrement de session, le stockage centralisé de mots de passe et bien plus.

En savoir plus.

Wayk Client + Wayk Bastion

Wayk Client est une solution d'accès au bureau à distance flexible, conviviale et légère, qui réduit le temps d'implantation et qui maintient les normes de sécurité rigoureuses de l'industrie. Wayk Client est la solution idéale d'accès de bureau à distance à la fois pour les professionnels des TI et pour fournisseurs de services gérés.

Wayk Bastion est le serveur centralisé de Wayk Client qui peut être hébergé sur vos propres serveurs ou dans le nuage informatique. Il permet d'accéder à toutes les machines dans plusieurs réseaux différents et de les surveiller à partir d'un tableau de bord Web facile à utiliser.

En savoir plus.

Devolutions

COMMENT JOINDRE DEVOLUTIONS

Basée à Lavaltrie, Québec, Canada, Devolutions offre des solutions alliant productivité et sécurité à plus de 500 000 professionnels des TI répartis dans 140 pays dans le monde. Pour toute question ou demande d'essai gratuit, veuillez communiquer avec nous :

Par courriel : sales@devolutions.net

Par téléphone : +1 844 463.0419

Par clavardage sur notre site Web : https://devolutions.net/fr