RAPPORT SPÉCIAL SUR LA CYBERSÉCURITÉ

PME

Petit mais puissant

Comment les PME peuvent renforcer leur protection contre les menaces d'aujourd'hui

CISCO

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

Près de

5 000

Nombre moyen d'alertes liées à la sécurité

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

29 % des entreprises de taille moyenne déclarent que les failles de sécurité leur coûtent moins de 100 000 $. 20 % d'entre elles affirment qu'elles leur coûtent entre 1 000 000 $ et 2 499 999 $.

De nombreuses PME travaillent à atteindre les standards des grands groupes en matière de cybersécurité. De nature dynamique, les PME sont les moteurs de l'innovation. Elles évoluent encore plus vite et travaillent intensivement. Elles sont également exposées aux mêmes cybermenaces.

Dans le monde actuel, aucune entreprise, petite ou grande, n'échappe au risque de cyberattaque. Toutefois, les PME sont de plus en plus ciblées[1] et servent souvent aux hackers de tremplins ou de plates-formes de test avant de s'attaquer à des organisations de plus grande envergure. Les hackers voient dans les PME des cibles faciles dont l'infrastructure et les pratiques de sécurité sont moins sophistiquées et dont le manque de personnel qualifié ne permet pas de gérer ni de traiter efficacement les menaces.[1]

Beaucoup de PME commencent seulement à comprendre combien elles sont attrayantes aux yeux des cybercriminels. Bien souvent, ce constat a lieu trop tard, à savoir une fois qu'elles ont été affectées par une attaque. Selon la nature et l'ampleur de l'attaque, il peut être difficile et coûteux, voire impossible, pour ces entreprises de s'en remettre. Ce rapport présente les risques que courent les PME, compare leur approche de la sécurité par rapport à celle des grandes entreprises et fournit quelques conseils à prendre en compte pour les années futures.

Selon l'enquête Cisco 2018 sur l'efficacité des mesures de sécurité, plus de la moitié (54 %) du nombre total de cyberattaques a entraîné des pertes financières de plus de 500 000 dollars, notamment (mais pas uniquement) en raison d'une perte de chiffre d'affaires, de clients ou d'opportunités commerciales, et de coûts directs. Pour une PME mal préparée, un tel montant peut signifier la fermeture permanente de ses portes.

Une étude récente du Better Business Bureau (BBB)[2] souligne combien il peut être difficile pour ces sociétés de survivre à une cyberattaque sévère en raison des difficultés financières qu'elle implique. Le BBB a demandé aux gérants de PME en Amérique du Nord combien de temps leur entreprise pouvait rester rentable s'ils ne pouvaient plus accéder du tout aux données essentielles. À peine un peu plus d'un tiers (35 %) pourrait tenir plus de trois mois. Plus de la moitié ne pourrait pas tenir plus d'un mois.

Dans ce rapport, nous définissons une petite entreprise comme comptant moins de 250 collaborateurs, tandis qu'une entreprise de taille moyenne compte entre 250 et 499 employés. Ces deux types d'entreprises sont concernés par le rapport.

Nous y analysons les résultats recueillis auprès des personnes interrogées dans l'enquête Cisco 2018 sur l'efficacité des mesures de sécurité. Celle-ci offre un aperçu des pratiques de sécurité actuelles et compare les résultats complets à ceux des trois dernières années.

1 816 personnes réparties dans 26 pays ont participé à cette enquête sur les PME.

1 « Cyberthreats and Solutions for Small and Midsize Businesses », Vistage Research Center, 2018. 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/.

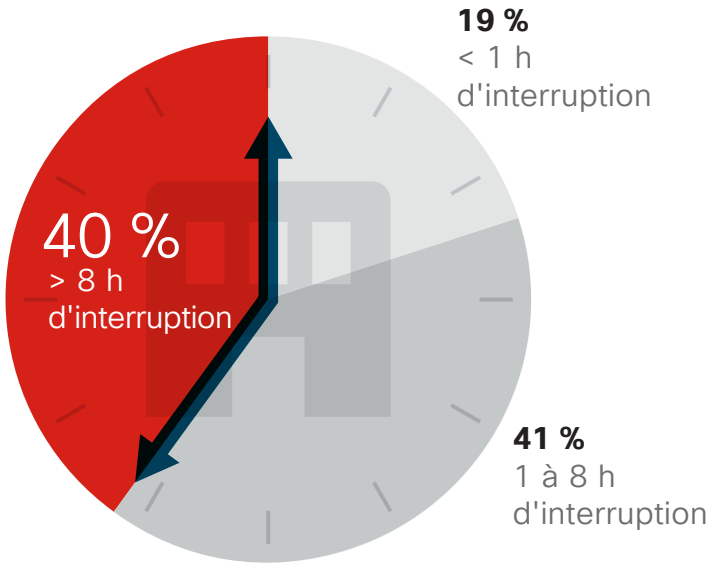
2 « 2017 State of Cybersecurity Among Small Businesses in North America », BBB, 2017 : https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf.

