Devolutions

PORTRAIT DE LA CYBERSÉCURITÉ DANS LES PME

en 2021-2022

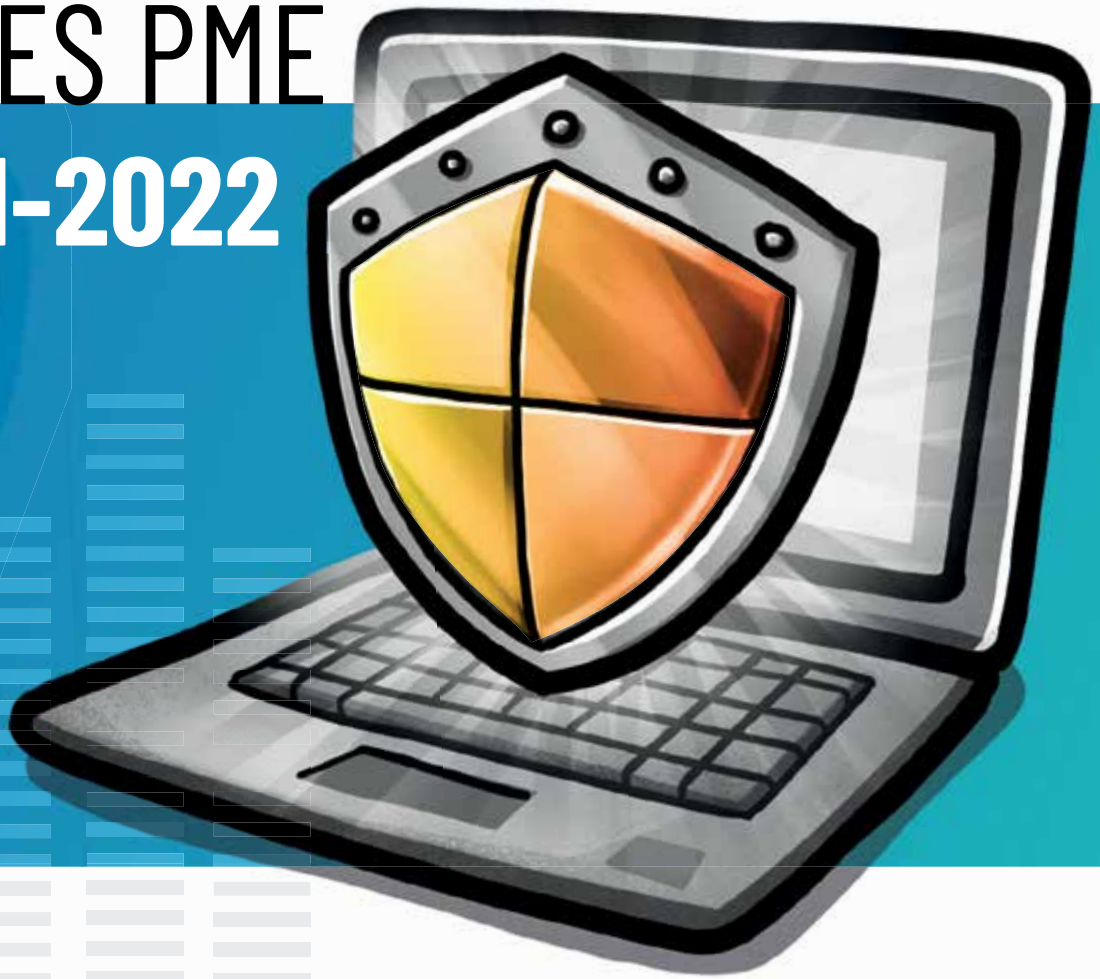


TABLE DES MATIÈRES

RÉSUMÉ

Alors que la pandémie a obligé de nombreuses petites et moyennes entreprises (PME) à réduire leurs activités, les pirates informatiques sont passés à la vitesse supérieure. Les cyberattaques contre les PME (notamment contre leurs travailleurs à distance) ont augmenté en 2020 et 2021.

Par ailleurs, les conséquences d'une violation n'ont jamais été aussi sévères. La cybercriminalité mondiale coûte collectivement aux victimes 16,4 milliards US chaque jour, et en 2021, le coût moyen d'une violation de données dans les PME a atteint 2,98 millions US par incident. Il s'agit d'un prix vertigineux que de nombreuses entreprises ne peuvent tout simplement pas se permettre, ce qui explique que 60 % des PME cessent leurs activités dans les six mois suivant un piratage.

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 cinq sujets pertinents, notamment :

- **Les cyberattaques et les menaces chez les PME**
- **La gestion de mots de passe dans les PME**
- **La gestion d'accès privilégiés dans les PME**
- **La formation et la gestion de la cybersécurité chez les PME**
- **Les investissements en cybersécurité chez les PME**

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.

[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.

Voici quelques faits saillants du sondage :

72%

des PME ont affirmé qu'elles étaient plus préoccupées par la cybersécurité aujourd'hui qu'il y a un an.

Ce degré accru d'inquiétude parmi les PME est justifié. L'année dernière, nous avons assisté à une augmentation spectaculaire de la fréquence, de la taille et de la gravité des cyberattaques (y compris la violation ultra-sophistiquée de la chaîne d'approvisionnement de SolarWinds/Solorigate qui a ciblé des victimes très médiatisées).

Les rançongiciels, l'hameçonnage et les logiciels malveillants sont les trois cybermenaces les plus inquiétantes selon les PME.

C'est un changement par rapport à l'enquête de Devolutions sur le portrait de la cybersécurité dans les PME en 2020-2021, qui a révélé que la principale préoccupation des PME en matière de cybersécurité était les vulnérabilités infonuagiques. Cependant, il n'est pas surprenant que les rançongiciels occupent désormais la première place.

Considérez ces statistiques inquiétantes :

des fournisseurs de services gérés considèrent les rançongiciels comme une menace courante pour les PME.

des victimes de rançongiciel sont des PME.

En 2021, une organisation sera victime d'une attaque par rançongiciel une fois toutes les 11 secondes.

Les coûts mondiaux des rançongiciels devraient atteindre 20 milliards de dollars d'ici la fin de 2021.

52% des PME **ont été victimes d'au moins une cyberattaque** dans la dernière année.

10% ont subi **plus de 10 cyberattaques.**

Cela signifie-t-il que 48 % des PME sont en sécurité? Non, ce n'est pas le cas, car il est pratiquement assuré que certaines, ou la plupart, voire toutes les PME, qui n'ont pas signalé de cyber-attaque l'année dernière ont en fait été ciblées (probablement à plusieurs reprises), mais ne le savent pas.

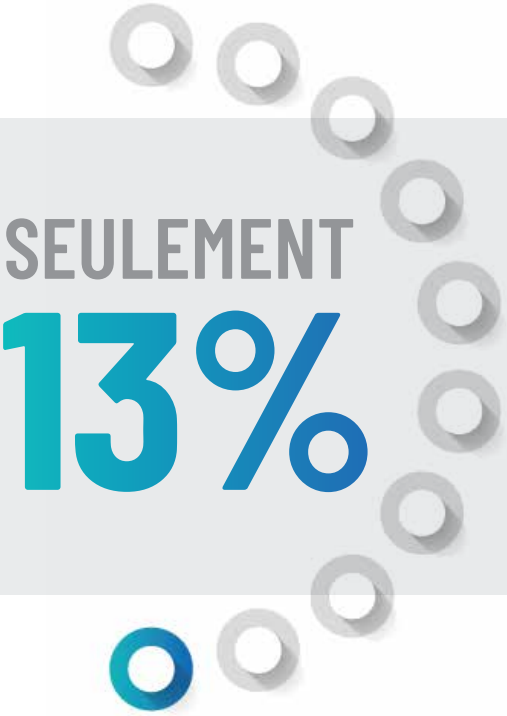
> Il n'y a que deux types d'organisations : celles qui ont été piratées et celles qui ne le savent pas encore!
>
> - ITPortal.com

1/5

utilise **des méthodes non sécurisées pour stocker les mots de passe**, comme des feuilles de calcul, des documents non chiffrés et des Post-it.

Cela est probablement dû à un faux sentiment de sécurité, c'est-à-dire : « Nous n'avons pas encore été piratés, et donc nos pratiques de gestion des mots de passe doivent être bonnes et sûres. »

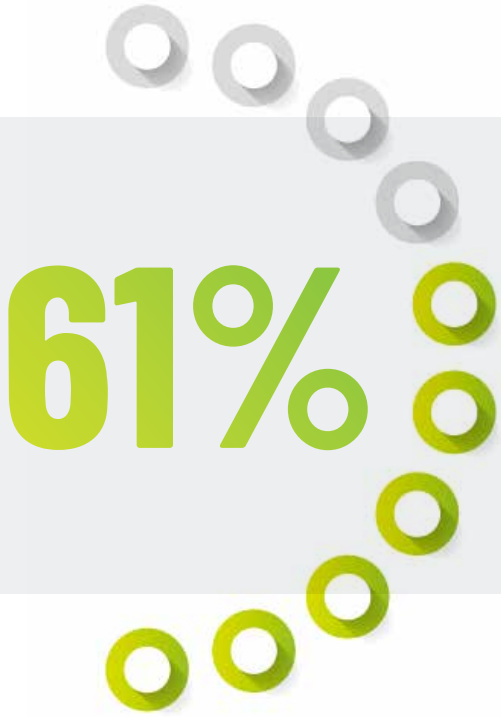
Malheureusement, c'est le contraire qui est vrai. Il suffit d'une seule violation pour entraîner des conséquences énormes et potentiellement catastrophiques, notamment la perte de clients et une atteinte durable à la réputation.



des PME **ont déployé une solution de gestion d'accès privilégiés au sein de leur entreprise.**

Ce chiffre est en baisse par rapport aux 24 % de l'enquête de Devolutions sur le portrait de la cybersécurité dans les PME en 2020-2021. Si de nombreuses raisons peuvent expliquer cette baisse, l'un des facteurs probables est que certaines PME se rabattent sur les gestionnaires de mots de passe pour remplacer une solution de gestion d'accès privilégiés.

C'est une erreur! **Certes, les gestionnaires de mots de passe jouent un rôle important dans l'ensemble des mesures de sécurité**, mais ils ne sont pas foncièrement conçus pour gérer l'accès aux comptes privilégiés et ne peuvent pas fournir la visibilité, le contrôle et la gouvernance nécessaires pour sauvegarder les données sensibles, respecter les exigences de conformité et gérer à l'échelle.



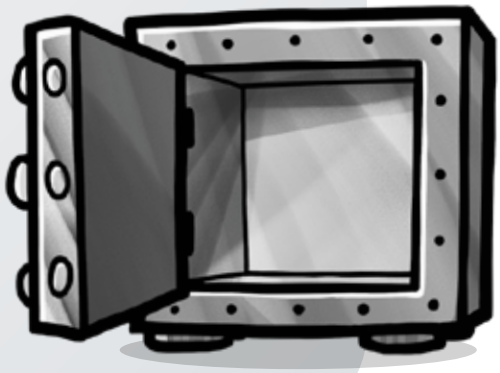
61% des PME **ne surveillent pas la totalité de leurs comptes privilégiés.**

Il s'agit d'une vulnérabilité majeure, qui a peut-être déjà été exploitée plusieurs fois sans être décelée. Par exemple, les pirates ciblent régulièrement les comptes d'administrateur local, car de nombreuses PME accordent ce niveau d'accès à tous les employés.

Une fois à l'intérieur, les pirates se cachent sans être détectés pendant qu'ils scrutent les défenses de la PME et mènent des cyberattaques efficaces.

79%

des PME **considèrent que les utilisateurs finaux sont responsables en cas de brèche de données.**



Des études ont révélé que près de la moitié des violations de données sont dues à la négligence ou à l'imprudence des employés. Cela signifie que les PME qui consacrent la totalité de leurs investissements et de leurs efforts en matière de cybersécurité à essayer d'arrêter les pirates sont toujours vulnérables, car leurs propres employés peuvent être à l'origine de violations coûteuses.

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

Il s'agit d'une baisse de 14 % par rapport à l'enquête de Devolutions sur le portrait de la cybersécurité en 2020-2021. Qu'est-ce qui explique cette chute? La cause première la plus probable est la pandémie. Faire face à des changements rapides et sans précédent a obligé de nombreuses PME à se concentrer exclusivement sur les activités fondamentales de l'entreprise.

Or, la formation de leur personnel à la cybersécurité doit faire partie de cette priorité! Les pirates ont multiplié les attaques contre les PME pendant la pandémie et s'en prennent aux travailleurs à distance, qui sont souvent beaucoup plus vulnérables en dehors de l'environnement du réseau de l'entreprise.

40%

des PME **n'ont pas un plan d'intervention en cas d'incident complet et à jour.**

Des recherches ont démontré que les organisations disposant d'un plan d'intervention en cas d'incident de cybersécurité complet et bien rodé ont réduit le coût d'une violation de 2 millions de dollars en moyenne, par rapport aux organisations ne disposant pas d'un plan solide et d'une équipe adéquate. **Nous avons tous entendu le dicton « le temps, c'est de l'argent ». Dans ce cas précis, c'est une vérité absolue!**

26%

des PME **consacrent moins de 5 % de leur budget en TI à la cybersécurité.**

S'il est vrai que consacrer de l'argent à la cybersécurité n'est pas une baguette magique qui rendra les PME invulnérables, il n'en reste pas moins que, tout bien considéré, une PME dont le profil de cybersécurité est complet sera beaucoup plus sûre qu'une PME présentant des vulnérabilités.

Les experts conseillent aux entreprises **d'allouer entre 7 et 10 % de leur budget informatique** aux technologies et aux formations en matière de cybersécurité.

RECOMMANDATIONS

Dans le rapport du portrait de la cybersécurité dans les PME en 2021-2022, nous avons également intégré 15 recommandations spécifiques pour aider les PME à combler les lacunes, les vulnérabilités et les préoccupations mises en évidence par l'enquête.

Toutes ces recommandations sont pratiques, éprouvées et abordables pour les PME.

À PROPOS DE CE RAPPORT

Au total, 440 répondants ont reçu le questionnaire contenant 25 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 sept parties :

PARTIE 1
Les cyberattaques et les menaces chez les PME

PARTIE 2
La gestion de mots de passe dans les PME

PARTIE 3
La gestion d'accès privilégiés dans les PME

PARTIE 4
La formation et la gestion de la cybersécurité chez les PME

PARTIE 5
Les investissements en cybersécurité chez les PME

PARTIE 6
Recommandations

PARTIE 7
Profil des répondants

PARTIE 1

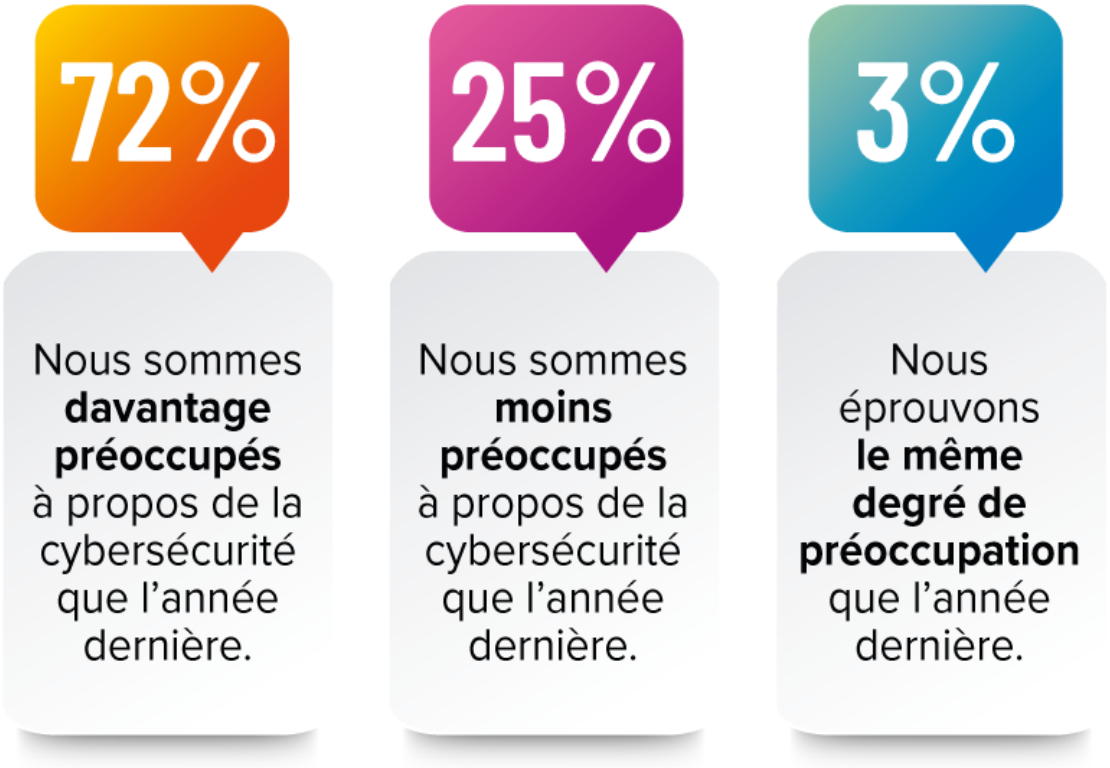
LES CYBERATTAQUES ET LES MENACES CHEZ LES PME

Les pirates ont multiplié les attaques contre les PME lors de la pandémie. Parallèlement, la migration croissante des services vers le nuage ainsi que l'augmentation du nombre de télétravailleurs ont grandement étendu la surface d'attaque : cela offre aux pirates davantage de portes d'entrée et de possibilités pour voler des données sensibles et confidentielles.

Dans la première partie de notre sondage, nous avons interrogé les PME sur leur degré d'inquiétude concernant la confidentialité et la sécurité des données de leur entreprise, de même que leur expérience quant aux cyberattaques et aux brèches au cours de l'année dernière.

Question 1

En raison de l'année difficile venant de s'écouler et des importantes brèches de données survenues récemment, veuillez indiquer votre degré de préoccupation en lien avec la confidentialité ainsi que la sécurité des données de votre entreprise.

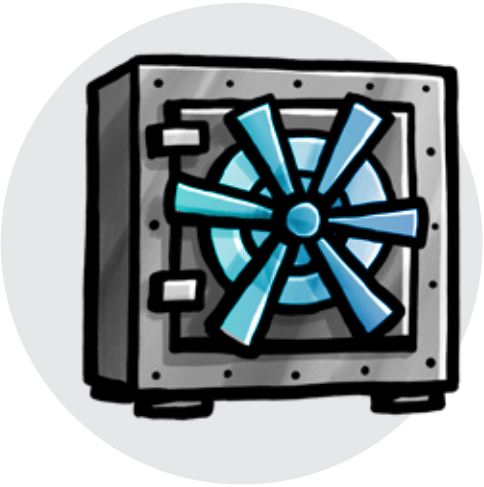


Commentaires

Près de 3 PME sur 4 (72 %) ont affirmé qu'elles étaient plus préoccupées par la cybersécurité aujourd'hui qu'il y a un an. **Cet état d'esprit confirme une tendance que nous avons constatée dans le rapport sur le portrait de la cybersécurité en 2020-2021, où approximativement 9 PME sur 10 (88 %) ont reconnu qu'elles étaient davantage préoccupées par la cybersécurité qu'il y a cinq ans.**

Ce degré élevé d'inquiétude chez les PME est légitime. Il y a eu une augmentation spectaculaire de la fréquence, de la taille et de la gravité des cyberattaques l'année dernière. On ne peut que mentionner la brèche hautement sophistiquée de SolarWinds/Solorigate ciblant des victimes très réputées comme le Pentagone, le Trésor américain, le ministère américain de la Sécurité intérieure, Microsoft, Cisco, Intel, FireEye, Deloitte et plusieurs autres. Hélas, comme les pirates informatiques sont connus pour répéter la même tactique jusqu'à ce qu'elle ne fonctionne plus, les experts estiment que de nombreuses autres attaques de la chaîne d'approvisionnement se multiplieront dans les mois et années à venir.

