L'IMPACT FINANCIER DE LA SÉCURITÉ INFORMATIQUE SUR LES ENTREPRISES EUROPÉENNES

Risques liés à la sécurité informatique 2016

Kaspersky Lab

TABLE

INTRODUCTION

Une quantité croissante d'informations circule instantanément à travers le monde sous forme numérique. Les moyens d'accès et de création de celles-ci continuent à évoluer et il en va de même pour les risques de cyberattaques. De ce fait, la cybersécurité est devenue un sujet majeur à l'ordre du jour des gouvernements, des organismes de réglementation et des entreprises du monde entier. Aujourd'hui plus que jamais, les ressources consacrées à la sécurité informatique font l'objet de toutes les attentions dans la mesure où l'ensemble des systèmes de protection en dépend.

Kaspersky Lab s'est associé à B2B International pour déterminer si les budgets consacrés à la protection des entreprises étaient à la hauteur des pertes financières potentielles liées aux incidents de sécurité. Cette enquête mondiale porte sur plus de 4 000 entreprises dans 25 pays et analyse les budgets consacrés à la sécurité informatique, les attitudes et les solutions adoptées face aux menaces de sécurité, ainsi que le coût des violations de données.

Au cours des trois prochaines années, une immense majorité (**70%**) des entreprises européennes envisagent d'augmenter entre **10%** et **29%** (contre une moyenne mondiale de **35%**) leurs dépenses en matière de sécurité informatique. Mais les déclarations d'intention et les ressources engagées sont-elles suffisantes pour faire face aux dangers réels qui menacent les entreprises européennes de toutes tailles?

LEVER LE VOILE SUR LES BUDGETS

À mesure que les entreprises exploitent la technologie dans leurs opérations, interactions et communications quotidiennes, la sécurité informatique fait l'objet d'une attention accrue. Il s'agit de protéger les plates-formes et les infrastructures dont elles dépendent. Selon un tiers (**35%**) des acteurs interrogés, la complexité des infrastructures informatiques est le principal facteur d'augmentation des budgets consacrés à la sécurité dans les entreprises européennes, suivie en deuxième position par la création et l'expansion des entreprises (**32%**).

Bien qu'elles aient conscience de leur besoin d'augmenter les budgets, plus d'un tiers (**39%**) des entreprises européennes estiment qu'il est difficile de provisionner les dépenses nécessaires à la protection de leur organisation. Cette proportion est inférieure à la moyenne mondiale des entreprises (**47%**). Face aux défis de la mise en œuvre des mesures de sécurité informatique, plus d'un tiers (**41%**) des acteurs interrogés estiment qu'il est difficile de prouver le retour sur investissement (ROI) de la sécurité informatique à la direction générale.

Les entreprises européennes, ainsi que celles du reste du monde, s'accordent à penser qu'il faut continuer à investir dans l'amélioration de la sécurité informatique. La moitié (56%) d'entre elles, en Europe et dans le monde, estime en effet qu'il vaut mieux prévenir que guérir.

Dans leur contexte, l'analyse de la réalité des dépenses en sécurité informatique révèle que celles-ci ne représentent qu'une petite part du budget informatique total. Effectivement, la compréhension de la menace ne se traduit pas nécessairement par des mesures concrètes. En Europe, la plupart des entreprises (**76%**) affirment ne consacrer que moins de **20%** de leur budget informatique à la sécurité. Même si cette proportion est supérieure à la moyenne mondiale (**69%**), en valeur nominale et à l'échelle de l'Europe, 1 entreprise sur 10 (**13%**) dépense moins de 2 500 dollars au total en approvisionnement informatique par an (contre **8%** des entreprises au niveau mondial).

