RAPPORT SPÉCIAL SUR LA CYBERSÉCURITÉ

DES PETITES ET MOYENNES ENTREPRISES

Petites et puissantes

Comment les petites et les moyennes entreprises peuvent renforcer leurs défenses contre les menaces actuelles

CISCO

53 % des entreprises de taille moyenne ont connu une brèche de sécurité

jusqu'à

5 000

Nombre moyen d'alertes de sécurité

Les entreprises de taille moyenne enquêtent sur 55,6 % des alertes de sécurité

29 % des entreprises de taille moyenne affirment que les brèches de sécurité leur coûtent moins que 100 000 $. 20 % d'entre elles affirment que leurs coûts associés aux brèches de sécurité se situent entre 1 000 000 $ et 2 499 999 $

De nombreuses petites et moyennes entreprises aspirent à des pratiques plus efficaces en matière de cybersécurité, semblables à celles de leurs homologues de plus grande taille. Les petites et moyennes entreprises (PME) sont dynamiques. Elles sont aux premières loges de l'innovation et constituent le symbole même du travail acharné. Elles travaillent à un rythme bien plus rapide et soutenu que leurs pendants de plus grande taille. Et elles font face aux mêmes menaces de cybersécurité.

Dans le paysage actuel des cybermenaces, chaque organisation, grande ou petite, est vulnérable aux cyberattaques. Mais de plus en plus, les PME sont ciblées par des attaques[1] et servent souvent de tremplin ou d'intermédiaire pour des assauts de plus grande envergure. Les cybercriminels perçoivent les PME comme des cibles faciles dotées d'infrastructures et de protocoles de sécurité moins évolués, et possédant un nombre insuffisant d'employés qualifiés pour prévenir les menaces et y répondre.[1]

De nombreuses PME commencent à peine à réaliser à quel point elles sont intéressantes pour les cybercriminels. Souvent, cette prise de conscience survient trop tard, soit après une attaque. Se remettre d'une cyberattaque peut être difficile et onéreux – et parfois impossible – pour ces entreprises, selon la nature et l'ampleur de l'attaque. Ce rapport donnera une compréhension des risques auxquels sont confrontées les plus petites organisations, partagera des renseignements sur les comparaisons entre les plus petites organisations et leurs paires en matière de sécurité, et offrira quelques conseils à garder en tête pour 2018 et après.

Examinez cette conclusion provenant de l'étude comparative de 2018 sur les capacités en matière de sécurité, effectuée par Cisco : plus de la moitié (54 %) de toutes les cyberattaques entraînent des pertes financières de plus de 500 000 $ US, y compris, mais sans s'y limiter, une perte de recettes, de clients et d'occasions d'affaires, ainsi que des coûts directement reliés aux attaques en tant que telles. Ce montant est suffisant pour mettre fin aux activités d'une PME qui n'est pas préparée à de telles attaques, et de manière permanente.

Une étude récente menée par le Better Business Bureau (BBB)[2] aide à comprendre comment il peut être difficile financièrement pour une PME de survivre à une grave cyberattaque. Le BBB a demandé aux propriétaires des petites entreprises en Amérique du Nord : « Combien de temps est-ce que votre entreprise demeurerait rentable si vous perdiez de manière permanente l'accès à vos données essentielles? » Seulement qu'environ un tiers (35 %) des répondants ont affirmé qu'ils pourraient demeurer rentables pendant plus de trois mois. Plus de la moitié des répondants ont indiqué qu'ils deviendraient déficitaires en moins d'un mois.

En passant, nous considérons comme petites les entreprises comptant moins de 250 employés, et comme moyennes celles qui comptent entre 250 et 499 employés. Les deux types d'entreprises sont inclus dans ce rapport.

Nous analysons les conclusions transmises par les répondants des PME à notre étude comparative de 2018 sur les capacités en matière de sécurité, que nous appellerons plus simplement notre étude comparative. Elle offre un aperçu sur les pratiques de sécurité utilisées actuellement, et compare l'ensemble des résultats à ceux obtenus au cours des trois dernières années.

Nos données sur les PME et le marché intermédiaire regroupent 1 816 répondants répartis dans 26 pays.

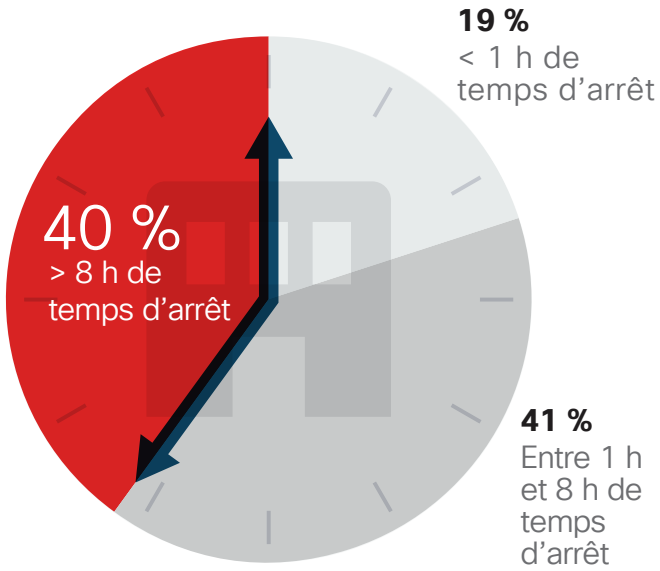
1 Cyberthreats and Solutions for Small and Midsize Businesses, Vistage Research Center, 2018. Créé en collaboration avec Cisco et le National Center for the Middle Market. Disponible à l'adresse : https://www.vistage.com/research-center/business-operations/risk-management/20180503-22912/.
2 2017 State of Cybersecurity Among Small Businesses in North America, BBB, 2017 : https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf.

