Devolutions

PORTRAIT DE LA SÉCURITÉ INFORMATIQUE DANS LES PME 2022-2023

TABLE DES MATIÈRES

RÉSUMÉ

Les petites et moyennes entreprises (PME) de par le monde se remettent petit à petit et doivent trouver leur voie dans la « nouvelle réalité » de l'après-pandémie. Malgré les nombreux changements qui sont survenus dans les dernières années, la sécurité informatique n'a pas perdu en importance. Au contraire, le travail à distance et les solutions infonuagiques exercent une pression croissante sur les systèmes de sécurité informatique des PME.

Aujourd'hui, les pirates se servent de méthodes très sophistiquées pour infiltrer les réseaux et les comptes, ce qui leur permet de voler des données et d'usurper des identités. Dans bien des cas, ils accomplissent leurs méfaits avec une facilité désarmante et évitent de se faire détecter pendant des semaines, des mois, voire même des années. En outre, les PME doivent se protéger contre des utilisateurs « malveillants » à l'interne, en plus de ceux qui, par ignorance ou négligence, rendent possible une violation de données.

En conclusion? La surface d'attaque est plus grande que jamais, la fréquence et la diversité des menaces sont sans précédent, et les PME doivent être proactives en matière de sécurité informatique.

Le coût moyen d'une violation de données pour l'ensemble des organisations a grimpé à une moyenne de 4,24 millions USD, ce qui représente le montant le plus élevé jamais observé. [source]

Si l'on se concentre uniquement sur l'impact dans les PME, le coût peut aller de 120 000 USD à 1,24 million USD par incident. [source]

Afin d'aider les PME à mieux comprendre l'envergure du monde de la sécurité informatique postpandémie ainsi que les dynamiques qui le caractérisent, **Devolutions a interrogé, pour la troisième année consécutive, des dirigeants et décideurs de PME**[1] de par le monde à propos de cinq sujets cruciaux :

- **Les cybermenaces qui touchent les PME**
- **La gestion des accès privilégiés chez les PME**
- **La sensibilisation à la sécurité informatique chez les PME**
- **La gestion des accès à distance chez les PME**
- **La gestion de la sécurité informatique chez les PME**

Voici quelques révélations dignes de mention du sondage de Devolutions sur le Portrait de la sécurité informatique dans les PME de 2022-2023 :

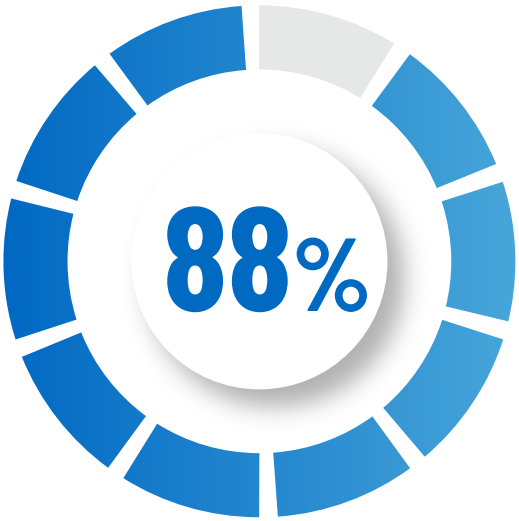
67%

des PME **se disent plus préoccupées par les cybermenaces** que l'année dernière.

[1] Les organisations qui ont participé au sondage sont celles qui s'identifient en tant que PME. Cette démarche prend en compte que la définition d'une PME varie en fonction du secteur d'activité et du domaine.

60%

des PME ont essuyé au moins une cyberattaque au courant de la dernière année et **18 % d'entre elles en ont subi six ou plus.**



des PME **ne disposent pas d'une solution PAM complètement déployée.**

des PME ont **embauché de nouveaux employés pour s'occuper de la sécurité informatique** depuis le début de la pandémie.

L’outil de gestion des accès à distance de **prédilection des PME est le réseau virtuel privé (VPN).**

Le travail à distance entraîne de nouveaux défis pour les PME en matière de sécurité informatique. C’est particulièrement le cas dans les quatre catégories suivantes : **la sécurité, l’efficacité, la gouvernance, et l’abordabilité.**

32 % des PME allouent moins de 5 % de leur budget en informatique à la sécurité, ce qui est bien en deça des recommandations minimales.

Ces statistiques ne constituent qu'une petite partie des révélations que contient ce rapport. Rapport qui, d'ailleurs, répond à des questions pressantes telles que :

- Quelles sont les cybermenaces qui inquiètent le plus les PME?
- Comment les PME arrivent-elles à se protéger contre les pirates et les menaces internes?
- Comment les PME gèrent-elles les comptes privilégiés?
- Comment les PME sensibilisent-elles les utilisateurs finaux à la sécurité informatique?
- Comment l'avènement du travail à distance influence-t-il le milieu changeant de la sécurité informatique?

RECOMMANDATIONS

Ce rapport contient également 10 recommandations à l'intention des PME pour réduire l'incidence des cybermenaces; augmenter la sensibilisation à la sécurité informatique; renforcer la gestion des accès à distance; et améliorer la gestion de la sécurité informatique.

1. Les PME doivent se protéger contre les plus grandes menaces, c'est-à-dire les rançongiciels, l'hameçonnage, les logiciels malveillants, les vulnérabilités infonuagiques et les attaques de la chaîne d'approvisionnement.

2. Les PME doivent implémenter un ensemble de principes de base en matière de sécurité informatique : le principe de moindre privilège, la Confiance zéro, la séparation des tâches, et le principe « des quatre yeux ».

3. Pour améliorer leur posture de sécurité informatique et ainsi réduire le risque d'une violation de données potentiellement catastrophique, les PME se doivent d'implémenter une solution de gestion des accès privilégiés qui sert de passerelle entre l'authentification et l'autorisation.

4. Les PME ont besoin d'un plan exhaustif pour faire en sorte que les objectifs et demandes en matière de cybersécurité soient communiqués à temps avec toutes les personnes concernées, en plus d'être continuellement surveillés et mis en application.

5. Les PME devraient offrir aux utilisateurs des formations en cybersécurité qui traitent des enjeux, des menaces et des risques fondamentaux.

6. Les PME qui ne disposent pas d'une structure de sécurité informatique, ne veulent pas embaucher du personnel et manquent d'expertise en ce qui a trait à la sécurité infonuagique devraient se tourner vers des fournisseurs de services gérés (MSP) pour combler ces lacunes.

7. Les PME se doivent d'implémenter une solution de passerelle juste-à-temps pour éliminer les vulnérabilités engendrées par les réseaux privés virtuels (VPN).

8. Les PME doivent prendre en compte les vulnérabilités rendues possibles par le travail à distance.

9. Les PME devraient exiger, lors du choix d'un outil de gestion des accès à distance, une amélioration marquée dans les quatre catégories suivantes : la sécurité, l'efficacité, la gouvernance et l'abordabilité.

10. Pour obtenir un budget plus élevé pour la sécurité informatique, les professionnels de l'informatique devraient mettre l'accent sur cinq éléments lors de leurs présentations, propositions ou argumentaires, à savoir : la confiance, la conformité, les assurances, les employés et l'éthique.

Les conseils et étapes contenus dans chaque recommandation ont fait leurs preuves, sont concrets et demeurent abordables pour les PME.

EXTRAIT DE LA SECTION RECOMMANDATIONS :

« Les PME doivent réaliser que leur niveau de sécurité informatique ne se mesure pas qu'en fonction de leur budget, mais aussi par la constance de leur approche. Autrement, les PME peuvent se convaincre qu'elles n'ont rien à craindre, un sentiment maintes fois exploité par les pirates et les utilisateurs finaux malveillants ».

À PROPOS DE CE RAPPORT

262 personnes ont répondu à 24 questions. Toutes les réponses, ainsi que les commentaires, les sources d'informations, sources d'informations complémentaires et recommandations ciblées sont présentées dans la suite de ce rapport.

PARTIE 1

MENACES DE CYBERSÉCURITÉ AU SEIN DES PME

Il n'est pas nécessaire d'être un génie ou un visionnaire pour réaliser l'importance de la sécurité informatique. Ce qui est réellement nouveau et frappant, c'est l'augmentation de la fréquence, de la sévérité, de la sophistication et de l'impact financier des menaces liées à la sécurité informatique (incluant les cybermenaces).

En effet, révolue est l'époque où les gouvernements et les grandes entreprises n'avaient pour seuls soucis que le vandalisme et le chaos provoqués par des pirates du dimanche. Les acteurs malveillants d'aujourd'hui sont plus méthodiques, plus influents, et semblent disposer de ressources infinies. Leur objectif reste cependant inchangé : s'enrichir davantage en usurpant l'identité de leurs victimes. Certains de ces acteurs deviennent ainsi extrêmement prospères.

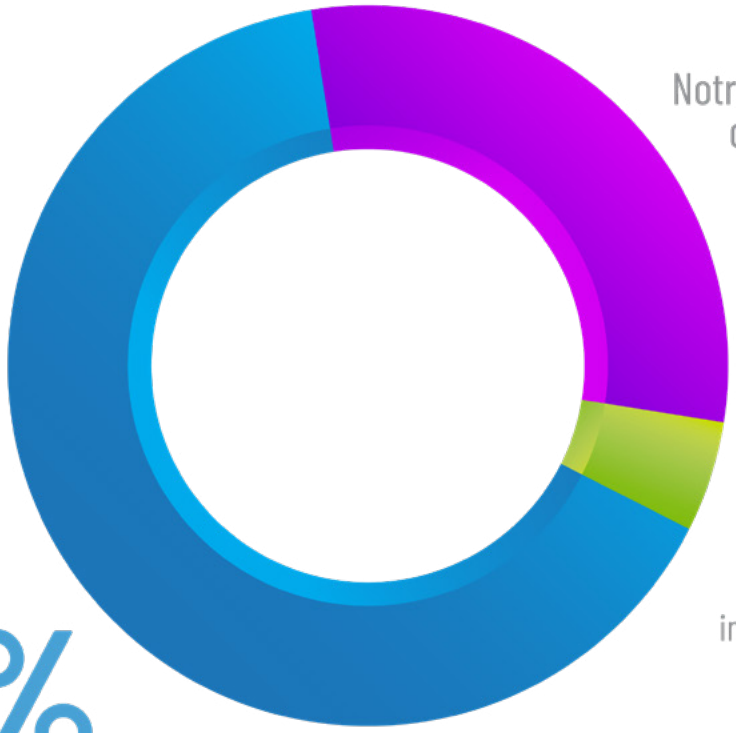
Qui plus est, leurs démarches ne visent plus seulement les grandes organisations. En effet, les cybercriminels s'en prennent de plus en plus aux PME en exploitant les failles de leurs systèmes de sécurité informatique (la menace est encore plus sévère pour celles qui pratiquent le travail à distance). Étant donné les conséquences potentiellement désastreuses d'une seule brèche dans leur sécurité, toutes les PME devraient réaliser que la sécurité informatique n'est pas qu'une simple question de technologie. Il s'agit d'une priorité entrepreneuriale.

QUESTIONS

Dans le cadre du sondage de Devolutions sur le Portrait de la sécurité informatique dans les PME de 2022-2023, nous avons demandé à des dirigeants et décideurs issus de PME à travers le monde de nous faire part de leurs points de vue concernant la sécurité informatique. Nos questions portaient sur leurs expériences au courant de la dernière année, ce qui les préoccupe le plus aujourd'hui, ainsi que les mesures de protection qu'ils ont adoptées.

QUESTION 1

Quel est votre niveau d'inquiétude en ce qui a trait aux dangers des cyberattaques contre votre organisation par rapport à l'an dernier ?



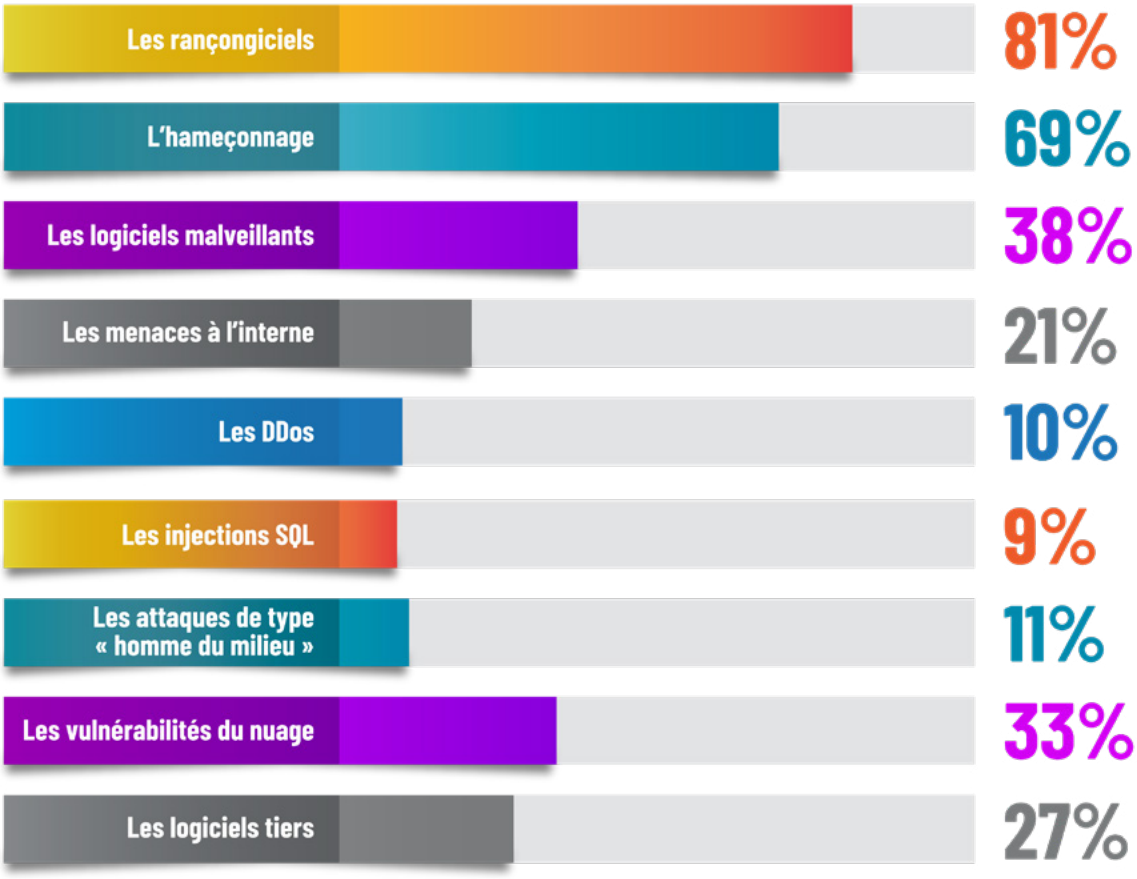
28%
Notre niveau d'inquiétude demeure le même

5%
Nous sommes moins inquiets que l'an dernier

67%
Nous sommes plus inquiets que l'an dernier

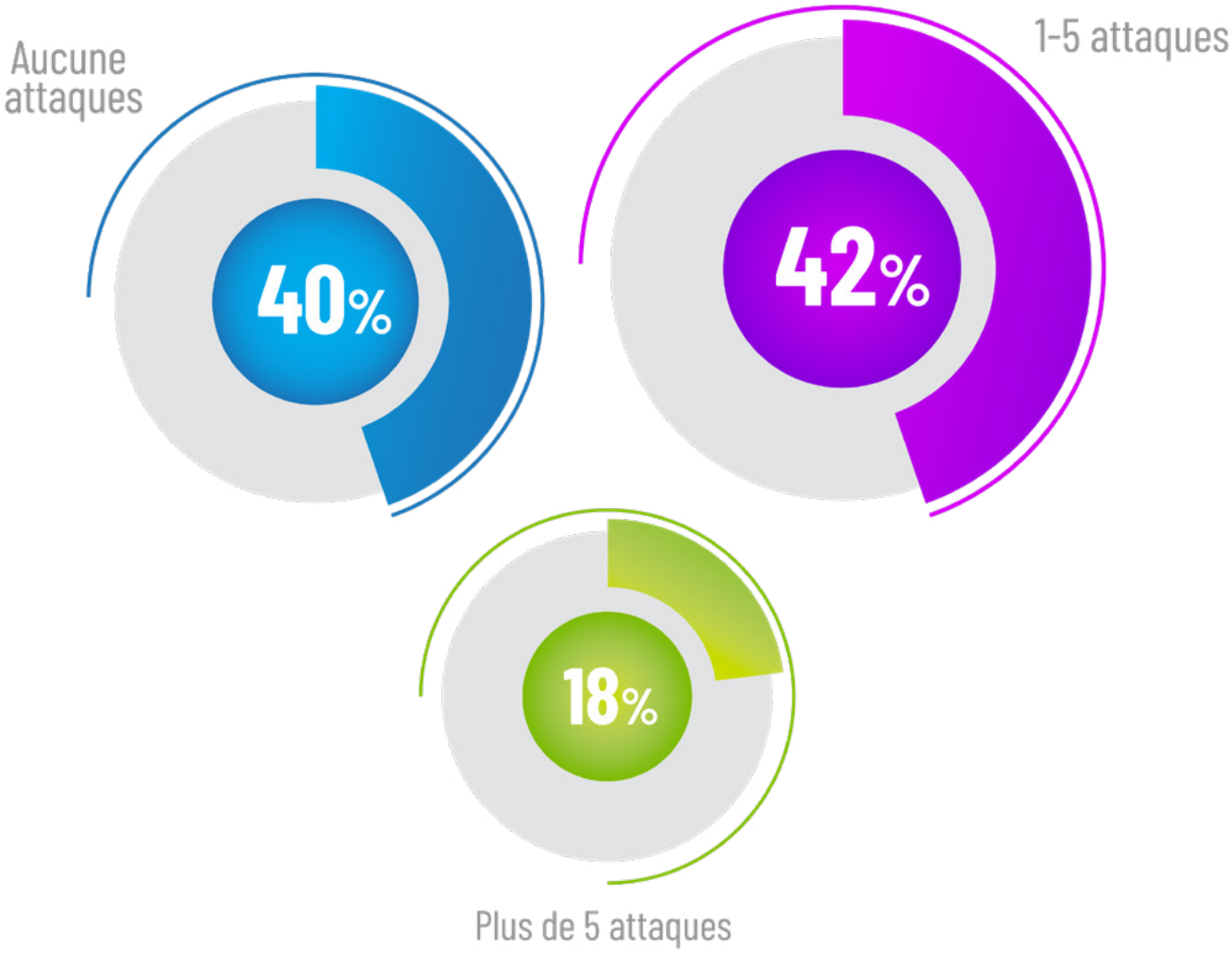
QUESTION 2

Veuillez indiquer les 3 types de cybermenaces qui vous préoccupent le plus.