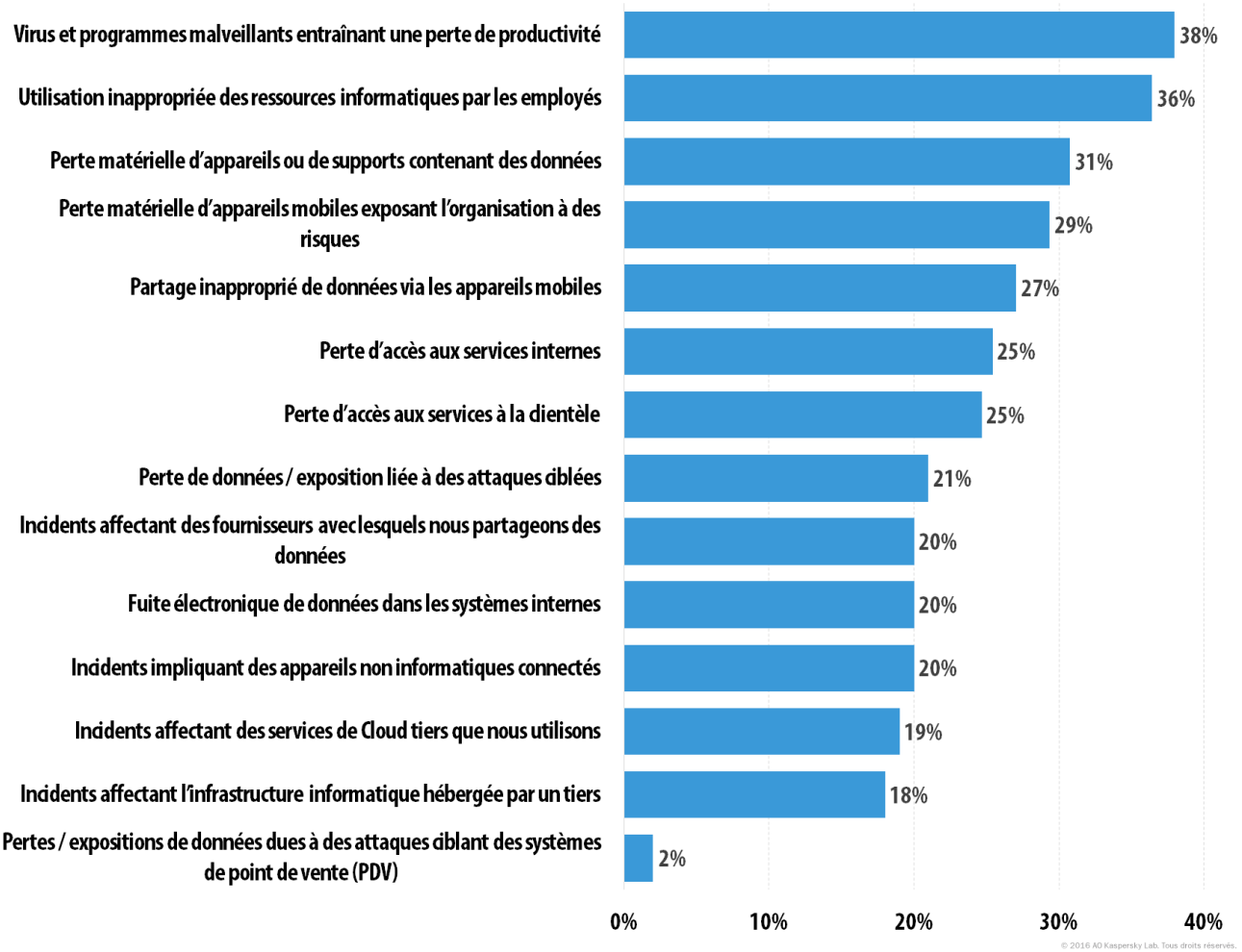
Pour de nombreuses entreprises européennes, les stratégies de sécurité informatique s'accompagnent d'une augmentation du personnel. Pratiquement deux tiers (**64%**) d'entre elles s'attendent à ce que le nombre de spécialistes en sécurité informatique employés par leur organisation augmente au cours des 3 prochaines années. Même si ce chiffre est légèrement en deçà de la moyenne mondiale (**68%**), la moitié (**47%**) des entreprises européennes s'attend à ce que la proportion des dépenses de recrutement et de rémunération en spécialistes internes de sécurité informatique augmente, contre **54%** au niveau mondial.

ESTIMATION DES COÛTS

Lors de l'estimation des budgets, la plupart des entreprises a conscience que les coûts réels d'un incident de sécurité ou d'une violation de données peuvent s'avérer énormes au vu des conséquences financières et des effets négatifs en termes de réputation.

Alors qu'à peine moins de la moitié (**47%**) des entreprises européennes (**52%** au niveau mondial) estiment que leur sécurité informatique sera compromise à un certain moment, nos recherches ont révélé qu'au cours des 12 derniers mois, un tiers (**32%**) des entreprises européennes (**38%** au niveau mondial) ont été affectées par des virus et des programmes malveillants ayant occasionné une perte de productivité, et que **30%** ont été victimes d'une utilisation inappropriée des ressources informatiques par leurs employés (contre **36%** au niveau mondial).

Types d'incidents de sécurité au cours des 12 derniers mois (% de toutes les entreprises ayant été victimes de chaque type d'attaque)



La conscience du véritable impact financier de ces types d'incidents permet de prendre la pleine mesure de l'importance de la préparation, ainsi que de l'utilisation optimale du budget. Notre enquête a révélé que plus des trois quarts (**84%**) des entreprises européennes ont été victimes de 1 à 5 incidents impliquant la perte, la fuite ou l'exposition de données au cours des 12 derniers mois (contre **82%** au niveau mondial).