Une journée de travail perdue entre collègues? Aucun problème

Aucun administrateur des TI ne dira jamais ça. Les temps d'arrêt du système, qui viennent saper la productivité et la rentabilité de l'entreprise, sont un problème important pour les entreprises à la suite une cyberattaque. Une recherche de l'étude comparative a révélé que 40 % des répondants (entre 250 et 499 employés) avaient subi huit heures ou plus de temps d'arrêt du système en raison d'une grave brèche de sécurité au cours de l'année dernière (Figure 1). Cisco a constaté des résultats similaires pour les grandes entreprises faisant partie de l'échantillon étudié (celles comptant 500 employés ou plus). La différence, toutefois, est que les organisations de plus grande taille ont tendance à être plus résilientes que les PME à la suite d'une cyberattaque, car elles ont plus de ressources pour y répondre et s'en remettre.

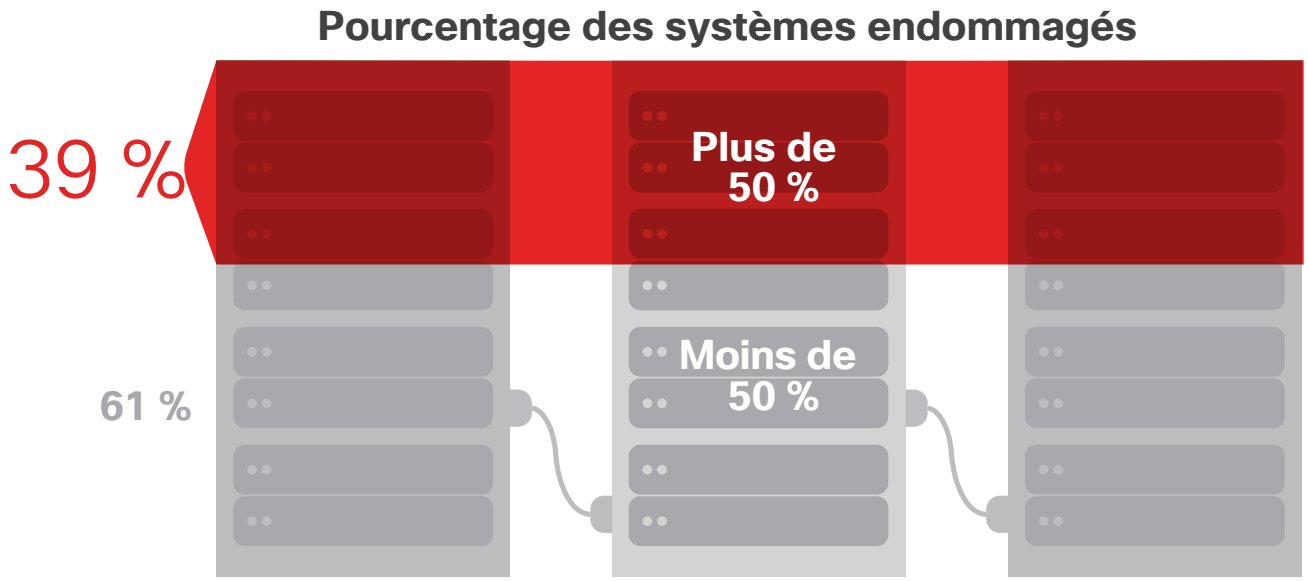
Également, 39 % des répondants ont affirmé qu'au moins la moitié de leurs systèmes avaient été touchés par une grave brèche de sécurité. Il est moins probable que les petites entreprises aient plusieurs sites ou secteurs d'activités, et leurs systèmes centraux sont généralement plus interconnectés. Lorsque ces organisations subissent une cyberattaque, la menace peut se propager rapidement et facilement aux autres systèmes à partir du réseau.

