L'ÉVOLUTION DU RÔLE DES PRODUITS SAAS ET DE LA SOUS-TRAITANCE DE LA SÉCURITÉ INFORMATIQUE DANS LES PME

Série de rapports spéciaux 2016 sur les risques liés à la sécurité informatique des entreprises

Kaspersky Lab

TABLE DES MATIÈRES

INTRODUCTION

Pour les PME, obtenir la meilleure efficacité et les meilleures performances possibles de chaque ressource est essentiel à leur rentabilité ainsi qu'à leur réussite à long terme. L'évolution de l'informatique a joué un rôle important en aidant les PME à renforcer leur compétitivité face aux grandes entreprises, et selon IDC[1], ces investissements devraient continuer d'augmenter jusqu'en 2019 à un taux de 4,4 %, d'une année à l'autre.

Du fait de leur nature même, les PME ont des exigences et des défis différents à relever en matière d'informatique comparé aux grandes entreprises, et malgré l'augmentation des dépenses en informatique, les contraintes budgétaires et la dotation en personnel ne permettent pas toujours de suivre le rythme infligé par l'environnement technologique dans lequel nous évoluons.

Avec le recours croissant aux périphériques mobiles et l'utilisation d'appareils personnels au sein de l'entreprise, l'écosystème informatique des PME a considérablement changé au cours des cinq dernières années, et s'accompagne de nouveaux défis avec lesquels les petites entreprises doivent se familiariser. L'utilisation toujours grandissante d'appareils personnels au sein de l'entreprise témoigne de l'incroyable complexité de l'infrastructure informatique à laquelle les PME sont confrontées. Selon nos recherches, la majorité des PME gèrent actuellement plus de 50 appareils mobiles, plus de 60 % d'entre elles admettant que ce chiffre a augmenté au cours des trois dernières années.

1 Prévisions mondiales concernant les petites et moyennes entreprises, 2015-2019 : Dépenses informatiques en fonction de la taille de l'entreprise et de la région pour les catégories matériel, logiciels et services, IDC, juillet 2015

Afin de comprendre les défis et menaces que rencontrent les entreprises aujourd'hui, Kaspersky Lab a réalisé une étude mondiale auprès de 4 395 dirigeants d'entreprises de 25 pays en association avec B2B International et leur a posé une série de questions quant à leur perception des menaces de sécurité informatique, la réalité de l'environnement des menaces et l'impact des piratages de données sur leurs activités.

Malgré leur taille, les PME sont tout autant menacées par une cyberattaque que n'importe quelle autre entreprise. En effet, un manque de ressources, de budgets et d'expertise en matière de sécurité figurent souvent parmi les principales raisons citées qui expliquent qu'elles sont devenues des cibles de choix faciles pour les cybercriminels par rapport aux grandes entreprises. Il est donc plus important que jamais qu'elles emploient judicieusement les budgets et recherchent d'autres options qui leur permettront de rester attentives et de ne pas devenir des victimes.

Les produits SaaS (Security as a Service), qui fournissent un moyen économique de tirer avantage des technologies grâce à un modèle d'abonnement basé dans le Cloud, pourraient bien être la solution pour de nombreuses PME, en leur permettant de rester compétitives, de trouver de nouvelles méthodes pour optimiser les coûts et les ressources. Grâce au SaaS, les PME jusque-là mal préparées et manquant de ressources peuvent se familiariser avec la sécurité informatique et assurer leur protection totale. Ce type de solution présente également l'avantage de pouvoir évoluer jusqu'à une sous-traitance complète de l'informatique à mesure que les besoins de l'entreprise évoluent. En collaboration avec des fournisseurs de services, les PME peuvent passer au niveau supérieur en matière d'assistance, de veille stratégique et d'expertise concernant la sécurité, et ainsi permettre à leur activité de continuer à évoluer tout en assurant leur totale protection à mesure que leurs besoins technologiques et leur infrastructure informatique se développent.

Dans ce rapport, nous étudions les défis que rencontrent les PME en matière de sécurité informatique ainsi que le rôle de la sous-traitance des produits SaaS et de l'informatique pour les aider à rester au fait des menaces actuelles et futures