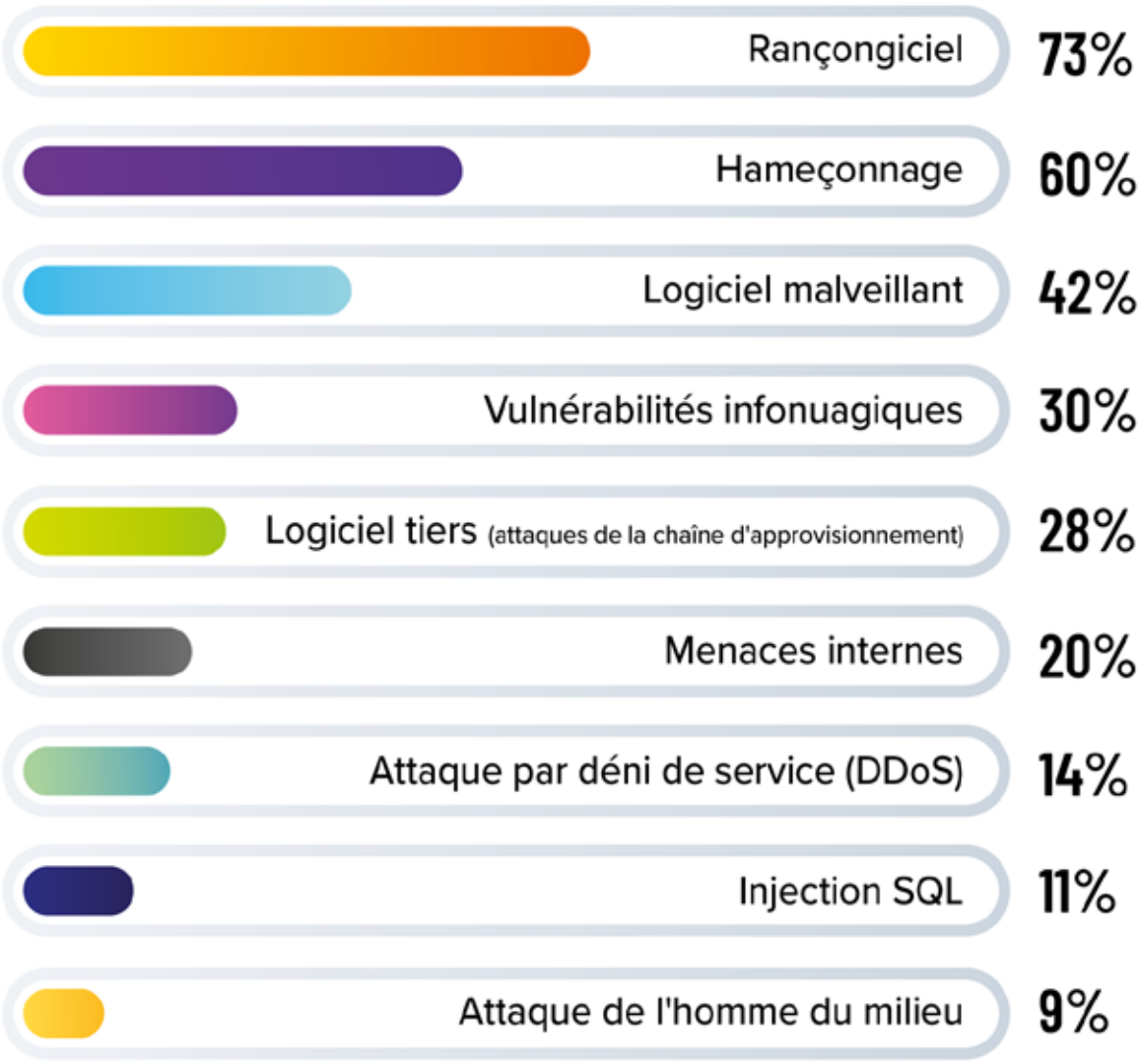
Le constat est clair : les entreprises doivent se concentrer sur cet enjeu et, plus important encore, prendre des décisions immédiates, mais également intelligentes, et les mettre en oeuvre afin de réduire les risques.



Dans la section des recommandations de ce rapport, nous listons plusieurs stratégies, politiques et outils de cybersécurité que les PME devraient déployer sans attendre.

Question 2

Choisissez les 3 cybermenaces qui vous préoccupent le plus.



Commentaires

Les rançongiciels remportent la palme du palmarès des cybermenaces préoccupant le plus les PME. Il s'agit d'un changement depuis le rapport sur le Portrait de la cybersécurité de 2020-2021, qui a révélé que la principale préoccupation des PME concernait les vulnérabilités infonuagiques. Cependant, il n'est pas surprenant que les rançongiciels aient pris la première place. Regardez ces statistiques effrayantes :

- **En 2021, une organisation est victime d'une attaque par rançongiciel une fois toutes les 11 secondes.**
- **Les coûts mondiaux devraient atteindre 20 milliards de dollars d'ici la fin de 2021.**
- **20 % des victimes de rançongiciels sont des PME.**
- **85 % des fournisseurs de services gérés considèrent les rançongiciels comme une menace courante pour les PME.**

Il est naturel que les PME soient également préoccupées par l'hameçonnage (60 %), et les chiffres le confirment :

- **94 % des logiciels malveillants sont diffusés par courrier électronique.**
- **90 % des incidents et des brèches comportent un élément d'hameçonnage.**
- **28 % des attaques par hameçonnage sont ciblées.**
- **21 % des rançongiciels impliquent de l'ingénierie sociale, comme l'hameçonnage.**

Les préoccupations relatives aux logiciels malveillants complètent le trio de tête des menaces les plus angoissantes.

De plus, il est remarquable et troublant de constater que seulement 28 % des PME sont préoccupées par les attaques de la chaîne d'approvisionnement. Comme nous l'avons souligné précédemment dans ce rapport, il y a une augmentation de ce type d'attaque. Bien que les fournisseurs tiers fassent assurément partie de la solution, les PME doivent également être proactives.

Dans la section des recommandations, nous prodiguons des conseils afin d'aider les entreprises à se protéger contre les rançongiciels, l'hameçonnage et les attaques de la chaîne d'approvisionnement.

Question 3

Combien de fois votre entreprise a-t-elle subi une cyberattaque ou une brèche de sécurité l'année dernière?

Commentaires

Au premier abord, cela peut ressembler à une histoire de « bonnes nouvelles, mauvaises nouvelles ». La bonne nouvelle est qu'environ la moitié des PME (48 %) sont a priori en sécurité, car elles n'ont pas été visées par des pirates au cours de l'année précédente. La mauvaise nouvelle est que la majorité (52 %) a été attaquée au moins une fois par mois et 8 % plus de 11 fois.

Malheureusement, il s'agit de toute évidence d'une histoire de « mauvaises nouvelles, pires nouvelles », car il est pratiquement assuré que certaines, la plupart, et même la totalité des 48 % de PME n'ayant pas signalé de cyberattaques au cours de l'année écoulée ont en fait été ciblées à de nombreuses reprises. Comme le souligne ITPortal.com : « Il n'y a que deux types d'organisations : celles qui ont été piratées et celles qui ne le savent pas encore! »

Un plan de réponse exhaustif et efficace est primordial pour réagir et se relever des attaques. Nous y reviendrons plus en détail **dans la section des recommandations de ce rapport.**

Question 4

Croyez-vous que votre entreprise soit susceptible d'être visée par des pirates maintenant ou dans un avenir rapproché?

OUI

81%

NON

19%

Commentaires

Le fait qu'environ 1 PME sur 5 ne croit pas qu'elle sera la cible de pirates, maintenant ou dans un avenir immédiat, met en évidence un mythe tenace, et potentiellement catastrophique, auquel croient de nombreux propriétaires et dirigeants d'entreprise : qu'ils sont trop petits pour être attaqués. En réalité, c'est le contraire qui est vrai.

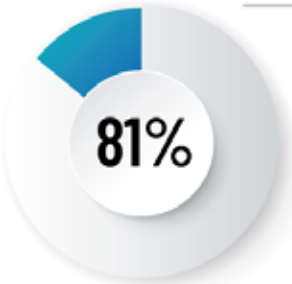
Non seulement les pirates ciblent les PME, mais ils intensifient leurs attaques pour une raison très simple : en comparaison avec la plupart des grandes organisations et entreprises, leurs moyens de défense sont plus limités ou, dans certains cas, pratiquement inexistants.

Ainsi, pour ce qui est de l'exposition aux menaces de cybersécurité, les PME doivent avant tout accepter que leur taille relativement petite ne soit pas un avantage. C'est plutôt un handicap, car les pirates supposeront qu'elles sont vulnérables. Les PME doivent démontrer le contraire. Sans quoi, la question ne sera pas de savoir si une attaque se produira, mais sa date et sa gravité. En effet, selon le rapport 2021 d'IBM sur le coût d'une brèche de données, il se chiffre en moyenne à 2,98 millions de dollars américains par incident : cela représente le plus haut montant en 17 ans d'existence du rapport.

PARTIE 2

LA GESTION DE MOTS DE PASSE DANS LES PME

Les employés autonomes sont très appréciés. Cependant, il y a un domaine essentiel où les PME doivent prendre les devants et appliquer les normes et les pratiques : la gestion des mots de passe. **Constatez ce qui suit :**



des violations de données sont causées par des mots de passe compromis, faibles et réutilisés.

59% des utilisateurs finaux réutilisent les mêmes mots de passe pour plusieurs comptes.

****

34% des utilisateurs ont admis avoir transgressé les règles et partagé leurs mots de passe au travail.

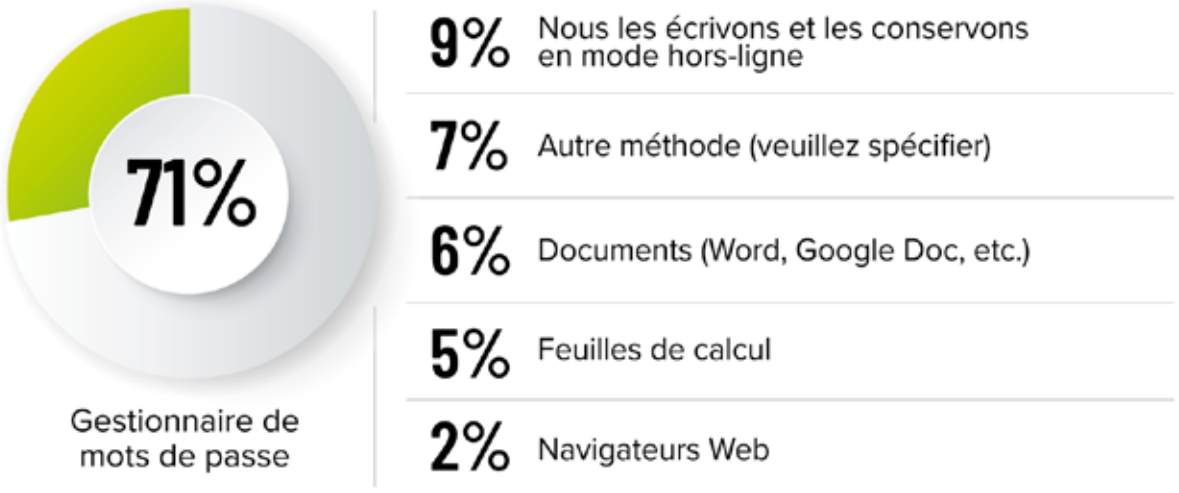
39%

des utilisateurs écrivent leurs mots de passe sur un morceau de papier, alors que 10 % les conservent sur un fichier dans leur ordinateur.

Dans la deuxième partie de notre enquête, nous avons demandé aux PME de faire part de leurs perspectives, pratiques et politiques en matière de gestion de mots de passe en 2021.

Question 5

Comment votre entreprise conserve-t-elle les mots de passe?



Commentaires

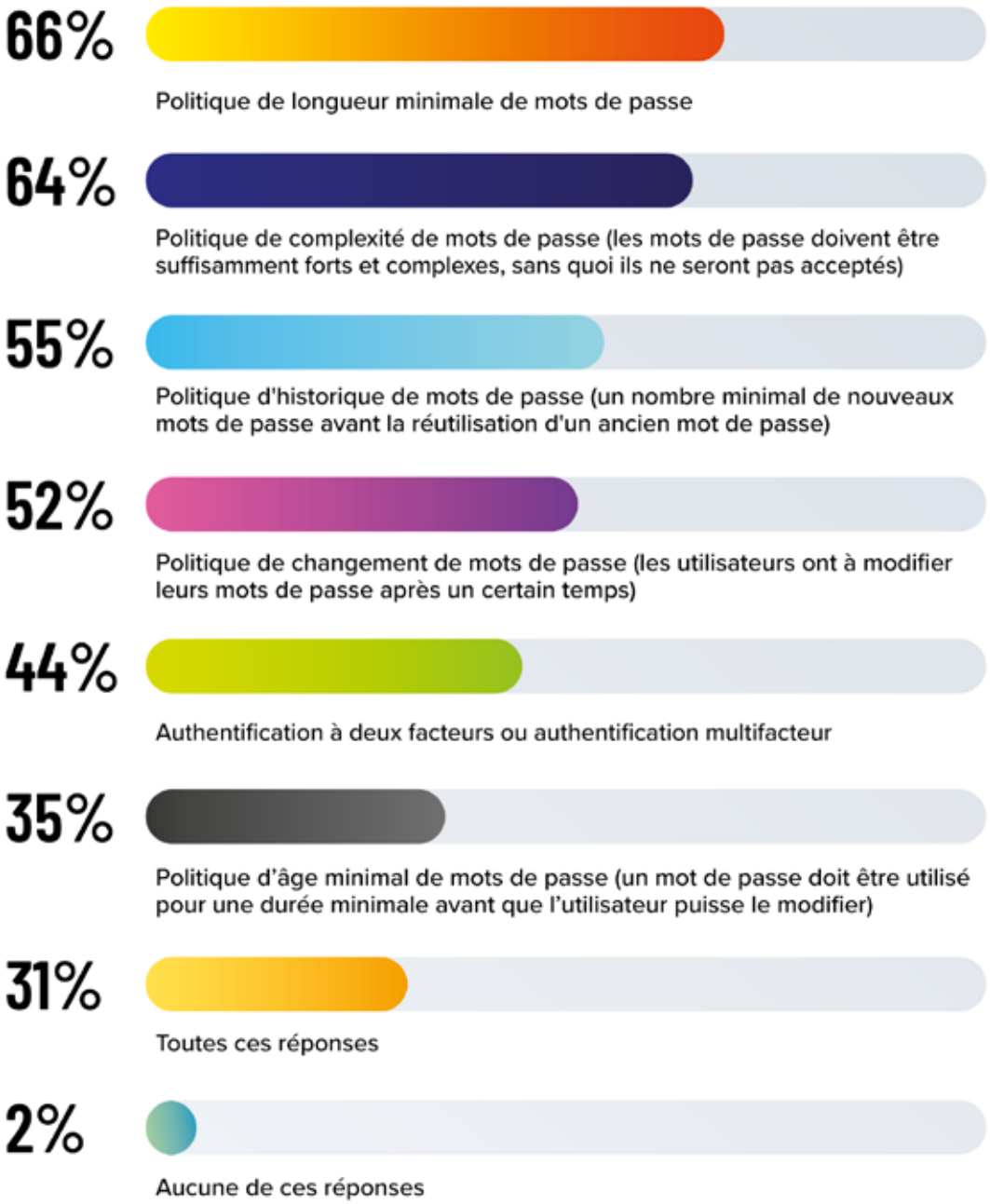
Dans notre sondage sur le portrait de la cybersécurité dans les PME en 2020-2021, 81 % de celles-ci avaient un gestionnaire de mots de passe pour stocker leurs mots de passe. Bien que de nombreux facteurs puissent être à l'origine de cette baisse de 10 % d'une année à l'autre, l'un des plus probables est la perception des PME selon laquelle elles ne sont pas aussi vulnérables que les grandes entreprises et les organisations gouvernementales.

Par ailleurs, 20 % des PME interrogées utilisent des méthodes non sécurisées pour stocker les mots de passe (feuilles de calcul, documents et écriture des mots de passe sur du papier). Là encore, cette situation est probablement due à un faux sentiment de sécurité. Malheureusement, il suffit d'une seule brèche qui entraînera des conséquences énormes et potentiellement catastrophiques.

Dans la section des recommandations de ce rapport, nous analysons les raisons pour lesquelles les gestionnaires de mots de passe constituent un outil de cybersécurité tout aussi important, de même que les caractéristiques et les fonctions que les PME doivent rechercher lorsqu'elles choisissent une solution.

Question 6

Parmi ces politiques et pratiques liées aux mots de passe, lesquelles utilisez-vous dans votre entreprise? Veuillez cocher tout ce qui s'applique.



Commentaires

Bien que le paysage de la cybersécurité se dégrade de plus en plus, seules trois PME sur dix (31 %) disposent d'une politique de gestion des mots de passe couvrant tous les éléments essentiels :

- **Longueur minimale de mots de passe**
- **Complexité de mots de passe**
- **Historique de mots de passe**
- **Âge minimal de mots de passe**
- **Authentification multifacteur ou à deux facteurs**

Pourquoi la politique du changement de mot de passe ne figure-t-elle pas parmi les éléments d'une approche robuste de la gestion des mots de passe? La perception de cette pratique a évolué au fil du temps. Auparavant, il était recommandé d'exiger des utilisateurs qu'ils changent leurs mots de passe à intervalles de quelques mois, ou au moins une fois par an. Cependant, le National Institute of Standards and Technology (NIST) a fait marche arrière et ne préconise désormais de changer les mots de passe qu'en cas de violation connue ou présumée des données. En effet, des recherches ont révélé que lorsque les utilisateurs sont contraints de modifier leurs mots de passe, ils ont tendance à choisir des identifiants faciles à retenir. Ils sont donc plus simples à pirater que ceux qu'ils utilisaient avant le changement.

Nous constatons également dans la réponse à cette question que seulement 44 % des PME appliquent l'authentification à deux facteurs (A2F) ou l'authentification multifacteur (AMF). Ce chiffre devrait être de 100 % pour être franc. Comment ce décalage s'explique-t-il? Cela vient vraisemblablement du fait que, lorsque l'AMF a fait son entrée sur la scène il y a plusieurs années, il s'agissait d'une fonctionnalité délicate à mettre en œuvre pour de nombreuses PME, car les outils étaient coûteux et complexes à configurer. Pour couronner le tout, les utilisateurs étaient soit réticents à y recourir parce qu'il s'agissait d'une étape de connexion supplémentaire qu'ils n'appréciaient pas, soit parce qu'ils ne possédaient pas de téléphone intelligent personnel ou fourni par l'entreprise (de nos jours, les téléphones intelligents sont abordables et partout, mais cela n'a pas toujours été vrai!).

À présent, il n'y a plus de motif ou de prétexte pour les PME de ne pas déployer l'AMF, que Microsoft qualifie « d'outil le plus efficace contre les cybermenaces au sein d'une organisation ». Fort heureusement, le marché mondial des solutions de gestion des mots de passe est en expansion, et l'on prévoit qu'il atteindra la somme considérable de 2,05 milliards de dollars d'ici 2025. Ainsi, les entreprises de toutes tailles, y compris les PME qui ont traditionnellement été négligées par de nombreux fournisseurs de services, peuvent choisir parmi un nombre croissant de produits.

Dans la section des recommandations de ce rapport, nous énumérons quelques facteurs pour aider les PME à choisir un outil AMF sécurisé, facile à utiliser, abordable, et que toutes les PME devraient adopter dès maintenant.

Question 7

Votre entreprise recommande-t-elle ou exige-t-elle que les employés utilisent un gestionnaire de mots de passe personnel afin de protéger leurs comptes privés?

OUI

47%

NON

53%

Commentaires

Les PME qui ne demandent pas à leurs employés de recourir à un gestionnaire de mots de passe personnels mettent potentiellement leur personnel et leur entreprise en danger. En effet, les pirates visent de plus en plus les comptes personnels, pour dérober des données qui peuvent être utilisées pour pénétrer dans les terminaux et les réseaux des entreprises. En effet, bien que les experts en cybersécurité déconseillent d'agir de la sorte, de nombreux employés utilisent leurs comptes personnels (messagerie électronique, médias sociaux, applications de clavardage, etc.). Si ce choix est commode et rapide, il présente également un risque important. Par exemple, des recherches ont révélé qu'environ 15 % des courriels envoyés à des comptes personnels contiennent des informations sensibles de l'entreprise.

Une autre raison pour laquelle les PME devraient exiger de leurs employés qu'ils utilisent un gestionnaire de mots de passe personnels est que cela encourage de bonnes habitudes d'hygiène concernant la sécurité comme le choix de mots de passe forts et uniques qui se transposent dans l'environnement de travail. En fait, la sensibilisation à la cybersécurité doit constituer un effort permanent, et non pas un élément auquel les employés ne pensent pas et ne se concentrent que pendant la journée de travail. Les pirates opèrent 24 heures sur 24, 7 jours sur 7, et les employés doivent toujours demeurer vigilants.

Question 8

Votre entreprise dispose-t-elle d'un processus pour révoquer l'accès aux comptes des anciens employés?

OUI

92%

NON

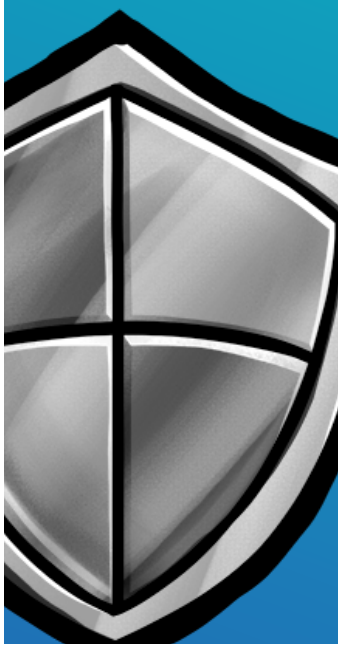
8%

Commentaires

Les quelque 9 PME sur 10 (92 %) qui ont mis en place un procédé pour révoquer l'accès aux comptes des ex-employés sont sur la bonne voie. Cependant, environ 1 sur 10 (8 %) fait fausse route, ce qui pourrait entraîner une violation des données.

Dans un sondage, 25 % des travailleurs ont déclaré qu'ils pouvaient encore se connecter aux comptes de leurs anciens emplois. Cela comprend les anciens employés et responsables informatiques ayant les « clés du royaume », c'est-à-dire l'accès aux comptes privilégiés. Il est vrai que la plupart de ces travailleurs n'ont pas pour objectif de voler des données, de provoquer des dégâts ou de se livrer à d'autres activités illégales. En revanche, que se passera-t-il s'ils sont attaqués par des pirates qui, en fouinant, découvrent ces anciens comptes et les identifiants correspondants? Les répercussions pourraient alors être lourdes, pour ne pas dire catastrophiques.

Dans la section des recommandations de ce rapport, nous examinons les trois étapes que toutes les PME devraient inclure dans leur processus de suppression des accès.