Figure 1 Temps d'arrêt du système à la suite d'une grave brèche



Source : Étude comparative 2018 de Cisco sur les fonctionnalités de sécurité

Figure 2 Pourcentage des systèmes touchés par une grave brèche de sécurité



Source : Étude comparative 2018 de Cisco sur les fonctionnalités de sécurité

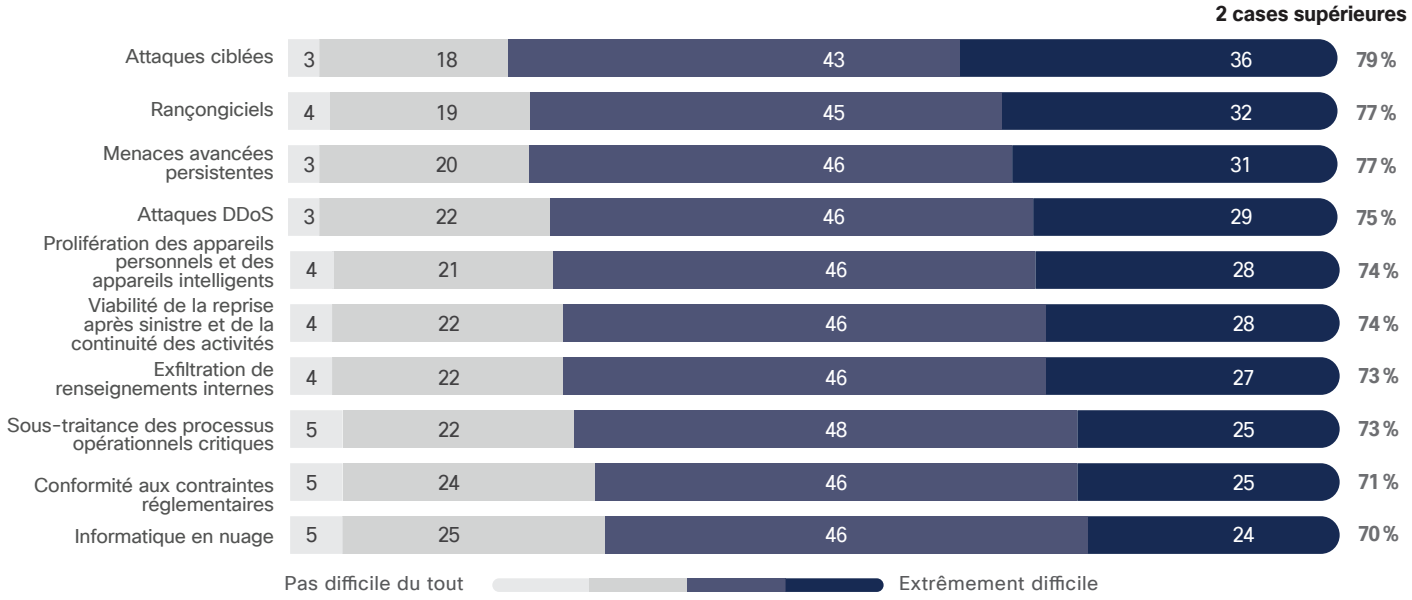
Nuits d'insomnie pour cause de cybersécurité

À la question concernant les plus grands défis de cybersécurité auxquels ils doivent faire face, les personnes interrogées ont répondu être davantage préoccupées par ces trois attaques potentielles :

- Des attaques ciblées contre les employés (comme un hameçonnage bien conçu)
- Des menaces avancées persistantes (comme des programmes malveillants jamais vus auparavant)
- Des rançongiciels

Les rançongiciels (qui, curieusement, ne sont pas cités comme étant l'une des trois principales préoccupations des grandes entreprises), sont, comme vous le savez sûrement maintenant, des programmes malveillants qui chiffrent des données, et ce, généralement jusqu'à ce que les utilisateurs touchés paient une rançon. Ces programmes malveillants peuvent également engendrer des perturbations et d'importants temps d'arrêt pour les petites et moyennes entreprises. Les rançongiciels sont également coûteux pour les organisations de cette taille, mais d'une manière différente : Les experts en sécurité de Cisco expliquent que les PME sont plus susceptibles de payer une demande de rançon aux cybercriminels, afin de reprendre rapidement leurs activités normales. Elles ne peuvent simplement pas se permettre les temps d'arrêt et l'incapacité d'accéder aux données importantes, y compris les données des clients. (Voir la figure 3.)

Figure 3 Les principales préoccupations pour les entreprises de taille moyenne[5]



Source : Étude comparative 2018 de Cisco sur les fonctionnalités de sécurité

Les autres menaces que les PME ne doivent pas ignorer

Malgré les soucis que causent les rançongiciels, les experts en sécurité de Cisco indiquent qu'il s'agit d'une menace dont l'importance va en décroissant, alors que de plus en plus de cybercriminels concentrent leurs activités sur le « cryptominage », soit le minage illicite de cryptomonnaie. L'attrait de cette activité criminelle est triple : elle peut être très lucrative, les paiements ne peuvent être retracés et les cybercriminels s'inquiètent donc moins de la responsabilité criminelle de leurs actions. (Par exemple, il n'y a aucun risque que des patients soient privés de soins essentiels parce que les systèmes et les données essentielles d'un hôpital sont verrouillés par un rançongiciel.) Les cybercriminels peuvent également envoyer des logiciels d'exploitation minière, des « mineurs », en utilisant diverses méthodes, notamment l'envoi par courriel de campagnes de pourriel et de trousses d'exploitation.[3]

3 Ransom Where? « Malicious Cryptocurrency Miners Takeover, Generating Millions », blogue de Cisco Talos, [3] janvier 2018 : https://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html.

Les chercheurs en cybermenace de Cisco expliquent que les acteurs malveillants utilisant le nouveau modèle d'affaires du cryptominage illicite « ne pénalisent plus de victimes pour avoir ouvert une pièce jointe ou n'utilisent plus de scripts malveillants prenant en otage des systèmes dans le but de faire une demande de rançon. Maintenant, ils tirent activement profit des ressources que représentent les systèmes infectés. »[4] Pour les PME contribuant à leur insu à des activités de cryptominage illicites, un ralentissement de leur système peut constituer le seul signal d'alarme indiquant qu'ils ont été victime d'une brèche de sécurité, à moins d'avoir en place la technologie adéquate pour détecter la présence d'activités de cryptominage.

Les menaces internes de l'ordre de 0,5 % : 100 % trop élevé?