LE DÉFI DES PME EN MATIÈRE DE SÉCURITÉ

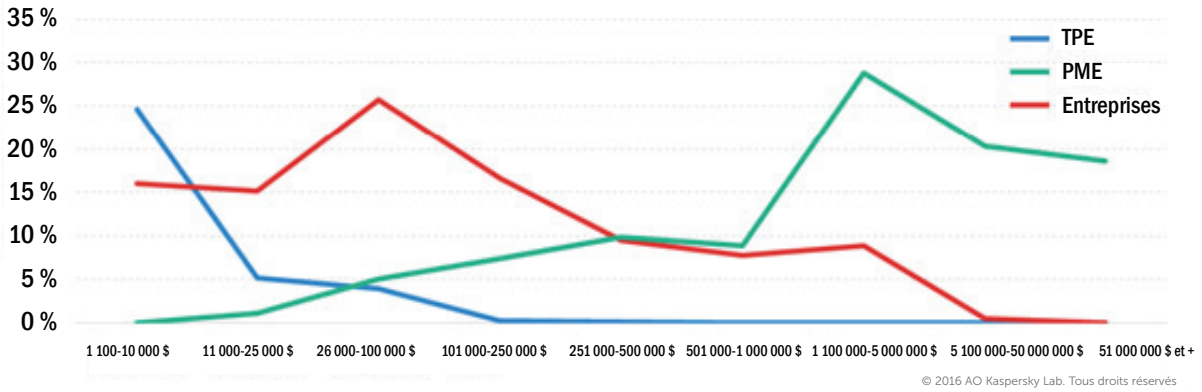
Gestion de la complexité

Mettre en place les ressources adéquates pour gérer l'informatique et suivre l'évolution des menaces constitue un élément clé du casse-tête de la sécurité. Mais cela semble plus facile à dire qu'à faire, puisque plus de la moitié des PME (55 %) mentionnent que la protection d'un nombre toujours grandissant d'appareils constitue pour elles un véritable défi. Les problèmes courants tels que des ressources, une expertise et un budget limités, pèsent tous sur la capacité des PME à faire face à l'évolution constante du paysage des menaces. Nombreuses sont les PME qui ont eu recours aux services Cloud pour gérer les coûts et la complexité, et qui continuent de le faire d'une année à l'autre. Selon les chiffres récents, près de 2/3 (64 %) des petites entreprises ont déjà mis en place en moyenne trois solutions de services Cloud.

Toutefois, lorsqu'il est question de la sécurité et de l'intégrité de ces services, nos résultats de recherche montrent qu'il subsiste des préoccupations, la moitié des TPE (52 %) et des PME (49 %) admettant se sentir vulnérables aux incidents qui affectent les services Cloud tiers qu'elles utilisent.

Petits budgets, grandes attentes

Comme on pouvait s'y attendre, les budgets alloués à la sécurité informatique sont faibles : 2/3 (66 %) des TPE dépensent moins de 1 000 $/an en matière de sécurité informatique contre 68 % des entreprises qui dépensent plus de 1 million de dollars chaque année. Pour mettre ces chiffres en perspective, les TPE dépensent en moyenne 13 % de leur budget informatique dans le domaine de la sécurité, mais espèrent que ce chiffre va augmenter modérément de 12,5 % au cours des trois prochaines années. Toutefois, malgré des budgets plus faibles, la majorité des PME investissent pour améliorer leur sécurité informatique, indépendamment du retour sur investissement (44 % des TPE, 59 % des PME).



Pourcentage des entreprises avec leur budget de sécurité informatique par tranche

Les ressources internes en matière de sécurité informatique restent faibles

Même si plus de la moitié (54 %) des PME pensent que leur sécurité informatique fera l'objet d'une attaque à un moment donné et qu'elles doivent s'y préparer, 40 % admettent que les informations ou les solutions de veille stratégique dont elles disposent sont insuffisantes. Toutefois, lorsqu'il s'agit d'allouer du budget pour renforcer les ressources internes et la veille stratégique en matière d'informatique, les chiffres indiquent que moins de la moitié des TPE (44 %) font appel à du personnel informatique spécialisé. Pour les PME qui emploient du personnel informatique, seule 1 sur 10 (13 %) est spécialisée dans le domaine de la sécurité informatique. Si l'on étudie différents secteurs, ce chiffre passe à 1 sur 5 (20 %) dans le domaine de l'immobilier, et 18 % pour le commerce en ligne/vente au détail en ligne. Dans le secteur de la fabrication sous propriété intellectuelle, ce chiffre ne dépasse pas 7 %.

En ce qui concerne les prévisions de croissance des spécialistes de la sécurité informatique au sein des PME, plus de 60 % prévoient d'augmenter les chiffres au cours des trois prochaines années, un tiers (32 %) s'attend à ce que les niveaux ne changent pas, mais 1 sur 5 (19 %) s'attend à une augmentation considérable. Toutefois, la moitié des PME (50 %) ne prévoient pas que le budget alloué à l'embauche de nouveaux employés en sécurité informatique augmente également et seules 10 % déclarent que ce chiffre va augmenter considérablement. Pour un tiers des PME (35 %), améliorer l'expertise spécialisée en sécurité constitue le troisième plus important facteur d'augmentation des investissements en matière de sécurité informatique.