PARTIE 3

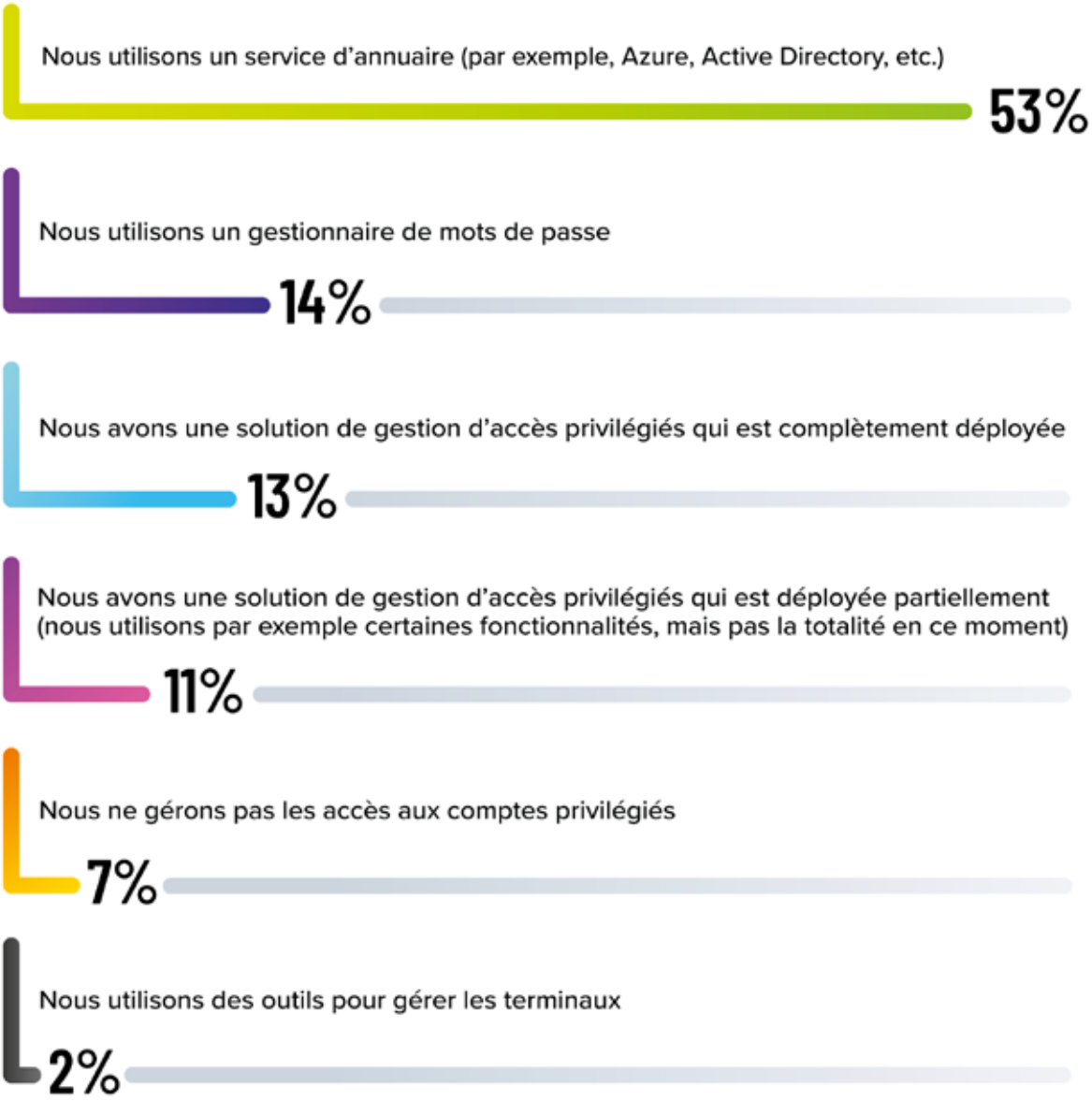
LA GESTION D'ACCÈS PRIVILÉGIÉS DANS LES PME

Auparavant, la gestion des accès privilégiés (de l'anglais *Privileged Access Management* ou PAM) était essentiellement considérée comme une façon d'optimiser l'efficacité administrative au moyen de la gestion des mots de passe. Lors des dernières années, en revanche, la gestion des accès privilégiés est devenue une technologie incontournable pour se prémunir contre les brèches de sécurité et les vols d'identifiants, y compris ceux perpétrés par des employés malhonnêtes.

Dans la troisième partie de notre sondage, nous nous sommes penchés sur l'utilisation de la gestion des accès privilégiés dans les PME :

Question 9

Comment gérez-vous les accès aux comptes privilégiés dans votre entreprise?



Commentaires

Un peu plus de la moitié (53 %) des PME ont recours à un service d'annuaire comme Azure et Active Directory (AD) afin de gérer l'accès aux comptes privilégiés. Même si cette solution est pratique, elle n'est pas robuste. La majorité des menaces de sécurité dans un environnement de service d'annuaire résultent d'un accès non autorisé. Une solution PAM instaure un environnement sûr où seuls les utilisateurs de confiance ont accès à des fichiers, des dossiers et des groupes déterminés.

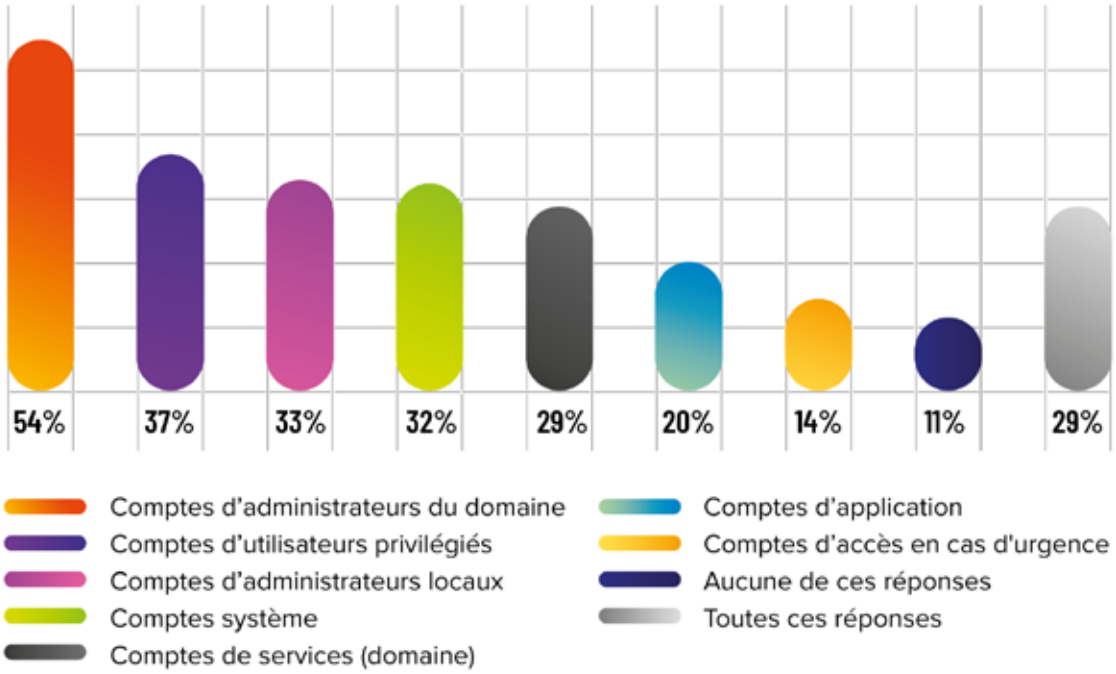
Il convient également de souligner que 13 % des PME ont une solution PAM entièrement déployée, ce qui constitue une baisse de 24 % par rapport au rapport sur le portrait de la cybersécurité dans les PME en 2020-2021. Si de multiples raisons sont susceptibles d'expliquer cette baisse, l'une des plus probables est que certaines (14 % dans le sondage de cette année) optent pour des gestionnaires de mots de passe comme une solution de rechange au PAM. Néanmoins, cette solution n'est pas tenable. Certes, les gestionnaires de mots de passe occupent un rôle important dans le paysage général de la sécurité, en limitant notamment la lassitude des utilisateurs en ce qui a trait à la cybersécurité, mais ils ne sont pas pour autant conçus pour gérer l'accès aux comptes privilégiés. En effet, ils ne procurent pas la visibilité, le contrôle et la gouvernance exigés pour la protection des données sensibles, le respect des normes de conformité et la gestion à grande échelle.

Pour ce qui est des 7 % de PME qui ne gèrent pas l'accès aux comptes privilégiés, le message est sans équivoque : il faut en faire une priorité absolue dès maintenant. Il ne s'agit pas seulement du succès de leur entreprise qui en question. Sachant que 60 % des PME disparaissent dans les six mois suivant une cyberattaque, c'est leur survie même qui est en jeu.

Dans les recommandations de ce rapport, nous nous penchons sur comment les PME peuvent recourir à une solution PAM pour combler le fossé entre l'authentification et l'autorisation. Nous insistons également sur ce qu'elles doivent rechercher lorsqu'elles analysent des solutions PAM potentielles.

Question 10

Lesquels de ces comptes privilégiés surveillez-vous dans votre entreprise? Veuillez cocher tout ce qui s'applique.



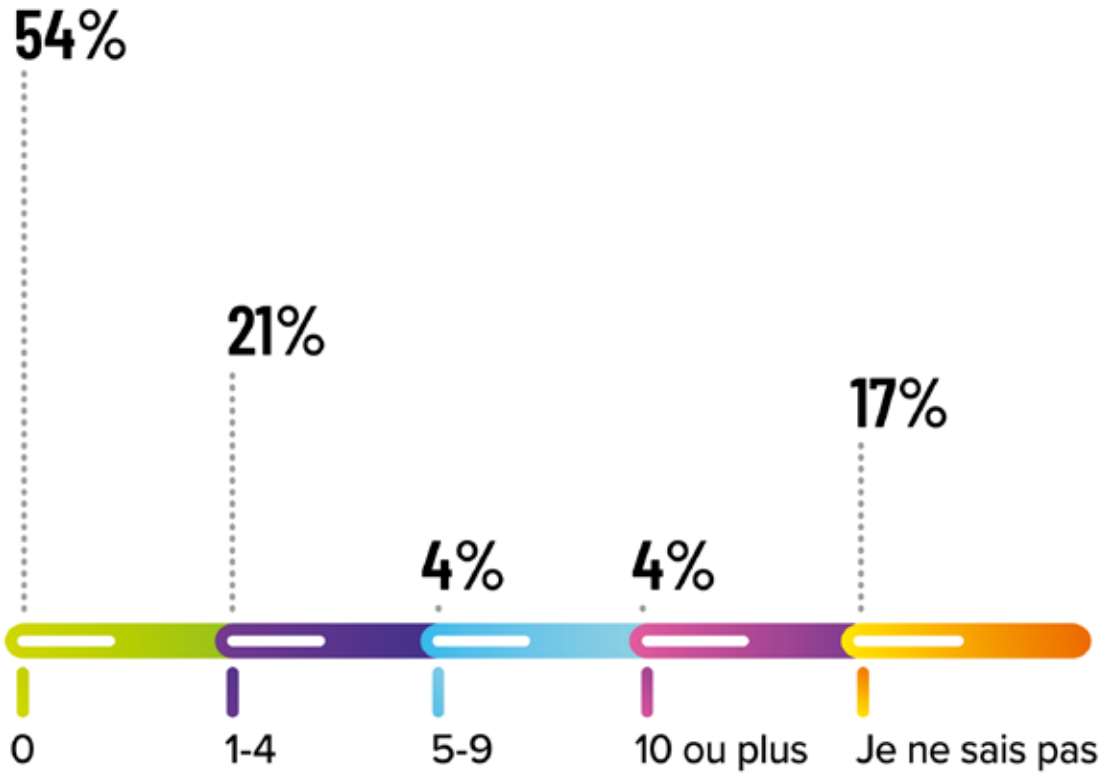
Commentaires

61 % des PME ne surveillent pas la totalité des comptes privilégiés de leur organisation, ce qui implique que les pirates pourraient les exploiter, ou qu'ils l'ont déjà fait à plusieurs reprises. Ainsi, les pirates visent régulièrement les comptes d'administrateur local, car plusieurs PME attribuent ce niveau d'accès à l'ensemble des employés. Cependant, dès que la vulnérabilité est exploitée, les pirates se cachent sans être détectés tandis qu'ils examinent les défenses de l'organisation et préparent ce qui sera sans aucun doute une attaque réussie pouvant durer des jours, des semaines, des mois, voire des années.

Dans les recommandations de ce rapport, nous fournissons davantage d'information sur les différents types de comptes privilégiés, et présentons les bonnes pratiques pour les garder en sécurité.

Question 11

Pendant l'année écoulée, combien de violations de comptes privilégiés avez-vous eues dans votre entreprise?



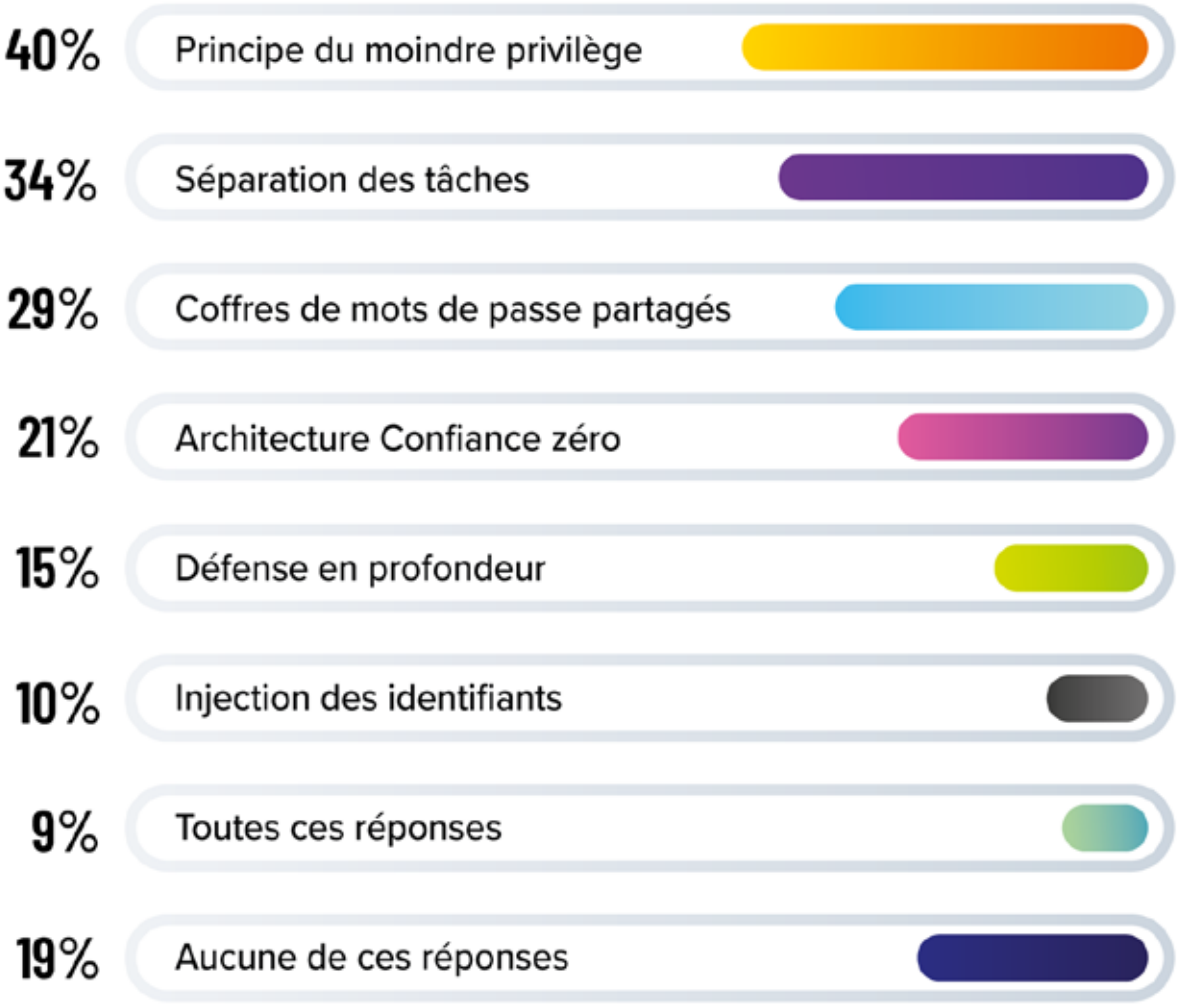
Commentaires

32 % des PME ont été affectées par des violations d'accès privilégiés au cours de l'année dernière, et 4 % d'entre elles ont subi plus de 10 incidents. De surcroît, compte tenu de la fréquence de ce vecteur de menace, il est plus que probable que la majorité des PME qui n'ont pas eu conscience de violations d'accès privilégiés au cours des 12 derniers mois en ont été victimes au moins une fois, si ce n'est plusieurs.

Il est certain que 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.

Question 12

Quelles politiques, pratiques ou quels outils avez-vous à votre disposition afin de soutenir la gestion des comptes privilégiés dans votre entreprise? Veuillez cocher tout ce qui s'applique.



Commentaires

Alors, pourquoi seulement 9 % des PME sélectionnent-elles toutes ces réponses lorsqu'il s'agit de gérer les comptes privilégiés? Tout simplement qu'elles sont convaincues d'être trop petites pour subir une attaque. Or, les faits démontrent l'inverse.

Selon les réponses à la question 3 (dans la partie 1 du sondage), 52 % des PME ont subi entre 1 et 10 cyberattaques l'année dernière, et 10 % en ont subi 10 ou plus. Manifestement, il y a un écart entre la perception de certaines PME et ce qui se déroule réellement. Hélas, les pirates exploitent cet écart avec un éventail croissant de cybermenaces avancées, dont des rançongiciels de nouvelle génération, des attaques de la chaîne d'approvisionnement, des logiciels espions, l'hameçonnage, etc.

Dans la section des recommandations de ce rapport, nous considérons les bonnes pratiques pour la mise en oeuvre du principe de moindre privilège, de la séparation des tâches, du partage des coffres de mots de passe, de l'architecture de Confiance zéro, de la défense en profondeur et de l'injection d'identifiants.

PARTIE 4

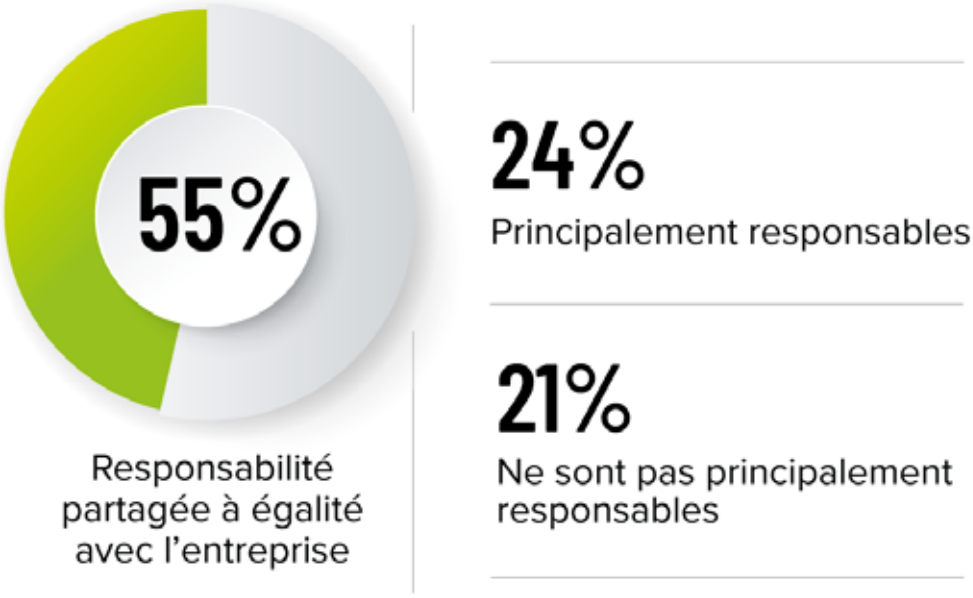
FORMATION ET GESTION DE LA CYBERSÉCURITÉ CHEZ LES PME

S'il est crucial pour les PME de déployer des outils robustes qui déjouent les pirates, elles doivent également se concentrer sur leurs politiques, pratiques et protocoles internes (ou ce que les experts en sécurité informatique appellent « le pare-feu humain ») pour se protéger des utilisateurs malhonnêtes ou négligents.

Dans la quatrième partie de notre sondage, nous nous sommes penchés sur la formation et la gestion de la cybersécurité dans les PME :

Question 13

Globalement, dans quelle mesure pensez-vous que les utilisateurs finaux sont responsables lors d'une brèche de données?



Commentaires

La plupart (79 %) des PME ont la conviction que les utilisateurs ont une part de responsabilité en cas de violation de données. Néanmoins, près d'un quart d'entre elles (24 %) considèrent que les utilisateurs finaux sont les premiers responsables, ce qui est inquiétant. Pourquoi? Parce que des études ont révélé que près de la moitié des violations de données sont dues à la négligence ou le laisser-aller d'un employé. Cela signifie que les PME qui concentrent tous leurs investissements et leurs efforts en matière de cybersécurité sur la lutte contre les pirates externes et les utilisateurs malhonnêtes internes restent vulnérables, car leurs employés pourraient involontairement provoquer des violations coûteuses.

Dans la section des recommandations de ce rapport, nous examinons comment les PME peuvent accroître la sensibilisation de leur personnel à la cybersécurité.

Question 14

Votre entreprise offre-t-elle une formation continue en cybersécurité en lien avec le signalement d'incidents, les risques liés aux médias sociaux, la sécurité de mots de passe, l'hameçonnage, la protection de mots de passe, etc.?

OUI

74%

NON

26%

Commentaires

Il s'agit encore d'une bonne et mauvaise nouvelle. La bonne nouvelle est que 74 % offrent à leur personnel une formation en cybersécurité. L'envers de la médaille est que la proportion de PME assurant une formation continue en cybersécurité était de 88 % dans l'enquête sur le portrait de la cybersécurité en 2020-2021. Qu'est-ce qui justifie cette chute de 14 %?