QUESTION 3

L'année dernière, combien de cyberattaques votre organisation a-t-elle essuyées ?

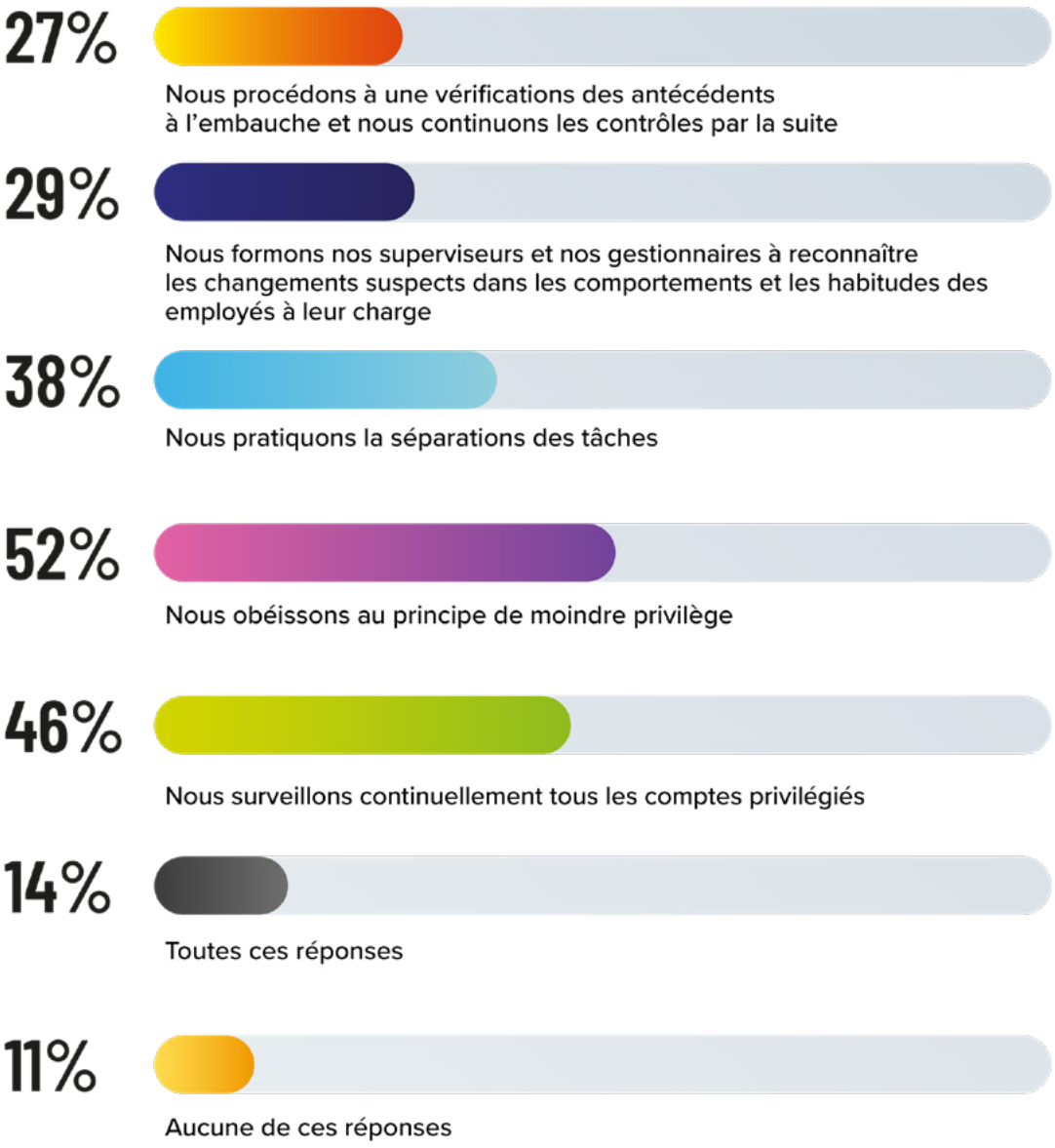


QUESTION 4

Quelles mesures avez-vous mises en place afin d'empêcher les pirates d'effectuer des cyberattaques ou des violations de données ?
Veuillez sélectionner tous les choix qui s'appliquent.

QUESTION 5

Quelles mesures pratiquez-vous afin de combattre les menaces internes ?



COMMENTAIRES

Les deux tiers (67 %) des dirigeants de PME se disent maintenant plus préoccupés à propos de la sécurité informatique que l'année dernière. Cette proportion a chuté de 5 % depuis le sondage de 2021-2022. Toutefois, cette légère baisse d'anxiété s'explique probablement par le retour au travail de nombreux travailleurs à distance au cours de la dernière année. Les PME ont profité de l'occasion pour resserrer certains contrôles de sécurité et affiner quelques-unes de leurs méthodes de gouvernance.

Les rançongiciels (81 %), l'hameçonnage (69 %) et les logiciels malveillants (38 %) sont les cybermenaces qui inquiètent le plus les dirigeants de PME en ce moment. Évidemment, toutes ces préoccupations sont légitimes, surtout en ce qui a trait à l'hameçonnage qui devient de plus en plus répandu et profitable. Cependant, seulement 27 % des PME ont placé les logiciels tiers dans le top trois de leurs inquiétudes sur la cybersécurité, ce qui laisse à penser que ces derniers ne sont pas considérés comme des menaces de premier ordre pour le moment. Selon Gartner, 45 % des organisations à travers le monde subiront des cyberattaques visant leur chaîne d'approvisionnement de logiciel d'ici 2025. Gardons également à l'esprit que, malgré que l'incident se soit produit en 2020, nous vivons toujours dans l'ombre de l'attaque sur la chaîne d'approvisionnement de SolarWinds/Solorigate (à ce jour considérée comme le sabotage informatique le plus sophistiqué jamais perpétré). Encore aujourd'hui, cet événement encourage les pirates à développer de nouveaux outils pour exploiter ce genre de failles.

Le sondage a également révélé que 60 % des PME ont essuyé au moins une cyberattaque au courant de la dernière année et que 18 % d'entre elles en ont subi six ou plus. Ces statistiques, qui d'ailleurs n'incluent pas les cyberattaques non signalées (voire non détectées), nous confirment que les PME ne peuvent plus se permettre de prendre la cybersécurité et la sécurité informatique à la légère. Les coûts moyens qu'entraîne une violation de données ont atteint 4,24 M$ US, le montant le plus élevé jamais enregistré. Si l'on se concentre uniquement sur les PME, l'impact financier varie de 120 000 $ US à 1,24 M$ US par incident (en fonction de nombreux facteurs tels que le nombre de registres compromis).

Maintenant que les dégâts que peut causer une violation de données sont bien connus, il serait logique que les PME adoptent les mesures de base de la sécurité informatique telles que : la séparation des tâches; le principe de moindre privilège; des audits réguliers des comptes privilégiés; le principe des « quatre yeux » (*four-eyes principle*); ainsi que la défense en profondeur. Détrompez-vous : il n'en est rien. Notre sondage a révélé que seulement 18 % des PME appliquent toutes ces recommandations. Pire encore, 13 % des PME affirment ne pas pratiquer aucune de ces mesures essentielles !

Dans la section Recommandations de ce rapport, nous nous penchons sur les méthodes qui aident les PME à se protéger dans un environnement de plus en plus menaçant à l'interne comme à l'externe.

PARTIE 2

GESTION DES ACCÈS PRIVILÉGIÉS DANS LES PME

Un accès privilégié est octroyé à une entité, humaine ou non (machine/application), qui fait usage d'un compte administratif ou d'un identifiant pourvu de droits élevés, afin d'effectuer des tâches de maintenance, de modification ou n'importe quel autre type d'opérations privilégiées.

Les comptes privilégiés fonctionnent en quelque sorte comme des « passe-partout informatiques », puisqu'ils permettent l'accès à des informations confidentielles hautement convoitées par les pirates et les utilisateurs malveillants.

Qui plus est, les comptes et identifiants privilégiés foisonnent au sein des petites et moyennes entreprises. 17 % des entreprises accordent l'accès à leurs dossiers sensibles à tous leurs employés, et 60 % d'entre elles disposent de plus de 500 comptes qui utilisent des mots de passe sans date d'expiration.

Les PME qui misent sur la gestion des accès privilégiés (PAM) dans le cadre de leur programme de sécurité informatique bénéficient de nombreux avantages tels que :

- La réduction des risques de sécurité;
- Réduire la taille globale de la surface d'attaque;
- La diminution du coût et de la complexité des opérations;
- L'amélioration de la visibilité et des capacités préventives;
- Plus grand respect des normes.

D'ailleurs, de plus en plus de sociétés d'assurance qui offrent des polices de cybersécurité insistent pour que leurs clients se munissent d'une solution PAM avant de leur proposer la moindre protection.

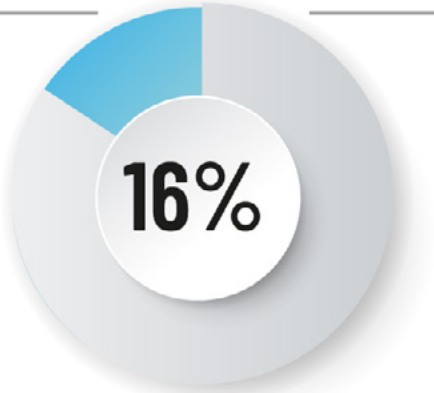
QUESTIONS

Dans le cadre du sondage de Devolutions sur le *Portrait de la sécurité informatique dans les PME de 2022-2023*, nous avons demandé à des dirigeants et décideurs issus de PME à travers le monde de nous faire part de leurs approches, méthodes et expériences concernant la gestion des accès privilégiés au sein de leur entreprise.

QUESTION 6

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

Nous avons recours à un service de répertoire (ex. : Azure ou Active Directory)



Nous possédons un gestionnaire de mot de passe

12%

Nous disposons d'une solution de gestion des accès privilégiés complètement déployée

9%

Nous disposons d'une solution de gestion des accès privilégiés, mais elle n'est que partiellement déployée (c.-à-d. nous n'utilisons que quelques fonctionnalités pour le moment)

3%

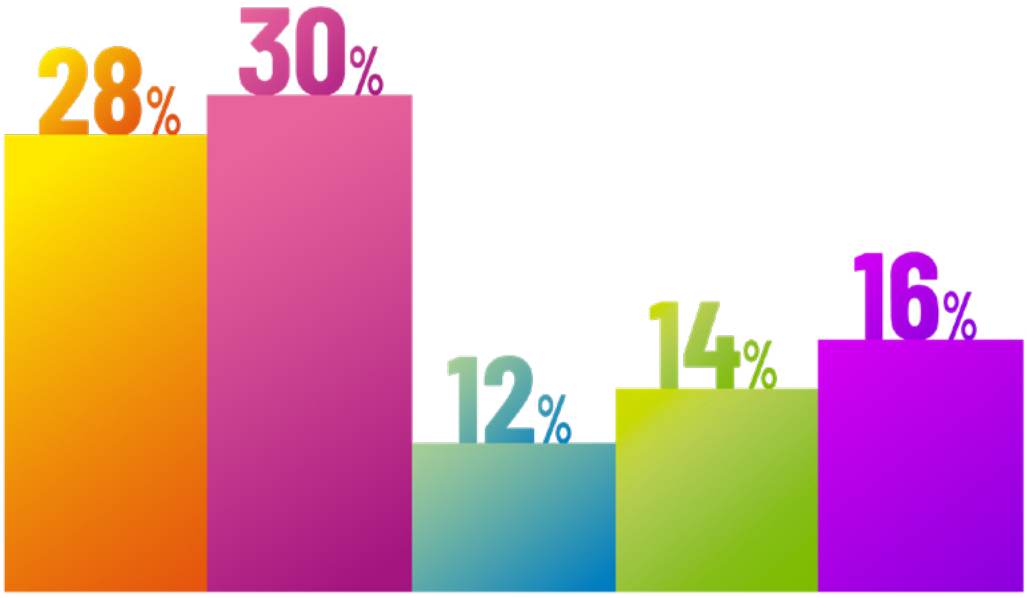
Nous utilisons des outils de sécurité des terminaux

2%

Nous ne gérons pas les accès aux comptes privilégiés

QUESTION 7

Si votre organisation ne dispose pas d'une solution de gestion des accès privilégiés complètement déployée, quelle en est la principale raison ?



- Notre budget ne le permet pas
- Nos outils de gestion des accès et des mots de passe actuels nous suffisent
- Nous considérons qu'une solution de gestion des accès privilégiés est trop complexe pour être implémentée et gérée efficacement
- Pour le moment, aucune des solutions de gestion des accès privilégiés que nous avons essayées ne répond à nos attentes
- Autres
  - Nous sommes présentement en processus de migration vers une nouvelle solution PAM.
  - Bien que l'implémentation d'une solution PAM fasse partie de nos objectifs, nous avons des priorités plus pressantes pour l'instant.
  - La direction de notre entreprise manifeste certaines réticences à l'endroit des solutions PAM.
  - Notre entreprise n'est pas prête à implémenter une solution PAM.
  - Nous utilisons les solutions PAM de nos clients pour gérer les comptes privilégiés.

QUESTION 8

Les mesures de gestion des accès privilégiés affectent-elles l'efficacité et la productivité du travail au sein de votre entreprise ?

11% Oui et l'impact est négatif, l'accès à certaines ressources est plus lent et ardu

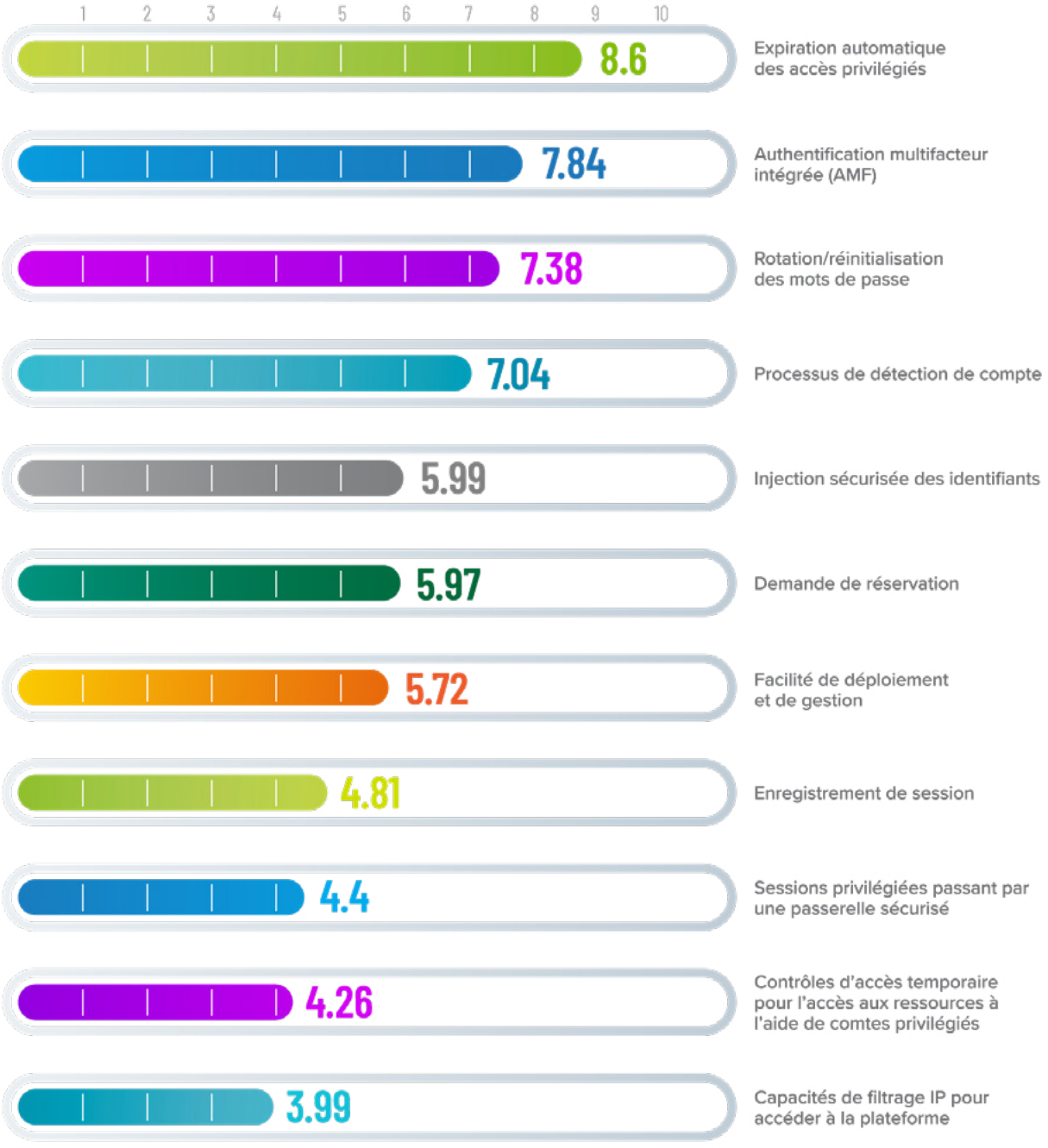
15% Oui et l'impact est positif, notre mécanisme d'approbation des informations et notre productivité s'en voient améliorés

22% Non, nous ne ressentons pas le moindre impact sur notre productivité

52% Nous n'avons pas encore implémenté les mesures de gestion des accès privilégiés

QUESTION 9

Veuillez classer les fonctionnalités de gestion d'accès privilégiés suivantes de la moins importante (11) à la plus importante (1) en fonction de la stratégie de sécurité informatique de votre entreprise.