« Il n'y a pas de quoi en faire tout un plat... »

Voilà une expression qui ne viendrait sans doute pas à l'esprit d'un administrateur informatique en cas de panne système généralisée. Les interruptions du système, qui affectent la productivité et la rentabilité, représentent un problème majeur pour les entreprises après une cyberattaque. Selon notre enquête, 40 % des personnes interrogées (dans les sociétés de 250 à 499 employés) ont connu une interruption de système pendant au moins huit heures en raison d'une faille de sécurité grave au cours de l'année passée (Figure 1). Cisco a constaté des résultats similaires avec les grandes entreprises interrogées dans le cadre de l'enquête (sociétés de 500 employés ou plus). Toutefois, la différence est que les grandes entreprises ont tendance à mieux résister aux attaques que les PME, car elles disposent de plus de ressources pour gérer les incidents et restaurer le système.

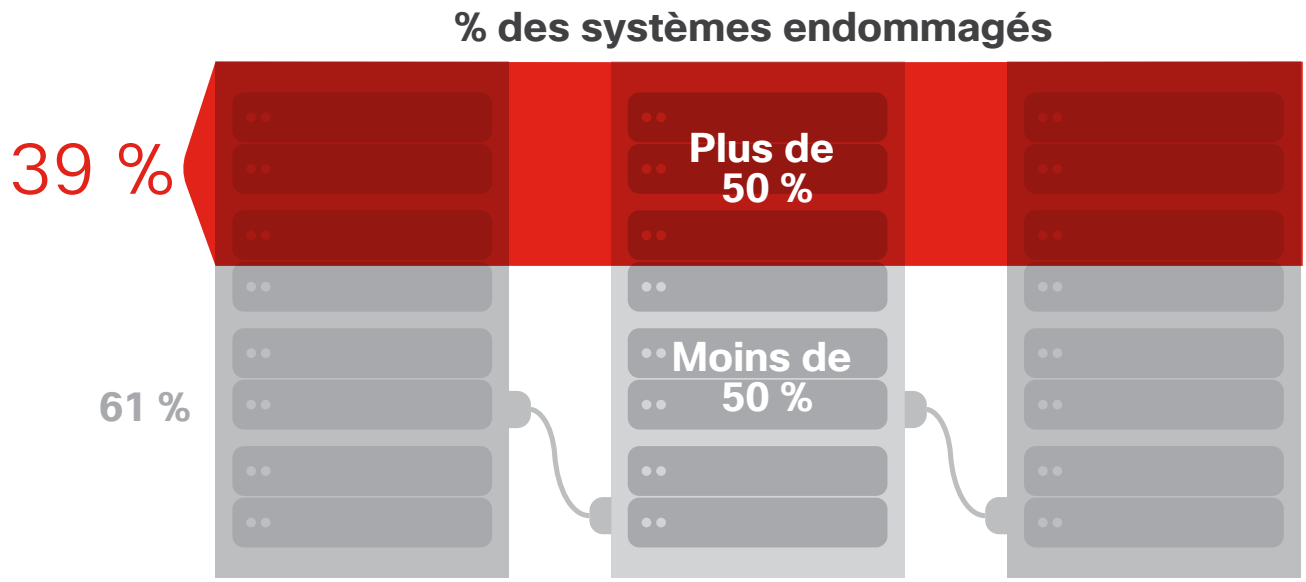
En outre, 39 % des personnes interrogées ont déclaré qu'au moins la moitié de leurs systèmes avait été affectée par une faille sévère (Figure 2). Les petites entreprises sont moins susceptibles d'avoir plusieurs sites ou filiales, et leurs systèmes de base sont généralement davantage interconnectés. Lorsqu'elles subissent une attaque sur le réseau, la menace peut se propager facilement et rapidement aux autres systèmes.

Figure 1 Interruption du système suite à une faille sévère



Source : enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Figure 2 Pourcentage des systèmes affectés par une faille sévère