À mesure que les entreprises répondantes transfèrent davantage de données et de processus vers le nuage, elles doivent également prendre des mesures visant à prévenir une autre menace potentielle : les travailleurs internes malveillants. Sans des outils pour détecter les activités suspectes (comme le téléchargement de renseignements confidentiels sur les clients), ces entreprises courent le risque de perdre des propriétés intellectuelles ainsi que des données confidentielles concernant leurs finances et leurs clients ayant été stockées dans le nuage.

Une enquête récente menée par les chercheurs en cybermenace de Cisco met l'accent sur les risques : de janvier à juin 2017, ils ont examiné les tendances d'exfiltration de données à l'aide de capacités d'apprentissage artificiel afin de dresser le profil de 150 000 utilisateurs de services infonuagiques, répartis dans 34 pays. Après un mois et demi d'examen, les chercheurs ont découvert que 0,5 % des utilisateurs avaient effectué des téléchargements suspects. Est-ce que la moitié d'un pour cent est un chiffre alarmant? Autrement dit, cela signifie que, pour une entreprise comptant 400 employés, deux d'entre eux seraient considérés comme des menaces internes. C'est 100 % trop élevé. Plus précisément, ces utilisateurs ont téléchargé à partir de systèmes d'infonuagique d'entreprise plus de 3,9 millions de documents au total. Cela représente une moyenne de 5 200 documents par utilisateur durant une période d'un mois et demi.[5]

Étude comparative 2018 de Cisco sur les fonctionnalités de sécurité

Ce rapport spécial présente certaines conclusions tirées de données provenant de l'étude comparative 2018 de Cisco sur les fonctionnalités de sécurité. L'étude a été menée auprès de plus de 3 600 répondants provenant de 26 pays. Pour obtenir plus d'information sur les pratiques de sécurité actuellement en cours d'utilisation par les entreprises de toutes tailles, et une comparaison des résultats avec les études précédentes de Cisco, téléchargez *l'étude comparative 2018 de Cisco sur les fonctionnalités de sécurité*, disponible à l'adresse https://www.cisco.com/c/en/us/products/security/security-reports.html.

4 Ibid.
5 Pour plus de détails, consultez a section « Insider threats: taking advantage of the cloud » dans l'étude comparative 2018 de Cisco sur les fonctionnalités de sécurité, disponible à l'adresse https://www.cisco.com/c/en/us/products/security/security-reports.html.

Défis

La meilleure défense contre les menaces décrites plus tôt nécessite la coordination et l'orchestration des ressources des TI. Ces ressources sont principalement le personnel, les processus et les technologies que les entreprises peuvent regrouper pour prévenir les attaques.

Cependant, de manière plus prononcée que les entreprises de grande taille, les petites entreprises doivent relever le défi de coordonner ces ressources de manière à fournir des indications sur les menaces et à stopper ou à atténuer les attaques avant qu'elles ne causent des dommages. Le manque perpétuel d'employés qualifiés en sécurité qui touche les grandes entreprises a des incidences encore plus grandes sur les entreprises de plus petite taille.

Tendances en matière de technologies de sécurité pour les PME

Continuant d'aller de l'avant, les organisations de plus petite taille cherchent réellement à relever les défis en matière de cybersécurité qui menacent leurs activités grâce aux nouveaux outils pouvant bloquer ces menaces.

Les répondants de l'étude comparative ont affirmé que, si la dotation en personnel n'était pas un problème, elles seraient plus susceptibles de :

- Mettre à niveau la sécurité de leurs points terminaux vers des protections plus perfectionnées contre les programmes malveillants. Cette réponse est la plus courante, à 19 %.
- Envisager de meilleures applications Web de sécurité pour contrer les attaques Web (18 %)
- Déployer des solutions de prévention d'intrusion, une technologie encore considérée comme essentielle pour contrer les attaques de réseau et les tentatives d'exploitation. (17 %) (Voir la figure 5.)

À mesure que les entreprises envisagent d'adopter de nouvelles technologies, un des défis est de déterminer la qualité de l'interopérabilité afin de protéger l'ensemble de leurs activités. La lourdeur de la tâche consistant à fouiller de nombreuses consoles afin de répondre aux menaces ou aux incidents de sécurité ne doit pas être sous-estimée.

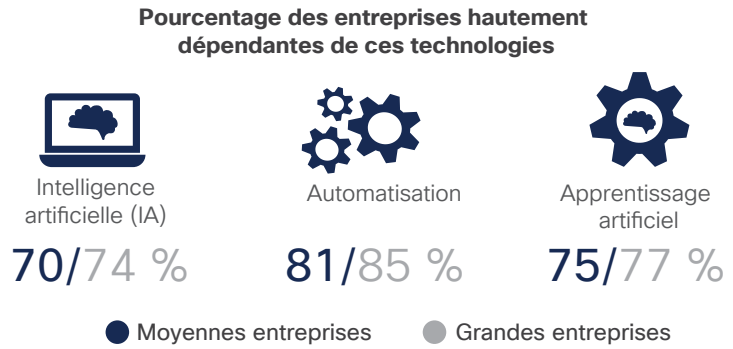
« De nombreuses personnes pensent que si elles font affaire avec un fournisseur multiservices avec une approche du "meilleur produit" , elles seront mieux protégées », affirme Ben M. Johnson, PDG de Liberty Technology, un partenaire de Cisco situé à Griffin en Géorgie. « Mais nous constatons que ce genre de service est plus difficile à gérer, est plus onéreux et diminue l'efficacité de la sécurité en général. »

Apprentissage artificiel : un atout en matière de sécurité ou la saveur du mois?