Du fait de leurs budgets restreints, les PME ont du mal à développer la veille stratégique dont elles ont besoin en matière d'informatique pour se protéger contre les menaces grandissantes. Ce qui rend la sous-traitance de l'expertise spécialisée en informatique encore plus attrayante, en particulier lorsque 53 % des PME déclarent qu'il existe une pénurie au niveau des professionnels de sécurité informatique à embaucher.

PANORAMA DES CYBERMENACES

Les entreprises de toutes sortes et de toutes tailles sont chaque jour confrontées à des cybermenaces toujours plus nombreuses. Les cybercriminels deviennent de plus en plus sophistiqués dans leur tentative de piéger les entreprises et les particuliers. Compte tenu des conséquences financières et réputationnelles en jeu, les PME sont fortement concernées par l'impact des piratages de données sur leurs activités.

La perte de données en tête de la liste des préoccupations

La perte de données internes et confidentielles est la principale préoccupation des petites entreprises en matière de sécurité informatique. Contrairement aux grandes entreprises, les TPE sont préoccupées par la perte physique d'appareils susceptible d'occasionner une fuite de données (48 % des personnes interrogées en conviennent). Outre les préoccupations concernant la perte d'appareils, un représentant de TPE sur cinq (21 %) se soucie de la rapidité à répondre aux menaces et à les corriger.

	Total	1 à 49 employés	50 à 999 employés	+ de 1000 employés
Perte/exposition de données liée à des attaques ciblées	45 %	46 %	44 %	47 %
Fuite électronique de données dans les systèmes internes	39 %	35 %	40 %	39 %
Perte matérielle d'appareils ou de supports contenant des données	38 %	48 %	35 %	34 %
Virus et programmes malveillants entraînant une perte de productivité	26 %	31 %	25 %	22 %
Utilisation inappropriée des ressources informatiques par les employés	23 %	18 %	23 %	26%
Surveillance/espionnage par les concurrents	22 %	18 %	23 %	25 %
Temps et coût lié au respect de la conformité auprès des employés	22 %	16%	23 %	24 %
Incidents affectant l'infrastructure informatique hébergée par un tiers	21 %	18 %	21 %	24 %
Gestion de la sécurité des appareils personnels des utilisateurs au travail	19 %	17 %	18 %	23 %
Incidents affectant des fournisseurs avec lesquels nous partageons des données	18 %	15 %	18 %	20 %
Temps nécessaire pour répondre aux menaces et les corriger	18 %	21 %	18 %	15 %
Temps et coût lié à la vérification de la conformité des tiers en matière de sécurité	16 %	13 %	17 %	17 %

Principales préoccupations en matière de sécurité informatique (principales différences en fonction de la taille de l'entreprise)

Lorsque l'on observe le nombre d'attaques subies par les PME au cours des 12 derniers mois, leurs préoccupations sont tout à fait justifiées. Il apparaît également évident que les mesures mises en place pour lutter contre les menaces n'assurent pas nécessairement des niveaux de protection adaptés dans tous les cas.

Parmi tous les incidents que rencontrent les PME, les virus et les programmes malveillants à l'origine d'une perte de productivité arrivent en tête de liste, plus de 41 % des personnes interrogées ayant été confrontées à ce problème.

		TPE	PME
Vecteurs d'attaque les plus courants	N°1	Virus/programmes malveillants/chevaux de Troie	Virus/programmes malveillants/chevaux de Troie
	N°2	Employés imprudents/mal informés	Employés imprudents/mal informés
	N°3	Phishing/ingénierie sociale	Employés imprudents/mal informés
	N°4	Exploitation de failles/perte via des appareils mobiles	Attaque ciblée
	N°5	Attaque ciblée	Exploitation de failles/perte via des appareils mobiles

Le temps coûte de l'argent

Pour de nombreuses PME, un piratage de données peut avoir un impact financier grave, notamment en raison des mesures à prendre et des coûts engendrés. En effet, selon les chiffres de la National Cyber Security Alliance, 60 % des PME faisant l'objet d'un piratage mettent la clé sous la porte dans les 6 mois. Continuer de penser que « cela n'arrive qu'aux autres » et mettre l'accent sur une attitude passive pourrait s'avérer désastreux.

On estime à 14 000 $ les rémunérations supplémentaires du personnel interne nécessaire pour stabiliser la situation après une attaque, et à 13 000 $ la perte d'activité résultant du piratage. Améliorer les systèmes logiciels et l'infrastructure suite à un piratage coûte aux PME en moyenne 10 000 $. L'impact financier total d'un piratage de données coûterait en moyenne à **une PME 86 500 $**.

Plus l'entreprise met de temps à constater le piratage, plus il lui en coûtera en termes financier et d'intégrité des données. Même en cas de détection quasi-immédiate des piratages, les PME en estiment le coût à 28 000 $, pouvant aller jusqu'à 105 000 $ si le piratage n'est détecté qu'au bout d'une semaine ou plus.