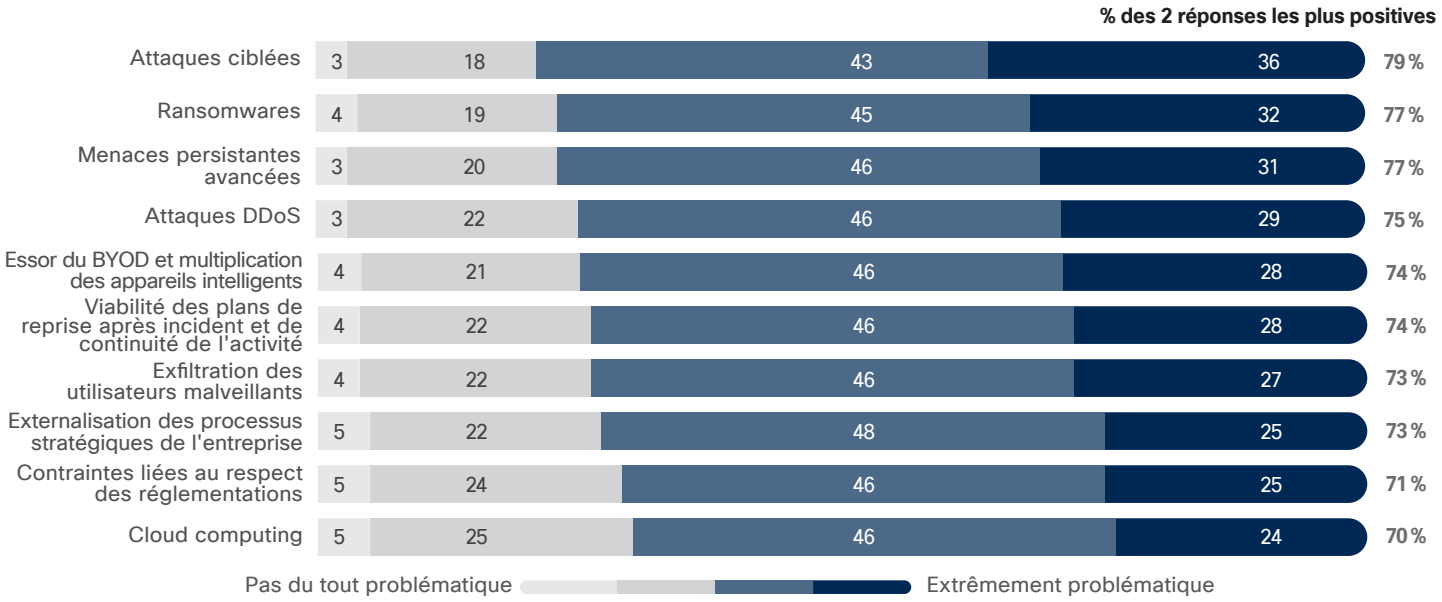
Source : enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Principales préoccupations en matière de sécurité

Lorsque les participants de l'enquête ont été interrogés sur les principales problématiques qu'ils rencontrent en matière de sécurité, les trois préoccupations suivantes sont ressorties :

- Attaques ciblées contre les employés (attaques de phishing efficaces, par exemple)
- Menaces avancées persistantes (malwares avancés que personne n'a encore vus)
- Ransomwares

Les ransomwares (dont il est intéressant de noter qu'ils ne font pas partie des trois principales préoccupations des grandes entreprises) sont des malwares qui chiffrent les données, généralement jusqu'à ce que les utilisateurs affectés payent une rançon pour pouvoir récupérer l'accès à ces données. Ce type d'attaque peut créer des perturbations et des temps d'arrêt système graves pour les PME. Les ransomwares ont également tendance à coûter facilement de l'argent à ces sociétés pour une raison plus insidieuse. En effet, les experts Cisco en sécurité expliquent qu'elles sont plus enclines à payer les rançons aux hackers afin de pouvoir reprendre leur activité le plus rapidement possible. Elles ne peuvent tout simplement pas se permettre ces interruptions et de ne pas avoir accès aux données essentielles, y compris aux données client. (Voir Figure 3.)



Source : enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Figure 3 Principaux problèmes de sécurité pour les entreprises de taille moyenne[5]

Autres menaces que les PME ne peuvent pas ignorer

Malgré les inquiétudes concernant les ransomwares, nos experts suggèrent que cette menace perd du terrain, car de plus en plus de hackers ont détourné leur attention sur le minage illicite de cryptomonnaie (également appelé « cryptomining »). L'attrait de cette activité est triple : elle peut être très lucrative, les paiements sont anonymes, et les hackers courent moins le risque d'être poursuivis en justice pour leurs actions. Par exemple, il n'y a pas de risque que des patients soient privés de soins intensifs, car les systèmes et les données essentielles de l'hôpital sont bloqués par un ransomware. Les hackers peuvent également distribuer des logiciels de minage (« mineurs ») via différentes méthodes, y compris des campagnes de spam par e-mails et des kits d'exploit. [3]

3 « Ransom Where? Malicious Cryptocurrency Miners Takeover, Generating Millions », blog Cisco Talos, 1er janvier[3] 2018 : https://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html.

Les chercheurs Cisco expliquent que les hackers qui utilisent le nouveau modèle commercial de cryptomining illicite ne pénalisent plus les victimes pour avoir ouvert une pièce jointe ou exécuté un script malveillant en prenant en otage les systèmes et en exigeant une rançon. Désormais, ils exploitent activement les ressources des systèmes infectés.[4] Pour les PME qui contribuent involontairement aux opérations illicites de cryptomining, le ralentissement des performances système est parfois le seul indicateur qu'elles ont été infectées, à moins qu'elles ne soient équipées de la technologie adéquate pour détecter ce type d'activité.