Nous avons tous entendu parler de l'apprentissage artificiel étant donné la récente médiatisation dont elle fait l'objet. Il s'avère que les entreprises de taille moyenne s'appuient dans la même mesure que les grandes entreprises sur les solutions d'analyse comportementale pouvant détecter de manière efficace les cyberattaques. Les entreprises de taille moyenne dépendent légèrement moins des solutions utilisant l'apprentissage artificiel et l'automatisation par rapport aux entreprises comptant plus de 1 000 employés (Figure 4).

L'apprentissage artificiel est plus efficace lorsqu'il constitue une couche supplémentaire de détection au sein d'un produit déjà déployé, plutôt que lorsqu'il consiste en un produit distinct visant à effectuer de « l'apprentissage artificiel. » De cette manière, les équipes profitent des avantages de l'apprentissage artificiel pour la détection des anomalies et des menaces à haute vitesse, sans ajouter une charge de travail à l'équipe.

Figure 4 Les entreprises de taille moyenne sont moins dépendantes de l'automatisation et des outils d'intelligence artificielle



Source : Étude comparative 2018 de Cisco sur les fonctionnalités de sécurité

Mobilité des entreprises de moyenne taille

Les entreprises reconnaissent également que leurs approches de sécurité doivent répondre aux exigences de l'environnement de travail moderne, en particulier la transition vers la mobilité et l'adoption des appareils cellulaires. 56 % des personnes interrogées ont affirmé que la défense des appareils cellulaires contre les cyberattaques est considérée comme un défi difficile ou extrêmement difficile.

Les entreprises de taille moyenne et l'infonuagique

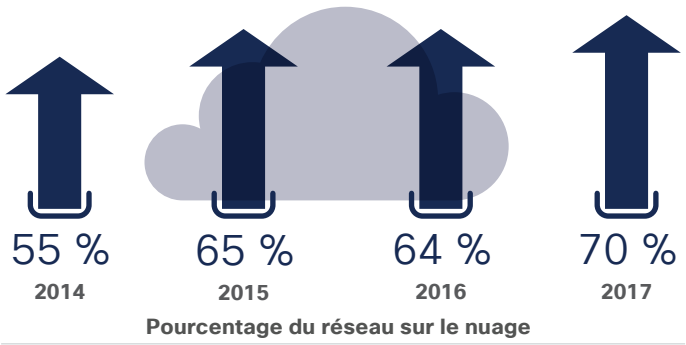
Conscients de leurs problèmes de sécurité, de nombreux répondants se tournent vers le nuage pour renforcer leurs défenses, sans ajouter de personnel ni mettre à rude épreuve les ressources existantes. La question est de savoir si le déplacement de la sécurité vers le nuage est une stratégie suffisante pour prévenir les attaques. En outre, les entreprises ne peuvent pas simplement se décharger de la responsabilité de la sécurité en transférant les données dans le nuage : elles doivent toujours connaître les contrôles de sécurité imposés par les fournisseurs de services dans le nuage ainsi que l'impact que des violations potentielles dans le nuage peuvent avoir sur les ressources sur place.

D'après les recherches de Cisco, l'adoption des services en nuage par les moyennes entreprises est clairement en hausse. En 2014, 55 % de ces entreprises ont déclaré héberger une partie de leurs réseaux dans une forme de nuage; en 2017, ce chiffre est passé à 70 % (figure 5).

De nombreux répondants croient que le nuage peut aider à combler certaines lacunes dans leurs défenses et à corriger certains manques dans leur infrastructure et dans les capacités de leur personnel. En fait, selon une étude de Cisco, la principale raison pour laquelle les moyennes entreprises hébergent des réseaux dans le nuage est la croyance que ce dernier offre une meilleure sécurité des données (68 %); la deuxième raison la plus populaire est que l'entreprise manque de travailleurs en TI à l'interne (49 %). (Voir la figure 6.)

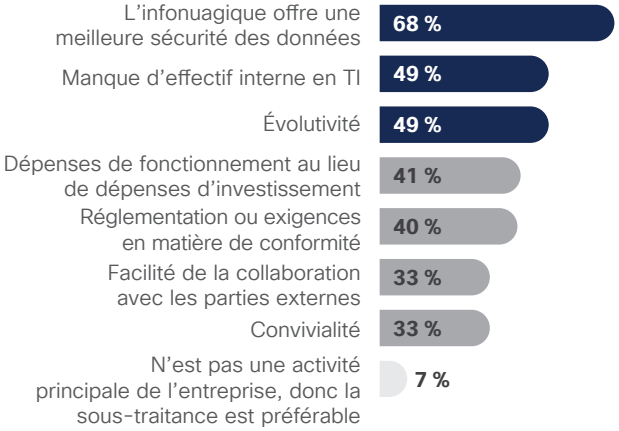
Les entreprises de taille moyenne favorisent elles aussi l'infonuagique en raison de son évolutivité, c'est-à-dire la possibilité de réduire la dépendance d'une entreprise à ses ressources internes et la transition souple vers des dépenses de fonctionnement plutôt que des dépenses d'investissement (Figure 6).