Sans surprise, la raison la plus plausible est la pandémie. Le fait de composer avec des changements rapides et sans précédent a obligé de nombreuses PME à se consacrer uniquement à leurs activités principales. Or, la sensibilisation de leur personnel à la cybersécurité doit faire partie de ces activités. Les pirates 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.

Dans la section des recommandations de ce rapport, nous présentons quelques moyens pratiques permettant aux PME de protéger leurs travailleurs à distance et leur entreprise.

Question 15

Votre entreprise possède-t-elle un plan d'intervention en cas d'incident complet et à jour?

OUI

60%

NON

40%

Commentaires

Il est coutume de dire que l'absence d'un plan est un plan d'échec. Pourtant, lorsqu'il s'agit de menaces de cybersécurité, ne pas disposer d'un plan d'intervention complet et à jour peut se révéler catastrophique. En effet, plus une entreprise est en mesure de réagir rapidement à une violation, moins elle risque de perdre des revenus, des clients et sa réputation. En outre, il est généralement beaucoup plus facile et beaucoup moins coûteux de repérer et de corriger une violation le plus tôt possible.

Si un plan de réponse aux incidents complet et à jour est si important, pourquoi 40 % des PME négligent-elles cette nécessité? Sans doute parce qu'elles ne savent pas par où commencer.

Dans la section des recommandations de ce rapport, nous énumérons les bonnes pratiques afin d'accompagner les PME dans la concrétisation de cet objectif essentiel. En fait, mettre en place un plan à toute épreuve se déroule avant une violation, et non pendant ou après.

Question 16

Effectuez-vous des audits de cybersécurité dans votre entreprise au moins deux fois par an?

OUI
50%

NON
50%

Commentaires

La moitié des répondants ont déclaré réaliser au moins deux audits de cybersécurité complets par an, ce qui représente une augmentation de 12 % en comparaison avec le rapport sur le portrait de la cybersécurité dans les PME en 2020-2021. Il est réjouissant de constater que davantage de PME sont conscientes de la pertinence de détecter elles-mêmes les vulnérabilités plutôt que d'attendre que des pirates ou des acteurs malveillants le fassent pour elles.

Néanmoins, la proportion de PME qui réalisent au moins deux audits de cybersécurité par an devrait être de 100 %, car il suffit d'une seule violation pour provoquer des pertes massives et susciter des regrets et du stress.

Pour aider les PME à ne pas tomber dans ce piège, nous mettons en évidence, **dans la section des recommandations de ce rapport,** les activités clés qui devraient être incluses dans un processus d'audit complet.

PARTIE 5

LES INVESTISSEMENTS EN CYBERSÉCURITÉ CHEZ LES PME

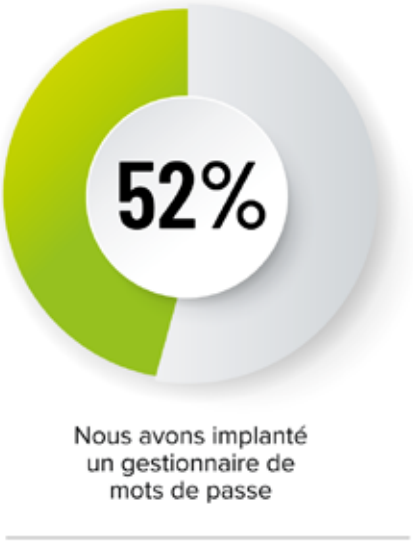
La volatilité de la pandémie a contraint toutes les organisations (particulièrement les PME) à examiner en profondeur, et parfois péniblement, leurs priorités et leurs stratégies. Elles doivent veiller à ce que l'accent soit mis sur les ressources nécessaires plutôt que sur celles dites agréables. Il est indéniable que l'investissement dans les outils et la formation en cybersécurité appartient à la première catégorie.

En fait, il suffit de réfléchir à l'attaque gigantesque de la chaîne d'approvisionnement de Solorigate, que plusieurs experts ont décrite comme la violation la plus complexe de l'histoire, et à la flambée des rançongiciels, l'hameçonnage, les logiciels espions et autres cybermenaces pour se rendre à l'évidence que le rendement d'un investissement avisé dans la cybersécurité peut représenter davantage qu'une question de profits et de pertes pour les PME. Cela peut signifier la différence entre la survie et l'extinction.

Dans la cinquième partie de notre sondage, nous avons examiné les investissements en cybersécurité dans les PME :

Question 17

Quels investissements en cybersécurité votre entreprise a-t-elle entrepris jusqu'à présent? Veuillez cocher tout ce qui s'applique.



30%	Nous avons engagé un responsable de la sécurité des systèmes d'information ou autre expert en sécurité
25%	Nous travaillons avec un fournisseur de services gérés
21%	Nous avons implanté une solution de gestion d'accès privilégiés
19%	Aucune de ces réponses
5%	Toutes ces réponses

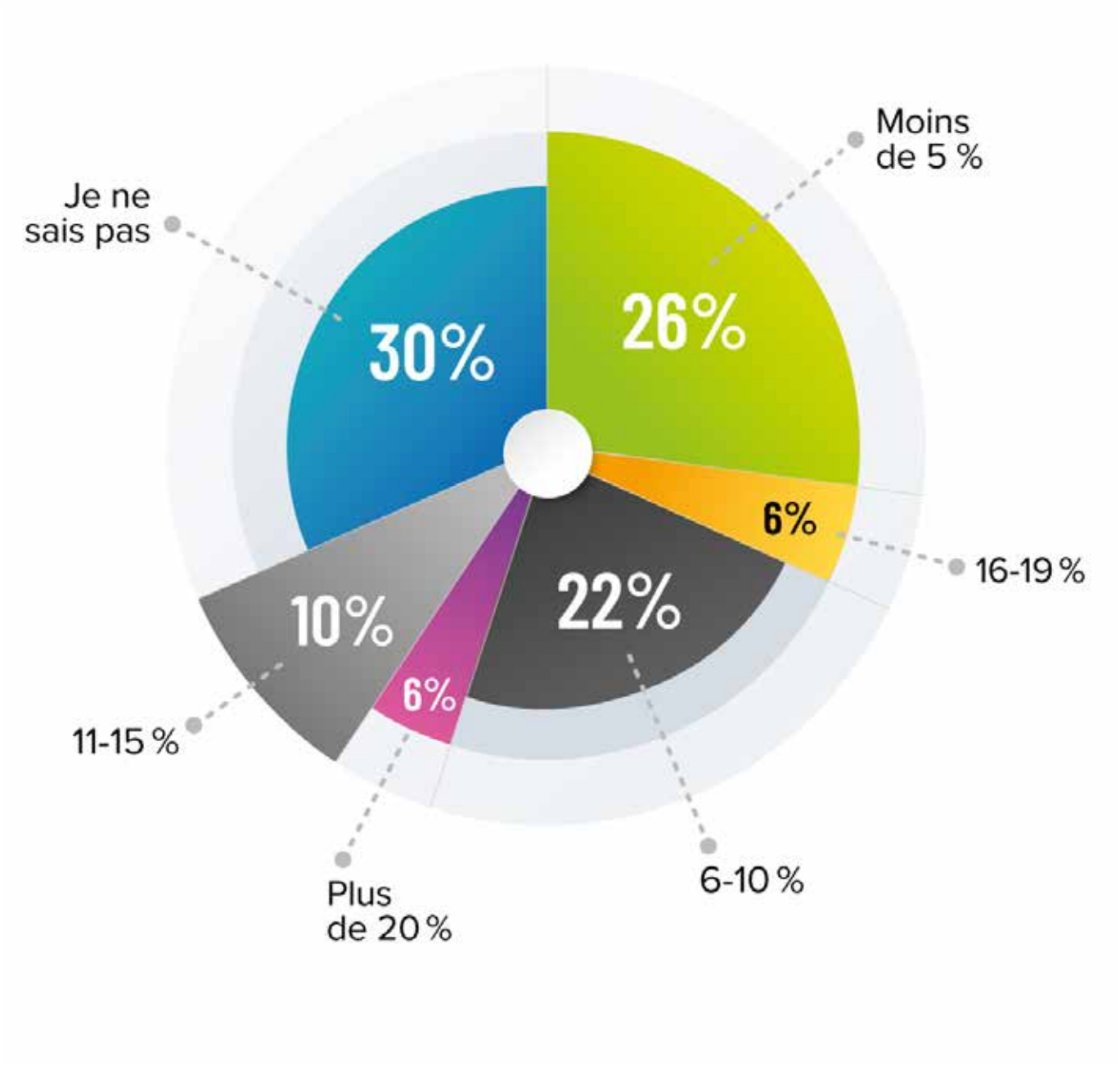
Commentaires

Il est préoccupant de constater que seule une PME sur quatre environ a déployé une solution de gestion d'accès privilégiés (ou PAM) dédiée. Comme indiqué dans la partie 4 de ce rapport, les solutions PAM ne sont pas uniquement conçues pour les grandes entreprises. Les PME doivent aussi identifier, contrôler et surveiller les accès aux comptes privilégiés. Sur une note plus positive, la plupart des PME (52 %) ont mis en place un gestionnaire de mots de passe, et 1 sur 4 fait appel à un fournisseur de services gérés.

Dans la section des recommandations de ce rapport, nous donnons des conseils afin d'aider les PME à choisir le meilleur fournisseur de services gérés pour leur organisation.

Question 18

À combien s'élève l'ensemble du budget TI dédié à la cybersécurité en pourcentage (incluant la technologie, la formation, etc.)



Commentaires

Depuis de nombreuses années, plusieurs experts recommandent aux entreprises de consacrer entre 7 et 10 % de leur budget informatique aux technologies et aux formations en cybersécurité. Toutefois, une étude de Gartner a révélé que la moyenne des dépenses de cybersécurité ne constitue que 5,7 % des dépenses informatiques. Cette proportion peut être nettement inférieure dans les PME.

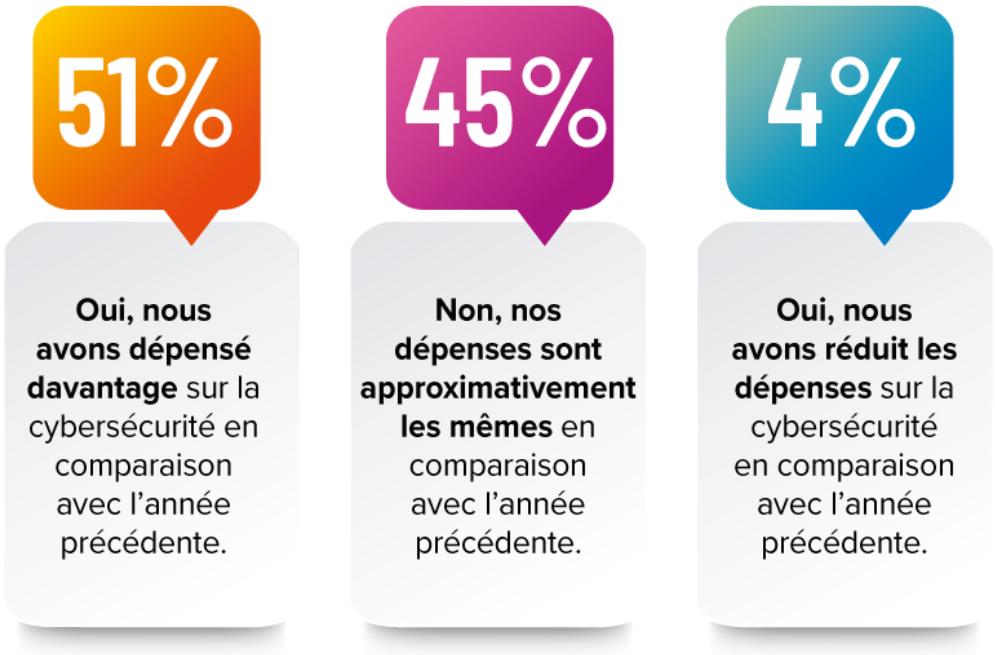
S'il est vrai que le simple fait d'investir en cybersécurité n'est pas une formule magique qui garantira l'invulnérabilité de l'entreprise, il n'en demeure pas moins qu'une PME dotée d'un profil de sécurité davantage robuste sera plus sûre qu'une autre présentant des vulnérabilités considérables. En outre, la première chose que les pirates font fréquemment après avoir pénétré dans une organisation (souvent par l'entremise de comptes privilégiés non protégés), c'est scruter l'ensemble de la défense de la PME afin de déterminer à quoi ils sont confrontés. Dans le cas où les pirates ont le sentiment qu'il leur sera difficile de ne pas être détecté, ils seront moins susceptibles de mener une attaque à grande échelle. Inversement, s'ils considèrent qu'ils peuvent aisément naviguer dans les réseaux et les terminaux sans se faire prendre, la préparation à une offensive silencieuse peut durer des mois, voire des années.

Les PME omettent souvent de consacrer une part adéquate de leur budget informatique à la cybersécurité, car les administrateurs système et les autres professionnels de la sécurité informatique ont du mal à convaincre les dirigeants que les dépenses dans ce domaine n'en sont pas. Il s'agit plutôt d'un investissement.

Dans la section des recommandations de ce rapport, nous présentons quelques conseils utiles afin d'aider les champions de la cybersécurité chez les PME à convaincre les décideurs à délier les cordons de leurs bourses. Ainsi, ces organisations seront plus résistantes et plus sûres.

Question 19

Au cours de l'année dernière, les dépenses totales de votre entreprise en matière de cybersécurité ont-elles changé?



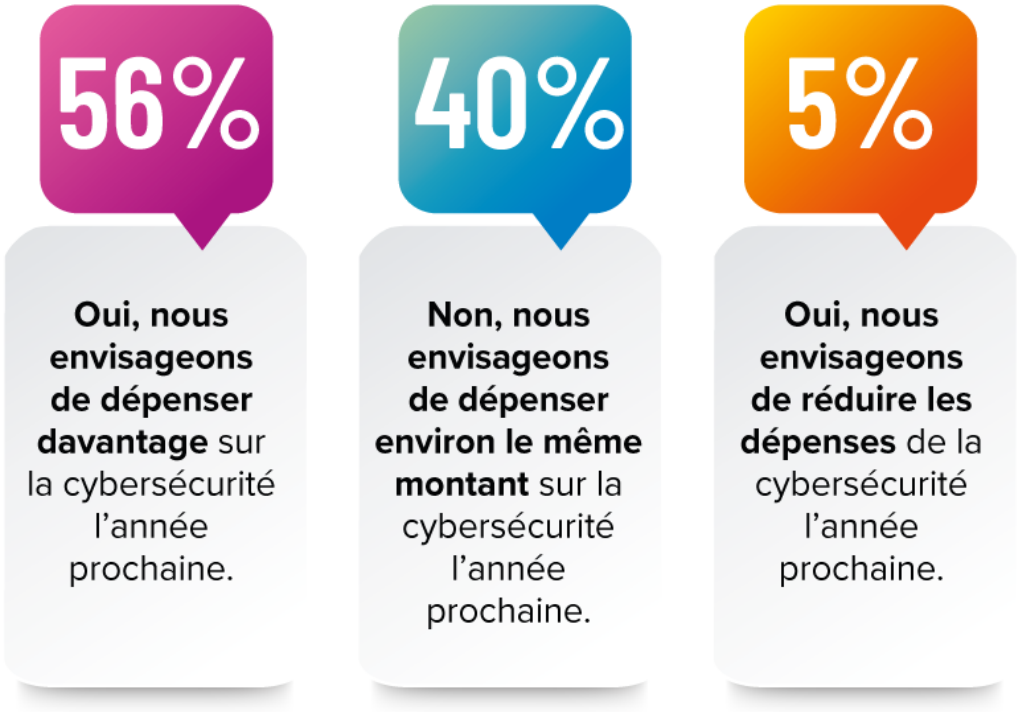
Commentaires

La plupart des PME investissent autant ou plus dans la cybersécurité que l'année précédente, ce qui n'est pas surprenant. La pandémie a imposé aux entreprises de toutes les dimensions à déployer sans tarder des mesures pour maintenir la poursuite de leurs activités, y compris en protégeant les travailleurs à distance contre les anciennes et les nouvelles cybermenaces, dont une hausse de 700 % des attaques par hameçonnage.

De plus, l'onde de choc provoquée par l'attaque massive de la chaîne d'approvisionnement, Solorigate, se poursuit, car les organisations du monde entier sont conscientes qu'il peut suffire d'une seule mise à jour SaaS, banale et apparemment inoffensive, pour que leurs données confidentielles soient volées et vendues au plus offrant sur le Web caché.

Question 20

Prévoyez-vous une variation des dépenses totales de votre entreprise en matière de cybersécurité l'année prochaine?



Commentaires

Bien que 96 % des PME investissent autant ou plus pour la cybersécurité aujourd'hui que l'année dernière est une bonne nouvelle, cela ne signifie pas forcément que toutes les priorités sont prises en compte. Il est hors de tout doute moins dispendieux, plus simple, et plus rapide de prévenir une cyberattaque que de réparer les pots cassés. Par ailleurs, dans certains cas, l'atteinte à la réputation peut se prolonger durant des années.

Dans la section des recommandations de ce rapport, nous mettons en évidence les projets de cybersécurité essentiels sur lesquels les PME doivent se concentrer et mettre en œuvre maintenant.

PARTIE 6
RECOMMANDATIONS

En ce qui concerne les stratégies et les solutions de cybersécurité, il y a plusieurs domaines où les PME peuvent, et dans plusieurs cas, doivent corriger les vulnérabilités maintenant plutôt que plus tard.

Nous encourageons vivement **toutes les PME à analyser et à auditer de manière proactive leur profil de cybersécurité actuel** et, si besoin, **à suivre ces recommandations ciblées :**

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 de mots de passe stricte.

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 oeuvre 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 d'audit complet 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.

1 RECOMMANDATION

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

Cette recommandation préconise que les décideurs des PME changent leur état d'esprit en passant de la croyance erronée « nous sommes trop petits pour être attaqués par les pirates » à « les pirates nous cibleront de plus en plus en raison de notre petite taille ».

En effet, le temps est révolu où les pirates visaient presque exclusivement les grandes entreprises et organisations. Aujourd'hui, ils tirent parti du fait que de nombreuses PME ont des défenses limitées ou pratiquement inexistantes, alors qu'elles possèdent d'abondantes données privées et confidentielles pouvant être subtilisées pour les vendre sur le Web caché.

LES PME DANS LE VISEUR :

- 43 % des cyberattaques **ciblent les petites entreprises.**
- **En 2021, le coût moyen d'une violation de données chez les PME a atteint** 2,98 millions de dollars US par incident.
- 81 % des violations de données **résultent de la compromission de mots de passe, et 30 % impliquent des utilisateurs malveillants internes.**

De surcroît, lors de la pandémie, les pirates ont intensifié leurs attaques contre les travailleurs à distance. Cette tendance négative ne disparaîtra pas lorsque la crise de la santé publique reprendra son cours normal. Bien au contraire, il faudra s'attendre dans les années à venir que les pirates ciblent de plus en plus les travailleurs à distance afin de s'attaquer aux terminaux, aux réseaux et aux serveurs.

Ainsi, lorsqu'il s'agit d'exposition aux cyber-menaces, la première et la plus importante chose que les PME doivent accepter sont que leur taille relativement petite n'est pas un avantage. C'est en fait un handicap, car les pirates supposent qu'elles sont vulnérables. C'est aux PME de démontrer le contraire, faute de quoi la question n'est pas de savoir si une cyberattaque va se produire. En effet, il faudra se demander quand et avec quelle ampleur.

2 RECOMMANDATION

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

Certes, les PME doivent s'inquiéter d'une large panoplie de cybermenaces comme les logiciels espions et les problèmes de sécurité liés à l'infonuagique, mais l'enquête a démontré que trois menaces suscitent le plus d'inquiétude : les rançongiciels, l'hameçonnage et les attaques de la chaîne d'approvisionnement. Nous fournissons ci-dessous des stratégies pour aider les PME à se protéger contre ces dangers courants, coûteux et potentiellement dévastateurs.

LES RANÇONGICIELS EN CHIFFRES :

- 20 % des victimes **de rançongiciels sont des PME.**
- 85 % des fournisseurs de services gérés **considèrent les rançongiciels comme une menace courante pour les PME.**
- **En 2021-2022, une organisation est victime d'une attaque par un rançongiciel une fois** toutes les 11 secondes.

Stratégies pour protéger les PME contre les rançongiciels :

• Élaborez un plan exhaustif de réponse aux incidents, qui identifie clairement ce qu'il faut faire et qui doit le faire en cas d'attaque par rançongiciel.

• Instaurez un système de sauvegarde prenant en charge plusieurs itérations ou données archivées au cas où une copie de la sauvegarde aurait des fichiers infectés ou chiffrés. Les sauvegardes doivent également être régulièrement testées pour vérifier l'intégrité des données et s'assurer de la disponibilité opérationnelle.

• Déployez des logiciels antivirus et antipourriels, et ajoutez une bannière/signature d'avertissement sur tous les courriels rappelant aux utilisateurs les dangers de cliquer sur les liens et d'ouvrir les pièces jointes.

• Si possible, désactivez les macros de script et obligez les utilisateurs à visualiser plutôt qu'à ouvrir les fichiers transmis par courrier électronique. L'intégration de logiciels malveillants à l'intérieur de macros Word/Excel est un vecteur courant d'attaques par rançongiciel.

• Conservez tous les appareils, logiciels, matériels et applications (y compris les emplacements dans le nuage) entièrement à jour et corrigés, de préférence au moyen d'un système centralisé de gestion des correctifs.

• Utilisez la liste blanche des applications et les politiques de restriction des logiciels pour bloquer l'exécution des programmes dans les emplacements fréquents des rançongiciels (par exemple, les dossiers temporaires).

• Utilisez un serveur proxy pour l'accès à Internet.