Les menaces internes : un fléau à éviter à tout prix

Alors que les entreprises interrogées migrent plus de données et de processus vers le cloud, elles doivent également prendre les mesures nécessaires pour gérer une autre menace potentielle : les utilisateurs internes. Sans outils pour détecter les activités suspectes (telles que le téléchargement d'informations client sensibles), les sociétés courent le risque que l'on porte atteinte à leur propriété intellectuelle, ainsi qu'à leurs données financières et clients sensibles via les systèmes cloud.

Une enquête récente menée par les chercheurs Cisco confirme ce risque : de janvier à juin 2017, ces derniers ont examiné les tendances d'exfiltration des données à l'aide de techniques d'apprentissage automatique afin de déterminer le profil de 150 000 utilisateurs du cloud répartis dans 34 pays. Sur une période de 1,5 mois, ces chercheurs ont découvert que 0,5 % des utilisateurs réalisait des téléchargements suspects. Ce chiffre peut paraître anodin. Toutefois, cela signifie tout de même que dans une entreprise de 400 personnes, deux employés constituent des menaces internes, ce qui est beaucoup trop. Plus précisément, ces utilisateurs ont téléchargé, au total, plus de 3,9 millions de documents à partir des systèmes cloud. Cela correspond à une moyenne de 5 200 documents par utilisateur sur une période de 1,5 mois.[5]

Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Ce rapport spécial présente des points clés tirés de l'enquête Cisco 2018 sur l'efficacité des mesures de sécurité. Plus de 3 600 personnes ont été interrogées dans 26 pays pour mener à bien cette recherche. Pour en savoir plus sur les pratiques de sécurité adoptées par les entreprises de toute taille et pour consulter une comparaison des résultats d'études antérieures de Cisco, téléchargez le *rapport annuel Cisco 2018 sur la cybersécurité* disponible à l'adresse : https://www.cisco.com/c/en/us/products/security/security-reports.html.

4 Ibid.

5 Pour en savoir plus, consultez « Insider threats: taking advantage of the cloud » dans le rapport annuel Cisco 2018 sur la cybersécurité, disponible à l'adresse : https://www.cisco.com/c/en/us/products/security/security-reports.html.

Les défis

La meilleure protection contre les menaces décrites précédemment implique la coordination et l'orchestration des ressources IT. Ces ressources sont le plus souvent des personnes, des processus et des technologies auxquels les entreprises peuvent avoir recours pour empêcher les attaques.

Cependant, les petites sociétés peinent encore plus que les grandes entreprises à coordonner ces ressources de façon à pouvoir tirer parti des données recueillies sur les menaces pour arrêter ou limiter les attaques avant qu'elles ne causent des dommages. La pénurie de main-d'œuvre qualifiée dans le domaine de la sécurité concerne certes toutes les sociétés, mais affecte encore plus les petites structures.

Tendances en matière de technologies de sécurité pour les PME

Par conséquent, les petites entreprises cherchent à mieux se protéger contre les cybermenaces avec de nouveaux outils visant à les arrêter.

L'enquête Cisco révèle que si elles disposaient du personnel requis, les entreprises interrogées seraient davantage disposées à :

- Remplacer les solutions de sécurité de leurs terminaux par des outils avancés de protection contre les malwares ou de détection et de réponse aux incidents (citée par 19 % des personnes interrogées. cette réponse vient en tête de liste)
- Envisager l'amélioration de la sécurité des applications web contre les attaques web (18 %)
- Déployer une solution de prévention des intrusions, qui reste considérée comme une technologie indispensable pour stopper les attaques du réseau et les tentatives d'exploit (17 %) (Voir Figure 5.)

Lorsque les départements IT se penchent sur de nouvelles technologies, un défi consiste à déterminer si les produits interagissent suffisamment efficacement pour assurer la protection de l'entreprise. Les difficultés d'administration inhérentes à l'utilisation de diverses consoles pour traiter les menaces ou les incidents liés à la sécurité ne doivent pas être sous-estimées.

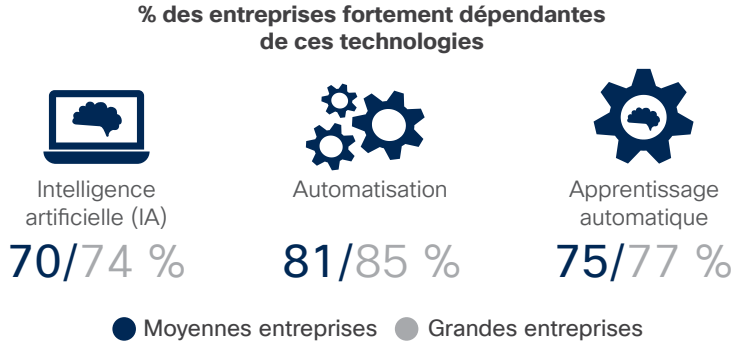
« Nombreux sont ceux qui pensent qu'ils seront mieux protégés s'ils optent pour une approche multifournisseur », explique Ben M. Johnson, partenaire Cisco et PDG de Liberty Technology à Griffin, aux États-Unis. « Toutefois, nous constatons que ce type de stratégie peut être couteuse, complexifier la gestion et diminuer l'efficacité de la sécurité globale ».