Figure 5 Les entreprises de taille moyenne affichent une hausse constante de l'adoption de l'infonuagique



Source : Étude comparative 2018 de Cisco sur les fonctionnalités de sécurité

Figure 6 Les entreprises de taille moyenne choisissent l'infonuagique pour sa sécurité et son efficacité



Source : Étude comparative 2018 de Cisco sur les fonctionnalités de sécurité

Ressources humaines : trouver du personnel pour renforcer la sécurité

La bonne nouvelle est que l'étude comparative montre que 92 % des entreprises de taille moyenne ont un cadre supérieur responsable de la sécurité (voir la figure 7.)

Avec des ressources en personnel suffisantes, les entreprises de taille moyenne seraient prêtes à ajouter davantage d'outils de sécurité tels que des protections évoluées de points d'accès ou des pare-feu pour les applications Web.

Les entreprises de taille moyenne ont un point en commun avec les entreprises de plus grande taille : une pénurie en personnel de TI faisant obstacle à la capacité de consolider les défenses. Selon une étude de Cisco, il n'y a tout simplement pas assez de gens à l'interne pour gérer les outils qui pourraient améliorer la sécurité.

Pour cette raison, de nombreuses PME font appel à la sous-traitance pour rassembler les talents dont ils ont besoin pour augmenter leurs connaissances en matière de menaces, pour économiser de l'argent et pour réagir plus rapidement aux brèches de sécurité. Le désir d'obtenir des renseignements impartiaux était la raison la plus courante donnée par les entreprises de taille moyenne pour offrir en sous-traitance leurs besoins en sécurité (figure 8), suivie par le rapport coût-efficacité et la nécessité de réagir rapidement aux incidents de sécurité.

L'aide obtenue par sous-traitance est un bon moyen pour les entreprises de tirer le meilleur parti de leurs ressources limitées. Mais ces entreprises peuvent se heurter à des difficultés si elles supposent qu'un fournisseur de services externes ou un partenaire en infonuagique fournira toutes les fonctionnalités dont elles ne disposent pas à l'interne.

Chad Paalman, PDG de NuWave Technology Partners à Kalamazoo au Michigan, un partenaire Cisco, révèle que de nombreuses PME ne sont pas au courant de la portée (ou de l'absence de portée) des services d'analyse et de surveillance que leur offre leur fournisseur externe de services de sécurité.

Figure 7 Cadres supérieurs responsables de la sécurité dans les entreprises de taille moyenne

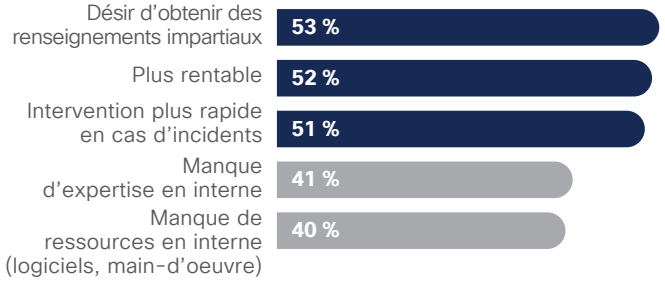
92 %
des entreprises ont un cadre supérieur responsable de la sécurité

Titre du cadre supérieur responsable de la sécurité

42 %	Directeur de la sécurité des systèmes d'information
24 %	Responsable de la sécurité
10 %	Président-directeur général (PDG)
8 %	Directeur des systèmes d'information
3 %	Directeur des systèmes d'information
5 %	Directeur des technologies
6 %	Vice-président directeur ou vice-président au service informatique
2 %	Directeur des risques ou directeur de la conformité

Source : Étude comparative 2018 de Cisco sur les fonctionnalités de sécurité

Figure 8 Les entreprises de taille moyenne utilisent de l'aide en sous-traitance le problème de manque de ressources à l'interne



Source : Étude comparative 2018 de Cisco sur les fonctionnalités de sécurité

« Plusieurs chefs d'entreprise connaissent mal leurs réseaux. Ils tiennent pour acquis qu'un pare-feu est suffisant pour empêcher les brèches de sécurité. Ils supposent également que si leurs besoins en sécurité ont été donnés en sous-traitance à un fournisseur de services gérés, la surveillance de connexion et la détection d'intrusion sont assurées. »

Chad Paalman, PDG de NuWave Technology Partners

La conclusion cependant est que les PME comptent sur leurs partenaires externes pour leur fournir :

- des services-conseils externes (57 %);
- des services de gestion des incidents (54 %);
- de la surveillance de sécurité (51 %).

Cependant, ils sont moins enclins à donner en sous-traitance certaines tâches comme la vigie des menaces (39 %) (voir la figure 9.)

La bonne nouvelle, c'est que les moyennes entreprises semblent mettre de côté une partie de leurs ressources limitées pour comprendre les menaces et y réagir, par exemple en renforçant les renseignements sur les menaces et la gestion des incidents.

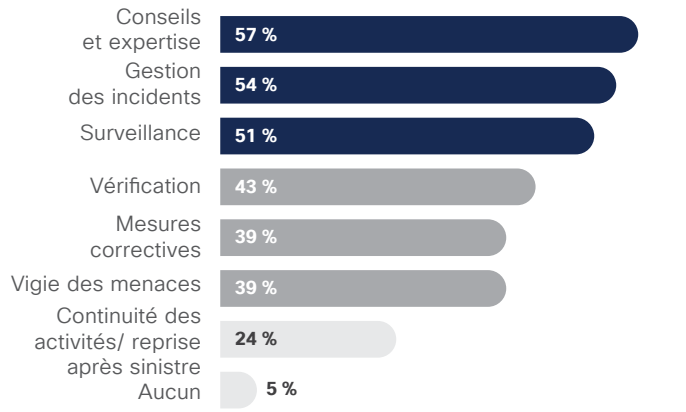
Processus : vérifications régulières pour gérer la sécurité

Des processus de sécurité complets et réguliers – tels que les contrôles des biens de grande valeur et l'examen des pratiques de sécurité – aident les organisations à identifier les faiblesses de leurs défenses en matière de sécurité. De tels processus ne sont pas aussi répandus dans les petites et moyennes entreprises qu'ils le devraient, peut-être en raison du manque de personnel.