COMMENTAIRES

En ce qui a trait aux PME et aux solutions PAM, il y a de bonnes et de mauvaises nouvelles. Côté bonnes nouvelles, seulement 2 % des PME n'utilisent pas de solution de gestion des accès privilégiés. Il s'agit d'une baisse de 5 % par rapport au sondage de 2021-2022, mais les réjouissances devront attendre.

Pourquoi me dites-vous? Eh bien parce qu'un maigre 12 % des PME disposent d'une solution de gestion des accès privilégiés complètement déployée. Bien qu'une baisse de 1 % par rapport à l'an dernier n'ait rien d'alarmant, il n'en demeure pas moins que ce pourcentage est 88 % en deçà de l'objectif à atteindre. Au même titre qu'une PME ne laisserait jamais ses portes déverrouillées en dehors des heures de bureau, il devrait lui être impensable de poursuivre ses activités sans recourir à une solution PAM robuste et englobante. En outre, les coûts engendrés par une violation de données peuvent largement dépasser ceux d'un cambriolage.

Il faut donc s'interroger quant aux raisons qui empêchent les PME de mettre en place des solutions PAM complètement déployées. Le sondage a révélé que 28 % d'entre elles se heurtent à des obstacles budgétaires, alors que 12 % estiment qu'une solution de gestion des accès privilégiés est trop complexe pour être implémentée et gérée efficacement. Certes, ces idées peuvent paraître logiques, mais elles sont en réalité bien dépassées. Il est vrai que pendant de nombreuses années, les prix des solutions de gestion d'accès privilégiés étaient déterminés en fonction des grandes organisations, les rendant ainsi inabordables pour les PME. De plus, les petites et moyennes entreprises ne pouvaient que rarement maintenir une équipe interne de spécialistes de la cybersécurité pour configurer, utiliser et adapter lesdites solutions aux besoins changeants du milieu. Heureusement, les choses se sont améliorées depuis!

Des solutions PAM abordables et faciles à utiliser existent désormais pour les PME qui éprouvent les mêmes besoins en matière de gestion des accès privilégiés que les grandes organisations. Nous appelons cette démocratisation du marché global de la gestion des accès privilégiés : PAM pour tous !

Certaines PME hésitent encore à déployer une solution PAM puisqu'elles craignent une baisse d'efficacité et de productivité. Toutefois, le sondage a également révélé que 15 % des PME considèrent que les mesures PAM améliorent leurs mécanismes d'approbation, augmentent leur productivité ainsi que la vitesse générale de leurs tâches. 22 % des PME ne remarquent aucune différence après le déploiement d'une solution PAM, alors que 11 % d'entre elles se disent gênées dans leurs activités. Il faut cependant garder à l'esprit que leurs solutions de gestion des accès privilégiés sont sans doute inutilement compliquées et mal adaptées aux besoins des PME.

Le sondage indique aussi que plus de la moitié des PME (52 %) n'ont pas encore implémenté de mesures de contrôle PAM. Les pirates et les utilisateurs malveillants sont les seuls gagnants de ce statu quo. Et puisque ces derniers ne font pas partie du marché visé par les PME, l'implémentation de mesures de contrôle devrait être LA priorité les PME.

Pour conclure, les trois fonctionnalités PAM qui intéressent le plus les PME sont : l'expiration automatique des accès privilégiés, l'authentification multifacteur (AMF) intégrée, ainsi que la rotation et la réinitialisation des mots de passe. Il est peu surprenant que toutes ces fonctionnalités relèvent de l'automatisation, puisque les PME sont toujours intéressées lorsqu'il est question d'améliorer leur efficacité et leur productivité de manière abordable.

Dans la section Recommandations de ce rapport, nous nous penchons sur les fonctions et les fonctionnalités PAM que recherchent les PME.

PARTIE 3

SENSIBILISATION À LA SÉCURITÉ INFORMATIQUE DANS LES PME

Il est de notoriété publique que, malgré les sempiternelles attaques des pirates et des acteurs malveillants à l'interne, ce sont les utilisateurs finaux et leur négligence qui constituent le maillon faible de la sécurité informatique.

Qu'ils cliquent sur des liens suspects ou partagent leurs mots de passe ou accèdent à des réseaux avec des connexions Wi-Fi non sécurisées (la liste complète est beaucoup trop longue pour être énumérée ici), les utilisateurs finaux peuvent entraîner des violations et des fuites de données très coûteuses.

Malheureusement, l'histoire ne s'arrête pas là : les utilisateurs finaux ne sont pas les seuls responsables des incidents informatiques évitables. Selon une étude, 60 % des organisations qui ont subi une violation de données considèrent que le problème émane d'une faille bien connue qu'elles n'avaient pas encore réparée. D'autres recherches ont révélé que les deux tiers des décideurs dans le domaine de l'informatique estiment que leurs équipes des opérations et de la sécurité informatique ne travaillent pas de concert pour protéger leur entreprise des menaces internes et externes.

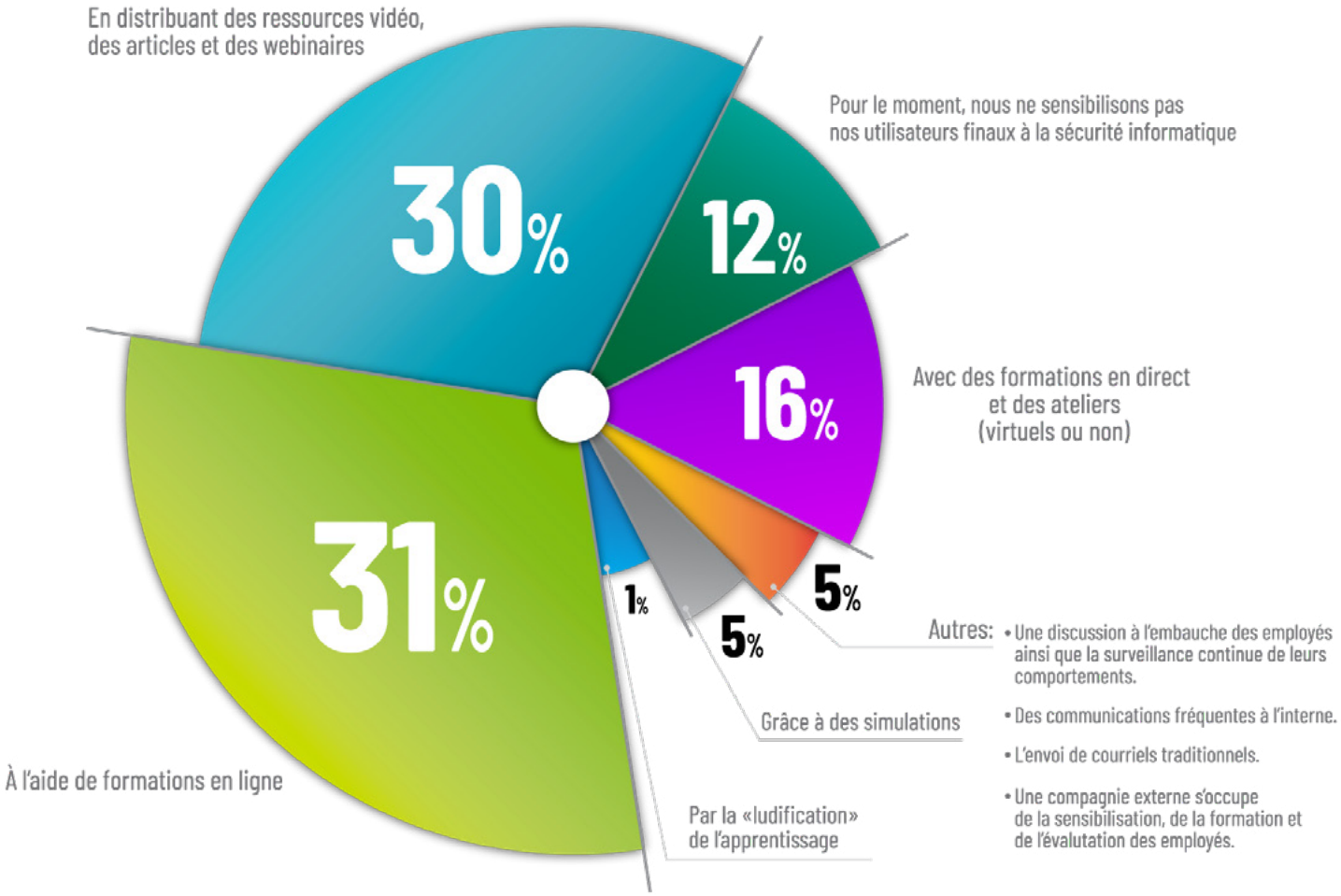
Il est vital de s'assurer que toutes les personnes au sein de l'organisation, des utilisateurs finaux aux dirigeants, en passant par les professionnels de l'informatique, participent à l'amélioration de la sécurité. Autrement, ils deviendront involontairement des facteurs de risque.

QUESTIONS

Dans le cadre du sondage de Devolutions sur le *Portrait de la sécurité informatique dans les PME de 2022-2023*, nous avons demandé à des dirigeants et décideurs issus de PME à travers le monde de nous faire part de la manière dont ils priorisent, implémentent et mesurent leurs efforts de sensibilisation à la sécurité informatique au sein de leur entreprise.

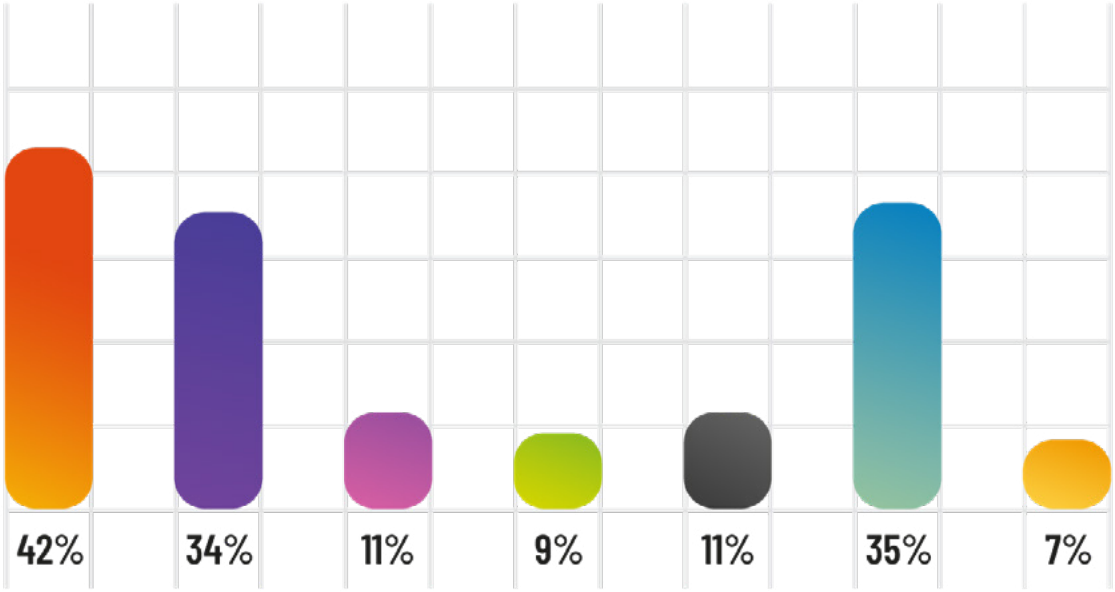
QUESTION 10

Comment votre entreprise sensibilise-t-elle les utilisateurs finaux à la sécurité informatique ?



QUESTION 11

Comment votre entreprise quantifie-t-elle les effets de cette sensibilisation ?



- Grâce à un suivi des résultats et des cotes de risque
- En procédant à des évalutions de la perception et des connaissances des utilisateurs finaux
- En se comparant avec nos pairs dans le domaine
- Le temps perdu à régler des problèmes de sécurité a diminué
- Les coûts associés aux incidents de sécurité ont diminué
- Nous ne mesurons pas les effets de cette sensibilisation pour le moment
- Aucune de ces réponses

QUESTION 12

Votre entreprise dispose-t-elle d'un plan d'intervention complet et moderne en cas de cyberincidents?

Oui
56%

Non
44%

QUESTION 13

Avez-vous augmenté vos effectifs de sécurité informatique depuis le début de la pandémie de 2020?

COMMENTAIRES

Commençons par le positif : 88 % des PME proposent de la formation sur la sécurité informatique à leurs utilisateurs finaux. Cette hausse de 14 % par rapport au sondage de l'année dernière laisse à penser que de plus en plus de dirigeants et de décideurs comprennent l'importance d'investir dans la sécurité informatique. Cette réalisation est fondamentale lorsque l'on soupèse les coûts et les conséquences gigantesques que peuvent entraîner des violations ou des fuites de données.

Il est pertinent de noter que la formation en ligne constitue désormais l'option de choix des PME (31 %) pour éduquer leurs employés à propos de la sécurité informatique. Cette tendance est probablement due à ces deux facteurs :

- Des formations pour les utilisateurs finaux, aussi formelles qu'improvisées, sont parfois nécessaires pour que les PME satisfassent certaines exigences externes telles que des contrats de clients, des polices d'assurance en cybersécurité ou encore des programmes de conformités (ex. : SOC 2, ISO/IEC 27001:2013, etc.);

- La formation en ligne porte sur l'utilisation de rapports et de tableaux de bord qui facilitent la surveillance des activités et du rendement des utilisateurs finaux. Au lieu de présumer ou d'espérer que les utilisateurs finaux progressent, les chefs d'équipes peuvent départager les gens qui s'améliorent de ceux qui ont besoin de plus de soutien (voire d'un avertissement).

Malheureusement, la situation n'est pas tout à fait positive : 35 % des PME omettent d'évaluer les résultats de leurs programmes de formation en sécurité informatique. Il est pourtant peu recommandé d'ignorer si les utilisateurs finaux sont formés et respectueux des normes. Durant un exercice de simulation d'hameçonnage dans le cadre d'une évaluation sur la sensibilisation à la sécurité informatique, 39 % des utilisateurs finaux, dont certains étaient détenteurs de comptes privilégiés, ont tout bonnement divulgué leurs mots de passe !

Le sondage a également révélé que 44 % des PME ne disposent pas d'un plan d'intervention complet et moderne en cas de cyberincidents. Cette augmentation de 4 % par rapport à l'an dernier est inquiétante alors que l'on constate que les répercussions et les risques liés à la sécurité informatique sont de plus en plus dramatiques. Mais qu'est-ce qui pourrait bien expliquer cette troublante observation ?

Il est fort probable qu'après les perturbations sans précédent de la pandémie, les PME n'aient pas encore eu l'occasion de combler leurs lacunes en matière de sécurité informatique. En revanche, les PME qui continuent de négliger cet aspect primordial de leur entreprise jouent avec le feu. Selon certaines estimations, les pirates informatiques lancent près de 2200 cyberattaques par jour (ou une chaque 39 secondes). Ces statistiques effraient puisque, bien souvent, un seule cyberattaque suffit pour que la victime réalise la valeur d'un plan d'intervention complet et moderne en cas de cyberincidents. C'est d'autant plus vrai pour les entreprises qui ne disposent pas d'un tel plan.

Et finalement, le sondage indique que 36 % des PME ont augmenté leurs effectifs de sécurité informatique depuis le début de la pandémie alors que 8 % travaillent maintenant avec un vendeur externe tel qu'un fournisseur de services gérés (MSP). Selon nous, le nombre de PME qui font affaire avec des fournisseurs de services gérés sera porté à augmenter pour les deux raisons suivantes :

- La pénurie généralisée des talents en sécurité informatique continue de s'aggraver. D'ailleurs, il est prédit que 3,5 millions d'emplois dans le domaine de la sécurité informatique seront vacants d'ici 2025, alors que ce nombre ne s'élevait qu'à un million en 2014. Bien que le travail à distance permette aux PME de trouver des professionnels aguerris en dehors de leur marché du travail local, le salaire de ces individus ne cesse d'augmenter. Évidemment, ces coûts varient en fonction de nombreux facteurs, mais il n'est pas rare pour les professionnels en sécurité informatique de gagner deux fois le salaire moyen de leurs collègues issus d'autres milieux. La vérité, c'est que pour beaucoup de PME, la seule solution abordable pour maintenir un profil de sécurité fort et respectueux des normes demeure de travailler avec un fournisseur de services gérés.

- Les fournisseurs de services gérés, qui jusqu'à présent offraient leurs services principalement aux entreprises de taille moyenne, réalisent maintenant que le marché des PME est inexploité et potentiellement très lucratif. Il existe approximativement 400 millions de PME disséminées à travers le monde. Nul besoin de spécifier que la plupart d'entre elles ne disposent pas d'une sécurité informatique adéquate.