• Utilisez un logiciel de blocage des publicités.

• Restreignez l'accès aux vecteurs courants de rançongiciel, tels que les sites de réseaux sociaux et les comptes de messagerie personnels.

• Évaluez et surveillez les tiers qui accèdent au réseau, et assurez-vous qu'ils appliquent consciencieusement les bonnes pratiques en matière de cybersécurité.

• Participez aux programmes et organisations de partage d'informations sur la cybersécurité (par exemple, MS-ISAC et InfraGard).

• Offrez aux utilisateurs finaux une formation continue en matière de cybersécurité sur des sujets tels que l'ingénierie sociale et l'hameçonnage. Nous examinons ce point plus attentivement dans la recommandation n° 10.

• Mettez en place un plan de signalement précisant aux utilisateurs finaux comment et quand signaler toute activité inhabituelle ou suspecte.

Stratégies pour protéger les PME contre l'hameçonnage :

• Formez les employés sur la manière de déceler les courriels malveillants. L'une des façons d'y arriver consiste à organiser des campagnes d'hameçonnage simulées, ce qui donne parfois des résultats surprenants (dans un sens inquiétant). Par exemple, en 2020, 14 % des travailleurs du secteur de l'assurance ont échoué à un test d'hameçonnage global.

• Exigez de tous les employés qu'ils choisissent des mots de passe complexes et uniques pour leur compte. L'utilisation d'un gestionnaire de mots de passe reconnu est fortement recommandée.

• Appliquez l'authentification multifacteur (AMF) pour réduire le risque de prise de contrôle des comptes.

• Déployez une passerelle de messagerie sécurisée qui automatise le filtrage antipourriel, anti-logiciel malveillant et basé sur des politiques.

• Afin d'accroître la capacité à identifier et à bloquer des pourriels, mettez en œuvre SPF (Sender Policy Framework), DMARC (Domain-Based Message Authentication, Reporting & Conformance) et DKIM (Domain Keys Identified Mail).

• Instaurez la détection des irrégularités au sein du réseau pour les courriels entrants et sortants.

L'HAMEÇONNAGE EN QUELQUES CHIFFRES :

- **Au premier semestre de 2021, le nombre d'attaques par hameçonnage a augmenté de 22 % en comparaison avec la même période en 2020.**
- **Près de 1,5 million de nouveaux sites d'hameçonnage sont créés chaque mois.**
- **1 courriel sur 99 est une attaque d'hameçonnage.**

Stratégies pour protéger les PME contre les attaques de la chaîne d'approvisionnement :

• Procédez à une évaluation exhaustive des fournisseurs et veillez à ce que les tiers respectent les points suivants : mettre régulièrement à l'épreuve la force de leur résilience concernant la cybersécurité; fournir la preuve de la dernière analyse du code source et de l'intrusion des applications; déployer des applications pare-feu ou une segmentation du réseau limitant l'accès aux programmes d'application ou au code source objet; se conformer aux politiques et réglementations pertinentes (par exemple, SOC 2, RGPD, CCPA, NIST, COBIT, ISO-27001/2, etc.); mener un programme de sensibilisation des employés à la sécurité.

• Utilisez une solution de gestion des accès privilégiés (PAM) pour faire obstacle aux pirates informatiques qui cherchent à suivre une trajectoire d'attaque classique (« connue sous le nom de voie privilégiée ») qui débute par une intrusion du périmètre, puis comprend les appareils et les terminaux privilégiés, et aboutit à une violation de données. Nous examinons les éléments d'une solution PAM dans la recommandation n° 7.

• Utilisez des *honeytokens* dans lesquels un compte privilégié inactif est créé et surveillé. En cas de tentative de violation du compte par des pirates, une alerte est déclenchée, indiquant que l'environnement a été pénétré.

LES ATTAQUES DE LA CHAÎNE D'APPROVISIONNEMENT EN CHIFFRES :

- **Au premier trimestre de 2021,** 42 % d'organisations de plus ont été touchées **par une attaque de la chaîne d'approvisionnement par rapport au dernier trimestre de 2020.**
- **Les attaques de la chaîne d'approvisionnement en 2021 devraient** augmenter de 400 % **en comparaison avec 2020.**
- **Une analyse des attaques de la chaîne d'approvisionnement très médiatisées entre** janvier 2020 et juillet 2021 **a révélé que 20 % ciblaient les données, 12 % les processus internes des fournisseurs, 16 % les personnes et 8 % les actifs financiers.**

Afin de se prémunir contre ces 3 menaces ainsi que les autres, l'équipe de sécurité de Devolutions conseille aux PME de mettre en œuvre les principes suivants :

Le principe de moindre privilège, ce qui signifie que les utilisateurs n'ont que les accès nécessaires pour mener à bien leurs activités quotidiennes. Si des privilèges élevés sont requis pour un projet ou une activité spécifique, ils doivent être octroyés temporairement, puis supprimés dès qu'ils ne sont plus sollicités.

La Confiance zéro, impliquant que personne n'est pas automatiquement digne de confiance et que toute activité sur le réseau est présumée par défaut être malveillante.

La séparation des tâches, qui se fonde sur l'idée que lorsque plusieurs personnes sont engagées dans un flux de travail confidentiel, le risque qu'une personne manipule ou utilise abusivement les ressources de l'organisation est réduit.

La défense en profondeur, qui consiste en plusieurs couches de protection afin de ralentir les pirates informatiques voulant se frayer un chemin à travers le périmètre jusqu'aux ressources vitales.

Nous approfondissons ces principes et présentons les bonnes pratiques dans la recommandation n° 9.

3 RECOMMANDATION

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

Un plan d'intervention exhaustif et efficace en cas de cyberattaque comprend les six éléments suivants : préparation, identification, confinement, éradication, récupération et leçons apprises.

Les tâches de préparation comprennent :

- Réviser la politique de sécurité.
- Mettre à jour la politique de sécurité.
- Documenter la politique de sécurité.
- Standardiser la politique de sécurité.
- Procéder à une évaluation des risques.
- Déterminer les ressources sensibles, privées et confidentielles.
- Définir et hiérarchiser les incidents de sécurité cruciaux sur lesquels il faut se concentrer.
- Créer une équipe de réponse aux incidents (voir encadré à la page suivante).

Les tâches d'identification comprennent :

- Surveiller les systèmes informatiques pour repérer les écarts par rapport aux opérations normales, et confirmer s'il s'agit d'incidents de sécurité réels et non de faux positifs.
- Lors de la vérification des incidents de sécurité réels, collecter des preuves, et établir le type et la sévérité.
- Documenter entièrement toutes les observations et constatations.

En tant que bonne pratique, l'équipe de réponse aux incidents doit être composée des rôles suivants :

Chef d'équipe : Pilote et coordonne les activités de l'équipe et l'aide à rester concentrée sur l'atténuation des dommages et l'accélération de la récupération.

Enquêteur(rice) en chef : Collecte et analyse les preuves, identifie la cause fondamentale, dirige les analystes de sécurité et mets en œuvre une restauration rapide des systèmes et des services.

Responsable de la communication : Gère les messages et les communications à l'intérieur et à l'extérieur de l'entreprise.

Responsable de la documentation et du calendrier : Documente toutes les activités de l'équipe avec un accent sur les activités d'enquête, de découverte et de récupération. Il élabore également des calendriers concrets pour chaque étape de l'incident.

Représentant(e) RH/juridique : Fournit des conseils stratégiques et opérationnels, car un incident peut aboutir à des accusations criminelles.

Les PME qui ne comptent pas de spécialistes à l'interne pour remplir tous ces rôles devraient faire appel à une société de conseil externe ou à un fournisseur de services gérés. **Nous fournissons des informations supplémentaires sur ce que les PME devraient rechercher chez un fournisseur de services gérés dans la recommandation n° 13.**

Les tâches de confinement comprennent :

- Appliquer des tactiques de confinement à court terme (par exemple, l'isolement du segment de réseau violé).
- Se consacrer à des stratégies de confinement à long terme.
- Appliquer des correctifs temporaires pour soutenir les opérations quotidiennes tout en reconstruisant simultanément les systèmes nettoyés.

Les tâches liées aux leçons apprises comprennent :

- Effectuer une rétrospective de l'incident dans les deux semaines suivant l'incident.
- Documenter intégralement l'incident, notamment les actions adoptés pour le limiter.
- Déterminer tous les aspects du processus ou du plan de réponse en cas d'incident qui pourraient être perfectionnés.

Pour davantage de précisions, nous recommandons vivement aux PME de télécharger le manuel de gestion des incidents (Incident Handler's Handbook) élaboré par le SANS Institute. Les éléments abordés dans cette section sont fondés sur cette référence précieuse et pratique.

Les tâches d'éradication comprennent :

- Supprimer les virus, les logiciels malveillants et toutes autres menaces des systèmes concernés.
- Identifier la cause fondamentale d'une attaque.
- Prendre des mesures pour empêcher des attaques identiques ou similaires à l'avenir.

Les tâches de restauration comprennent :

- Remettre en ligne, de manière méthodique et prudente, les systèmes de production affectés.
- Tester et vérifier les systèmes de production atteints pour veiller à leur retour à un fonctionnement normal.

4 RECOMMANDATION

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

Une solution de gestion des mots de passe permet aux utilisateurs de ne retenir que deux séries d'identifiants plutôt que des dizaines de sorte qu'ils n'ont pratiquement plus de mot de passe. La première série d'identifiants est réservée à leur propre système, et la seconde à l'accès à la solution.

En outre, lorsque la solution de gestion des mots de passe est compatible avec l'authentification unique (de l'anglais *Single Sign-On* ou SSO) de Microsoft, les utilisateurs ne pas sont tenus de créer et de mémoriser qu'un seul ensemble d'identifiants. Les PME utilisant le SSO peuvent même franchir une étape supplémentaire et implémenter une authentification sans mot de passe avec des solutions recourant au matériel ou à la biométrie.

Les caractéristiques et fonctions clés que les PME doivent rechercher lorsqu'elles choisissent une solution de gestion des mots de passe comprennent :

- **Le chiffrement de bout en bout (AES-256)**
- **L'authentification multifacteur (AMF)**
- **Coffre des mots de passe sécurisé (la gestion du partage)**
- **Générateur de mots de passe robustes**
- **Autorisations reposant sur des rôles**

Solutions de gestion des mots de passe : Nuage ou sur site?

Ni les solutions de gestion de mots de passe infonuagiques ni celles sur site ne sont fondamentalement supérieures. Il y a des avantages et des inconvénients pour chaque modèle :

Déploiement

• Nuage : contrairement à la croyance populaire, les solutions de gestion des mots de passe dans le nuage ne sont pas hébergées « dans les airs ». Ils sont au contraire hébergés par un fournisseur de services. Les clients peuvent accéder à ces ressources aussi souvent qu'ils le souhaitent, à partir de n'importe quel appareil connecté à Internet.

• Sur site : les solutions de gestion des mots de passe sur site sont déployées à l'interne, au sein de l'infrastructure d'une entreprise. Contrairement au modèle infonuagique, c'est l'entreprise et non le fournisseur de services qui est responsable de la maintenance de la solution et des processus associés.

Contrôle

• Nuage : les solutions infonuagiques permettent aux fournisseurs de services de garder le contrôle, non pas pour diminuer celui des clients, mais plutôt (comme mentionné récemment) parce qu'ils sont responsables de l'hébergement et de la maintenance de la solution. Ils ont donc besoin d'un certain contrôle pour garder le tout opérationnel et sécuritaire.

• Sur site : avec les solutions de gestion des mots de passe sur site, les entreprises conservent et contrôlent leurs ressources à l'interne. Même s'il s'agit d'un avantage pour certaines entreprises, cela peut aussi devenir un inconvénient pour d'autres (surtout pour les PME qui n'ont pas les infrastructures et les employés spécialisés pour optimiser et sécuriser en permanence leur solution).

Sécurité

• Nuage : dans le passé, les soucis de sécurité constituaient la principale raison pour laquelle les entreprises hésitaient à adopter des applications, ressources et solutions infonuagiques (notamment, mais pas exclusivement, les solutions de gestion des mots de passe dans le nuage). Depuis quelques années, la sécurité du nuage s'est considérablement améliorée. Par exemple, les fournisseurs de services de gestion des mots de passe dans le nuage font de la surveillance 24 heures sur 24, 7 jours sur 7, effectuent continuellement des tests d'intrusion, etc. Ce niveau élevé et continu de sécurité ne peut souvent pas être atteint par les PME à cause de leurs budgets limités et du manque de spécialistes en cybersécurité.

• Sur site : étant donné que les solutions de gestion des mots de passe sur site sont hébergées, maintenues et contrôlées au sein même de l'infrastructure informatique de l'entreprise, elles sont par nature plus sécurisées que les solutions infonuagiques. Cependant, comme mentionné précédemment, cela ne signifie pas que ces solutions ne sont pas pour autant sécuritaires. Au contraire, cela signifie simplement que celles sur site offrent un niveau de sécurité supplémentaire. Pour certaines entreprises, ce niveau est important, voire essentiel pour des raisons de conformité. Pour plus d'informations à ce sujet, rendez-vous dans la section suivante. Pour d'autres entreprises, ce niveau n'est pas nécessaire et le choix d'une solution infonuagique est plus pratique et abordable.

Conformité

• Nuage : en matière de conformité, les entreprises devraient toujours s'assurer que le fournisseur de services infonuagiques respecte des normes de conformité pertinentes comme SOC 2 de type II et ISO 27001:2013. Les fournisseurs de services devraient, notamment, utiliser le chiffrement.

• Sur site : certaines entreprises de secteurs comme la santé peuvent être tenues de maintenir un contrôle interne complet de leurs données (leurs données ne peuvent pas être stockées en dehors de leur environnement avec un fournisseur de services tiers). Dans ce cas, il est nécessaire de choisir une solution de gestion des mots de passe sur site.

Coût

• Nuage : avec les solutions infonuagiques de gestion des mots de passe, les entreprises n'ont pas besoin d'acheter de logiciel ou de matériel. Elles achètent plutôt une licence ou un abonnement permettant d'accéder à la solution via Internet. Le type d'accès auquel elles ont droit dépend du type de licence ou d'abonnement dont elles disposent. Par exemple, certaines solutions permettent d'accéder à des machines spécifiques, tandis que d'autres vont donner accès à des utilisateurs spécifiques. Ce dernier est beaucoup plus convivial, parce qu'il permet aux utilisateurs finaux d'accéder à la solution où qu'ils se trouvent, à partir de n'importe quel appareil.

• Sur site : les solutions de gestion des mots de passe sur site sont généralement plus coûteuses que celles dans le nuage. Cela s'explique par le fait que les entreprises doivent mettre sur pied l'infrastructure et les processus informatiques nécessaires tout en couvrant les coûts d'exploitation et de maintenance continuellement. Plusieurs PME manquent de budget et de personnel pour répondre à ces exigences. C'est pour cette raison qu'elles choisissent des solutions infonuagiques.

Mise en œuvre

• Nuage : normalement, les solutions infonuagiques « devraient » être faciles à implanter. Nous insistons sur « devraient », parce que ce n'est malheureusement pas toujours le cas. Certaines solutions sont simples et se déploient rapidement, tandis que d'autres sont très (et inutilement) complexes, nécessitant une configuration difficile et plusieurs tests. Toute entreprise qui opte pour une solution infonuagique devrait s'assurer qu'elle ne devienne pas une source de stress supplémentaire. Lire des témoignages et profiter des périodes d'essai gratuites sont de bons moyens de vérifier le tout.

• Sur site : les solutions de gestion des mots de passe sur site sont plus complexes à mettre en œuvre que celles dans le nuage, parce qu'elles sont hébergées et gérées à l'interne. Elles doivent donc être configurées et intégrées à l'environnement existant. Toute entreprise qui choisit une option sur site devrait s'assurer que son fournisseur de services dispose des ressources et des programmes pour rendre l'implantation aussi rapide et facile que possible.

L'équipe de sécurité de Devolutions propose les conseils suivants aux décideurs des PME :

L'interminable débat entre le nuage et l'auto-hébergement frappe à nouveau, cette fois-ci en matière de solutions de gestion de mots de passe. À notre avis, la discussion devrait surtout évoluer autour des besoins de gestion des mots de passe d'une entreprise. Ces besoins peuvent varier en fonction d'une multitude de facteurs comme :

• L'emplacement et les rôles des utilisateurs
• Les exigences de disponibilité
• La taille et la complexité de l'environnement informatique
• La valeur des données à protéger
• Les exigences de conformité et de sécurité

Les déploiements hybrides, comme les solutions infonuagiques et sur site, pourraient ainsi résoudre des besoins distincts au lieu d'un seul produit plus restrictif. Une même solution peut être déployée plusieurs fois pour résoudre des problèmes comme la séparation des tâches. Indépendamment de leur choix (sur site ou dans le nuage, gratuit ou payant), les PME doivent bien cerner tous leurs besoins avant d'acheter une technologie. S'il est manifestement nécessaire de répondre aux besoins actuels, il est tout aussi essentiel d'anticiper les besoins futurs.

5 RECOMMANDATION

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

Nous invitons toutes les PME à établir et à appliquer une politique rigoureuse de gestion des mots de passe comprenant tous les éléments suivants :

Mettre en place l'authentification multifacteur (AMF)
Même l'utilisateur final le plus prudent peut faire une erreur coûteuse liée à un mot 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'AMF empêchera les acteurs malveillants d'accéder aux comptes, même s'ils disposent des informations de connexion correctes.

Implanter un gestionnaire de mots de passe
Lorsqu'ils disposent d'un gestionnaire de mots de passe, les utilisateurs ne doivent se souvenir que de deux séries d'identifiants de connexion au lieu de dizaines, ce qui leur permet de ne quasiment plus avoir besoin de mots de passe. Pour un approfondissement sur les caractéristiques et fonctions que les PME doivent rechercher dans une solution de gestion des mots de passe, ainsi qu'une analyse des avantages et inconvénients du déploiement dans le nuage par rapport au déploiement sur site, voir la recommandation n° 4.

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. Cependant, la grande majorité des utilisateurs ne peuvent pas se souvenir d'un mot de passe de plus de 16 caractères sans recourir à des schémas et à des astuces comme « Leetspeak ». Cela consiste à changer des lettres pour des caractères similaires (par exemple « motdep@55e » au lieu de « mot de passe »). Malheureusement, ces techniques sont largement connues et exploitées par les pirates.

Une phrase secrète est beaucoup plus longue qu'un mot de passe classique (ce qui la rend moins vulnérable aux attaques par force brute). Elle contient des lettres, des symboles, des espaces et des chiffres. Par exemple : « Paul, mon chien violet, aime quand je joue au frisbee avec lui ». Comme vous l'aurez peut-être constaté, il est plus sage de choisir une phrase secrète qui n'a pas de sens logique et qui n'est pas associée à l'utilisateur. Pour une sécurité accrue, les utilisateurs peuvent aussi mélanger les langues.

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 informations d'identification plus faibles et plus faciles à identifier. Parmi les mots de passe les plus courants en 2021, on trouve : 123456, qwerty et iloveyou. Aucun changement ne devrait donc être effectué à moins de preuves de compromission.

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 sélectionné. Il est important que cette liste comprenne des mots liés à l'environnement personnel ou professionnel de l'utilisateur, tels que 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 ». La liste de mots de passe la plus connue est rockyou.txt.

Pour vérifier si elles ont été compromises, les PME peuvent utiliser des services comme 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. Cela aide à empêcher les pirates de contourner les doubles facteurs d'authentification par l'ingénierie sociale, car la PME saura quand changer les mots de passe et sur quels services.

Au-delà de la vérification de tous les mots de passe éventuels pour les comptes professionnels, les PME doivent conseiller fortement aux utilisateurs de vérifier également les mots de passe de leurs comptes personnels. En effet, les pirates s'introduisent souvent dans ces comptes afin de voler des données qui sont ensuite utilisées pour mener des attaques d'hameçonnage ciblées. Par exemple :

• Un utilisateur ajoute dans un courriel personnel à un ami qui est aussi un fournisseur : « au passage, n'oublie pas d'envoyer ta facture à Sheila de la comptabilité lundi matin ».

• Un pirate fouineur fait semblant d'être le fournisseur, et envoie un courriel à Sheila lui demandant de mettre à jour le numéro de compte bancaire figurant dans le dossier.

• Puisque le courriel semble être légitime et ordinaire, Sheila se conforme à la demande.

• Le véritable fournisseur fait parvenir une facture qui est payée, mais sur le compte bancaire mis à jour (frauduleusement).

Lorsque le vol est découvert, ce qui peut être des jours, des semaines, voire des mois plus tard, les pirates ont vidé le compte. Et pour comble de malheur, la PME responsable est toujours tenue de payer le fournisseur légitime, et ce montant peut inclure des intérêts!

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 créer 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 des accès privilégiés. Nous examinons les éléments d'une solution PAM dans la recommandation n° 7.

Appliquer une politique d'historique des mots de passe.

Les entreprises doivent se doter d'une politique d'historique des mots de passe pour garantir que les utilisateurs finaux ne sélectionnent pas les anciens mots de passe. Le Center for Internet Security (CIS) recommande de définir cette valeur à 24 ou plus. 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.

Éliminer la réutilisation des mots de passe

En parlant de réutilisation de 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 (c'est-à-dire des comptes de porte dérobée pour les administrateurs). Malheureusement, cela signifie que la compromission d'un appareil les déverrouille tous.

Une excellente solution à ce problème consiste à installer *Local Administrator Password Server* (LAPS) pour les domaines 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.