L'apprentissage automatique contribue à la sécurité : info ou intox ?

Compte tenu de sa récente popularité, nous avons tous entendu parler de l'apprentissage automatique. Il s'avère que les entreprises de taille moyenne ont recours aux solutions d'analytique comportementale presque autant que les grandes entreprises pour détecter efficacement les attaques. Les solutions qui reposent sur l'automatisation et l'apprentissage automatique sont un peu moins prisées par les entreprises de taille moyenne que par les entreprises de plus de 1 000 employés (Figure 4).

L'apprentissage automatique est plus efficace lorsqu'il est utilisé comme couche de détection supplémentaire dans un produit déjà déployé que lorsqu'il est acheté comme produit séparé. De cette façon, les équipes peuvent tirer parti de l'apprentissage automatique pour détecter les anomalies et les menaces à la vitesse machine sans ajouter de la complexité.

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



Source : enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Les entreprises de taille moyenne et la mobilité

Les entreprises reconnaissent également que leurs stratégies de sécurité doivent répondre aux besoins de l'environnement professionnel moderne. Par conséquent, elles doivent notamment tenir compte de la mobilité et de l'utilisation généralisée des terminaux mobiles. 56 % des personnes interrogées trouvent très difficile, voire extrêmement difficile, de protéger les terminaux mobiles contre les cyberattaques.

Les entreprises de taille moyenne et le cloud

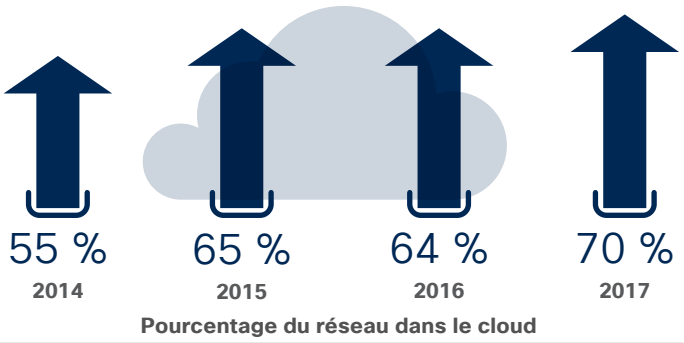
Pour trouver une réponse à leurs problèmes de sécurité, un grand nombre de personnes que nous avons interrogées se tournent vers le cloud pour renforcer la protection sans avoir à recourir à des ressources supplémentaires ou à surcharger les ressources actuelles. Toutefois, la migration de la sécurité vers le cloud est-elle une stratégie suffisante pour repousser les attaques ? En outre, les entreprises ne peuvent pas se décharger de leur responsabilité de sécurité en migrant leurs données vers le cloud : elles doivent se tenir informées sur les contrôles de sécurité imposés par les fournisseurs de services cloud, ainsi que sur l'impact des failles susceptibles d'affecter le cloud sur les ressources sur site.

Selon l'enquête Cisco, l'adoption de services cloud parmi les entreprises de taille moyenne est clairement à la hausse. En 2014, 55 % d'entre elles indiquaient qu'elles hébergeaient une partie de leurs réseaux via une plate-forme cloud. En 2017, ce chiffre est passé à 70 % (Figure 5).

De nombreuses personnes interrogées pensent que le cloud peut les aider à combler certaines lacunes liées à leur système de protection, à leur infrastructure et aux compétences de leur personnel. Selon l'enquête Cisco, la raison principale pour laquelle les entreprises de taille moyenne hébergent leurs réseaux dans le cloud repose sur la conviction selon laquelle il renforce la sécurité des données (68 %). La deuxième raison est qu'elles ne disposent pas de suffisamment de professionnels IT en interne (49 %). (Voir Figure 6.)

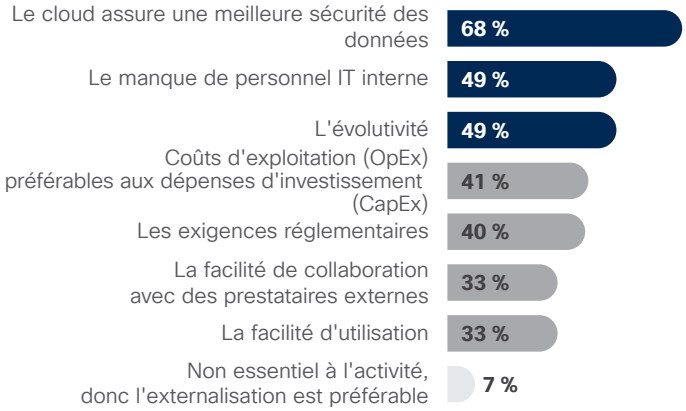
Les entreprises de taille moyenne favorisent également le cloud parce qu'il est évolutif (ce qui leur permet d'être moins dépendantes de leurs ressources internes) et parce qu'il entre dans la catégorie des coûts d'exploitation, et non pas des dépenses d'investissement (Figure 6).