Dans la section Recommandations de ce rapport, nous vous ferons part des quelques pratiques permettant aux PME de préparer, diffuser, et mettre à jour un plan d'intervention complet et moderne en cas de cyberincidents. Nous nous penchons également sur les principaux sujets qui devraient figurer dans une formation de sensibilisation à la sécurité informatique, en plus de donner quelques conseils aux PME en matière de fournisseurs de services gérés.

PARTIE 4

GESTION DE L'ACCÈS À DISTANCE DANS LES PME

Pour se connecter à des systèmes distants et effectuer diverses tâches de gestion, les professionnels de l'informatique ont souvent recours à des identifiants d'administration. Cette façon de faire est certes efficace et pratique, mais elle comporte des risques pour la sécurité. En effet, l'abus ou la compromission d'un compte privilégié peut entraîner une violation de données très coûteuse.

Les pirates disposent de nombreuses méthodes pour s'emparer des identifiants de comptes privilégiés. Les deux tactiques les plus répandues consistent à fureter sur des connexions à distance mal protégées et à déployer des maliciels sur des appareils d'utilisateurs finaux. Et puisqu'il est question d'utilisateurs finaux, il faut savoir que nombre d'entre eux, incluant des cadres supérieurs et des professionnels de l'informatique, se servent du même mot de passe pour plusieurs comptes. Ce phénomène constitue une réelle aubaine pour les pirates, mais un vrai désastre pour leurs victimes.

D'ailleurs, toute discussion de la gestion des accès à distance se doit d'aborder l'événement mondial le plus important depuis des générations : la pandémie de COVID-19. Depuis quelques années, le nombre de PME qui utilisent des outils de connexion à distance pour accommoder leurs employés et clients augmente exponentiellement. Ce faisant, la superficie de la surface d'attaque a augmenté également, en plus d'offrir aux pirates de nouveaux vecteurs de menaces à exploiter.

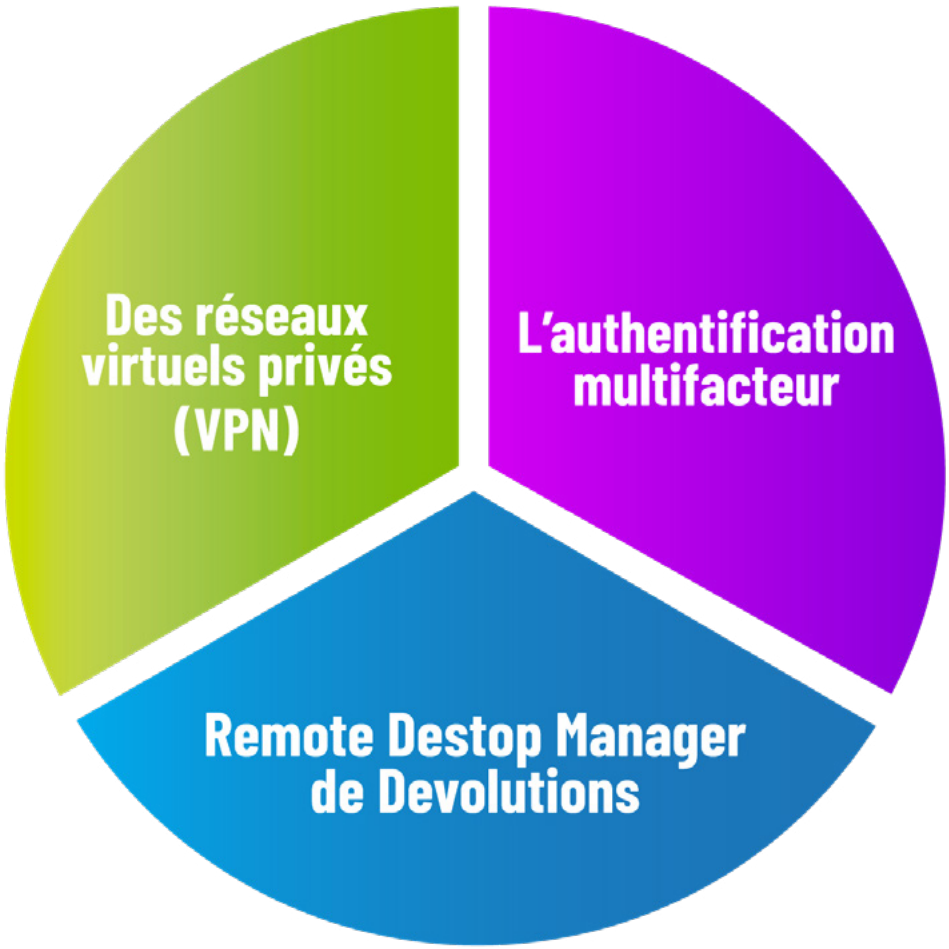
QUESTIONS

Dans le cadre du sondage de Devolutions sur le *Portrait de la sécurité informatique dans les PME de 2022-2023*, nous avons demandé à des dirigeants et décideurs issus de PME à travers le monde de nous exposer leurs méthodes de gestion des accès à distance et de nous faire part de quelques-unes des inquiétudes et des épreuves auxquelles ils font face.

QUESTION 14

Quels outils et technologies de sécurité informatique votre entreprise utilise-t-elle pour gérer ses connexions à distance en ce moment?

Les trois réponses les plus populaires sont de loin :



QUESTION 15

Quelle est la situation dans votre entreprise en ce qui concerne le travail à distance ?

75%

Nous permettons à quelques-uns/tous nos employés de choisir leur mode de travail (à distance ou au bureau)

19%

Tous nos employés travaillent au bureau à temps plein

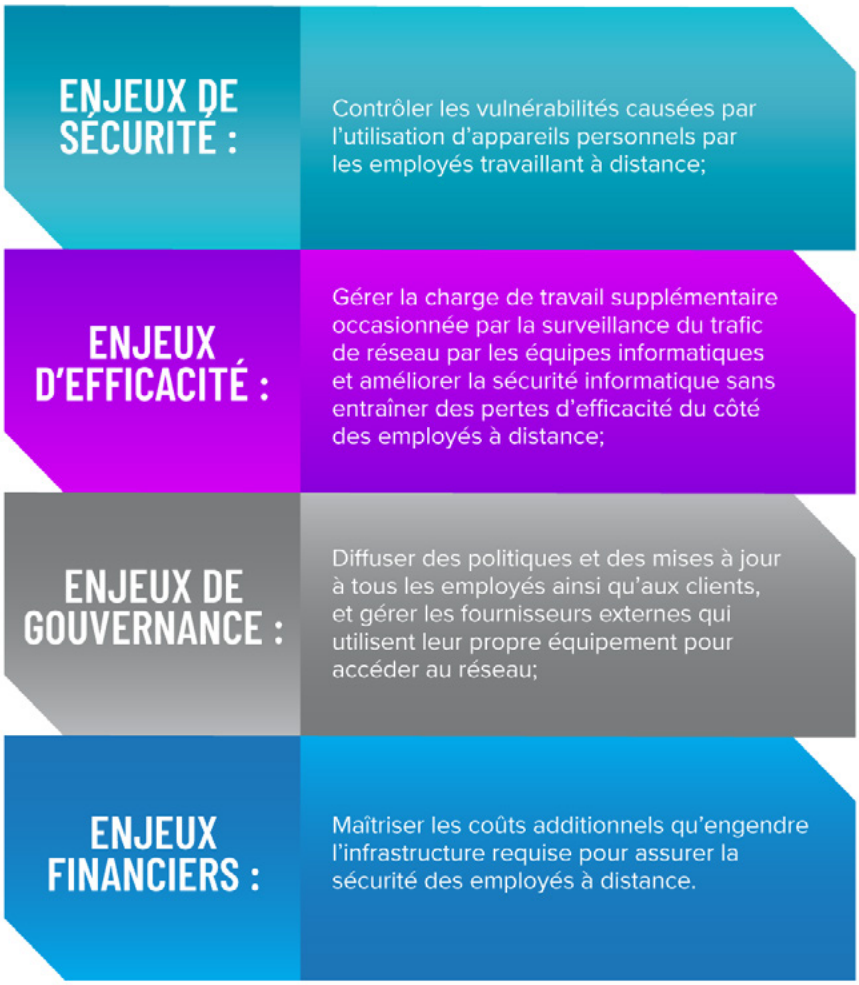
6%

Nos employés travaillent tous à distance

QUESTION 16

Le travail à distance connaît une hausse fulgurante depuis quelques années. Veuillez nous faire part des enjeux pour la sécurité informatique qu'entraîne le travail à distance au sein de votre organisation ainsi que les solutions trouvées.

Nous avons reçu beaucoup de réponses et les avons regroupées en quatre catégories :



COMMENTAIRES

L'outil de gestion des accès à distance de prédilection des PME est le réseau virtuel privé (VPN). De fait, la pandémie a poussé l'adoption en masse de VPN à travers le monde, et ce, tout particulièrement dans les pays qui enregistrent un nombre élevé de cas de COVID-19. Cependant, si les VPN sont susceptibles de réduire les risques, ils peuvent également présenter des inconvénients pour les PME en matière de déploiement, de gestion et de sécurité. Nous explorons ces problèmes et proposons des solutions dans la section des recommandations de ce rapport.

Notre sondage a également révélé que la grande majorité des PME ont implémenté un processus d'authentification multifacteur comme mesure de sécurité supplémentaire. Les employés à distance doivent ainsi confirmer leur identité en saisissant leurs informations d'identification et en fournissant une preuve supplémentaire qui repose sur :

- Un renseignement écrit (la réponse à une question secrète, un NIP, un mot de passe);
- Une possession physique (un téléphone ou un jeton);
- Une caractéristique biométrique (empreinte digitale, reconnaissance vocale ou oculaire).

En principe, même après l'usurpation des identifiants d'un employé à distance, il est rare que les pirates soient en mesure de fournir les preuves d'identification mentionnées plus haut pour accéder frauduleusement à des appareils, des applications, des systèmes ou des réseaux.

En outre, beaucoup de PME utilisent Remote Desktop Manager de Devolutions[2] pour gérer leurs accès à distance. En centralisant les mots de passe et les données d'entreprise en un seul endroit sécurisé, les professionnels de l'informatique peuvent accéder rapidement à toutes les informations dont ils ont besoin, en tout temps, et en s'assurant de la sécurité des sessions à distance.

En ce qui a trait à la situation générale du travail à distance, 75 % des PME préconisent un mode de travail hybride pour une partie, voire l'entièreté de leurs employés, alors que 6 % d'entre elles fonctionnent désormais complètement à distance. Bien que le travail à distance comporte de nombreux avantages non négligeables, notamment une réduction des coûts pour les employeurs et un confort accru pour les employés, il s'accompagne aussi d'un agrandissement important de la surface d'attaque. Les PME doivent donc s'affairer à enrayer ces vulnérabilités pour maintenir la sécurité et le respect des normes dans le cadre du travail à distance.

Finalement, nous avons demandé à des dirigeants et décideurs de nous faire part des enjeux pour la sécurité informatique qu'occasionne le travail à distance au sein de leur entreprise. La majorité des réponses relevaient de quatre catégories : la sécurité, l'efficacité, la gouvernance, et l'abordabilité. Ce qu'il faut retenir, c'est que lors de l'évaluation (et du choix) des outils de gestion des accès à distance, les PME doivent s'assurer que ces quatre éléments soient pris en compte. En d'autres termes, chaque outil potentiel d'accès à distance se doit d'apporter des améliorations substantielles à la sécurité ainsi qu'à l'efficacité de l'entreprise, en plus d'en faciliter la gouvernance et d'être peu coûteux. Si l'un de ces aspects est négligé, alors la PME en question se verra confrontée à des lacunes, des problèmes et des obstacles.

Dans la section Recommandations de ce rapport, nous examinons les raisons pour lesquelles les PME devraient déployer une solution de passerelle juste-à-temps pour résoudre les problèmes et les difficultés dus aux VPN. Nous soulignons également les approches pratiques et efficaces pour remédier aux vulnérabilités de sécurité déclenchées par les travailleurs à distance, et nous fournissons une liste de vérification pour aider les PME à tirer quatre avantages essentiels de leurs outils d'accès à distance : amélioration de la sécurité, efficacité, gouvernance et abordabilité.

[2]Par souci de transparence et pour garantir l'intégrité du sondage, nous désirons préciser que nous n'avons PAS inclus Remote Desktop Manager comme une réponse possible à la question 14. Les participants étaient invités à donner la réponse qu'ils désiraient à la question ouverte. Bien que Remote Desktop Manager ait été parmi les réponses les plus populaires, nous n'avons pas influencé directement ou indirectement les participants.

PARTIE 5

GESTION DE LA SÉCURITÉ INFORMATIQUE DANS LES PME

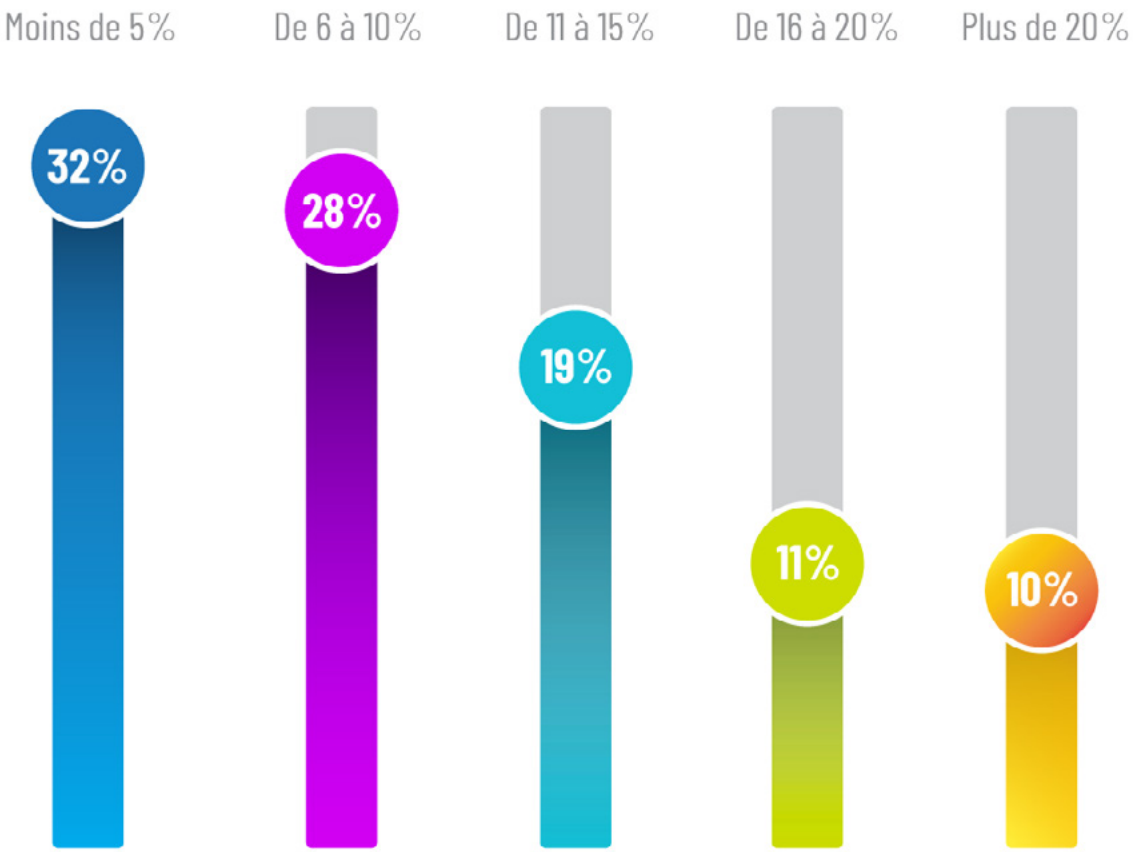
La gestion de la sécurité informatique comprend des stratégies, des politiques, des procédés, des technologies et des outils qui assurent la confidentialité, la protection, l'intégrité et la disponibilité des systèmes informatiques. Dans beaucoup de PME, la sécurité informatique et la cybersécurité sont gérées par une seule et même équipe. D'ailleurs, même lorsque ces tâches reviennent à des départements différents, il arrive bien souvent que les équipes de sécurité informatique et de cybersécurité travaillent de concert pour implémenter, gérer et améliorer des stratégies de sécurité robustes dans toute l'organisation. Notons qu'il s'agit d'un engagement à long terme et non d'un objectif ponctuel.

QUESTIONS

Dans le cadre du sondage de Devolutions sur le *Portrait de la sécurité informatique dans les PME de 2022- 2023*, nous avons demandé à des dirigeants et décideurs issus de PME à travers le monde de détailler leurs expériences et appréhensions en ce qui concerne la gestion de la sécurité des TI, en particulier en ce qui a trait aux dépenses et à la planification.

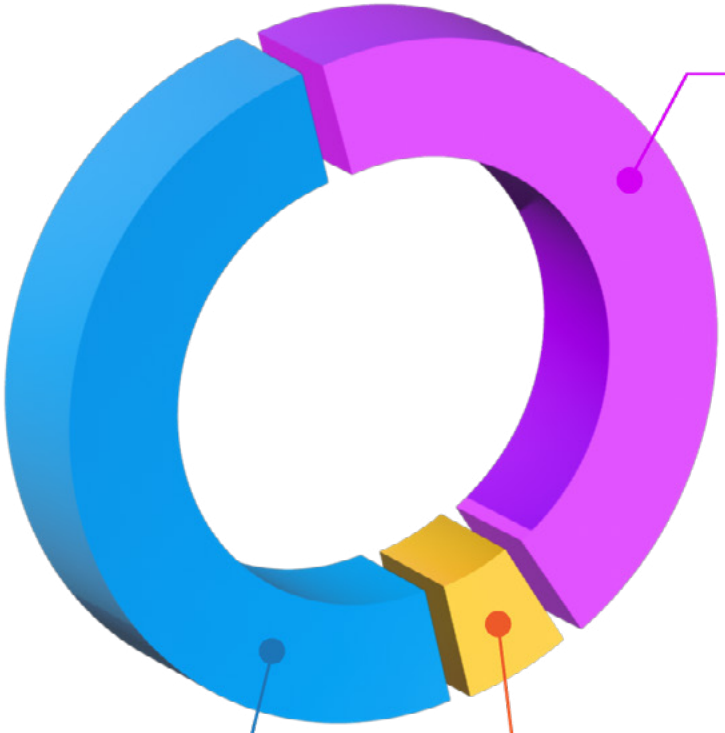
QUESTION 17

Quel pourcentage de votre budget informatique est alloué à la sécurité informatique (ex. : pour la technologie, la sensibilisation, la formation, etc.)?