Activer le copier/coller des mots de passe

En théorie, les utilisateurs ne devraient pas être autorisés à copier/coller des mots de passe. Dans la réalité, c'est toutefois conseillé, car cela empêche les utilisateurs de choisir des mots de passe simples et faciles à retenir. Voici ce que dit le NIST : « Les vérificateurs DEVRAIENT permettre aux demandeurs d'utiliser la fonctionnalité "coller" lors de la saisie d'un mot de passe. Cela facilite l'utilisation de gestionnaires de mots de passe, qui sont largement utilisés et, dans de nombreux cas, augmentent la probabilité que les utilisateurs choisissent des mots de passe plus forts. »

Inscrire les utilisateurs finaux à une plateforme de formation sur la cybersécurité

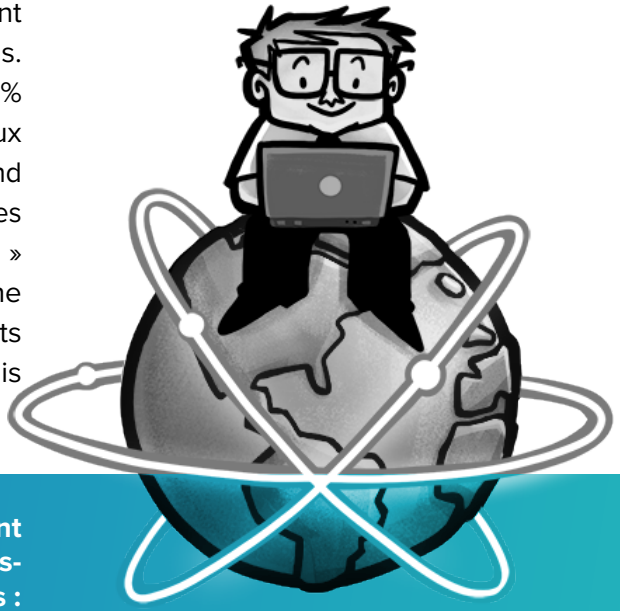
Les PME devraient inscrire leurs utilisateurs finaux sur une plateforme de formation sur la cybersécurité qui couvre des sujets tels que l'ingénierie sociale, la sécurité des courriels, la sécurité des appareils mobiles, la navigation Web sécurisée, les réseaux sociaux sécurisés, la protection des informations sur la santé, etc. Les gestionnaires peuvent également suivre les progrès de l'utilisateur final pour identifier les lacunes dans les connaissances et les besoins de formation. Nous approfondissons cette question dans la **recommandation n° 10**.

6 RECOMMANDATION

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

Dans de nombreuses PME, lorsqu'un employé quitte (volontairement ou non), l'accent est mis sur la récupération des ressources. Ainsi, il est demandé à un employé de remettre son ordinateur portable, son téléphone intelligent, ses dossiers de clients, sa carte d'accès au bâtiment, etc. De toute évidence, la récupération des ressources est un élément essentiel de la procédure de cessation d'emploi, mais ce n'est pas tout.

Dans le cadre d'une stratégie exhaustive de gestion des départs d'employés, il est également essentiel pour les PME de supprimer les accès. En effet, une étude récente a constaté que 25 % des travailleurs affirment avoir encore accès aux comptes de leur ancien emploi : cela comprend les anciens employés et responsables informatiques possédant les légendaires « clés du royaume » (c'est-à-dire l'accès aux comptes privilégiés). Une autre étude a révélé que plus de 50 % des mots de passe de comptes privilégiés ne sont jamais supprimés!



Afin de rectifier cette situation, les PME doivent mettre en place un processus efficace de suppression des accès comprenant les étapes suivantes :

Changer aussitôt le mot de passe de l'employé

La première étape, et la plus importante, consiste à changer le mot de passe de l'employé, afin qu'il ne puisse pas accéder à son (ses) ancien(s) compte(s), ou qu'une personne agissant en son nom, avec son autorisation ou non.

Désactiver l'accès à tous les comptes

Il existe deux options pour retirer l'accès aux employés : la suppression des comptes et le verrouillage des comptes. La suppression des comptes est préférable, car elle exclut toute possibilité d'accès futur. Néanmoins, il peut y avoir des cas où il est nécessaire de préserver les comptes s'ils renferment des données précieuses, comme des fichiers importants, des courriels, etc. Dans ce contexte, les PME doivent verrouiller les comptes jusqu'à ce que les données puissent être archivées ailleurs de manière sûre et adéquate (les comptes pourront ensuite être supprimés).

Changer les mots de passe des comptes privilégiés partagés

Les PME doivent modifier les identifiants de l'ensemble des comptes privilégiés qui ont été partagés avec l'employé. Ces comptes comprennent tous ceux qui confèrent des droits d'utilisateur élevés, ainsi que :

- Les comptes d'administrateur de domaine
- Les comptes d'administrateur local
- Les comptes d'accès d'urgence
- Les comptes d'application
- Les comptes système
- Les comptes de services du domaine

Nous abordons ces types de comptes privilégiés plus en détail dans la recommandation n° 8.

7 RECOMMANDATION

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

Les utilisateurs bénéficiant d'un accès privilégié reçoivent les « clés du royaume » afin d'être davantage productifs et efficaces dans la réalisation de leurs tâches quotidiennes. Hélas, les utilisateurs privilégiés sont aussi des proies de prédilection pour les pirates qui veulent pénétrer dans les appareils et les réseaux, et finalement voler des données. **En fait, 74 % des violations de données sont dues à un abus de compte privilégié.**

Par ailleurs, 72 % des entreprises ne stockent pas tous leurs comptes à privilèges dans un coffre sécurisé, 58 % des entreprises comptent plus de 100 000 dossiers accessibles à tous les employés et, dans plus de 50 % des entreprises, les comptes à privilèges n'expirent jamais ou ne sont pas supprimés.

De nombreux experts en sécurité informatique considèrent que les comptes d'utilisateurs privilégiés représentent le type d'accès privilégié le plus vulnérable et le plus dangereux, en raison de leur nombre, de l'accès aux données sensibles qu'ils accordent et de la facilité avec laquelle les pirates peuvent les compromettre.

Tout cela nous amène à la question suivante : pourquoi les PME ne ferment-elles pas tout bonnement tous les comptes privilégiés? La réponse est que l'identité n'est pas toujours liée à un utilisateur spécifique. Elle est plutôt attribuée à un rôle, une équipe ou un groupe. Voici des exemples de comptes pour lesquels l'accès partagé est habituellement une exigence :

- Comptes d'administrateur de domaine
- Comptes d'administrateur local
- Comptes d'accès d'urgence
- Comptes d'application
- Compte système
- Compte de services de domaine

Nous examinons de plus près ces types de comptes dans la recommandation n° 8.

BON À SAVOIR

Il est recommandé aux PME de créer deux comptes pour les utilisateurs à privilèges élevés. Le premier compte a un accès plutôt limité et est destiné aux tâches quotidiennes. Le second compte a un accès plus étendu et est réservé aux tâches administratives. Le second compte est géré par le système PAM et configuré avec une sécurité accrue, comme l'injection d'identifiants et la rotation des mots de passe après utilisation.

Heureusement, il existe un moyen concret pour les PME de combler le fossé entre la gestion des identités (authentification) et la gestion des accès (autorisation) : adopter une solution PAM.

Une solution PAM fait appel au contrôle d'accès basé sur les rôles (*Role-Based Access Control* ou RBAC) pour faire office de gardien des comptes partagés, ajoutant un niveau crucial de surveillance et d'audit des comptes privilégiés. Les caractéristiques clés sur lesquelles les PME doivent se baser pour choisir une solution PAM sont les suivantes :

• Un coffre sécurisé qui stocke adéquatement et en toute sécurité les identifiants et autres données sensibles qui doivent être répartis entre plusieurs utilisateurs (par exemple, les clés de licence des logiciels, etc.).

• Fonctionnalité de demande de réservation de compte, permettant aux administrateurs d'approuver ou de rejeter les demandes au cas par cas (et, en cas d'approbation, de définir une limite de temps pour l'accès afin d'éviter que des comptes privilégiés soient laissés sans surveillance).

• Réinitialisation automatique du mot de passe lors de la restitution.

• Authentification multifacteur (AMF) intégrée.

• L'injection des identifiants, qui autorise les utilisateurs à accéder à des comptes privilégiés sans jamais voir les identifiants. Ce procédé limite aussi l'accès des utilisateurs aux ressources en dehors d'un flux de travail fourni par la solution PAM, ce qui diminue potentiellement le risque d'abus d'identifiants.

• La détection de comptes, qui analyse et détecte automatiquement les comptes privilégiés à partir d'un fournisseur Active Directory. Pour les PME, cette solution est beaucoup plus concrète et efficace que l'utilisation de fournisseurs d'identification autonomes comme les systèmes de gestion des identités et des accès (GIA), les bases de données, les équipements réseau et les serveurs qui doivent être interrogés manuellement pour détecter les comptes.

• Facilité de déploiement et de gestion.

Par ailleurs, les solutions PAM les plus complexes prennent en charge la gestion des sessions privilégiées. Cette fonctionnalité fait appel à un serveur spécialisé qui gère l'authentification en arrière-plan et peut même enregistrer l'activité des sessions à distance. La gestion des sessions privilégiées est très importante pour les PME qui ont des sous-traitants et des employés « boomerang » (c'est-à-dire des employés qui quittent l'organisation et y reviennent par la suite). Ces utilisateurs doivent généralement faire l'objet d'une surveillance accrue et d'un accès limité.

8 RECOMMANDATION

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

En dépit de l'importance cruciale de la protection des comptes privilégiés, des études ont démontré que 55 % des entreprises ne savent pas le nombre de comptes privilégiés qu'elles possèdent ni où ils se trouvent.

L'une des principales raisons de cette omission est que de nombreuses PME ne savent pas quels types de comptes privilégiés elles doivent protéger, surveiller et mettre à jour. Il s'agit notamment de :

Comptes d'administrateur de domaine
Ils détiennent les « clés du royaume » parce qu'ils ont le contrôle de l'ensemble du domaine Active Directory (tous les contrôleurs, postes de travail et serveurs membres). Il va sans dire (mais il n'y a pas de mal à le répéter) que l'accès aux comptes d'administrateur de domaine devrait être accordé seulement si nécessaire.

Comptes d'utilisateurs privilégiés
Comme son nom l'indique, les comptes d'utilisateurs privilégiés accordent plus de privilèges (et donc plus de risques) que les comptes d'utilisateurs ordinaires sur un ou plusieurs systèmes. Par exemple, les utilisateurs peuvent modifier ou supprimer des logiciels, changer les configurations d'application, etc.

Comptes d'administrateur local
Les comptes administrateur local accordent un accès de niveau administrateur aux appareils locaux et sont généralement utilisés par les équipes informatiques pour configurer de nouveaux postes de travail et effectuer des tâches de maintenance. Les pirates ciblent souvent les comptes administrateur local vulnérables pour établir un point d'ancrage à l'intérieur d'un réseau. À partir de là, ils évaluent les outils et systèmes de défense de leurs victimes avant de lancer une attaque.

Compte d'accès d'urgence
Parfois désignés par l'expression compte *break-the-glass* ou compte *firecall*, ils sont habituellement désactivés par défaut en attendant un incident critique, comme une cyberattaque. Dans ce cas, des utilisateurs spécifiques peuvent y accéder pour rétablir la sécurité des systèmes et récupérer les journaux d'utilisation.

Comptes d'application

Les comptes d'application sont utilisés par les applications pour accéder à diverses ressources fonctionnelles comme les bases de données et les réseaux. Ils sont également utilisés pour effectuer des tâches automatisées comme les mises à jour logicielles. Habituellement, les mots de passe du compte d'application sont stockés dans des fichiers texte non chiffrés sur le réseau, afin qu'ils puissent être rapidement et facilement récupérés par les utilisateurs au sein de l'entreprise. Malheureusement, les pirates ciblent des vulnérabilités connues (et non corrigées) pour voler ces mots de passe et établir un accès à distance. Ils peuvent alors modifier les fichiers binaires du système et même élever les comptes standards en comptes privilégiés pour se déplacer à travers le réseau.

BON À SAVOIR

Dans de nombreux cas, les comptes d'utilisateur privilégiés ne sont pas associés à un utilisateur spécifique, mais sont plutôt répartis entre les administrateurs. Fondamentalement, la règle que les PME devraient observer est la suivante : lorsqu'un compte confère aux utilisateurs des droits supérieurs à ceux d'un compte standard, il est considéré comme un compte privilégié et doit être géré et surveillé en conséquence.

Comptes système

Les comptes système sont utilisés par les services et les applications (au lieu des utilisateurs humains) pour lancer des processus et exécuter des tâches planifiées. La bonne nouvelle est que les comptes système n'ont généralement pas la possibilité de se connecter aux systèmes. La mauvaise nouvelle est qu'ils ont souvent des mots de passe qui ne changent jamais, parce que les entreprises les oublient complètement ou ne connaissent même pas leur existence. Ainsi, les comptes système sont fréquemment ciblés par des pirates, qui lancent des fichiers binaires avec des privilèges élevés pour mener leurs attaques.

Comptes de services (domaine)

Ils permettent à diverses applications et systèmes de communiquer et d'accéder à différentes ressources, afin de faire appel à des API (*Application Programming Interface*), d'exécuter des rapports, etc. Ils sont généralement utilisés pour mettre à jour les correctifs de sécurité, les sauvegardes et le déploiement de logiciels. En conséquence, de nombreuses PME modifient rarement, voire jamais, le mot de passe, ce qui est précisément ce sur quoi les acteurs malveillants comptent.

Toutes les organisations doivent être préoccupées par l'abus de comptes privilégiés commis par des employés malhonnêtes, ainsi que par des pirates qui se sont emparés de comptes d'utilisateurs (et souvent sans que les victimes ne s'en rendent compte). Voici quelques-uns des signes à surveiller :

• Un utilisateur déroge de ses activités habituelles. Cela peut vouloir dire une durée de session inhabituellement courte ou longue, un accès, l'affichage ou des modifications de fichiers qui ne font pas partie de sa routine ou des séquences de touches atypiques (qui peuvent être détectées par des analyses biométriques qui utilisent l'apprentissage automatique pour étudier un utilisateur au fil du temps).

• Un utilisateur transfère des fichiers vers un poste de travail personnel alors qu'il n'est autorisé qu'à transférer des fichiers vers des systèmes qui appartiennent à l'entreprise.

• Un compte utilisateur est accessible par plusieurs points d'extrémité (ordinateurs, serveurs) en même temps.

• Plusieurs utilisateurs sont connectés à partir du même point d'extrémité.

• Des comptes en dormance reprennent vie.

• Des titres de fenêtres inhabituels apparaissent.

Les PME doivent également garder à l'esprit que les pirates lancent fréquemment de petits tests pour voir si leur présence est détectée. Ils créent également des comptes et les ajoutent à des groupes bénéficiant d'un accès privilégié, puis attendent des semaines ou des mois avant d'y accéder.

Afin de combler cette lacune, les PME doivent déployer une solution de gestion des accès à privilèges (PAM) complète, mais simple à utiliser et à gérer, afin de sécuriser et de surveiller tous leurs comptes à privilèges. Dans le cas contraire, ne pas le faire peut aboutir à des violations de données coûteuses, à des atteintes permanentes à la réputation et, dans certains cas, à une fermeture pure et simple. **Dans la recommandation n° 7, nous approfondissons l'objectif d'une solution PAM et mettons en évidence les facteurs que les PME doivent prendre en compte lors du choix d'une solution.**

9 RECOMMANDATION

Les PME doivent mettre en œuvre 4 principes de sécurité primordiaux : le principe de moindre privilège, la séparation des tâches, la Confiance zéro et la défense en profondeur.

Le principe de moindre privilège

Le principe de moindre privilège (connu sous l'abréviation POLP en anglais) est une politique selon laquelle les utilisateurs finaux ne bénéficient que des accès dont ils ont besoin pour effectuer leur travail ni plus ni moins. En plus de réduire la taille de la surface d'attaque, le POLP offre des avantages supplémentaires 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 un accès trop important aux réseaux 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 appareil ou 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 PME 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 principe de moindre privilège 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.)**
- **Départements (par exemple, développement, marketing, RH, etc.)**
- **Emplacement (par exemple, le siège social, les bureaux extérieurs, etc.)**
- **Heure (par exemple, les heures de bureau, après les heures de bureau, etc.)**

Règle générale, les administrateurs système personnalisent ce principe en fonction des besoins spécifiques de leur entreprise et cherchent à trouver un équilibre entre le besoin d'une sécurité renforcée et la productivité des utilisateurs.

Les bonnes pratiques du POLP sont les suivantes :

Évaluer les niveaux d'accès : En consultation avec les utilisateurs, les PME doivent évaluer chaque rôle pour déterminer le niveau d'accès approprié. L'accès par défaut doit être défini comme le « moindre privilège », et un accès plus important ne doit être accordé que si nécessaire.

Communiquer efficacement : Les PME doivent communiquer l'objectif du POLP à tous les utilisateurs afin qu'ils comprennent que l'approche ne vise pas à diminuer leur productivité, mais plutôt à protéger l'organisation.

Utiliser des mots de passe à usage unique : Lorsqu'un accès privilégié temporaire est requis, les PME devraient utiliser des mots de passe à usage unique qui sont accordés au dernier moment et qui sont révoqués immédiatement après l'utilisation. Cette approche, connue sous le nom de bracketing de privilèges, peut être utilisée pour des utilisateurs finaux individuels ainsi que pour des processus ou des systèmes.

Appliquer la séparation des comptes : Les PME devraient séparer les comptes administrateur des comptes standards et les fonctions des systèmes de niveau supérieur de celles de niveau inférieur (voir la section suivante sur la séparation des tâches).

Surveiller en permanence et auditer régulièrement : Il est très important pour les PME d'avoir une visibilité totale afin de voir exactement ce que font les utilisateurs finaux et quand ils le font. De plus, les PME devraient régulièrement auditer les privilèges des utilisateurs finaux pour s'assurer que leur accès est approprié. Cela inclut la suppression de l'accès pour tous les employés qui ont quitté l'entreprise et de disposer d'un moyen de révoquer automatiquement l'accès privilégié en cas d'urgence.

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 (parfois appelée ségrégation des tâches) entre en scène.

La séparation des tâches (de l'anglais *Segregation of Duties* ou SoD) 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/CEI 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. Ce principe est utilisé depuis plusieurs décennies dans la comptabilité, la gestion de risques et l'administration financière.

Les bonnes pratiques concernant la séparation des tâches

Définir et attribuer les rôles de manière à mitiger les risques : prévenez les conflits d'intérêts (réels ou apparents), les actes illicites, la fraude et les abus lorsque vous confiez un ou plusieurs rôles à un employé.

Aligner les tâches sur les rôles : Les PME doivent mettre en place des permissions et des droits d'accès pour s'aligner sur la séparation des tâches et des rôles, qui doit être basée sur le principe du moindre privilège (comme indiqué ci-dessus).

Analyser les niveaux d'accès pour la hiérarchisation : Les PME doivent s'assurer qu'aucun individu n'a la possibilité de combiner plusieurs accès pour accéder à un niveau d'accès supérieur (et non autorisé) sur un système ou un domaine donné à un moment quelconque.

Mettre en place des politiques de ressources humaines appropriées : Les PME devraient mettre en place des politiques de ressources humaines qui soutiennent un programme SoD complet. Il s'agit notamment de former les superviseurs et les gestionnaires à reconnaître lorsqu'un subordonné ou tout autre collègue a un ensemble de tâches conflictuelles, risquées ou inutiles qui pourraient être transférées à un autre rôle plus adéquat.

En outre, une certaine confiance dans le SoD peut être atteinte en réalisant les opérations suivantes :

Auditer fréquemment
Les PME devraient réaliser des audits de cybersécurité permanents et prêter une attention particulière aux activités potentiellement frauduleuses. Nous examinons les éléments d'un audit de cybersécurité dans la recommandation n° 12.

S'appuyer sur l'expertise d'un tiers pour la surveillance
Il est conseillé aux PME qui ne bénéficient pas d'une expertise interne dans ce domaine de travailler avec un fournisseur de services gérés (MSP), car les activités malveillantes sont presque toujours cachées et difficiles à détecter. Ce dernier accordera aussi l'avantage d'appliquer le SoD entre l'audit interne et les rôles opérationnels. Nous insistons sur les facteurs sur lesquels les PME doivent prendre en compte lors du choix d'un MSP dans la recommandation n° 13.

La Confiance zéro

La Confiance zéro repose sur l'idée que personne ne devrait être automatiquement digne de confiance, même s'il se trouve derrière le périmètre ou utilise un réseau de confiance. Au contraire, avant d'accéder à certaines parties du réseau, les utilisateurs, les machines et les applications doivent être authentifiées par des technologies telles que l'authentificateur multifacteur, la gestion des identités et des accès, le chiffrement, l'analyse, etc. Un élément clé de la Confiance zéro est le POLP, dont nous avons parlé plus haut.

Il est important de préciser qu'une approche de Confiance zéro n'implique pas la suppression du périmètre. Elle s'appuie plutôt sur la micro-segmentation du réseau pour déplacer le périmètre aussi près que possible des applications privilégiées et des surfaces protégées. Autrement dit, plutôt que de mettre un agent de sécurité dans le hall d'un bâtiment, la Confiance zéro met un agent de sécurité devant les ascenseurs, les cages d'escalier, chaque bureau, etc.

Le concept de Confiance zéro correspond à ce que de nombreux administrateurs et autres professionnels de la sécurité de l'information disent depuis des années : présumer que tout le monde (même au sein de la PME) représente une menace pour la cybersécurité jusqu'à preuve du contraire. Le prolongement de cette vision est que l'approche « château et douves » de la sécurité du périmètre est révolue, et que la micro-segmentation et l'application granulaire du périmètre sont à la mode.

Les bonnes pratiques par rapport à l'approche Confiance zéro :

• Ajouter des technologies infonuagiques pour remplacer les services et systèmes hérités non authentifiés.

• Concevoir une architecture Confiance zéro en fonction de la manière dont les données se déplacent sur le réseau et dont les utilisateurs et les applications accèdent aux informations sensibles.