Par exemple, selon l'étude comparative 2018 de Cisco sur les fonctionnalités de sécurité, les moyennes entreprises sont moins susceptibles que les grandes entreprises de dire qu'elles examinent régulièrement leurs pratiques de sécurité, qu'elles ont des outils en place pour examiner leurs capacités de sécurité et qu'elles font régulièrement enquête sur les incidents de sécurité (figure 10).

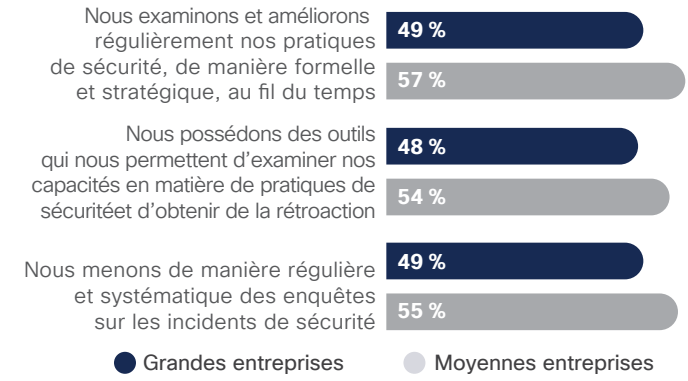
Sur une note positive, 91 pour cent des moyennes entreprises ont déclaré qu'elles organisent des exercices pour tester leurs plans de gestion des incidents au moins une fois par an. Cependant, comme dans le cas de leur dépendance à l'égard du nuage et des partenaires en sous-traitance, la question est de savoir si ces plans de gestion des incidents sont adéquats pour repousser des attaquants de plus en plus sophistiqués.

Figure 9 Les moyennes entreprises externalisent des services de conseil et d'expertise



Source : Étude comparative 2018 de Cisco sur les fonctionnalités de sécurité

Figure 10 Les moyennes entreprises externalisent des services de conseil ainsi que la gestion des incidents et d'expertise ainsi que la gestion des incidents



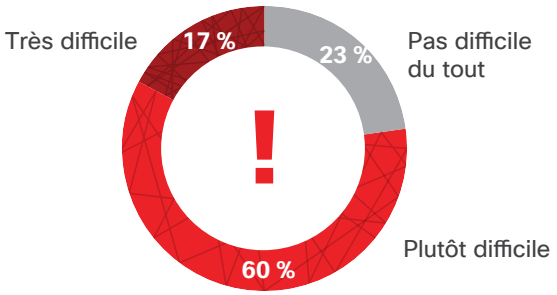
Connecter les personnes, les processus et la technologie : le défi de l'orchestration

Si les petites et moyennes entreprises ajoutent plus de produits de sécurité et de fournisseurs à leurs défenses – et déplacent leurs ressources informatiques vers la gestion de ces produits – leurs organisations pourront-elles mieux gérer la sécurité? L'inverse peut être vrai, du moins en ce qui concerne la compréhension et l'orchestration des alertes de sécurité.

La plupart des petites et moyennes entreprises reconnaissent aujourd'hui qu'à mesure qu'elles créent un environnement de produits et de fournisseurs plus complexe, leurs responsabilités augmentent. Par exemple, 77 pour cent des moyennes entreprises ont trouvé difficile ou très difficile d'orchestrer des alertes à partir de ces nombreuses solutions (figure 11).

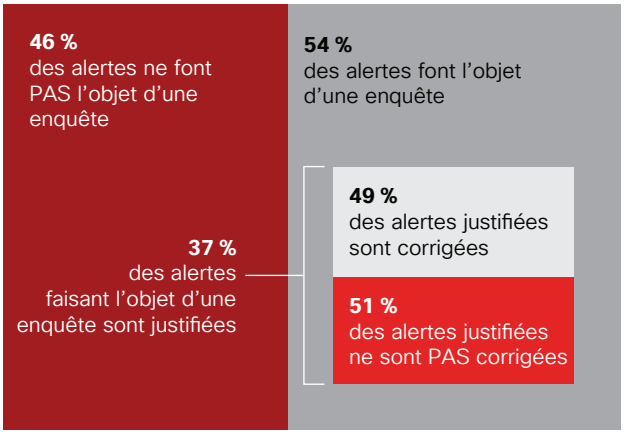
Lorsque les entreprises tentent d'analyser ces alertes, les défis combinés qui entourent les personnes, les processus et la technologie peuvent faire en sorte que de nombreuses alertes ne fassent pas l'objet d'une enquête, comme le montre l'étude comparative (figure 12) :

Figure 11 Les moyennes entreprises sont moins susceptibles d'être tout à fait d'accord avec l'énoncé sur l'utilisation des processus opérationnels



Source : Étude comparative 2018 de Cisco sur les fonctionnalités de sécurité

Figure 12 Pourcentage d'alertes de sécurité qui ne font pas l'objet d'une enquête



Source : Étude comparative 2018 de Cisco sur les fonctionnalités de sécurité

Recommandations pour l'avenir

Technologies

Lorsque les organisations envisagent de nouveaux outils, idéalement, elles peuvent éviter d'ajouter des fournisseurs et de générer encore plus d'alertes.