QUESTION 18

Vos dépenses totales liées à la sécurité informatique ont-elles changé au cours de la dernière année ?



45%

Non, nos dépenses liées à la sécurité informatique sont approximativement les mêmes que l'an dernier

49%

Oui, nos dépenses liées à la sécurité informatique ont augmenté par rapport à l'an dernier

6%

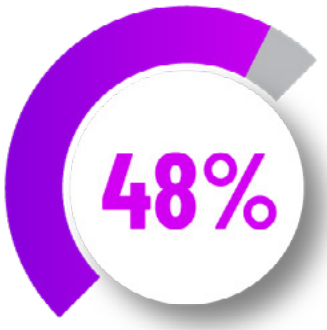
Oui, nos dépenses liées à la sécurité informatique ont diminué par rapport à l'an dernier

QUESTION 19

Vous attendez-vous à ce que vos dépenses liées à la sécurité informatique changent au cours des 12 prochains mois ?

Oui, nous prévoyons investir **plus** dans la sécurité informatique au cours des 12 prochains mois

Oui, nous prévoyons investir **moins** dans la sécurité informatique au au cours des 12 prochains mois



Non, nous prévoyons investir **approximativement le même** montant dans la sécurité informatique au cours des 12 prochains mois

QUESTION 20

Quels projets en lien avec la sécurité informatique prévoyez-vous essayer, voire implémenter, au cours des 12 prochains mois ?

Les 18 projets informatiques qui ont suscité le plus d'entrain sont les suivants (classés par ordre de popularité) :

- L'implémentation d'une solution de gestion des accès privilégiés;
- L'introduction ou l'intégration complète de mesures d'authentification à deux facteurs;
- La provision (directement ou avec l'aide d'un tiers) de formations pour les utilisateurs finaux;
- La refonte des stratégies relatives aux VPN;
- L'implémentation d'un mécanisme de rotation automatique des mots de passe;
- L'extension des outils de gestion des mots de passe à tous les employés (et non seulement au personnel informatique);
- L'amélioration de la sécurité des courriels;
- Le renforcement d'Active Directory;
- L'ajout d'une assurance en cybersécurité;
- L'implémentation d'un accès aux ressources plus granulaire et juste-à-temps;
- Le transfert des sauvegardes de données vers le nuage;
- La mise en place de tests d'intrusion et de méthodes de « l'équipe rouge »;
- La conduite d'évaluations de vulnérabilité objectives et exhaustives de la part des vendeurs;
- L'implémentation d'une solution SIEM;
- L'adoption d'une solution SOC;
- La mise en place d'un processus d'authentification sans mots de passe;
- L'ajout de membres expérimentés et accrédités à l'équipe de sécurité;
- La ségrégation de l'infrastructure réseau.

COMMENTAIRES

Lorsqu'il est question de la sécurité informatique, quelle est la somme optimale à débourser? Il n'existe malheureusement aucun montant qui fasse consensus. Chaque PME a sa propre dynamique et compose avec une pléthore de risques et d'épreuves en lien avec :

- **La taille, la profondeur ainsi que les caractéristiques de leur surface d'attaque;**
- **Le type de données qu'elles stockent, partagent et transmettent;**
- **Les menaces auxquelles elles seront confrontées aujourd'hui et à l'avenir;**
- **Les normes de conformités et les règlements qu'elles doivent respecter;**
- **La disponibilité et le salaire des spécialistes de la sécurité informatique.**

Si l'on prend en compte tous ces facteurs, il devient normal que le montant accordé à la sécurité informatique varie grandement d'une PME à l'autre. Encore une fois, il n'existe pas de prix prédéterminé. Le montant optimal pour une PME peut donc être considéré comme un dépassement ou une sous-utilisation du budget d'une autre.

Ceci étant dit, de nombreux experts (dont ceux de Devolutions) conseillent aux PME d'allouer entre 6 et 15 % du budget informatique de leur organisation à la sécurité informatique (ce qui comprend la cybersécurité).

En nous basant sur ces réflexions, la question se pose d'elle-même : les PME déboursent-elles en deçà, au-dessus, ou proportionnellement au budget recommandé? Concentrons-nous d'abord sur les scénarios où les PME investissent proportionnellement et au-dessus du budget recommandé, avant d'aborder les cas où elles dépensent en deçà du budget conseillé.

Le sondage a révélé que pour 68 % des PME attribuent 6 à 15 % de leur budget informatique à la sécurité informatique, ce qui coïncide avec l'investissement recommandé. Il s'agit d'une augmentation marquée par rapport au sondage de l'an dernier, lequel indiquait que seulement 32 % des PME investissaient de 6 à 15 % de leur budget informatique dans la sécurité. Cette avancée non négligeable est probablement due à une combinaison des trois facteurs suivants :

- L'explosion du travail à distance durant la pandémie a mis la puce à l'oreille des PME par rapport aux risques grandissants, autant internes qu'externes, auxquels elles sont confrontées (idéalement de leur plein gré et non en réaction à une attaque);

- De plus en plus de compagnies d'assurance en cybersécurité insistent pour que leurs clients investissent dans la formation destinée aux utilisateurs finaux ainsi que dans l'implémentation de solutions PAM;

- De plus en plus de clients, surtout ceux qui pratiquent le commerce électronique interentreprises, exigent que les entreprises avec lesquelles ils traitent mettent en place des mesures de sécurité informatique solides. De plus, les PME qui participent à un processus de demande de soumissions se voient de plus en plus forcées de prouver qu'elles disposent de mesures de sécurité robustes. Autrement, elles n'obtiennent aucun contrat.

Le sondage a également révélé que 21 % des PME allouent plus de 16 % de leur budget informatique à la sécurité informatique. S'agit-il d'une autre évolution positive? Oui et non. Pour certaines PME, il se peut que le budget total alloué à la sécurité informatique soit insuffisant. Dans ce cas, ces dépenses peuvent sembler appropriées, mais elles sont en réalité bien insuffisantes (et parfois de beaucoup).

Il est également possible que certaines PME investissent un montant substantiel dans leur sécurité informatique, mais que le rendement ne soit pas optimal. Les PME qui croient se trouver dans cette situation, et même celles qui ne le pensent pas ,mais qui réalisent l'importance d'évaluer leur profil de sécurité ainsi que leur infrastructure, devraient faire affaire avec des entreprises de sécurité informatique réputées qui se spécialisent dans les services aux PME. Ces entreprises comprennent que les PME sont confrontées à des réalités et limitations qui diffèrent de celles des grandes organisations.

Qu'en est-il des PME dont l'investissement en sécurité informatique n'atteint pas la cible recommandée? Le sondage indique que 32 % des PME appartiennent à cette catégorie, ce qui constitue une augmentation de 6 % par rapport à l'an dernier. Mais qu'est-ce qui explique ce déclin d'année en année? Encore une fois, force est de constater que la réponse la plus probable demeure la pandémie.

Comme mentionné précédemment, la pandémie a poussé (et parfois forcé) de nombreuses PME à allouer une fraction plus grande de leur budget informatique à la sécurité informatique. La pandémie a cependant engendré des dommages financiers sans précédent. Par exemple, entre avril 2020 et avril 2021, environ 200 000 PME américaines ont dû fermer leurs portes définitivement en raison des mesures prises pour contrer la pandémie. Beaucoup de PME ayant survécu à ce carnage financier ont néanmoins été forcées de réduire leurs opérations, ce qui a parfois entraîné un blocage du recrutement, certains congédiements ainsi que l'annulation ou la remise à plus tard de plans d'investissement et d'agrandissement.

Compte tenu de ces risques et pressions, qui par ailleurs pèsent encore sur certaines PME, il est tout à fait naturel que la réduction des dépenses liées à la sécurité informatique puisse paraître logique en ce moment. Cependant, les PME doivent réaliser que les dommages financiers causés par une seule cyberattaque dépassent de loin les coûts d'investir activement dans les technologies, outils et formations de sécurité informatique. Effectivement, bien qu'il existe plusieurs manières pour les PME de limiter leurs dépenses, il est déconseillé de couper dans le budget alloué à la sécurité informatique. Et pour cause : les résultats pourraient être regrettables.

Le sondage a également révélé que presque la moitié (49 %) des PME dépensent plus en matière de sécurité informatique que l'année dernière. Ce phénomène s'explique sans doute par l'augmentation du coût de la main-d'œuvre. Nous avons établi dans la partie 3 de ce rapport que 36 % des PME ont embauché au moins un employé pour s'occuper de la sécurité informatique au cours de la dernière année.

De plus, 45 % des PME maintiennent que leur budget dédié à la sécurité informatique demeure inchangé cette année. Cette nouvelle n'a rien de particulièrement surprenant ou d'alarmant, mais elle peut inquiéter : en effet, la menace que posent les cyberattaques s'intensifie avec les années, et ce, tout particulièrement lorsqu'il est question des rançongiciels et des attaques visant les chaînes d'approvisionnement. Les PME doivent réaliser que leur niveau de sécurité informatique ne se mesure pas qu'en fonction de leur budget, mais aussi par la constance de leur approche. Autrement, les PME peuvent se convaincre qu'elles n'ont rien à craindre, un sentiment maintes fois exploité par les pirates et les utilisateurs finaux malveillants.

Le sondage indique aussi que 6 % des PME investissent moins dans la sécurité informatique en 2022 qu'en 2021. Cette fois encore, nous pouvons constater que cette réduction ne résulte pas d'une décision qui vise délibérément à couper dans les dépenses de sécurité informatique, mais plutôt de la nécessité de réduire les dépenses totales de l'entreprise. Comme mentionné plus haut, cette approche est logique, mais malavisée. Et curieusement, il se peut qu'elle ne soit même pas nécessaire. Comme nous l'avons vu précédemment, les PME qui traitent avec des entreprises de sécurité informatique spécialisées dans les services aux PME reçoivent généralement des conseils et des solutions qui renforcent leur profil de sécurité informatique, tout en réduisant leurs dépenses totales. En d'autres termes, elles obtiennent plus pour moins cher, chose que les PME affectionnent tout particulièrement.

Mais que recèle l'avenir pour les PME en ce qui a trait aux dépenses en sécurité informatique? Le sondage a révélé que 46 % des PME projettent de dépenser davantage dans la sécurité informatique au cours de la prochaine année, alors que 48 % d'entre elles désirent investir le même montant que l'année dernière. Les cinq projets les plus couramment envisagés sont :

- **L'implémentation d'une solution PAM;**
- **L'introduction ou l'intégration complète de mesures d'authentification à deux facteurs;**
- **L'extension des outils de gestion des mots de passe à tous les employés (et non seulement au personnel informatique);**
- **L'implémentation d'un mécanisme de rotation automatique des mots de passe;**
- **La refonte des stratégies relatives aux VPN.**

Notons que tous ces projets en lien avec la sécurité informatique touchent à la gestion des identités et des accès.

La gestion des identités combine des éléments numériques et des entrées dans une base de données centralisée afin de créer une désignation unique pour chaque utilisateur. Les administrateurs peuvent surveiller, changer, ou supprimer ces désignations à des fins de sécurité, en plus de pouvoir accorder des permissions aux utilisateurs finaux pour qu'ils puissent accomplir leur travail sans encombre. La gestion des accès englobe les permissions des utilisateurs finaux en ce qui a trait aux réseaux, ressources, applications, base de données, etc. Ce concept couvre tous les procédés, pratiques, méthodes, systèmes et outils nécessaires au maintien des accès privilégiés au sein d'un environnement numérique. En somme, la gestion des identités sert à déterminer qui sont les utilisateurs finaux, alors que la gestion des accès vise à définir les actions qu'ils ont l'autorisation d'effectuer.

Et pour finir, 6 % des PME prévoient réduire leurs dépenses en sécurité informatique durant les 12 prochains mois. Ces révélations corroborent celles que nous avons soulignées dans la première partie de ce rapport, à savoir que 5 % des PME sont moins préoccupées par la sécurité informatique que l'an dernier. Mais ce relâchement est-il justifié? Nous n'y croyons pas. La fréquence ainsi que l'intensité des risques et des menaces pour la sécurité informatique sont en pleine croissance. Les PME qui refusent de s'adapter à cette réalité, ce qui signifie parfois d'investir davantage (ou plus intelligemment) dans la sécurité informatique, pourraient très bien essuyer une énorme, voire catastrophique attaque.

Dans la section Recommandations de ce rapport, nous donnons quelques conseils aux professionnels de la sécurité informatique afin qu'ils obtiennent plus de fonds ou de soutien pour leurs besoins et projets (ex. : PAM, AMF, etc.).

PARTIE 6
RECOMMANDATIONS

Cette section présente 10 recommandations concrètes pour aider les PME à réduire les menaces de cybersécurité, à renforcer la gestion des accès privilégiés, à accroître la sensibilisation à la sécurité informatique ainsi que sa gestion, et à améliorer la gestion des accès à distance.

Les conseils et les mesures que nous préconisons pour chaque recommandation sont éprouvés, pratiques et abordables pour les PME :

Recommandation #1 :

Les PME doivent se protéger de manière préventive contre les menaces de cybersécurité plutôt que d'adopter une attitude passive ou de supposer à tort qu'elles sont « trop petites pour être attaquées ». Les pirates visent de plus en plus les PME, afin de tirer parti de défenses de cybersécurité affaiblies (et dans certains cas pratiquement inexistantes).

Recommandation #2 :

Les PME doivent mettre en œuvre une série de principes et de politiques qui réduisent considérablement les risques de cybersécurité, tout en augmentant la visibilité, la gouvernance et le contrôle. Ces principes et politiques comprennent: le principe de moindre privilège, la Confiance zéro, la séparation des tâches, la défense en profondeur et le principe des quatre yeux.

Recommandation #3 :

Les PME doivent mettre en place une solution de gestion des accès privilégiés (PAM) qui comble le fossé entre l'authentification et l'autorisation afin de renforcer leur position en matière de sécurité et limiter le risque d'une violation potentiellement catastrophique.

Recommandation #4 :

Les PME ont besoin d'un plan complet pour s'assurer que les objectifs et les exigences en matière de cybersécurité sont transmis au moment opportun à toutes les parties prenantes concernées, et qu'ils sont suivis et appliqués en permanence.

Recommandation #5 :

Les PME devraient offrir aux utilisateurs des formations en cybersécurité qui traitent d'enjeux, de menaces et de risques fondamentaux.

Recommandation #6 :

Les PME qui ne disposent pas d'une structure de sécurité informatique, ne veulent pas embaucher du personnel additionnel et manquent d'expertise en ce qui a trait à la sécurité infonuagique devraient se tourner vers des fournisseurs de services gérés (MSP) pour combler ce manque.

Recommandation #7 :

Les PME se doivent d'implémenter une solution de passerelle juste-à-temps pour éliminer les vulnérabilités engendrées par les réseaux privés virtuels (VPN).

Recommandation #8 :

Les PME doivent prendre en compte les vulnérabilités qu'entraîne le travail à distance.

Recommandation #9 :

Les PME devraient exiger, lors du choix d'un outil de gestion des accès à distance, des améliorations dans les quatre catégories suivantes: la sécurité, l'efficacité, la gouvernance et l'abordabilité.

Recommandation #10 :

Pour obtenir un budget plus élevé, les professionnels de l'informatique devraient mettre l'accent sur les cinq éléments suivants: la confiance, la conformité, les assurances, les employés et l'éthique.

RECOMMANDATIONS AUX PME POUR LIMITER LES MENACES DE CYBERSÉCURITÉ

1 **Les PME doivent se protéger de manière préventive contre les menaces de cybersécurité plutôt que d'adopter une attitude passive ou de supposer à tort qu'elles sont « trop petites pour être attaquées ». Les pirates visent de plus en plus les PME, afin de tirer parti de défenses de cybersécurité affaiblies (et dans certains cas pratiquement inexistantes).**

Le sondage a révélé les cinq principales menaces qui préoccupent le plus les PME, à savoir : les rançongiciels, l'hameçonnage, les logiciels malveillants, les vulnérabilités infonuagiques, et les attaques de la chaîne d'approvisionnement. Il ne s'agit pas d'une surprise, car ces menaces sont étroitement liées. Par exemple, les rançongiciels sont généralement des logiciels malveillants diffusés par le biais de l'hameçonnage, d'une vulnérabilité exploitée ou d'une chaîne d'approvisionnement compromise.

Se prémunir contre toutes les cyberattaques est un défi énorme et irréaliste pour beaucoup d'entreprises. Fort heureusement, une préparation adéquate permet de réduire considérablement l'impact des rançongiciels et autres menaces. Un bon point de départ pour les PME est de développer une stratégie de défense qui :

- Réduit la capacité d'un pirate à se déplacer librement dans l'environnement.
- Permet une visibilité et des capacités de réponse.
- Empêche toute exposition inutile.
- Met en place une reprise des opérations robuste et efficace.