• Vérifier la confiance lors de l'accès à toute ressource réseau à l'aide de l'authentification multifacteur en temps réel.

• Étendre les contrôles d'identité aux terminaux pour détecter et valider tous les appareils. La seule vérification des utilisateurs ne suffit pas.

• Organiser les utilisateurs par groupe/rôle pour prendre en charge les stratégies d'appareil. Pour en savoir plus sur la mise en œuvre de la gestion des identités privilégiées (PIM), lisez notre article ici.

• Utiliser le déprovisionnement automatique, ainsi que la capacité d'effacer, de verrouiller et de désinscrire les appareils volés ou perdus.

• Former les utilisateurs pour qu'ils participent à la solution dans le nouvel environnement de Confiance zéro. Par exemple, les utilisateurs doivent être incités à signaler immédiatement les tentatives d'hameçonnage ou tout autre comportement suspect. Comme le précise Deloitte : « Le changement d'état d'esprit de la confiance zéro apporte avec lui un ensemble de principes de conception qui guident le développement de l'architecture de sécurité et s'appuient sur les investissements et les processus de sécurité existants. Afin d'appliquer le contrôle d'accès, les entreprises doivent avoir une connaissance situationnelle de leurs données et de leurs actifs : les entreprises qui sont en décalage avec les principes et les pratiques de base de la cyberhygiène risquent d'avoir du mal à profiter pleinement des avantages de la Confiance zéro. » Nous explorons les façons dont les PME peuvent améliorer les principes de cyberhygiène et la sensibilisation dans la recommandation n° 10.

• Mettre régulièrement à jour les droits des utilisateurs finaux en fonction des modifications apportées aux rôles/tâches et des modifications des politiques de sécurité ou des exigences de conformité en vigueur.

BON À SAVOIR

Il est essentiel de comprendre que le passage à la Confiance zéro est un processus de longue haleine et qu'il y aura des embûches en cours de route qui mettront la patience des dirigeants, des responsables informatiques et des utilisateurs finaux à rude épreuve. Toutefois, le jeu en vaut la chandelle, car en matière de sécurité des réseaux, la confiance doit être gagnée plutôt que supposée. La Confiance zéro n'est pas un projet ponctuel : c'est un engagement et un objectif stratégique à long terme qui doit être appliqué dans tous les domaines de l'entreprise.

La défense en profondeur

La défense en profondeur ajoute plusieurs contrôles diversifiés dans un environnement, ce qui crée plusieurs niveaux de sécurité et qui vont ralentir les pirates au maximum.

Une analogie fréquemment utilisée pour décrire cette méthode est le « modèle du fromage suisse ». Imaginez un rayon de lumière qui brille d'un bout à l'autre d'une table. Maintenant, commencez à placer des tranches de fromage suisse en ligne pour obstruer le rayon de lumière. Bien que chaque tranche ait des trous, ceux-ci ne se trouvent pas exactement au même endroit. Ainsi, la lumière est bloquée davantage à chaque fois qu'une tranche est ajoutée.

La lumière, dans cette analogie, est une cyberattaque. Les tranches de fromage suisse sont les différents outils de défense : stratégies, politiques et processus. L'objectif n'est pas d'arrêter complètement la totalité des cyberattaques, car ce n'est pas réaliste. Il s'agit plutôt de faciliter considérablement et efficacement la détection des pirates par les PME lorsqu'ils tentent de contourner les contrôles pour atteindre les actifs sensibles.

Les bonnes pratiques de la défense en profondeur :

Supposer une violation

Les pirates ont tout le temps nécessaire pour saisir l'occasion de lancer une attaque réussie sur une cible. Par conséquent, les niveaux de contrôle doivent être conçus comme si une violation s'était déjà produite (c'est-à-dire en répondant à la question « et si? ») et les PME doivent mettre en œuvre des défenses appropriées pour empêcher ou limiter les prochaines actions des pirates.

Combiner les principes et les stratégies de sécurité

Lorsqu'ils sont combinés, ils produisent un effet de synergie en restreignant et en prévenant leurs faiblesses respectives, ainsi qu'en renforçant leur efficacité générale. Ainsi, le SoD et le POLP contiendront les menaces pesant sur un sous-ensemble de l'environnement de l'entreprise, ce qui constitue une excellente occasion de mettre en place des niveaux de contrôle entre eux. En outre, le principe des quatre yeux pourrait être ajouté pour l'utilisation des accès privilégiés à l'aide de l'approbation de réservation afin de prévenir, ou du moins de détecter, les tentatives d'accès non autorisées. Le principe des quatre yeux exige que toute activité d'un employé impliquant un risque important soit examinée et approuvée par un second employé indépendant et compétent.

Opter pour une diversité des contrôles technologiques

Installez des solutions de cybersécurité qui fonctionnent différemment et constituent des contrôles distincts. Ainsi, si un filtre réseau anti-maliciel, une application de liste blanche et un analyseur de pièces jointes sont tous des outils anti-maliciel, ils agissent différemment et peuvent donc couvrir une plus grande surface d'attaque.

Surveiller activement des comportements inhabituels

Une fois que les pirates ont contourné un niveau de contrôle, ils doivent déterminer comment atteindre leur objectif global. Cela implique de recueillir des informations et, dans certains cas, de vérifier des hypothèses. La surveillance active de ces comportements est l'élément fondamental pour détecter les intrusions entre les niveaux de contrôle. En omettant cette pratique, les pirates auront tout le temps de profiter d'une faille sans être détectés.

Réaliser régulièrement des tests d'intrusion

Cette pratique est idéale pour repérer les faiblesses dans la conception des niveaux de contrôle, en procédant à des attaques simulées sur un niveau de contrôle spécifique ou une combinaison de niveaux de contrôle. Parfois, les pirates sont assez imaginatifs pour choisir un chemin d'attaque qui n'a pas été préalablement identifié et sécurisé par la PME.

10 RECOMMANDATION

Les PME doivent sensibiliser davantage leur personnel à la cybersécurité.

Les PME qui estiment que « puisque nous n'avons pas encore été attaqués, notre personnel doit être sensibilisé aux cybermenaces » exposent leurs données, leurs clients et leur réputation à des risques. Dans les cas extrêmes, elles risquent de ne pas survivre pour remédier à cette situation : 60 % d'entre elles font faillite dans les six mois suivant une cyberattaque.

Il existe plusieurs moyens pour les PME de sensibiliser leur personnel à la cybersécurité, mais l'un des plus pratiques, efficaces et abordables est une plateforme de cybersécurité en ligne. Il s'agit d'un portail qui fournit aux employés une formation autonome, concrète et axée sur les compétences en matière de détection et d'atténuation des menaces dans un environnement simulé dynamique et en direct.

Un grand nombre de menaces sont couvertes, notamment les « trois grandes » qui inquiètent le plus les PME d'après notre enquête : les rançongiciels, l'hameçonnage et les attaques de la chaîne d'approvisionnement. Nous examinons plus en détail ces menaces et la manière de s'en protéger dans la recommandation n° 2).

L'un des principaux avantages de la formation en ligne est que les employés reçoivent un retour immédiat sur leur prise de décision et progressent dans la formation en fonction de leurs performances. Les superviseurs et les gestionnaires accèdent à un tableau de bord et suivent les progrès réalisés afin d'identifier les points forts et les points faibles. Par exemple, un employé peut être compétent lorsqu'il s'agit d'éviter les tentatives d'hameçonnage, mais il peut avoir besoin d'une formation supplémentaire sur la sécurité des appareils mobiles.

11 RECOMMANDATION

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

De nombreuses PME du monde entier se sont lancées dans une course folle pour trouver une solution sûre et sécurisée pour déployer et maintenir l'accès à distance. Bien que certaines PME reviennent à des bureaux physiques, une grande partie de la main-d'œuvre restera à distance à temps plein ou partiel. Cela signifie qu'il y a des centaines de nouveaux points d'entrée qui doivent être protégés contre les pirates potentiels. C'est un défi de taille, surtout que la plupart des PME ne disposent pas de grandes équipes informatiques.

Pour faire face à cet enjeu, les PME doivent mettre en place et appliquer une politique de cybersécurité pour les télétravailleurs qui comprend les éléments suivants :

Utiliser des points d'accès WiFi mobiles ou des RPV

Les télétravailleurs adorent les réseaux WiFi publics, car ils sont disponibles presque partout ces jours-ci : cabinets de médecins, aéroports, restaurants, etc. Malheureusement, les pirates informatiques apprécient également les réseaux sans fil publics, parce qu'ils peuvent facilement espionner, hameçonner et usurper des identités. Pour gérer ce risque, vous pouvez fournir aux travailleurs à distance des points d'accès WiFi mobiles. Si cela est trop coûteux, les travailleurs à distance devraient au moins utiliser un bon réseau privé virtuel (RPV).

Segmenter le réseau domestique

De nombreux travailleurs à distance croient à tort que leur réseau domestique est sécurisé, alors qu'il peut être tout aussi vulnérable qu'un réseau WiFi public. L'utilisation d'un RPV (comme indiqué ci-dessus) permet de réduire les risques, mais les travailleurs à distance devraient aller encore plus loin en segmentant leur réseau domestique et en l'isolant derrière un pare-feu de calibre professionnel.

Utiliser l'authentification multifacteur

L'authentification multifacteur est un niveau de sécurité supplémentaire qui oblige les travailleurs à distance à vérifier leur identité en fournissant leurs identifiants de connexion, ainsi que d'autres informations qui peuvent être :

- Quelque chose qu'ils savent, comme la réponse à une question secrète, un NIP ou un mot de passe.
- Quelque chose qu'ils ont, comme un téléphone intelligent, un jeton ou une carte de crédit.
- Ce qu'ils sont, par exemple leur empreinte digitale, leur voix ou leurs yeux.

L'idée est que, même si les identifiants de connexion d'un travailleur à distance sont volés, il est peu probable (bien que ce ne soit pas impossible) que les pirates informatiques soient en mesure de fournir les informations supplémentaires et d'accéder à un appareil, une application, un réseau ou un système.

Utiliser un gestionnaire de mots de passe

Pour renforcer la sécurité, les travailleurs à distance (ainsi que les travailleurs au bureau) doivent utiliser un gestionnaire de mots de passe qui offre des fonctionnalités comme la rotation des mots de passe, un générateur de mots de passe robustes, des contrôles automatiques des mots de passe exposés lors de piratages et des alertes par courriels en temps réel en cas de tentatives d'accès non autorisé. Nous examinons ces caractéristiques de plus près dans la recommandation n° 4.

Installer des logiciels de sécurité sur les terminaux

Les solutions de sécurité des terminaux sont une ligne de défense essentielle pour empêcher les pirates informatiques de lancer des attaques contre des appareils pour, ultimement, attaquer des réseaux et des systèmes. Les principaux outils de sécurité des terminaux comptent :

- Pare-feu de réseau (sur les terminaux et les réseaux domestiques)
- Logiciel antivirus
- Mises à jour logicielles (plus ci-dessous)

Si certaines PME ont intérêt à laisser leurs experts TI qui travaillent à distance décider du moment de la mise à jour de leurs logiciels, la bonne pratique à adopter pour les autres utilisateurs consiste à utiliser une image standard pour les appareils distants et à activer les mises à jour automatiques pour toutes les applications et tous les programmes, en particulier les logiciels de sécurité.

Utiliser un bloqueur de données USB

Si les télétravailleurs doivent charger leur appareil et que la seule option est une station de chargement USB publique, ils doivent toujours utiliser un bloqueur de données USB. Cela permet aux câbles d'alimentation de se connecter (et la charge de s'effectuer), sans exposer les données à l'intérieur de l'appareil, ce qui empêche l'échange de données et assure la protection contre les logiciels malveillants.

Utiliser une solution sécurisée de gestion des connexions à distance

En matière de travail à distance, les professionnels de l'informatique doivent toujours disposer d'un accès sécurisé aux actifs. Qu'ils aient besoin de mettre à jour les machines du réseau informatique ou d'assister les utilisateurs à distance, le mieux est d'utiliser une solution de gestion des connexions à distance complète, rapide et facile à déployer. Nous y reviendrons dans la recommandation n° 15.

Fournir de la formation continue sur la cybersécurité

Tous les employés ont besoin d'une formation continue en cybersécurité, mais c'est encore plus vrai pour les travailleurs à distance qui peuvent parfois laisser tomber leurs gardes, car on ne leur rappelle pas constamment de suivre les bonnes pratiques.

De plus, les travailleurs à distance doivent être mis en garde contre le partage excessif sur les médias sociaux (les fameux *check-ins* dans les applications quand ils arrivent dans des hôtels ou des aéroports par exemple) parce que les pirates se servent de ces informations pour traquer leurs victimes. Les travailleurs à distance doivent également garder leurs appareils avec eux et ne jamais les laisser sans surveillance, même pendant quelques secondes. Lorsque vous quittez votre domicile, les appareils doivent toujours être verrouillés. Nous fournissons davantage de conseils sur la sensibilisation du personnel à la cybersécurité dans la recommandation n° 10.

Passer au stockage infonuagique

Stocker des données dans le nuage n'est pas simplement plus pratique pour les travailleurs à distance, il améliore également la protection contre les cybermenaces au moyen de mesures telles que le déploiement de l'accès conditionnel, la gestion des droits numériques, l'UEBA, le DPL, le chiffrement, etc. De plus, si un appareil est volé, l'accès aux données dans le nuage peut être révoqué immédiatement. Les PME qui doivent ou veulent utiliser des plateformes sur site plutôt que dans le nuage devront recourir à leur solution RPV ou à une autre suite tierce pour offrir un niveau de protection similaire.

Utiliser des protecteurs d'écran

Les protecteurs d'écran sont un moyen très sûr d'empêcher la technique d'ingénierie sociale « regarder par-dessus l'épaule » (de l'anglais *Shoulder surfing*) de fouiner et de dérober des données. Bien que la distanciation sociale due à la pandémie ait atténué ce risque dans certains endroits, elle ne l'a pas fait disparaître. Sachant que les protecteurs d'écran sont assez peu dispendieux, chaque travailleur à distance devrait en avoir un!

12 RECOMMANDATION

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

La mission d'un audit de cybersécurité est de s'assurer que les contrôles nécessaires (données, opérations, réseau, système, physique, etc.) sont en place et diminuent les risques comme attendu selon un niveau acceptable. Selon le « modèle des trois lignes » largement approuvé par l'Institut des Auditeurs Internes, l'audit constitue la troisième ligne de défense après les contrôles de gestion et les mesures de contrôle interne.

Afin de combler de façon proactive les lacunes de leurs défenses, les PME devraient réaliser au moins deux audits de cybersécurité par an qui portent sur les aspects suivants :

- **Sécurité des données :** audit du contrôle d'accès au réseau, de l'utilisation du chiffrement, de la sécurité des données inactives et des transmissions.

- **Sécurité opérationnelle :** audit des politiques, procédures et contrôles de sécurité.

- **Sécurité du réseau :** audit des contrôles de réseau et de sécurité, du centre opérationnel de sécurité (SOC), des configurations antivirus, des capacités de surveillance de la sécurité, etc.

- **Sécurité du système :** audit des processus de renforcement, des processus de correction, de la gestion des comptes privilégiés, de l'accès basé sur les rôles, etc.

- **Sécurité physique :** audit du chiffrement des disques, des données biométriques, de l'authentification multifacteur, etc.

Non seulement les audits contribuent à aider les PME à harmoniser et à surveiller le rendement de leurs investissements en cybersécurité, mais il peuvent aussi accroître la confiance des clients et des partenaires commerciaux. Ainsi, les rapports d'audit peuvent être diffusés en privé ou en public et ainsi bonifier les offres de services et les présentations.

À quelle fréquence les audits de cybersécurité doivent-ils être réalisés?

De nombreuses PME réalisent un audit de sécurité une ou deux fois par an. Cependant, dans certains cas, ils devraient être effectués plus fréquemment. TechTarget.com déclare :

> *Parfois, des audits trimestriels ou mensuels représentent plus que le temps et les ressources dont disposent la plupart des PME. Les facteurs décisifs de la fréquence à laquelle une PME décide d'effectuer des audits de sécurité reposent sur la complexité des systèmes de même que sur le type et l'importance des données contenues dans ces systèmes. Lorsque les données d'un système sont considérées comme fondamentales, alors ce système peut faire l'objet d'un audit plus régulièrement, mais les systèmes complexes nécessitant un temps d'audit plus long peuvent être audités moins fréquemment.*

Bonnes pratiques pour la réalisation d'un audit de cybersécurité :

- Définir la portée de l'audit de cybersécurité.
- Identifier et documenter les risques et les vulnérabilités.
- Regrouper toutes les politiques de sécurité qui couvrent la sécurité des données, la sécurité opérationnelle, la sécurité des réseaux, la sécurité des systèmes et la sécurité physique.
- Examiner les normes de conformité applicables.
- Créer une vue de haut en bas du réseau, ce qui permet de révéler les faiblesses éventuelles et les points sensibles.
- Dresser une liste des membres de l'équipe de sécurité, et détailler leurs responsabilités.
- Évaluer les performances existantes en matière de gestion des risques de cybersécurité.
- Établir des priorités dans la réponse aux risques.

Procéder à l'interne ou faire appel à une firme externe?

La plupart des PME ne disposent pas des spécialistes internes nécessaires pour réaliser un audit complet de la cybersécurité. Parmi celles qui en disposent, beaucoup choisissent néanmoins de travailler avec un tiers externe, afin d'éliminer les préjugés et les conflits d'intérêts. Elles obtiennent ainsi une représentation exacte de ce qui se passe réellement et, en fin de compte, de ce qui doit changer pour combler efficacement les lacunes et gérer les risques de manière appropriée.

13 RECOMMANDATION

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

Les fournisseurs de services gérés (ou MSP) aident les PME à accroître leurs capacités et leurs compétences, à réduire les risques, à exploiter les perspectives de croissance, à améliorer l'expérience des utilisateurs/clients et, le plus important peut-être en ces temps de pandémie, à s'adapter aux changements et à tirer parti de l'incertitude.

Pour choisir le bon fournisseur de services gérés, les PME doivent évaluer les facteurs suivants :

Services

Certains MSP fournissent une gamme complète de services, alors que d'autres se concentrent sur des éléments spécifiques tels que la sécurité de l'information. Pour les PME, le plus important est que le MSP qu'elles choisissent ait la capacité éprouvée de répondre à leurs besoins et objectifs particuliers. Parallèlement, l'un des services les plus importants qu'un MSP devrait offrir (si ce n'est le plus vital) sont des conseils fiables, impartiaux et personnalisés.

Réactivité

Les PME doivent accorder une attention toute particulière aux normes de réactivité. Il est essentiel de savoir combien de temps il faut généralement à un MSP pour répondre, à quelle vitesse il résout les problèmes et à quoi il faut s'attendre si une assistance sur site est nécessaire. Et bien sûr, tous ces engagements et normes doivent être intégrés dans l'entente de niveau de service.

Couverture

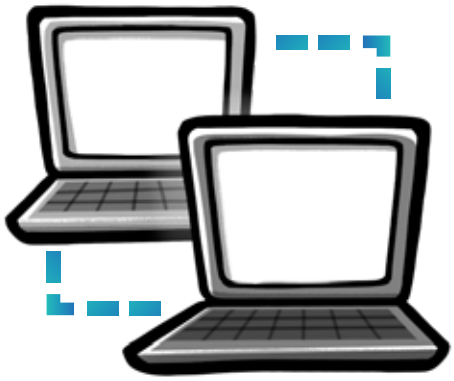
Un MSP doit surveiller l'infrastructure 24 heures sur 24, 7 jours sur 7 et 365 jours par an, au cas où le réseau ou les systèmes seraient hors ligne ou se détérioreraient pour une raison ou une autre.

Continuité des activités et reprise après incident

Les PME ne peuvent pas se permettre de se « couper du réseau » en cas de dysfonctionnement matériel, de défaillance logicielle, de panne de courant locale, de cyberattaque ou de tout autre événement, car si cela se produit, la productivité des employés cesse et les clients se tournent vers la concurrence. Pour prévenir ce genre de situation, les PME doivent choisir un MSP qui dispose d'outils et de politiques pour assurer la continuité des activités et la reprise après incident.

Neutralité vis-à-vis de la technologie et des fournisseurs

En raison de leur vaste expérience, les bons MSP ont des opinions avisées sur le choix d'une technologie ou d'un fournisseur par rapport à un autre. Cela est parfaitement normal et, en fait, tirer parti de ces connaissances est l'un des avantages de travailler avec un MSP. Cependant, un MSP ne doit pas insister agressivement sur une technologie ou un fournisseur spécifique. Il doit plutôt s'adapter et répondre aux préférences et à l'infrastructure actuelle de la PME, et maintenir de bonnes relations professionnelles avec plusieurs fournisseurs, car une fois embauché, il sera chargé d'interagir avec eux et de leur demander des comptes.



Communication

La plupart des MSP peuvent avoir des discussions d'expert à expert avec les membres d'une équipe informatique interne. Toutefois, lorsqu'il s'agit de parler avec des non-techniciens, ils sont tenus d'adapter leur vocabulaire et leur approche en conséquence, notamment lorsqu'il s'agit de former les utilisateurs à des sujets comme les politiques de gestion des mots de passe et des accès. Tout MSP qui ne peut pas communiquer efficacement avec des publics variés fera partie du problème, et non de la solution.

Cohérence

Dans le paysage informatique, il y a de bons et de mauvais jours. Il est évident que les PME ne peuvent pas attendre d'un MSP qu'il les protège à 100 % des cyberattaques ou des pannes matérielles, car cela n'est tout simplement pas réaliste. Mais les PME peuvent et doivent insister pour qu'un MSP soit cohérent dans son approche et ses normes professionnelles. Ils ne doivent jamais oublier qu'ils travaillent pour les PME, et non l'inverse!