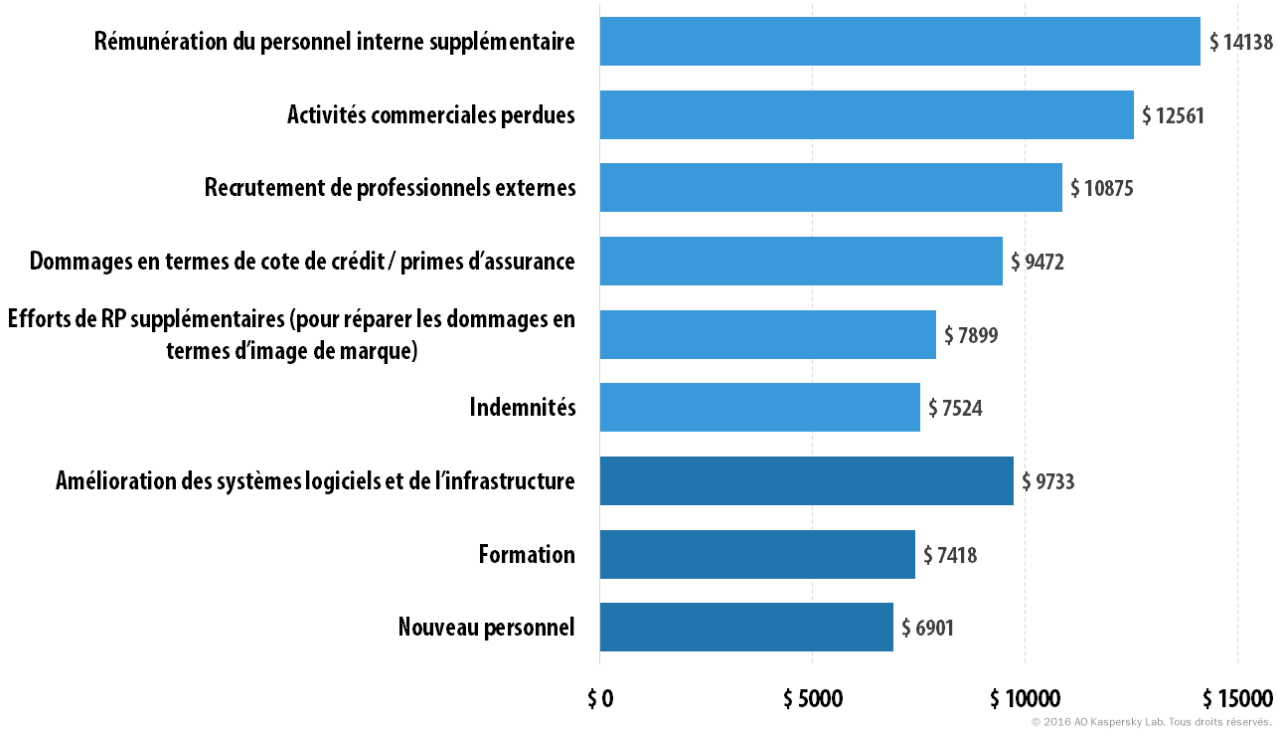
Suite à ces incidents, **10%** des entreprises européennes ont perdu leur accès à des informations commerciales clés pendant une semaine (contre une entreprise sur dix au niveau mondial) tandis que **15%** d'entre elles ont été obligées d'interrompre leurs activités commerciales pendant plus de sept jours. Une entreprise sur dix (**10%**) de la zone met parfois un an avant de découvrir qu'elle a été victime de piratage. Ce manque de conscience et de préparation face à des incidents que la majorité considère comme des conséquences inévitables dues à la complexité de l'environnement technologique peut avoir d'énormes répercussions financières.

Pour mettre les choses en perspective, l'impact financier moyen d'une seule faille de sécurité et d'un vecteur d'attaque pour une PME est estimé à **86 500 dollars** au niveau mondial et, plus étonnamment, à **861 000 dollars** pour les grandes entreprises. Selon la même estimation, la redistribution du temps du personnel informatique représente le coût supplémentaire le plus élevé, à la fois pour les PME et les grandes entreprise.