Nous examinons en détail chacun de ces éléments ci-dessous :

Réduire la capacité d'un pirate à se déplacer librement dans l'environnement

Dès que l'accès initial est obtenu, les pirates tenteront de rechercher (s'ils ne l'ont pas déjà) des informations d'identification de grande valeur, afin d'obtenir un accès administratif dans l'environnement. L'élévation verticale nécessite souvent de se déplacer de système en système. Par exemple, le bureau d'un utilisateur peut être compromis sans autre accès de valeur. Ainsi, un pirate tentera de se connecter sur d'autres postes de travail ou serveurs, afin d'extraire les informations d'identification des comptes administratifs (la connexion sur d'autres systèmes est appelée mouvement latéral).

Une bonne hygiène des comptes, ainsi qu'un contrôle et une gouvernance appropriés des accès privilégiés, complique la tâche des pirates qui veulent accomplir leur objectif sans être détectés. Les principales mesures que les PME devraient suivre sont :

- Le déploiement intégral d'une solution PAM complète, mais facile à utiliser et à gérer (voir la recommandation #3).
- L'implémentation d'une double autorisation, également connue sous le nom de « principe des quatre yeux » (voir la recommandation #2).
- Établir des flux d'approbation pertinents, selon lesquels les individus doivent approuver des données ou des tâches à des moments précis d'un processus.
- L'implémentation de la solution LAPS (de l'anglais Local Administrator Password Solutions), qui offre une gestion des mots de passe des comptes locaux des ordinateurs joints au domaine. Les mots de passe sont stockés dans Active Directory (AD) et protégés par une liste de contrôle d'accès (ACL ou access control list), de sorte que seuls les utilisateurs éligibles peuvent lire/demander une réinitialisation.

Favoriser la visibilité et les capacités de réaction

Ce n'est pas pessimiste, mais plutôt réaliste de reconnaître la possibilité d'intrusion de pirates (si ceux-ci sont assez persistants et sophistiqués) dans un système de défense de cybersécurité robuste. Par chance, les solutions de détection et de réponse aux menaces ont beaucoup évolué depuis l'époque où de nombreuses organisations (et la plupart des PME) comptaient sur les logiciels antivirus classiques.

Près de 1,5 million de nouveaux sites d'hameçonnage sont créés chaque mois. [source]

De nos jours, les solutions de détection et de réponse aux points d'extrémité (EDR) sont indispensables pour détecter et contrer les logiciels malveillants connus et inconnus. Les autres mesures que les PME devraient adopter pour améliorer considérablement leurs capacités de visibilité et de réponse sont :

- L'analyse comportementale utilisant l'apprentissage automatique, l'intelligence artificielle, les mégadonnées et l'analytique pour identifier les comportements malveillants en analysant les différences dans les activités normales et quotidiennes.
- La capacité de confinement, qui est une méthodologie par laquelle l'accès aux informations, aux fichiers, aux systèmes et aux réseaux est contrôlé par le biais de points d'accès.
- La surveillance centralisée, qui consiste à gérer les processus de cybersécurité dans toute l'organisation à l'aide d'un ensemble unique et centralisé d'outils, de procédures et de systèmes. Cette approche évite les silos entre les départements de cybersécurité et utilise un réseau centralisé pour tout regrouper au même endroit.
- Externaliser une partie ou l'ensemble des tâches de sécurité informatique auprès d'un fournisseur de services gérés (voir la recommandation #6).

Éviter les expositions inutiles

La réduction de la taille de la surface d'attaque est cruciale pour bloquer l'accès initial, l'élévation et le mouvement latéral dans l'environnement. Les systèmes qui ne sont pas requis pour les opérations commerciales, ou qui ne sont pas corrigés à temps, peuvent exposer des vulnérabilités. Les systèmes qui ne sont pas nécessaires ou qui ne peuvent pas être corrigés doivent être gérés de manière à ce que les pirates n'aient pas l'occasion de les exploiter.

Instaurer un plan de sauvegarde et de récupération robuste

Il convient de mettre en place un plan de sauvegarde et de récupération robuste afin de faciliter une récupération rapide en cas de rançongiciel très perturbateur. Cela permet de réduire les répercussions sur la continuité de l'activité et des opérations. Voici les meilleures pratiques conseillées[3] :

- **Augmenter la fréquence des sauvegardes.** Dû au fait des rançongiciels, sauvegarder les données une seule fois par nuit n'est plus suffisant. Tous les ensembles de données doivent être protégés plusieurs fois par jour.
- **Aligner la stratégie de sauvegarde sur les exigences du niveau de service.** Par exemple, si le niveau de service est de 15 minutes, les sauvegardes doivent être exécutées au moins toutes les 15 minutes.
- **Respecter la « règle de sauvegarde 3-2-1 ».** Cette règle consiste à conserver trois copies complètes des données : deux copies locales, mais sur deux types de supports différents (ou deux systèmes de stockage de sauvegarde locaux différents sur site), et une copie stockée hors site.
- **Faire preuve de vigilance lorsque vous transférez des données vers le nuage.** Méfiez-vous de la déclaration d'un fournisseur qui prétend offrir la reprise après sinistre en tant que service (DRaaS ou Disaster recovery as a service en anglais). Bien que les avantages du DRaaS soient considérables, il ne s'agit pas d'une baguette magique. Les PME doivent se rappeler qu'une reprise après sinistre « par bouton de commande » ne signifie pas nécessairement une reprise « instantanée ».
- **Automatiser les dossiers d'exploitation après sinistre.** Cela signifie qu'il faut prédéfinir l'ordre de récupération et exécuter le processus de récupération adéquat en un seul clic. Cette approche peut se révéler très avantageuse pour les PME dont les applications sont multiniveaux et utilisent des serveurs interdépendants. En effet, elle permet de rétablir les données à l'endroit et au moment où elles sont le plus nécessaires.
- **Ne pas utiliser la sauvegarde pour conserver les données.** Gardez à l'esprit que la majorité des restaurations proviennent de la sauvegarde la plus récente, et non d'une sauvegarde vieille de plusieurs mois, voire de plusieurs années.
- **Protéger les points de terminaison et les applications SaaS.** Les ordinateurs portables, les ordinateurs de bureau, les téléphones intelligents et les tablettes peuvent renfermer des données uniques et précieuses. Celles-ci ne sont jamais stockées dans un dispositif de stockage du centre de données, sauf si elles sont expressément et délibérément sauvegardées.

[3] Ces meilleures pratiques sur la création et la gestion d'un plan de sauvegarde et de récupération robuste sont basées sur les conseils publiés par TechTarget.

2 **Les PME doivent mettre en œuvre une série de principes et de politiques qui réduisent considérablement les risques de cybersécurité, tout en augmentant la visibilité, la gouvernance et le contrôle. Ces principes et politiques comprennent : le principe de moindre privilège, la Confiance zéro, la séparation des tâches, la défense en profondeur et le principe des quatre yeux.**

Principe de moindre privilège :

Le principe de moindre privilège (ou POLP, de l'anglais *Principle of Least Privilege*) 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. Voici les bonnes pratiques :

- 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.
- 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 contre une violation coûteuse et potentiellement catastrophique.
- 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 stratégie, connue sous le nom de bracketing de privilèges, peut être mise en œuvre pour les utilisateurs individuels, ainsi que pour les processus et les systèmes.
- Séparer les comptes administrateur des comptes standards et les fonctions des systèmes de niveau supérieur de celles de niveau inférieur.
- Assurer une visibilité totale pour voir ce que font les utilisateurs, et quand ils le font.
- Auditer régulièrement les privilèges des utilisateurs pour s'assurer que l'accès est approprié.
- Supprimer immédiatement l'accès des utilisateurs qui quittent l'organisation.
- Disposer de la capacité de révoquer automatiquement les accès privilégiés en cas d'urgence.

Confiance zéro

La Confiance zéro implique que personne n'est automatiquement digne de confiance. L'approche consiste plutôt à « faire confiance, mais vérifier ». La gestion de l'accès doit être analysée à l'aide de données contextuelles, plutôt que de faire simplement confiance aux secrets d'authentification fournis lors de la connexion.

Cette stratégie est très adaptée à la nouvelle réalité du travail à domicile (WFH ou *work from home*), qui gomme la frontière entre le réseau d'entreprise et l'utilisation du nuage, car les travailleurs se connectent de n'importe où et accèdent à de nombreuses ressources décentralisées. Les contrôles doivent être axés sur le contexte, le comportement et l'emplacement de l'utilisateur final. Voici les meilleures pratiques :

- Utiliser l'authentification multifacteur (AMF) en temps réel pour vérifier la confiance lors de toute tentative d'accès à une ressource du réseau.
- Étendre les contrôles d'identité aux terminaux pour détecter et valider tous les appareils.
- Organiser les utilisateurs par groupe ou par rôle pour prendre en charge les stratégies d'appareil.
- Utiliser le déprovisionnement automatique, ainsi que la capacité d'effacer, de verrouiller et de désinscrire les appareils volés ou perdus.
- Mettre régulièrement à jour les droits des utilisateurs finaux en fonction des modifications apportées aux rôles ou aux tâches ainsi que des modifications des politiques de sécurité ou des exigences de conformité en vigueur.
- Surveiller le comportement et permettre des alertes lorsque des activités suspectes sont détectées.

La séparation des tâches

La séparation des tâches (de l'anglais *Segregation of Duties* ou SoD), 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. Voici les bonnes pratiques :

- Définir et attribuer les rôles de manière à mitiger les risques de manière à prévenir les conflits d'intérêts (réels ou apparents), les actes illicites, la fraude et les abus lorsqu'un ou plusieurs rôles sont attribués à un employé.
- 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 afin de s'assurer qu'aucun individu n'a la possibilité de combiner plusieurs accès et ainsi 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 qui soutiennent un programme SoD complet. Il s'agit notamment de former les superviseurs et les gestionnaires à reconnaître lorsqu'un de leurs employés (ou tout autre collègue) dispose d'un ensemble de tâches conflictuelles, risquées ou inutiles qui pourraient être transférées à un autre rôle plus adéquat.

Défense en profondeur

La défense en profondeur consiste en plusieurs couches de protection afin de ralentir les pirates informatiques voulant se frayer un chemin à travers le périmètre jusqu'à certaines ressources vitales pour mener à bien une tâche. Voici les bonnes pratiques :

- Concevoir des couches de contrôle comme si une violation de données s'était déjà produite (c'est-à-dire répondre à la question « et si ? »), et mettre en place des défenses pour empêcher ou contenir la prochaine action des pirates.
- Combiner les principes et les stratégies de sécurité pour produire un effet de synergie. Ainsi, le SoD et le POLP contiendront les menaces pesant sur un sous-ensemble de l'environnement de l'entreprise, ce qui crée une excellente occasion de mettre en place des niveaux de contrôle entre eux.
- Implémenter le principe des quatre yeux (évoqué ci-dessous) pour les accès privilégiés avec l'approbation de réservation afin de prévenir, ou du moins de détecter, les tentatives d'accès non autorisées.
- Installer 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.
- N'oubliez pas la surveillance! Ralentir un pirate avec de multiples contrôles de prévention ne suffit pas si les accès non autorisés ou les tentatives d'élévation ne sont pas surveillés et détectés.

Principe des quatre yeux

Le principe des quatre yeux (parfois appelé principe ou règle des deux personnes) exige que toute activité d'un employé présentant un risque important soit examinée et approuvée par un second employé indépendant et compétent. Voici les bonnes pratiques :

- Mettre en place des flux de travail à double autorisation pour accéder à des informations sensibles, ou effectuer des actions élevées.
- Examiner les pistes d'audit des actions effectuées sur les systèmes ou les données à risque.
- Les rôles professionnels qui impliquent des procédures ou des accès à haut risque doivent être attribués à plusieurs employés.
- Enregistrer les actions effectuées sur les systèmes lorsque des utilisateurs externes accèdent aux ressources de l'entreprise. Ces enregistrements doivent être examinés pour garantir qu'aucune action suspecte n'a été tentée.

RECOMMANDATIONS AUX PME POUR RENFORCER LA GESTION DES ACCÈS PRIVILÉGIÉS

3 **Les PME doivent mettre en place une solution de gestion des accès privilégiés (PAM) qui comble le fossé entre l'authentification et l'autorisation afin de renforcer leur position en matière de sécurité et limiter le risque d'une violation potentiellement catastrophique.**

La gestion des identités regroupe les éléments et les entrées numériques dans une base de données centralisée, afin de créer une désignation unique pour chaque utilisateur. Ces désignations sont surveillées, modifiées et supprimées si nécessaire dans le but de renforcer la sécurité, tout en accordant aux utilisateurs finaux les autorisations dont ils ont besoin pour effectuer diverses tâches professionnelles.

La gestion des accès détermine si les utilisateurs finaux sont autorisés ou non à accéder aux réseaux, ressources, applications, bases de données, etc. Ce concept intègre l'ensemble des politiques, processus, méthodes, systèmes et outils nécessaires au maintien d'un accès privilégié dans un environnement numérique.

En résumé, la gestion des identités s'interroge sur *qui* est l'utilisateur alors que la gestion des accès est liée aux *activités* de l'utilisateur.

Cependant, la plus grande problématique que les PME doivent affronter lorsqu'elles tentent d'appliquer la gestion des identités (IAM) est que certaines technologies (telles que les systèmes hérités, les cellulaires et les caméras) ne peuvent pas utiliser un système fédéré. Bien qu'il est possible de créer et de conserver manuellement des comptes d'identité pour chaque utilisateur, ce n'est pas une solution pratique.

Pourquoi les PME n'évitent-elles pas tout simplement le problème en supprimant les comptes privilégiés qui sont partagés entre les rôles, équipes, et groupes ? La réponse est que certains groupes privilégiés sont nécessaires, par exemple :

- 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 service de domaine.

La solution à ce dilemme pour les PME est de mettre en place une solution PAM qui étend la protection offerte par un système IAM à l'espace d'identité non fédéré.

Éléments clés d'une solution PAM robuste

Les PME doivent se tourner vers une solution PAM robuste qui offre tous les éléments suivants :

- Un coffre qui stocke les mots de passe (et autres données sensibles, comme les codes d'alarme des bâtiments, les clés de licence des logiciels, etc.), et qui est partagé en toute sécurité entre plusieurs utilisateurs finaux;
- Une fonctionnalité de demande de réservation de compte permettant aux administrateurs d'approuver ou de rejeter les demandes au cas par cas et de fixer des limites de temps au besoin;
- Des notifications qui préviennent les administrateurs lorsque certains événements ou actions impliquent les utilisateurs finaux, les rôles, les coffres, etc.;
- La rotation obligatoire et automatisée du mot de passe;
- Une fonctionnalité d'injection d'identifiants qui automatise les flux de travail (par exemple, ouvrir un client VPN, lancer un protocole d'accès à distance et accéder à un compte privilégié) sans fournir de mots de passe aux utilisateurs finaux;
- L'enregistrement de l'activité de la session;
- La rotation des informations d'identification à chaque réservation d'une session RDP, ce qui atténue l'exploitation potentielle des informations d'identification RDP (elles n'ont pas besoin d'être transmises aux utilisateurs, car chaque authentification a lieu une fois, ce qui élimine la nécessité de rotation des informations d'identification);
- Une certaine facilité de déploiement et de gestion;
- Un prix abordable et adapté aux budgets de sécurité informatique des PME, qui sont nettement inférieurs à ceux des grandes entreprises.

De plus, 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 (voir l'encadré).

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.

RECOMMANDATIONS AUX PME POUR ACCROÎTRE LA SENSIBILISATION À LA SÉCURITÉ INFORMATIQUE

4 **Les PME ont besoin d'un plan complet pour s'assurer que les objectifs et les exigences en matière de cybersécurité sont transmis au moment opportun à toutes les parties prenantes concernées, et qu'ils sont suivis et appliqués en permanence.**

Les politiques qui ne comportent pas de contrôles techniques pour assurer leur implémentation sont inefficaces. Plus grave encore, les politiques sont mal communiquées et ne sont ni mises en œuvre ni suivies. Pour éviter ces écueils, il est crucial pour les PME de :

- Définir et documenter les objectifs;
- Définir les rôles et les responsabilités;
- Communiquer en aval et surveiller en amont.

Nous examinons chacun de ces points ci-dessous :

Les organisations disposant d'un plan de réponse aux incidents de cybersécurité complet et éprouvé ont réduit le coût d'une violation de 2 millions USD en moyenne, par rapport aux organisations ne disposant pas d'un plan rigoureux et bien adapté. [source]

Définir et documenter les objectifs

Les objectifs de cybersécurité doivent être clairement définis et documentés. Ils doivent également être spécifiques, mesurables, réalisables, réalistes et situés dans un cadre temporel défini (alias « SMART »).

La sensibilisation à la sécurité informatique dans l'ensemble de l'organisation ne peut être optimisée sans objectifs adéquats. Ainsi, de nombreuses organisations se préoccupent entièrement de la vigilance de l'utilisateur final (par exemple, éviter l'hameçonnage, appliquer des contrôles de cybersécurité, etc.) mais négligent de valider la compréhension des objectifs.

Définir les rôles et les responsabilités

La définition des rôles et des responsabilités est le coeur d'une politique et d'un plan à toute épreuve. Pour s'assurer que les principales parties prenantes internes comprennent les exigences de cybersécurité dans l'ensemble de l'entreprise, ces rôles et responsabilités doivent être mis en parallèle avec un tableau RACI (de l'anglais *Responsible, Accountable, Consulted, Informed*).

Voici un exemple de tableau RACI pour les rôles et responsabilités de haut niveau en matière de cybersécurité

	Conseil d'administration	Direction	Directeur informatique	Chef d'équipe
Évaluer, diriger et superviser les objectifs de cybersécurité	A	R	I	
Aligner, planifier et organiser les initiatives de cybersécurité		A	R	I
Élaborer, adopter et implémenter des initiatives de cybersécurité			A	R
Fournir, entretenir et soutenir les services de cybersécurité			A	R
Évaluer, surveiller et analyser les performances des initiatives et des services de cybersécurité	I	A	R	

Les tableaux RACI peuvent également être utilisés pour des exigences de cybersécurité plus détaillées afin de déterminer qui est responsable de l'acceptation des risques de cybersécurité, ou qui est chargé de signaler un nouveau risque de cybersécurité.