Figure 5 L'adoption des technologies cloud par les entreprises de taille moyenne croît régulièrement



Source : enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Figure 6 Les entreprises de taille moyenne se tournent vers le cloud pour la sécurité et l'efficacité



Source : enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Ressources humaines : trouver le personnel requis pour renforcer la sécurité

La bonne nouvelle est que l'enquête démontre que 92 % des entreprises de taille moyenne ont un dirigeant chargé de la sécurité. (Voir Figure 7.)

Si elles avaient plus de personnel, les entreprises de taille moyenne seraient prêtes à ajouter d'autres outils de sécurité tels que des systèmes avancés de protection des terminaux ou des pare-feu pour les applications web.

Ces sociétés ont un point commun avec les grandes entreprises : la pénurie de personnel IT entrave la capacité à renforcer la protection. Selon l'enquête Cisco, les ressources humaines requises pour gérer les outils qui pourraient améliorer la sécurité ne sont tout simplement pas suffisantes.

C'est pourquoi beaucoup de PME se tournent vers des services d'assistance externalisés pour trouver les compétences dont elles ont besoin pour accroître leur connaissance des menaces, faire des économies et traiter plus rapidement les failles de sécurité. Le désir de bénéficier d'informations impartiales est la raison que les sociétés de taille moyenne citent en premier pour justifier l'externalisation de leurs opérations de sécurité (Figure 8). Viennent ensuite le rapport coût/efficacité et la nécessité de répondre aux incidents au plus vite.

Faire appel à un sous-traitant pour assurer la sécurité est un bon moyen pour les sociétés de tirer le meilleur parti de ressources limitées. Toutefois, elles peuvent rencontrer des difficultés si elles s'attendent à ce qu'une société externalisée ou un partenaire cloud réponde à tous les besoins qu'elles ne sont pas en mesure de gérer en interne.

Selon Chad Paalman, PDG de NuWave Technology Partners à Kalamazoo aux États-Unis et partenaire Cisco, beaucoup de PME n'ont pas vraiment conscience des efforts (ou du peu d'efforts) que les fournisseurs de sécurité externalisés consacrent à l'analyse et au suivi.

Figure 7 Les entreprises de taille moyenne ont au moins un dirigeant ayant la responsabilité de la sécurité

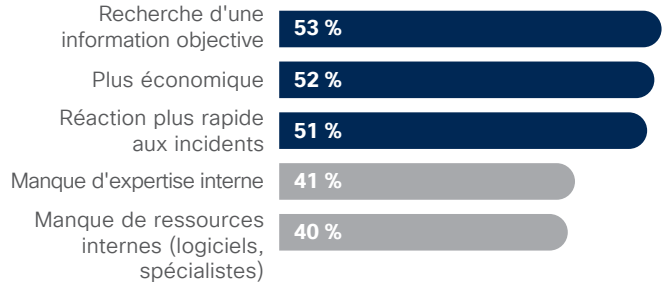
92 %
désignent un dirigeant responsable de la sécurité

Titre du responsable de sécurité

42 %	Directeur de la sécurité des systèmes d'information (CISO)
24 %	Directeur de la sécurité (CSO)
10 %	Président-directeur général (PDG)
8 %	Directeur informatique (CIO)
3 %	Directeur opérationnel (COO)
5 %	Directeur des technologies (CTO)
6 %	Vice-président directeur ou vice-président du département IT (SVP ou VP)
2 %	Directeur des risques ou directeur de la conformité (CRO ou CCO)

Source : enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Figure 8 Les PME ont recours à l'externalisation pour pallier le manque de ressources internes



Source : enquête Cisco 2018 sur l'efficacité des mesures de sécurité

« De nombreux dirigeants ne savent pas comment fonctionnent leurs réseaux. Ils supposent qu'un pare-feu suffit pour bloquer l'accès aux hackers. Ils pensent également que, si leur sécurité a été confiée à un fournisseur de services managés, cela inclut la surveillance des journaux ou la détection des intrusions. »

Chad Paalman, PDG de NuWave Technology Partners

Toutefois, les PME comptent sur leurs partenaires externalisés pour fournir les services suivants :

- Conseils (57 %)
- Gestion des incidents (54 %)
- Suivi de la sécurité (51 %)

Cependant, elles sont moins susceptibles d'externaliser des tâches telles que la Threat Intelligence (39 %). (Voir Figure 9.)

La bonne nouvelle est que les entreprises de taille moyenne semblent consacrer certaines de leurs ressources limitées à l'identification et au traitement des menaces afin d'améliorer leur Threat Intelligence et la gestion des incidents.