14 RECOMMANDATION

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

Souvent, les responsable de la sécurité de l'information (RSI) et autres professionnels de l'informatique qui tirent la sonnette d'alarme sur les vulnérabilités de leur PME en matière de cybersécurité sont confrontés à des questions difficiles telles que :

- Quel est notre retour sur investissement?
- Dépensons-nous de l'argent qui pourrait être réparti ailleurs?
- Sommes-nous en train de réagir de manière disproportionnée et de surestimer les risques?

Les conseils suivants peuvent améliorer considérablement les chances de convertir les sceptiques en défenseurs, et d'obtenir leur appui et un budget :

- Démontrez les risques et les répercussions d'une cyberattaque. Par exemple, un exercice réaliste reproduisant une attaque par rançongiciel peut ouvrir les yeux des décideurs.

- Utilisez un langage simple et évitez le jargon. Ce qui est connu des RSI et autres (par exemple, l'authentification multifacteur, la Confiance zéro, la gestion des accès privilégiés, etc.) peut ne pas être familier aux PDG, aux directeurs financiers et aux autres intervenants. Ceux-ci peuvent avoir une certaine connaissance et des informations, mais elles sont partielles ou dépassées.

• Lorsque cela est possible, quantifiez les risques à l'aide de chiffres (par exemple, « ce type de violation a coûté à une entreprise de taille similaire de notre marché 1,25 million de dollars pour l'enquête et le nettoyage ») plutôt que de dangers abstraits (par exemple, « ce type de violation implique des pirates informatiques dérobant des courriels »).

• Préparez une proposition de plan comportant une stratégie pour le budget de la cybersécurité et une liste détaillée des dépenses liées aux technologies, à des formations et au personnel à embaucher. Comme le recommande ZDNet.com : « Il ne sert à rien de demander un budget puis d'improviser : le conseil d'administration sera plus susceptible d'accorder le financement requis s'il existe un plan établi, une stratégie qu'il peut voir et soutenir. »

• Identifiez les fournisseurs qui proposent un essai gratuit sans risque, afin que les outils potentiels puissent être testés pour garantir la sécurité, la convivialité, l'évolutivité, la flexibilité, etc.

En définitive, le message clé à transmettre (cela peut nécessiter de nombreuses réunions et discussions) est que l'investissement en cybersécurité ne se réduit pas à la protection des données, mais qu'il apporte une valeur ajoutée à l'entreprise en :

• Augmentant la fidélité et la confiance du marché, ce qui se manifeste par des revenus plus élevés et un engagement accru des clients.

• Réduisant les coûts en tirant parti de l'automatisation pour remplacer les tâches manuelles fastidieuses et chronophages.

• Créant un meilleur environnement décisionnel, où les risques prioritaires en matière de cybersécurité sont pris en considération.

• Mettant en place des outils et des flux de travail fiables pour la continuité des affaires et la reprise après incident.

• Rendant les PME plus attirantes pour les partenaires stratégiques et les investisseurs.

15 RECOMMANDATION

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

Dans un passé pas si lointain, la majorité des pirates étaient des *script kiddies* qui avaient l'intention de détruire les appareils et de causer des ravages. Cette époque est révolue. Les cybercriminels sophistiqués d'aujourd'hui rêvent de gains énormes. Ils envahissent les PME par le biais de multiples vecteurs de menaces tels que les centres de données, la périphérie du réseau et les bureaux à distance : bref, tout endroit où les utilisateurs finaux accèdent à des applications, des données ou des services par l'intermédiaire du réseau de l'entreprise ou de l'internet public.

Afin d'aider les PME à survivre plutôt qu'à crouler sous un large éventail de cybermenaces sophistiquées (y compris celles qui déjouent les outils antivirus conventionnels), voici cinq solutions de base à mettre en œuvre maintenant plutôt que plus tard :

Gestion sécurisée des accès à distance

La pandémie a considérablement accéléré le passage au télétravail. Néanmoins, les avantages d'une main-d'œuvre dispersée comportent des risques de sécurité importants. Les PME doivent remédier à ces lacunes en gérant de manière sécurisée l'accès des employés et des sous-traitants. Des RPV, IPSec et SSL abordables et simples à déployer sont vivement recommandés pour cela. En outre, si les services infonuagiques sont excellents pour la mobilité et la disponibilité, il est important de bien comprendre le modèle de risque qui prédomine et les limites des responsabilités du fournisseur de services.

Coffre numérique sécurisé

Alors que de plus en plus de tâches sont effectuées en ligne, les entreprises doivent protéger les mots de passe des employés, la propriété intellectuelle et les dossiers privés. C'est un défi pour de nombreuses PME, car elles ont pour habitude de se concentrer uniquement sur le périmètre et n'ont que peu ou pas de visibilité sur les pratiques (souvent mauvaises) de gestion des mots de passe de leurs employés. Un coffre numérique sécurisé utilisant un chiffrement et une authentification robustes permet aux employés de stocker en toute sécurité les mots de passe et les identifier. Parallèlement, il permet aux PME de détecter les vulnérabilités et de renforcer l'hygiène de la sécurité à l'échelle individuelle, collective et de l'entreprise.

Gestion sécurisée des mots de passe

En raison principalement de leurs avantages en termes de coût, d'intégration, d'accessibilité et d'évolutivité, de nombreuses PME se tournent vers les solutions numériques, qu'il s'agisse d'applications logicielles ou d'entrées de bâtiments. Cependant, bon nombre de ces ressources ne disposent pas d'une structure de défense assez solide en matière de cybersécurité. La gestion des mots de passe, qui va de pair avec la gestion des accès, permet aux bons d'entrer et de fermer la porte au nez des méchants. Les principaux avantages sont les suivants : appliquer les privilèges appropriés, permettre une gestion automatisée des politiques lorsque les employés changent de rôle, et s'assurer que les employés sont contrôlés lorsqu'ils accèdent aux ressources numériques (par exemple, les applications) et aux lieux physiques (par exemple, les bâtiments). Il est également crucial de noter que les tableurs protégés par mot de passe et autres solutions de gestion des mots de passe axées sur un seul utilisateur sont totalement inadéquats. Non seulement elles sont fastidieuses à gérer, mais elles sont d'une insécurité alarmante.

Authentification multifacteur

Les rumeurs de la mort des mots de passe ont été largement exagérées. Ils sont toujours bien vivants, mais il est désormais communément admis qu'ils ne constituent qu'une partie du casse-tête de l'authentification, et non la totalité du tableau. Les PME doivent compléter les mots de passe forts par un second facteur : un élément que les employés ont (par exemple, un appareil), connaissent (par exemple, un code PIN) ou sont (par exemple, la biométrie).

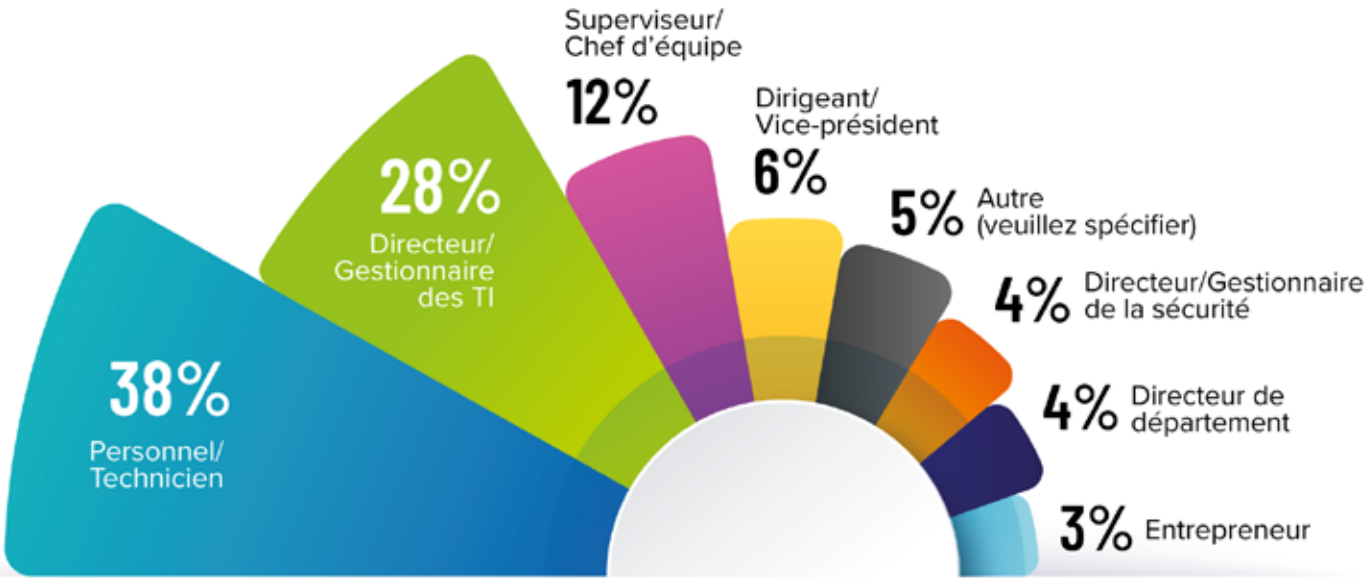
Automatisation

Pour éviter d'être victimes de pirates informatiques, les PME doivent automatiser, automatiser et encore automatiser! Cela est primordial compte tenu de la pénurie massive de professionnels qualifiés en matière de cybersécurité, notamment dans les PME, qui ne peuvent généralement pas rivaliser avec les grandes entreprises en termes de rémunération. Fort heureusement, de nouveaux outils d'automatisation facilitent la tâche des PME qui doivent gérer des problèmes de sécurité, sans avoir à embaucher une armada d'ingénieurs en sécurité ou à mettre en place un centre d'opérations de sécurité (SOC) à part entière. L'automatisation permet également d'atténuer les vulnérabilités de sécurité dues à l'erreur humaine, d'accélérer la réponse aux incidents et d'améliorer les performances générales des opérations de sécurité.

PARTIE 7

PROFIL DES RÉPONDANTS

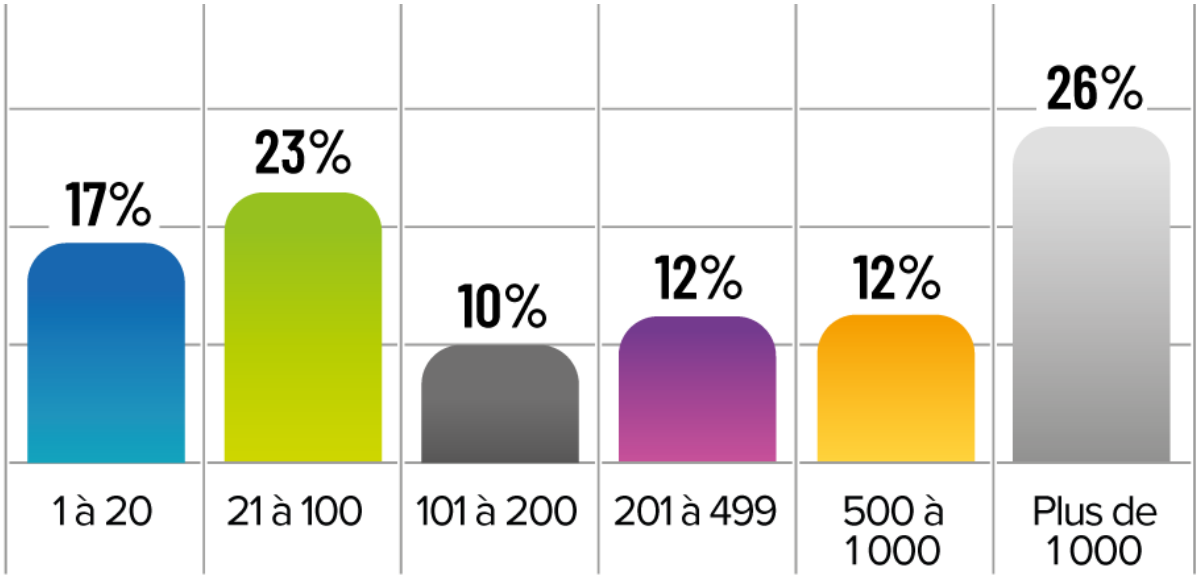
Quel nom de poste correspond le mieux à votre rôle dans votre entreprise?



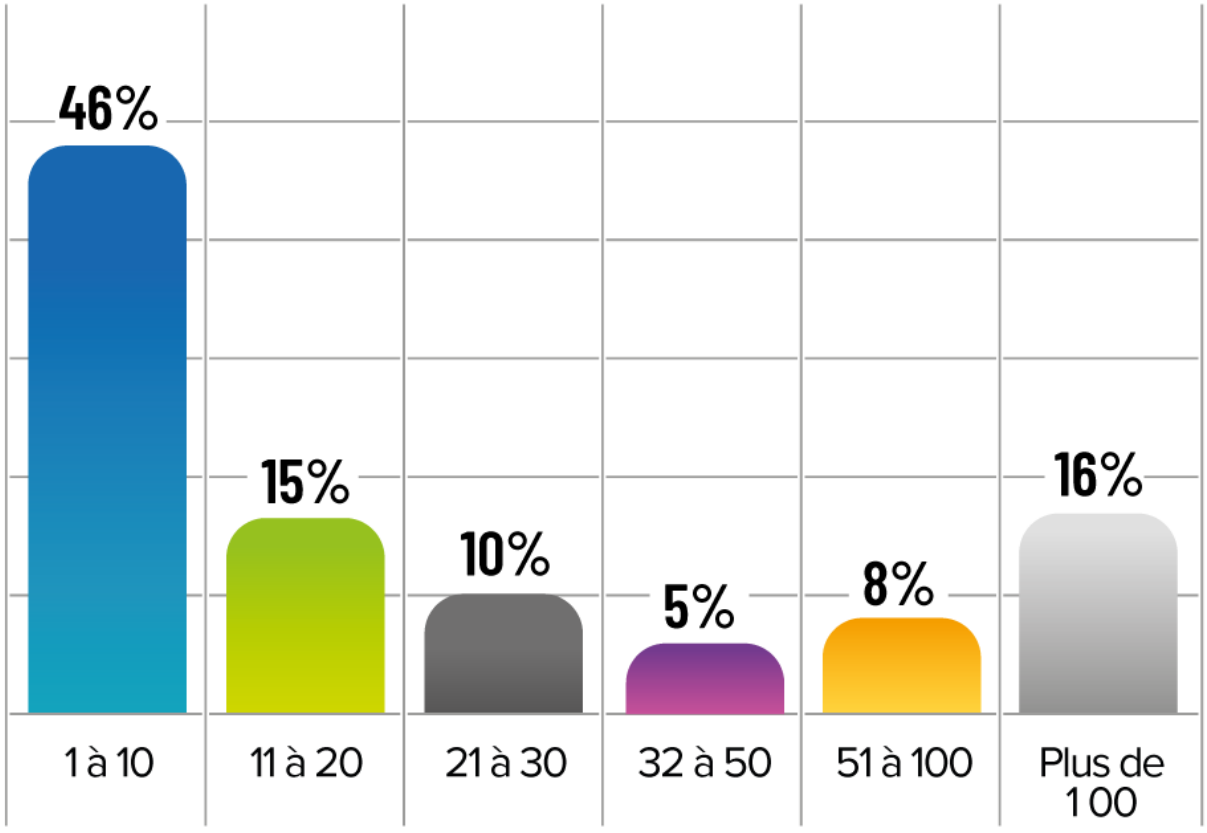
Qu'est-ce qui décrit le mieux le secteur d'activité de votre entreprise?

- 28% Services de TI
- 11% Finances et assurances
- 8% Éducation
- 8% Secteur manufacturier
- 7% Autre (veuillez spécifier)
- 6% Sécurité informatique et des réseaux
- 5% Gouvernement
- 5% Santé
- 3% Construction
- 3% Commerce de détail
- 3% Technologie
- 2% Services généraux aux entreprises
- 2% Service à la clientèle
- 2% Communications
- 2% Transport
- 1% Divertissement
- 1% Pétrole et autres énergies
- 1% Marketing et publicité
- 1% Administration publique
- 1% Infrastructures et technologies de défense et de sécurité
- 1% Services publics

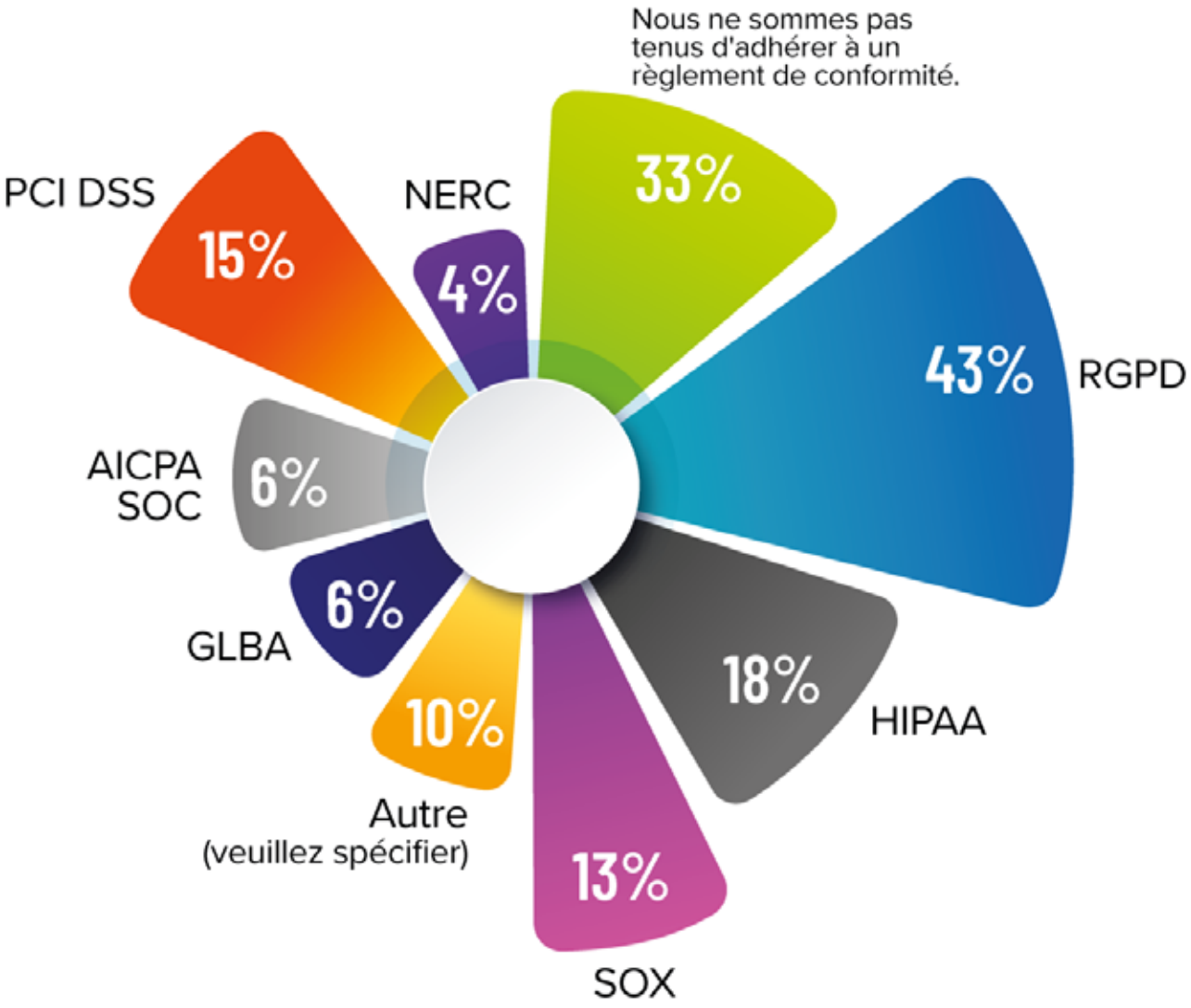
Combien de personnes travaillent pour votre entreprise à travers le monde?



Combien de personnes travaillent dans le département TI?



Veuillez sélectionner l'ensemble des règles de conformité auxquelles votre entreprise est tenue d'observer :



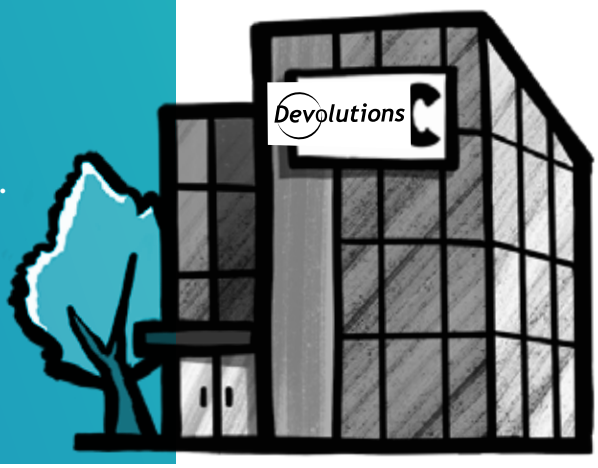
Devolutions

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, ainsi que les ralentir alors qu'elles doivent continuer d'évoluer dans l'ère post-pandémique.

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 créant des solutions de gestion universelle d'accès 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) 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.

Password Hub Personal

Password Hub Personal est un gestionnaire de mots de passe à la fois sécuritaire, convivial et gratuit, conçu pour les personnes qui souhaitent protéger leurs mots de passe personnels dans un coffre sécurisé. À partir de votre compte Devolutions, vous pouvez facilement créer votre propre Password Hub Personal et y accéder depuis votre appareil mobile.

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.

Devolutions

COMMENT JOINDRE DEVOLUTIONS

Basée à Lavaltrie, Québec, Canada, Devolutions offre des solutions alliant productivité et sécurité à plus de 800 000 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