Communiquer en aval et surveiller en amont.

Les politiques doivent être accessibles à toutes les parties prenantes (employés, fournisseurs, vendeurs, clients, etc.) et les mises à jour doivent être communiquées dans les meilleurs délais. Il est crucial d'établir des canaux de communication bidirectionnels. Les comités sont un moyen efficace et pratique de recueillir les commentaires des parties prenantes, de confirmer l'alignement et d'apporter des ajustements et des améliorations continus selon les besoins.

5

Les PME devraient offrir aux utilisateurs des formations en cybersécurité qui traitent d'enjeux, de menaces et de risques fondamentaux.

Bien qu'il existe de nombreuses manières pour les PME de sensibiliser leurs employés à la cybersécurité, la méthode la plus pratique, efficace et rentable – surtout pour les PME qui emploient des travailleurs à distance – demeure l'utilisation d'une plateforme de formation en ligne. Grâce à celle-ci, les employés peuvent bénéficier de formations concrètes portant sur la détection et l'atténuation des menaces. De plus, la nature dynamique de cet environnement virtuel en direct permet aux employés d'approfondir leurs connaissances à leur propre rythme.

Le fait que les employés puissent recevoir des commentaires ponctuels est l'un des principaux avantages que présente la formation en ligne. Ils peuvent ainsi être évalués sur leurs aptitudes décisionnelles et progresser en fonction de leur performance. Les superviseurs et gestionnaires ont aussi accès à un tableau de bord qui leur permet de suivre les progrès de chaque employé et d'identifier leurs forces et leurs faiblesses.

Près de la moitié des fuites de données résulte de la négligence d'un employé.

[source]

De nombreux programmes de formation en cybersécurité réputés sont disponibles en ligne. Nous recommandons à tout le moins que les PME choisissent un programme qui couvre les menaces, risques et enjeux fondamentaux suivants[4]:

- **Le contrôle d'accès;**
- **Le principe PAP (prenez vos appareils personnels);**
- **Les services infonuagiques;**
- **La fuite de données;**
- **L'usurpation d'identité;**
- **Déclaration d'incidents;**
- **La propriété intellectuelle;**
- **Une introduction à la sécurité de l'information;**
- **Les logiciels malveillants;**
- **Les appareils mobiles;**
- **Les risques liés à l'Open Wi-Fi;**
- **La gestion des mots de passe;**
- **L'hameçonnage;**
- **La sécurité physique;**
- **La confidentialité;**
- **La protection des données de cartes de paiement;**
- **L'utilisation responsable de l'Internet;**
- **Le piratage psychologique;**
- **Les réseaux sociaux;**
- **Les voyages sécuritaires;**
- **Le travail à distance.**

[4]Ces menaces, risques et enjeux fondamentaux sont issus du programme de formation « Security Awareness — General Knowledge » offert par la firme de formation en cybersécurité Terranova Security.

6 **Les PME qui ne disposent pas d'une structure de sécurité informatique, ne veulent pas embaucher du personnel additionnel et manquent d'expertise en ce qui a trait à la sécurité infonuagique devraient se tourner vers des fournisseurs de services gérés (MSP) pour combler ce manque.**

Les fournisseurs de services gérés (MSP) aident les PME à augmenter leur capacité et leur éventail de compétences; à réduire les coûts et les risques liés à leurs activités; à saisir les occasions de croissance; à améliorer l'expérience de leurs utilisateurs; à gérer l'incertitude et à mettre en place des plans pour l'avenir.

Afin de choisir le fournisseur de services gérés approprié, les petites et moyennes entreprises doivent prendre en compte les sept facteurs principaux que voici :

- **Les services :** un fournisseur de services gérés doit pouvoir s'occuper des besoins et des objectifs spécifiques d'une PME. Les fournisseurs de services gérés n'ont pas tous le même domaine de spécialité. Par exemple, certains d'entre eux offrent des services de sécurité informatique, mais ils ne s'y connaissent pas nécessairement en matière de sécurité infonuagique.

- **Les conseils :** un fournisseur de services gérés doit proposer des suggestions informées et objectives. Rappelons que l'objectif est de renforcer la sécurité de la PME et non d'enrichir le fournisseur.

- **Le budget :** un fournisseur de services gérés doit se montrer compréhensif en ce qui a trait au plus petit budget alloué à la sécurité informatique dans les PME que dans les grandes entreprises et organisations. En ce sens, les fournisseurs de services gérés devraient recommander des services essentiels, en plus d'aider les PME à utiliser intelligemment leur budget plus restreint afin qu'elles obtiennent « plus pour moins cher ».

- **La franchise :** un fournisseur de services gérés doit pouvoir dire aux dirigeants et aux décideurs ce qu'ils doivent entendre et non ce qu'ils veulent entendre. Si les PME prennent des décisions non éclairées ou erronées, alors il a le devoir de corriger le tir en recommandant des solutions plus appropriées.

- **La réactivité :** les PME ne devraient jamais au grand jamais sentir que leur fournisseur de services gérés les traite comme des « entreprises de seconde zone » en comparaison avec leurs clients issus d'organisations plus larges. Des normes de réactivité devraient donc figurer dans l'accord sur les niveaux de service (ANS), de sorte que le fournisseur de services gérés les respecte ou les dépasse.

- **La continuité des activités et la reprise sur sinistre :** un fournisseur de services gérés doit disposer des outils, du personnel et des politiques pour surveiller continuellement l'infrastructure de la PME de manière à garantir la continuité des activités et la reprise sur sinistre. La notion selon laquelle une PME devrait « se déconnecter » pour une durée substantielle à la suite d'une cyberattaque ou de tout autre événement (incluant ceux qui n'ont rien à voir avec la sécurité informatique) ne constitue pas une option viable.

- **La neutralité par rapport aux technologies et aux vendeurs :** si nécessaire (ou sur demande), un fournisseur de services gérés doit offrir des recommandations portant sur le matériel (physique ou logiciel), sur les fournisseurs de formation, ainsi que sur n'importe quels autres aspects qui relèvent des services offerts. Cependant, en aucun cas un fournisseur de services gérés ne devrait insister sur un produit ou un vendeur en particulier. Ils n'ont de comptes à rendre qu'à leurs clients.

- **La communication :** un fournisseur de services gérés digne de ce nom est en mesure de discuter d'experts à experts avec l'équipe informatique interne ou de sécurité informatique d'une PME. En revanche, un fournisseur de services gérés doit également être à l'aise de communiquer (verbalement et par écrit) avec des non-initiés. Autrement, il crée plus de problèmes qu'il n'en résout.

RECOMMANDATIONS AUX PME POUR AMÉLIORER LA GESTION DES ACCÈS À DISTANCE

7

Les PME doivent implémenter une solution de passerelle juste-à-temps pour éliminer les vulnérabilités causées par les réseaux privés virtuels (VPN).

La majorité des PME se servent de VPN pour établir une connexion réseau protégée lorsqu'elles utilisent des réseaux publics, ce qui est très important pour les travailleurs à distance. Bien que les VPN sont utiles, ils posent trois problèmes de taille :

- Les serveurs VPN sont réputés pour être difficiles et longs à déployer;
- Les clients VPN font transiter le trafic par le réseau privé, ce qui peut détériorer considérablement les performances du réseau;
- Lorsqu'ils accordent un accès temporaire, les administrateurs doivent passer du temps à mettre à jour et à suivre les règles du VPN et du pare-feu.

Il existe une solution concrète afin d'aider les PME à combler leurs lacunes en matière de sécurité et à renforcer la gestion des accès à distance : implémenter une solution de passerelle pour fournir un accès juste-à-temps aux ressources dans les réseaux segmentés. Par conséquent, les utilisateurs peuvent accéder en toute sécurité au réseau interne de l'entreprise depuis leur domicile. Une passerelle est également très avantageuse pour les fournisseurs de services gérés (MSP), car elle leur permet de se connecter rapidement et en toute sécurité à des réseaux clients distincts.

Pour ce qui est des principaux problèmes liés aux VPN mentionnés ci-dessus, une solution de passerelle :

- Se déploie rapidement et aisément, ce qui est essentiel pour les PME qui n'ont pas le budget ou la bande passante pour s'enliser dans les problèmes et les tracas liés au déploiement;
- Améliore les performances réseau en limitant les connexions RDP par tunnel.Cela signifie qu'il n'y a pas de répercussions négatives sur le reste du trafic réseau;
- Utilise des règles d'accès dynamique, ce qui évite aux administrateurs d'avoir à mettre à jour manuellement les règles de VPN et des pare-feu lorsqu'ils accordent un accès temporaire.

Pour en apprendre davantage sur une solution robuste et abordable qui répond à toutes ces exigences, nous invitons les PME à découvrir Devolutions Gateway.

8

Les PME doivent faire face aux vulnérabilités de sécurité des travailleurs à distance.

De nombreuses PME de par le monde se sont démenées afin de trouver une solution sûre et sécurisée pour déployer et maintenir les accès à distance. Bien que certaines PME effectuent un retour dans des bureaux physiques, une part importante de leurs employés devrait rester 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 :

L'accès distant sécurisé avec des passerelles juste-à-temps et des VPN

Les professionnels de l'informatique ont besoin en permanence d'un accès sécurisé aux ressources critiques de l'entreprise. Que ce soit pour mettre à jour les machines du réseau informatique ou pour assister les utilisateurs à distance, les PME doivent choisir une solution de passerelle ou de VPN juste-à-temps complète et hautement sécurisée, qui est rapide, robuste, sûre et facile à déployer.

L'authentification multifacteur (AMF)

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.

L'utilisation d'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;
- Des alertes par courriel en temps réel en cas de tentatives d'accès non autorisé.

La 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 afin d'attaquer des réseaux et des systèmes. Les principaux outils de sécurité des terminaux comptent :

- Des pare-feu de réseau (sur les terminaux et les réseaux domestiques);
- Des logiciels antivirus;
- Des mises à jour logicielles. 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.

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. Dans la section précédente, nous avons mis en évidence les sujets essentiels de cybersécurité que les PME devraient couvrir (qu'elles assurent elles-mêmes la formation ou qu'elles fassent appel à un consultant ou à une entreprise de formation tiers). De plus, les travailleurs à distance devraient :

- Être mis en garde contre le partage excessif sur les médias sociaux parce que les pirates se servent de ces informations pour traquer leurs victimes;
- Garder leurs appareils avec eux et ne jamais les laisser sans surveillance, même pendant quelques secondes. Dans les lieux publics tels que les cafés, les centres commerciaux, les aéroports, les hôtels, etc., les voleurs étudient attentivement une victime pendant de longues périodes, puis agissent rapidement dès qu'ils perçoivent une occasion.

Le passage 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, la prévention de la perte de données (DPL ou data loss prevention en anglais), le chiffrement, etc. De plus, si un appareil est volé, l'accès aux données dans le nuage peut être révoqué immédiatement.

9 **Les PME doivent tirer quatre avantages essentiels de leurs outils d'accès à distance : amélioration de la sécurité, de l'efficacité, de la gouvernance et de l'abordabilité.**

Le sondage a dévoilé que la croissance du travail à distance crée des défis pour les PME dans quatre domaines essentiels : la sécurité, l'efficacité, la gouvernance et l'abordabilité.

Afin de faire face à ces défis et préoccupations, nous fournissons ci-dessous une liste de contrôle pour aider les PME à choisir les bons outils d'accès à distance :

Relever les défis de la sécurité

Privilégier les outils d'accès à distance qui offre :

- **Un chiffrement robuste :** Tous les mots de passe stockés dans les sources de données doivent être chiffrés à l'aide d'un algorithme de chiffrement robuste. Ainsi, si un utilisateur final tente d'accéder aux données directement dans la base de données, celles-ci seront rendues illisibles.
- **Une injection des comptes :** Les informations d'identification peuvent être injectées pour un utilisateur lors du lancement d'une connexion, ce qui l'empêche de connaître les informations d'identification.
- **Un contrôle d'accès basé sur les rôles (RBAC) :** Toutes les restrictions peuvent être prédéfinies et appliquées par des autorisations de niveau granulaire.
- **Une authentification à deux facteurs (A2F) :** Imposer deux étapes d'authentification consécutives avant d'accorder l'accès à une source de données.
- **Des coffres d'utilisateurs :** Les coffres des utilisateurs donnent à des utilisateurs finaux uniques un accès à des comptes privilégiés spécifiques.

Relever les défis de l'efficacité

Privilégier les outils d'accès à distance qui offre :

- **Un coffre centralisé pour les mots de passe :** Stocker tous les mots de passe et les informations d'identification dans un coffre sécurisé, et connectez-vous à partir de n'importe où par le biais d'un module d'extension de navigateur sécurisé.

- **Un accès mobile :** Lancer des sessions, gérer des postes de travail et de serveurs, et récupérer des mots de passe en déplacement grâce à une application mobile sécurisée et facile à utiliser.

- **Un accès hors ligne :** Lancer des sessions sans connexion Internet en accédant à une copie modifiable hors ligne de la base de données qui est aussi sécurisée que la version en ligne.

- **Connexions automatiques :** Lancez des connexions directes et sécurisées vers des sessions privilégiées, y compris des serveurs distants, des machines virtuelles et d'autres actifs critiques.

- **Prise en charge de plusieurs outils et technologies :** La liste des intégrations doit comprendre RDP, SSH, VPN, Web, VNC, Telnet, ICA/HDX, ARD, etc.

- **Soutien de plusieurs sources de données :** Partagez facilement des bases de données, notamment SQL Server et autres.

- **Partage de session :** Partagez facilement et en toute sécurité toutes les sessions à distance dans toute l'équipe.

- **Plusieurs coffres :** Stocker et organiser les entrées dans un nombre illimité de coffres afin de gérer aisément des quantités massives d'entrées, de documents et d'autres données sensibles.

Relever les défis de la gouvernance

Privilégier les outils d'accès à distance qui offre :

- **La piste d'audit :** Surveiller, vérifier et analyser le temps écoulé par un utilisateur final sur un client ou une machine en particulier à des fins d'audit.
- **Journal des activités :** enregistrer quand, quoi et qui a exécuté une action sur une session, et surveillez toutes les sessions ouvertes pour tous les utilisateurs.
- **Connexion en temps réel :** savoir précisément qui est connecté en temps réel pour plusieurs types de sessions, et vérifier si un utilisateur final s'est connecté malgré un avertissement.
- **Console intégrée :** Obtenir un aperçu de l'état des machines et simplifier les tâches de gestion grâce aux consoles de virtualisation intégrées, telles que Hyper-V, Terminal Server et XenServer.

Relever les défis de l'abordabilité

Privilégier les outils d'accès à distance qui offre :

- **Un essai gratuit :** Évaluer l'outil dans votre propre environnement pour en vérifier la sécurité, les fonctionnalités, la convivialité et d'autres exigences avant de vous engager à l'acheter.
- **Une licence par utilisateur ou par installation :** Vérifier que la licence est accordée par utilisateur et non par installation. Cela procure aux PME beaucoup plus de souplesse et de liberté dans la gestion de leur budget.
- **Des options de licence multiples :** Les PME devraient avoir la possibilité de choisir parmi plusieurs options de licence, telles que : Site jusqu'à un nombre maximum d'utilisateurs ;Site pour un nombre illimité d'utilisateurs; et Multi-Site pour un nombre illimité d'utilisateurs sur plusieurs sites. Cette flexibilité permet aux PME de ne payer que l'accès dont elles ont besoin, et rien de plus.
- **Rendement avéré :** Le coût total de possession (TCO ou *Total cost of ownership* en anglais) ne doit pas dépasser le rendement pour la réduction des risques et les hausses de productivités.

RECOMMANDATIONS AUX PME POUR AMÉLIORER LA GESTION DE LA SÉCURITÉ INFORMATIQUE

10

Les professionnels de l'informatique devraient mettre l'accent sur cinq éléments lors de leurs présentations, propositions ou argumentaires, à savoir : la confiance, la conformité, les assurances, les employés et l'éthique.

L'histoire se ressemble pour beaucoup de professionnels de l'informatique issus du milieu des PME : ils travaillent continuellement à l'obtention d'un budget plus élevé pour la cybersécurité, non pas parce qu'ils souhaitent s'arroger toute la gloire, mais bien parce qu'ils ont à cœur la protection de l'entreprise contre les risques, les menaces, le manque de conformité et les atteintes à la réputation. Ces guerriers de l'ombre se voient trop souvent refuser catégoriquement leurs demandes, bien qu'ils obtiennent parfois de légères concessions.

Effectivement, ce scénario est si souvent répété, que bien des professionnels de l'informatique considèrent que leur patron (ou patrons) ne se soucie pas outre mesure de la sécurité informatique et ne réalisent pas son importance fondamentale. Y a-t-il une logique à dégager de cette situation malencontreuse ?

Pour répondre à cette question, Devolutions a consulté des milliers de dirigeants et de décideurs issus de PME de par le monde avant d'arriver à la conclusion suivante : contrairement à ce que croient de nombreux professionnels de l'informatique, le problème n'est pas dû au désintérêt de leurs collègues.

C'est plutôt une question d'ignorance. En effet, lesdits collègues (catégorie qui inclut de nombreux propriétaires, PDG, directeurs financiers, vice-présidents des opérations, etc.) ont tendance à croire, à tort, que leur entreprise investit déjà dans une sécurité informatique forte. C'est encore plus vrai lorsque l'organisation en question n'a pas encore essuyé une attaque sévère.