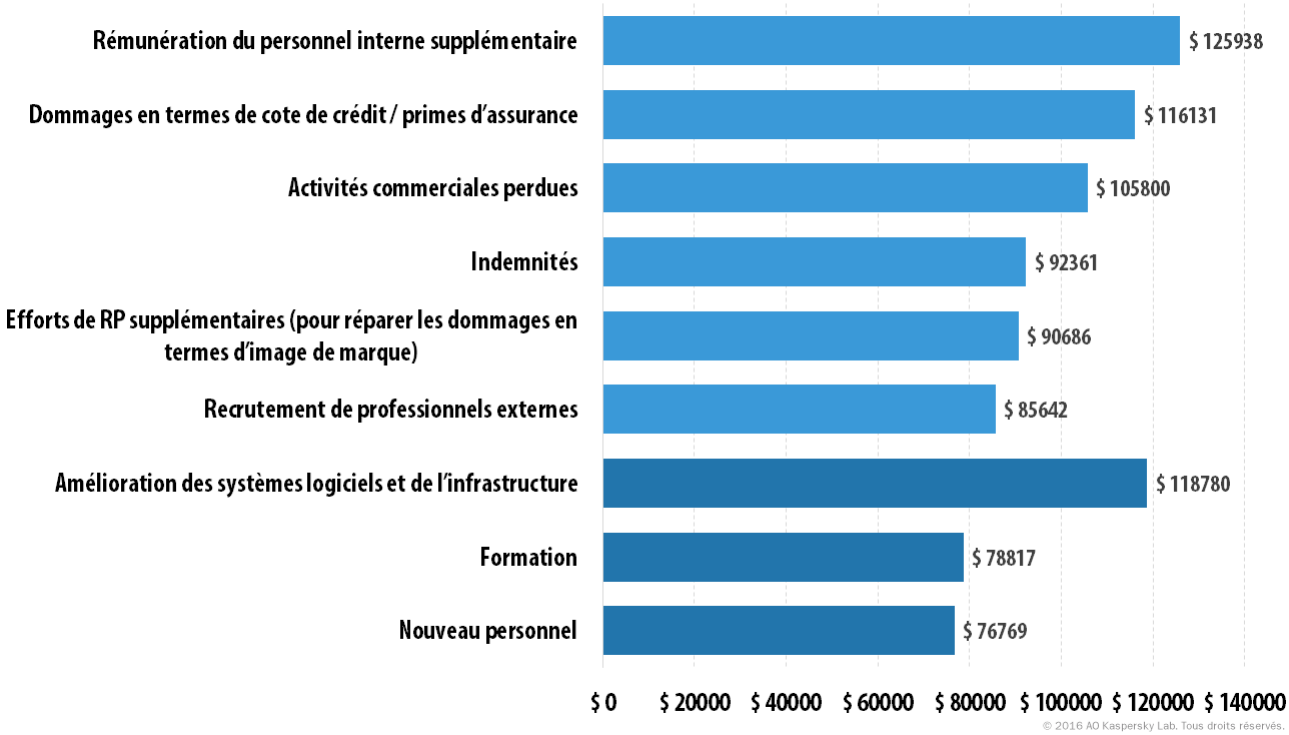
L'enquête a montré à quel point les budgets sont serrés et révélé le peu de marge d'erreur dont les entreprises disposent dans l'attribution de ressources pour la sécurité informatique en comparant les dépenses annuelles moyennes en sécurité informatique des PME et des grandes entreprises avec les pertes estimées liées à une seule attaque. En prenant la dépense moyenne en sécurité informatique d'une PME (**213 000 dollars**) et en la comparant au coût moyen d'une attaque (**86 500 dollars**), il suffirait que les dispositions en matière de sécurité informatique d'une PME empêchent **2,5** attaques pour économiser des fonds considérables, sans parler des atteintes à la réputation.

L'analyse de l'impact financier moyen d'un piratage de données

PME



Grandes entreprises



CONCLUSION

L'impact financier des cyberattaques doit être envisagé en fonction des ressources engagées pour les combattre. Les entreprises européennes reconnaissent le besoin de renforcer la sécurité informatique face à la multiplication des attaques. **26%** d'entre elles considèrent que l'augmentation du personnel informatique interne et des équipes de sécurité informatique est la bonne réponse à apporter au cours des 12 prochains mois, tandis que **36%** estiment qu'il serait préférable de mettre en œuvre des solutions logicielles de sécurité informatique plus complexes. Or, les budgets ne semblent pas offrir le soutien nécessaire.

La solution pour atténuer efficacement l'impact des attaques consiste à adopter une approche holistique de la sécurité informatique, plutôt que de compter uniquement sur les technologies de détection. La formation et la veille stratégique constituent un élément clé de la réduction des risques et de l'augmentation du retour sur investissement en sécurité informatique, que ce soit au niveau du personnel que des logiciels. La prévention passe avant tout par une bonne préparation et ce n'est qu'en abordant le problème en termes de reprise de l'activité et d'atténuation des risques, au-delà de la simple prévention, que les organisations pourront véritablement réduire leur exposition aux cyberattaques.