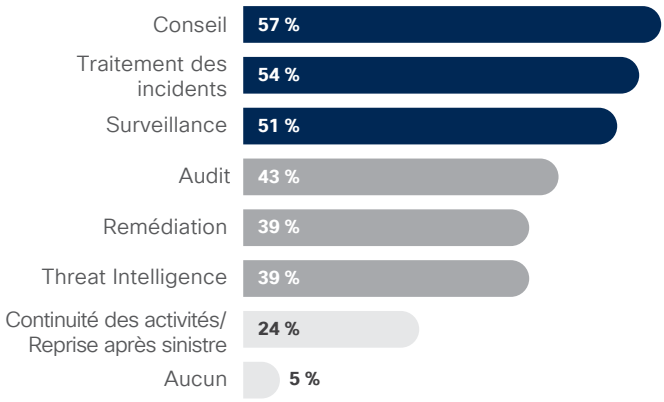
Processus : réaliser des bilans réguliers pour gérer la sécurité

Les processus de sécurité complets et réguliers, tels que le contrôle des ressources les plus importantes et la vérification des pratiques de sécurité, permettent aux entreprises d'identifier les faiblesses de leur stratégie de sécurité. Ces processus ne sont pas aussi répandus dans les PME qu'ils devraient l'être, peut-être en raison du manque de personnel.

Par exemple, selon l'enquête Cisco 2018 sur l'efficacité des mesures de sécurité, les entreprises de taille moyenne sont moins susceptibles que les grandes entreprises d'accepter de s'entendre sur l'examen régulier des pratiques de sécurité, sur les outils requis pour vérifier les fonctionnalités de sécurité et sur l'analyse systématique des incidents (Figure 10).

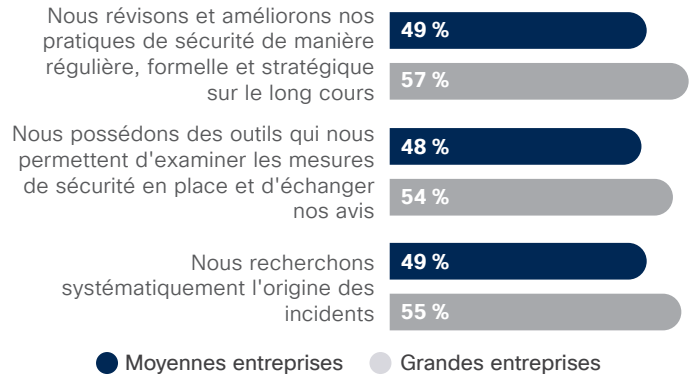
Toutefois, 91 % des entreprises de taille moyenne ont indiqué tester leurs plans de gestion des incidents au moins une fois par an, ce qui est un bon point. Cependant, comme pour le cloud et les partenaires externalisés, la question est de savoir si ces plans de gestion des incidents suffisent à repousser des attaques de plus en plus sophistiquées.

Figure 9 Les entreprises de taille moyenne externalisent les services de conseil et de gestion des incidents



Source : enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Figure 10 Les entreprises de taille moyenne sont moins susceptibles de s'entendre sur l'utilisation des processus opérationnels



Source : enquête Cisco 2018 sur l'efficacité des mesures de sécurité

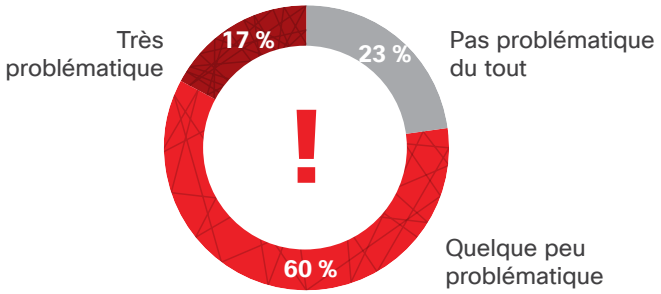
Connecter les personnes, les processus et les technologies : le défi de l'orchestration

Si les PME ajoutent des produits et des fournisseurs de sécurité à leur solution de protection et si elles consacrent leurs ressources IT à la gestion de ces produits, seront-elles plus à même de gérer la sécurité ? Rien n'est moins sûr, tout du moins en termes de compréhension et d'orchestration des alertes de sécurité.

La plupart des PME d'aujourd'hui reconnaissent que leurs responsabilités augmentent à mesure qu'elles créent un environnement produits et fournisseurs plus complexe. Par exemple, 77 % des entreprises de taille moyenne trouvent quelque peu problématique ou très problématique d'orchestrer les alertes de ces nombreuses solutions (Figure 11).