Plus l'entreprise met de temps à constater le piratage, plus les données sont également vulnérables, avec en moyenne 417 dossiers sensibles de clients/employés compromis, même en cas de détection immédiate, et plus de 70 000 exposés à un risque si le piratage n'est détecté qu'au bout d'une semaine ou plus.

LA SOLUTION POURRAIT VENIR DES SERVICES CLOUD ET D'ASSISTANCE EXTERNE

Alors comment les PME peuvent-elles combler l'écart existant entre des budgets et une expertise moindres, et la menace bien réelle et grandissante des cyberattaques ?

Outre une approche de sécurité traditionnelle sur site, les PME peuvent opter pour deux solutions viables qui leur apporteraient l'expertise et l'assistance qui leur fait défaut, tout en respectant leur budget et leurs ressources. Il existe plusieurs façons de résoudre un problème et pour les petites et moyennes entreprises, l'essentiel est de trouver la solution la plus avantageuse.

Nous avons déjà discuté des avantages qu'offrent les services Cloud pour réduire la complexité et profiter des économies d'échelle, et la réciproque vaut également pour la sécurité informatique.

En adoptant une approche de type SaaS en matière de sécurité, les PME peuvent profiter de solutions de sécurité des terminaux sans avoir à débloquer d'importants budgets comme les grandes entreprises. Les TPE peuvent ainsi contrôler facilement les coûts, simplifier et centraliser leur sécurité informatique tout en accédant à une protection et une expertise essentielles.

Malgré la diversité des solutions de sécurité disponibles actuellement sur le marché, les PME n'en restent pas moins limitées en termes de ressources et de budgets lorsqu'elles recherchent la solution la mieux adaptée. Les produits de sécurité de type SaaS disponibles via un abonnement, par exemple Kaspersky Endpoint Security Cloud, permettent aux petites entreprises de profiter d'une technologie leader sur le marché qui répond à leurs besoins, sans avoir à dépenser énormément en matériel. Elles peuvent ainsi exploiter au maximum les budgets et l'expertise à leur disposition pour investir les ressources essentielles dans le développement stratégique de l'entreprise et sa future croissance.

40 % des PME et 26 % des TPE conviennent que la sous-traitance pourrait être la solution et cherchent à sous-traiter leurs processus et leur infrastructure informatiques à des tiers.

Toutefois, en ce qui concerne la deuxième option, à savoir l'utilisation de fournisseurs de services de sécurité informatique externes, un tiers (36 %) des TPE n'y ont pas recours mais une entreprise sur cinq (20 %) prévoit de le faire dans les 12 prochains mois. Seules 17 % des PME ne prévoient

absolument pas de faire appel à un fournisseur de services de sécurité informatique externe mais quasiment un quart (23 %) pensent que ce chiffre va évoluer dans les 12 prochains mois.

Selon notre étude, de nombreuses PME rejettent, semble-t-il, une assistance tierce et n'investissent pas non plus de façon significative au niveau de leurs ressources internes en sécurité informatique, passant ainsi à côté d'un élément essentiel de la sécurité informatique que la technologie seule ne peut pas résoudre. Les entreprises qui sous-traitent et privilégient les produits de type SaaS (Security as a Service) perçoivent cette mesure de sécurité comme efficace (57 %).

Pour répondre à la complexité croissante concernant le volume d'appareils mobiles à protéger et l'évolution constante des menaces, travailler avec un spécialiste qui leur fournira des informations et des solutions de veille stratégique permettra aux PME de renforcer leurs défenses tout en tirant profit au maximum des budgets disponibles pour assurer leur protection optimale.

Travailler avec un tiers permettra aux PME d'intégrer dans l'équation des experts du domaine sans avoir à débloquer des budgets importants pour embaucher du personnel en interne, et ainsi bénéficier d'une expertise et d'une assistance en sécurité informatique de qualité supérieure. Ceci est d'autant plus important qu'il convient de développer en permanence les compétences, en fonction des changements et des implications des vecteurs de menaces.

Pour se protéger du nombre toujours croissant de menaces avec des budgets et une expertise limités, les PME peuvent recourir à la sous-traitance des produits SaaS et de l'informatique qui constituent des alternatives viables, en plus des approches de sécurité traditionnelles sur site, pour rentabiliser et exploiter au mieux les dépenses et les ressources disponibles.

Securelist, la ressource destinée à la recherche technique, l'analyse et la réflexion des experts de Kaspersky Lab.

Suivez-nous

Site Entreprises Kaspersky Lab

Blog d'Eugene Kaspersky

Blog B2C de Kaspersky Lab

Blog B2B de Kaspersky Lab

Service d'informations de sécurité de Kaspersky Lab

Académie Kaspersky Lab