Voilà pourquoi ils croient qu'il n'est pas nécessaire d'augmenter le budget relatif à la cybersécurité, ou encore d'octroyer une autorité plus importante à leurs techniciens en ce qui a trait aux accès dans l'entreprise (de façon à ce qu'ils puissent déterminer qui fait quoi, quand, comment et pourquoi).

Qui plus est, il peut sembler que les professionnels de l'informatique crient constamment aux loups, que ce soit par mémos ou durant les conversations et les rencontres, alors qu'ils ne font qu'être réalistes quant aux dangers qui guettent leur entreprise.

Que peuvent donc faire les professionnels de l'informatique lorsqu'ils n'ont pas les ressources nécessaires pour contrecarrer les plans des pirates et atténuer les dégâts et le chaos que peuvent entraîner les utilisateurs finaux malveillants ou négligents? Quels arguments peuvent-ils faire valoir pour définitivement convaincre leurs collègues que d'investir dans une défense informatique robuste est une valeur sûre ?

Pour répondre à ces questions des plus vitales, nous recommandons aux professionnels de l'informatique de se concentrer sur cinq éléments essentiels lorsqu'ils effectuent des demandes, émettent des propositions ou font des présentations :

1. Une sécurité informatique robuste renforce et maintient le lien de confiance avec le client

Selon Warren Buffet, PDG de Berkshire Hathaway, « il faut vingt ans pour se bâtir une réputation, alors que cinq minutes suffisent pour la ruiner ». Rappelons-nous que :

- Plus de 80 % des consommateurs considèrent la confiance comme un facteur déterminant de leurs décisions d'achat.
- 88 % d'entre eux disent que la confiance est encore plus importante en temps troubles (comme en ce moment!).
- 70 % des consommateurs veulent être rassurés que la protection des données est une priorité dans les entreprises avec lesquelles ils font des affaires.

Le message que doivent transmettre les professionnels de l'informatique est le suivant : dédier plus de ressources à la sécurité informatique n'est pas seulement un enjeu technique. Il s'agit plutôt d'une question fondamentale à l'installation et au maintien de la confiance avec les clients, ce qui en fait un enjeu d'affaires.

Effectivement, les entreprises qui sont considérées comme peu fiables en raison de leur négligence en ce qui a trait à la sécurité informatique se voient forcées d'investir des sommes faramineuses pour s'en sortir. Bien entendu, cette méthode est bien plus coûteuse que de se munir d'une sécurité informatique robuste dès le début.

2. La conformité exige une sécurité informatique robuste

Nous venons de remarquer que de nombreux clients ne feront plus affaire avec des entreprises qui ne réussissent pas à renforcer proactivement leur sécurité informatique (même si ces mêmes clients n'ont pas été affectés directement par une attaque).

En revanche, il existe aussi des clients qui refuseront catégoriquement de faire affaire avec une compagnie qui ne dispose pas d'une infrastructure de sécurité informatique, ainsi que d'une gouvernance et des contrôles évalués et certifiés par un tiers. À cet effet, il existe de nombreux programmes et normes de conformité, tels que :

- SOC 2
- ISO 27001:2013
- PCI DSS
- HIPAA

Puisque laisser des profits et des revenus sans protection est l'une des principales causes d'insomnie chez les patrons, un message concret de sensibilisation à la sécurité informatique peut provoquer un changement de paradigme. Paradigme selon lequel la sécurité informatique cesse d'être perçue comme une inévitable dépense et pour revêtir les atours d'un investissement profitable. Une sécurité informatique robuste agrandit le marché pour inclure plus de clients, alors qu'une sécurité informatique faible le circonscrit, en plus d'affaiblir les entreprises par rapport à leurs compétiteurs.

3. Une sécurité informatique robuste comme condition préalable pour les assureurs

Cette tendance connaît une croissance inouïe depuis quelques années. Les entreprises qui se sont munies d'une assurance en cybersécurité découvrent, lorsqu'elles renouvellent leurs polices d'assurance, que les assureurs exigent des contrôles de sécurité informatique robustes, en particulier en matière de gestion des accès privilégiés (PAM).

Mais qu'en est-il des professionnels de l'informatique travaillant au sein d'entreprises qui ne disposent pas d'assurances en cybersécurité? Ou dont l'assureur n'exige pas encore une sécurité informatique robuste? Eh bien, ils peuvent toujours mentionner cette tendance pour soutenir leurs arguments. Ils peuvent dire, par exemple : « Si un nombre croissant de compagnies d'assurance, lesquelles sont extrêmement pragmatiques, sont si préoccupées par les coûts qu'entraîne une fuite ou une violation de données, alors ne devrions-nous pas l'être également? ».

4. Une sécurité informatique robuste envoie un message clair aux employés

Qu'ils se fassent piéger par des courriels d'hameçonnage, partagent leurs mots de passe, perdent leurs ordinateurs portables, etc., les utilisateurs ont toujours constitué (et constitueront toujours) le maillon faible de la sécurité informatique.

Une PME qui investit dans la sécurité informatique de façon responsable et appropriée envoie un message clair à ses employés : « Nous prenons la sécurité informatique au sérieux ici, et nous vous demandons d'en faire de même ».

Une PME qui néglige cet aspect sera confrontée à des utilisateurs récalcitrants face à de nouvelles pratiques de sécurité informatique. Et pour cause! Les utilisateurs ne sont pas dupes et verront bien que l'entreprise ne pratique pas ce qu'elle prêche.

5. Une sécurité informatique robuste l'est également sur le plan éthique

Les professionnels de l'informatique devraient aider les dirigeants et décideurs à réaliser que d'investir dans la sécurité informatique n'est pas seulement une bonne stratégie; c'est la bonne stratégie. Ce n'est pas qu'une simple question de rognage de coûts. C'est aussi l'occasion d'être une entreprise éthique et socialement responsable.

Les PME qui mènent le bal en matière de sécurité informatique peuvent se vanter de « travailler selon leurs valeurs ». Gardons à l'esprit que chaque fois qu'une entreprise responsable renforce ses mesures de sécurité, les pirates et les utilisateurs malveillants reculent!

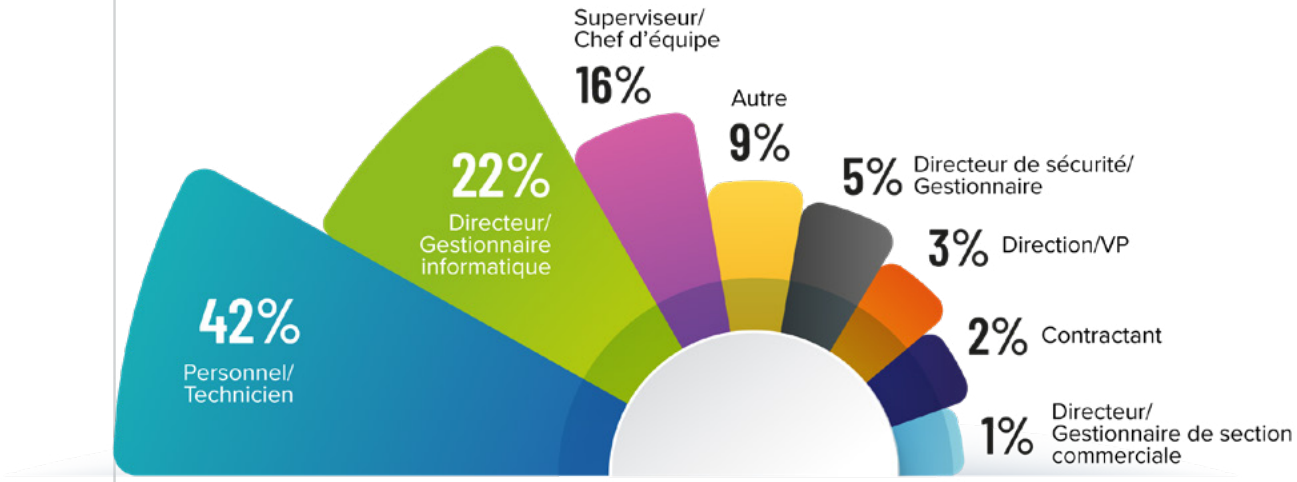
Autres conseils

Dans le cadre de leurs efforts pour convaincre leurs collègues, les professionnels de l'informatique devraient se rappeler des conseils suivants :

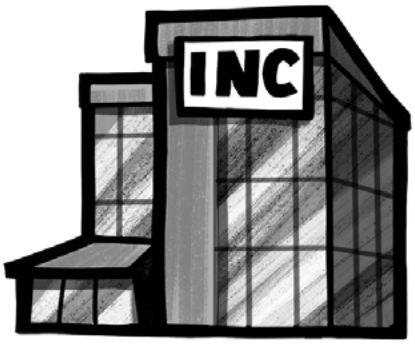
- Détailler les risques et l'impact d'une violation de données. Une simulation d'attaque par rançongiciel, par exemple, peut s'avérer très convaincante pour certains décideurs.
- Employer un langage simple et éviter le jargon. Bien qu'ils puissent être familiers pour de nombreux responsables de la sécurité de l'information et directeurs de la technologie, certains termes demeurent décidément obscurs pour bien des PDG et directeurs financiers.
- Lorsque possible, exprimer les risques par des chiffres (ex. : « Ce type de violation de données coûterait, en nous basant sur des données issues d'entreprises comparables dans notre secteur d'activité, 1,25 million de dollars en frais d'enquête et de récupération »), plutôt que d'instiller la crainte de dangers abstraits (ex. : « Ce type de violation est perpétrée par des pirates par le biais de courriels infectés »).
- Préparer une proposition de budget de sécurité ainsi qu'une liste détaillée d'outils, de technologies, de formations, de personnel, etc.
- Lors de l'évaluation d'outils et de technologies, utiliser les essais gratuits pour vérifier sa convivialité, sa sécurité, sa flexibilité, son extensibilité, etc.
- Travailler avec des vendeurs qui se spécialisent dans le service aux PME et peuvent démontrer ce qui suit :
    - Leurs solutions sont abordables et répondent aux exigences des affaires.
    - L'implémentation de leurs solutions est simple et rapide.
    - Ils fournissent des services de soutien technique exceptionnels.
    - Ils aident les PME à se concentrer sur des aspects cruciaux de leur sécurité, plutôt que d'offrir des options de moindre importance.
    - Ils aident les PME à obtenir plus pour moins cher.

PARTIE 7
PROFIL DES RÉPONDANTS

Quel titre décrit le mieux votre position au sein de l'organisation ?

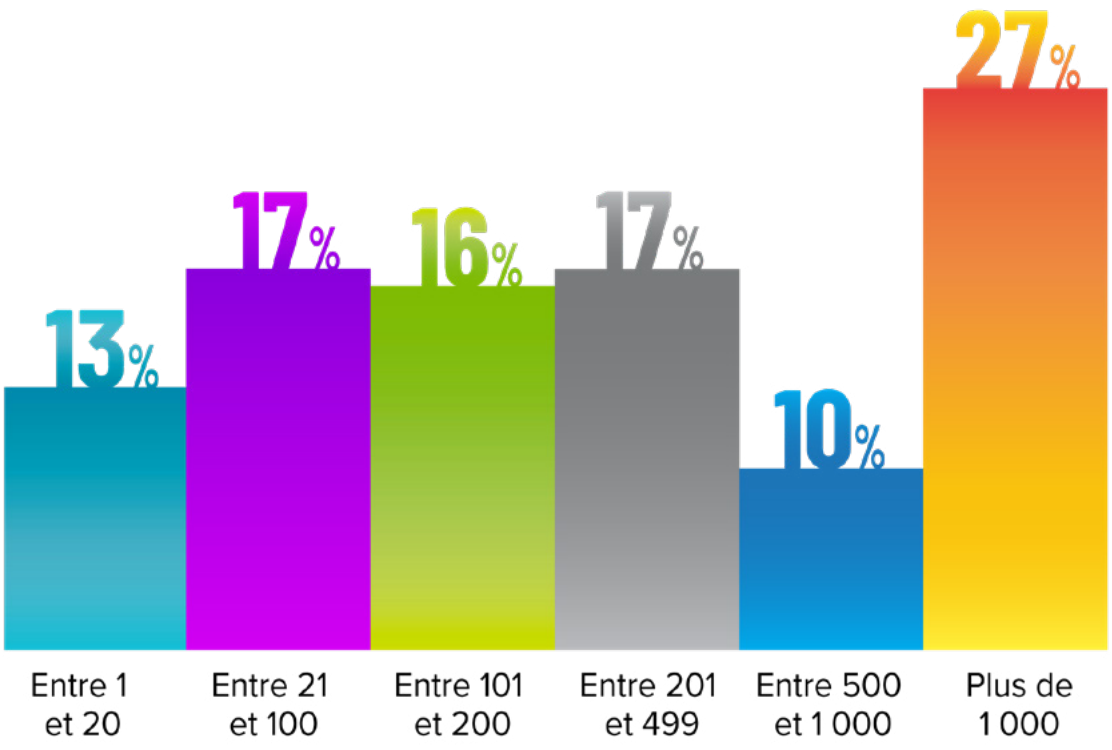


Quel secteur d'activité correspond le plus à votre entreprise ?

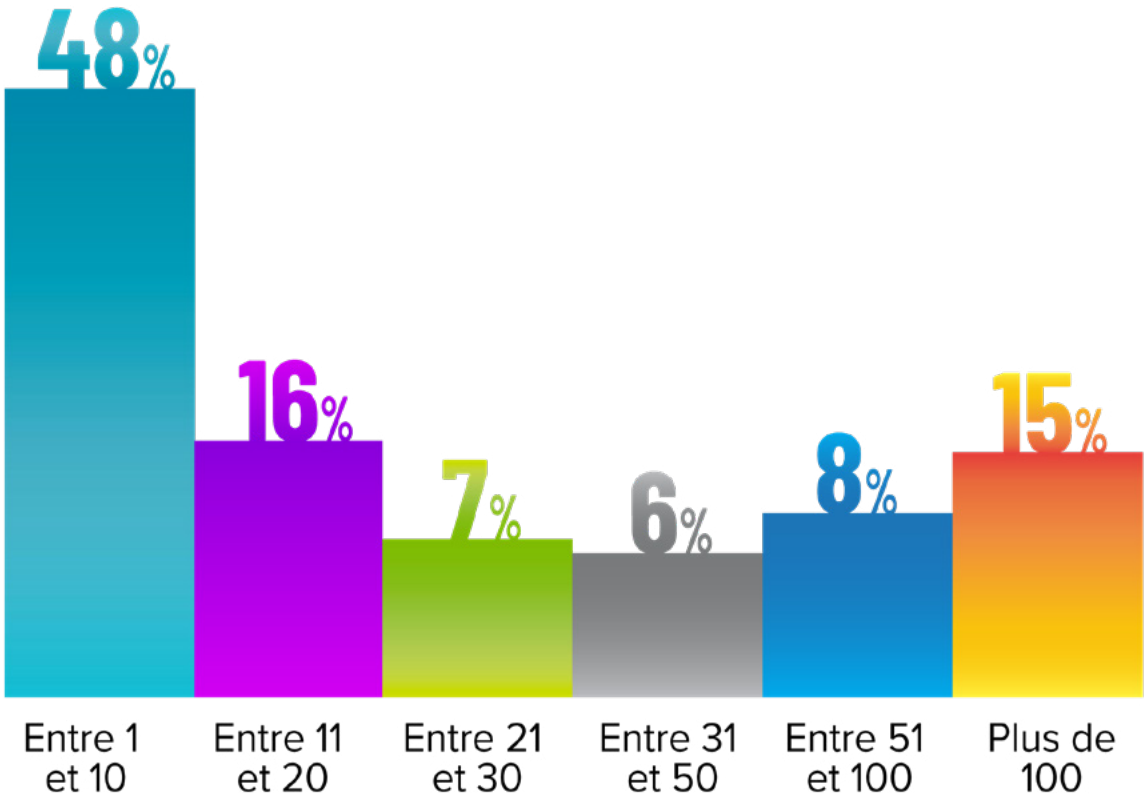


- 29% Services informatiques
- 12% Le secteur manufacturier
- 9% Finance et assurance
- 9% Technologie
- 5% Éducation
- 5% Gouvernement
- 3% Services généraux aux entreprises
- 3% Santé
- 3% Pétrole et énergie
- 3% Vente au détail
- 2% Communications
- 2% Sécurité des ordinateurs et des réseaux
- 2% Construction
- 2% Service à la clientèle
- 2% Divertissement
- 2% Sécurité, technologie de défense et infrastructure
- 2% Services publics
- 1% Mode et habillement
- 1% Transport
- 3% Autre

Combien de gens votre organisation emploie-t-elle à travers le monde ?



Combien d'employés travaillent dans le département informatique ?



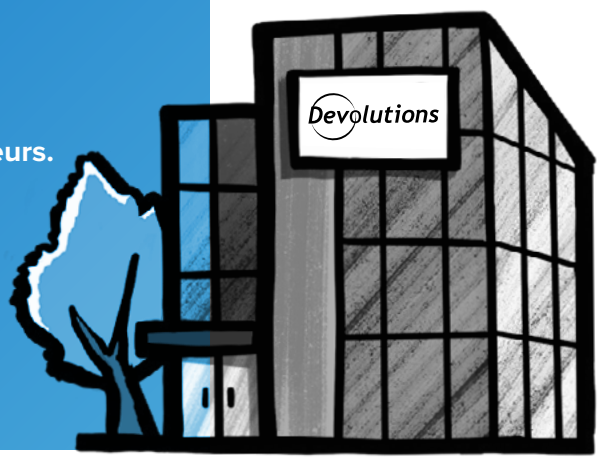
Devolutions

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! Nous appelons cela la **« gestion universelle des mots de passe et des accès pour le reste d'entre nous »!**

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 de l'informatique 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/