En gardant cela à l'esprit, les produits sont-ils construits dans un esprit d'ouverture? Comment s'intégreront-ils aux autres en ce qui concerne le partage de données et d'informations sur les menaces? Existe-t-il une intégration avec la console de gestion?

Si un fournisseur dit que les produits sont conçus pour s'adapter et fonctionner avec d'autres, est-ce que cela est vrai dès le début ou l'acheteur devra-t-il faire un travail considérable avec des API?

L'apprentissage artificiel, bien que faisant l'objet d'un battage publicitaire, a sa place dans la sécurité. Cependant, il vaut mieux rechercher des capacités d'apprentissage artificiel conçues comme une couche de détection à l'intérieur de produits déjà déployés plutôt que comme des produits autonomes d'autres fournisseurs qui s'ajoutent au nombre de ceux que vous devez gérer.

Personnes et processus

En clair, élaborez une stratégie pour améliorer la cybersécurité. Selon le Vistage Research Center, un centre de ressources pour les chefs d'entreprise, seulement 38 % des petites et moyennes entreprises ont mis en place une stratégie active en matière de cyberrisque.[6]

Votre planification inclut-elle une formation appropriée des utilisateurs finaux? Vos polices d'assurance couvrent-elles les pertes d'affaires découlant d'une cyberattaque? Pourquoi ne pas créer un plan de continuité des activités et de communication afin d'accélérer la reprise et de contribuer à éviter les dommages à la réputation de l'entreprise.

En outre, les responsables informatiques doivent expliquer en termes clairs ce que la direction de l'entreprise veut vraiment savoir en ce qui concerne les brèches :

- quel est l'impact sur l'organisation.
- quelles mesures l'équipe de sécurité prend pour enquêter sur la menace et la contenir. Le temps qu'il faudra pour reprendre les opérations normales.[7]

« En adoptant un ensemble de plateformes et d'outils de sécurité qui fonctionnent tous ensemble, plutôt que des éléments disparates qui peuvent entrer en conflit les uns avec les autres, vous obtenez une amplification de l'efficacité de la sécurité, ainsi qu'une simplification de la gestion. »

Ben M. Johnson, PDG de Liberty Technology

« Les petites et moyennes entreprises devraient évaluer ces risques et élaborer des plans d'intervention avant une brèche, et non après. »

Chad Paalman, NuWave Technology Partners

6 Cyberthreats and Solutions for Small and Midsize Businesses, Vistage Research Center, 2018. Créé en collaboration avec Cisco et le National Center for the Middle Market. Disponible à l'adresse : https://www. vistage.com/research-center/business-operations/risk-management/20180503-22912/.

7 Rapport semestriel sur la cybersécurité de Cisco 2017 : https://www.cisco.com/c/dam/global/es_mx/solutions/security/pdf/cisco-2017-midyear-cybersecurity-report.pdf. 13 Ibid.

Conclusion

Une dernière recommandation à l'intention des petites et moyennes entreprises pour améliorer la cybersécurité est de reconnaître que le changement progressif est préférable à l'absence de changement. Bref, ils ne doivent pas laisser le désir d'être « parfaits » dans leur approche de la sécurité les empêcher de devenir « meilleurs ». La perfection, comme en toute chose, n'existe pas.

Les petites et moyennes entreprises doivent également comprendre qu'il n'existe pas de solution technologique « miracle » pour résoudre tous leurs problèmes de cybersécurité. Le paysage des menaces est trop complexe et trop dynamique. La surface d'attaque est toujours en expansion et en évolution. Et, en réponse, les technologies et les stratégies de sécurité doivent aussi continuellement évoluer.

Pour en apprendre davantage à propos de l'approche de Cisco fondée sur les menaces en matière de sécurité, visitez le cisco.com/go/security.

Siège social aux États-Unis
Cisco Systems, Inc.
San Jose, Californie

Siège social d'Asie-Pacifique
Cisco Systems (USA) Pte. Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam,
Pays-Bas

Cisco compte plus de 200 bureaux à l'échelle mondiale. Les adresses, numéros de téléphone et numéros de télécopieur sont répertoriés sur le site Web de Cisco, à l'adresse www.cisco.com/go/offices.

Publié en juillet 2018

© Cisco ou ses sociétés affiliées, 2018. Tous droits réservés.

Cisco et le logo Cisco sont des marques de commerce ou marques de commerce déposées de Cisco ou de ses filiales aux États-Unis et dans d'autres pays. Pour consulter la liste des marques de commerce de Cisco, rendez-vous à l'adresse : www.cisco.com/go/trademarks. Les marques de commerce de tierces parties mentionnées appartiennent à leur détenteur respectif. L'utilisation du terme « partenaire » ne signifie pas nécessairement qu'il existe un partenariat entre Cisco et une autre entreprise. (1110R)

Adobe, Acrobat et Flash sont des marques de commerce déposées ou des marques de commerce d'Adobe Systems Incorporated aux États-Unis et dans d'autres pays.