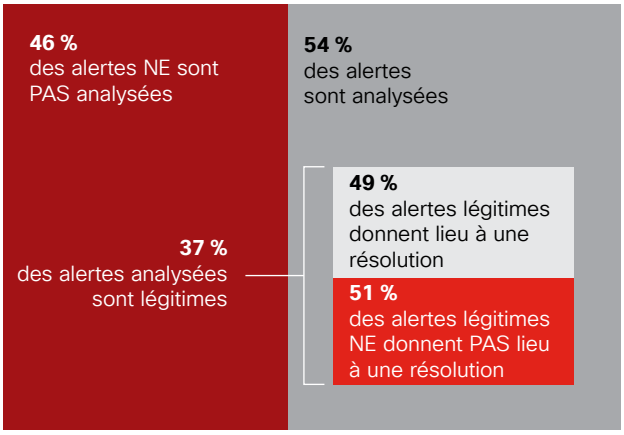
Comme l'enquête Cisco l'indique, lorsque les sociétés essaient d'analyser ces alertes, la difficulté à allier les ressources humaines, les processus et les technologies peut nuire à l'analyse des alertes (Figure 12) :

Figure 11 Les entreprises de taille moyenne sont moins susceptibles de s'entendre sur l'utilisation des processus opérationnels



Source : enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Figure 12 Pourcentage d'alertes de sécurité qui ne sont pas analysées ou ne donnent pas lieu à une résolution



Source : enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Recommandations pour l'avenir

Technologie

Lorsque les entreprises envisagent l'acquisition de nouveaux outils, idéalement, elles peuvent éviter d'avoir plus de fournisseurs à gérer et plus d'alertes à traiter.

Toutefois, plusieurs questions doivent se poser : le produit a-t-il été conçu pour interagir avec d'autres ? Dans quelle mesure permettra-t-il de partager les données et la Threat Intelligence ? La console d'administration est-elle intégrée ?

Si un fournisseur souligne l'interopérabilité d'un produit, cette interopérabilité est-elle prête à l'emploi ou l'acheteur devra-t-il faire des efforts de programmation considérable via une API ?

Qu'il soit populaire ou non, l'apprentissage automatique a un rôle à jouer en matière de sécurité. Cependant, mieux vaut qu'il fonctionne comme une couche de détection au sein de produits déjà déployés plutôt que comme la solution autonome d'un fournisseur tiers, ce qui élargirait le panel de produits à gérer.

Les personnes et les processus

En clair, développez une stratégie visant à améliorer la cybersécurité. Selon le centre de ressources Vistage Research Center, seules 38 % des PME ont une stratégie de cybersécurité active en place.[6]

Votre planification inclut-elle la formation des utilisateurs finaux ? Vos polices d'assurance couvrent-elles la perte d'activité découlant d'une cyberattaque ? Que diriez-vous de créer des stratégies de continuité d'activité et des plans de communication en situation de crise pour permettre une récupération plus rapide et limiter les dommages pour votre réputation ?

En outre, les responsables IT doivent expliquer clairement ce que la direction de l'entreprise veut vraiment savoir en ce qui concerne les attaques :

- Quel est l'impact pour l'entreprise ?
- Quelles mesures l'équipe de sécurité prend-elle pour contenir et analyser les menaces ? Combien de temps sera nécessaire pour reprendre le cours normal des choses ?[7]

« En adoptant un ensemble de plates-formes et d'outils de sécurité qui interagissent les uns avec les autres, au lieu de produits autonomes qui peuvent entrer en conflit avec les autres, vous renforcez l'efficacité de la sécurité tout en simplifiant la gestion. »

Ben M. Johnson, PDG de Liberty Technology

« Les PME doivent évaluer ces risques et élaborer des plans de réponse avant une attaque, pas après. »

Chad Paalman, NuWave Technology Partners

6 « Cyberthreats and Solutions for Small and Midsize Businesses », Vistage Research Center, 2018. 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 Cisco du 1er semestre 2017 sur la cybersécurité : https://www.cisco.com/c/dam/global/es_mx/solutions/security/pdf/cisco-2017-midyear-cybersecurity-report.pdf. 13 Ibid.

Conclusion

Pour finir, nous recommandons aux PME qui souhaitent améliorer la cybersécurité de comprendre qu'il est préférable de changer progressivement plutôt que de ne pas changer du tout. Autrement dit, elles ne doivent pas laisser le désir de perfection entraver l'amélioration graduelle de leur approche en matière de sécurité. Comme pour tout, la perfection n'existe pas.

Les PME doivent comprendre qu'il n'existe aucune solution technologique « miracle » pour résoudre tous les défis posés par la cybersécurité. Les menaces sont trop complexes et dynamiques. La surface d'attaque ne cesse de s'étendre et d'évoluer. Par conséquent, les stratégies et les technologies de sécurité doivent progresser en permanence.

Pour en savoir plus sur notre approche de la sécurité axée sur les menaces, rendez-vous sur cisco.com/go/security.

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

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) Pte. Ltd.
Singapour

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

Cisco compte plus de 200 bureaux à travers le monde. Leurs adresses, numéros de téléphone et numéros de fax sont répertoriés sur le site web www.cisco.com/go/offices.

Publié en juillet 2018

© 2018 Cisco et/ou ses filiales. Tous droits réservés.

Cisco et le logo Cisco sont des marques commerciales ou déposées de Cisco et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour consulter la liste des marques commerciales de Cisco, visitez : www.cisco.com/go/trademarks. Les autres marques commerciales mentionnées dans ce document sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et toute autre entreprise. (1110R)

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