Communiqué de presse,
Paris, le 13 décembre 2018

PME françaises : Des compétences numériques insuffisantes face aux grands enjeux de la sécurité informatique

52% des PME françaises n'ont pas encore renforcé leurs mesures de sécurité numérique

Le RGPD est une excellente nouvelle pour les entreprises, quels que soient leur taille et leur secteur, car il met sur un pied d'égalité tous les acteurs européens dans la bataille de l'économie numérique. Pourtant, selon une étude IFOP pour Kaspersky Lab et Euler Hermes, six mois après sa mise en application, 45% des décideurs au sein de PME reconnaissent que leur entreprise n'a pas renforcé ses mesures de sécurité. Cette part s'élève à 52% lorsqu'il s'agit de PME comptant entre 150 et 249 employés. Cela est d'autant plus inquiétant que 21% des PME ont été victimes d'une cyber-attaque au cours des 12 derniers mois. Un paradoxe qui démontre que les compétences numériques des PME sont insuffisantes face aux nouveaux enjeux de l'économie numérique.

Les PME doivent encore adresser les problématiques de mise en conformité avant de pouvoir espérer tirer des bénéfices économiques du RGPD, ce qui n'est pas chose aisée. En effet, malgré les nouvelles contraintes réglementaires, 77% des PME n'ont pas réalisé d'audit informatique en 2018. Un chiffre inquiétant qui atteint 82% dans le secteur des services qui, pourtant, est celui qui traite le plus de données personnelles clients (48% contre 43% en moyenne).

Il n'y a donc rien de surprenant à ce que 20% des répondants ne sachent toujours pas si leur entreprise traite des données personnelles ! Le secteur industriel est le plus en retard sur cette question (28%).

« Pour la survie d'une PME, la cybersécurité est essentielle, car les menaces sont omniprésentes : faux sites Web, logiciels malveillants, rançongiciels, réseaux et bornes Wi-Fi non sécurisés, voire équipements professionnels perdus ou volés, d'autant plus avec le développement du Bring Your Own Device (BYOD) au sein des entreprises. Mettant l'accent sur leur développement et sur leurs occupations quotidiennes, les PME n'accordent pas toujours la priorité à la prévention de ces attaques. Pourtant, un seul incident peut entraîner d'énormes coûts financiers, mais aussi la perte de confiance des partenaires et des clients, si ce n'est signer la fin de son activité, dans le cas où ses opérations seraient perturbées ou arrêtées, » **commente Tanguy de Coatpont, DG France et Afrique du Nord, Kaspersky Lab.**

Le paradoxe de la cybersécurité

Malgré les retards en matière de sécurité et de protection des données personnelles, 76% des entreprises consultées reconnaissent que la sécurité informatique est un réel sujet d'inquiétude.

Mais l'inquiétude n'empêche pas les décisionnaires de percevoir les bénéfices qu'ils peuvent retirer à améliorer la protection de leur entreprise.

Interrogés sur les technologies qu'ils identifiaient comme porteuses d'opportunités au cours des deux prochaines années, les répondants placent la cybersécurité en 2e position (39%). Elle arrive derrière le Big Data et l'analyse des données (47%), mais loin devant l'intelligence artificielle (29%), l'automatisation (29%) et même le Cloud Computing (30%).

Malgré ces résultats encourageants, et bien que 64% des PME fassent de l'amélioration de la cybersécurité une priorité, seules 19% d'entre elles peuvent d'ores et déjà affirmer que des investissements sont prévus.

La vulnérabilité technologique va de pair avec la vulnérabilité juridique et humaine. Elles sont moins d'une sur deux à être assurée (43%) et seulement 51% à former leurs employés.

Ce décalage peut s'expliquer par le fait que la définition des politiques de sécurité au sein des PME est la responsabilité conjointe de plusieurs équipes, ce qui peut ralentir le processus de prise de décision. Pour 61% des répondants, l'équipe informatique est impliquée, puis vient l'équipe dirigeante (45%) et enfin une équipe de sécurité dédiée (23%). Malgré un manque de compétentes informatiques reconnu dans les petites et moyennes entreprises, seules 9% invitent des partenaires extérieures à participer.

Les PME, aussi exposées que les grands groupes par les cyber-menaces

En octobre 2018, le secrétaire d'Etat au numérique Mounir Mahjoubi a annoncé un plan à destination de 2 millions de TPE/PME afin de diffuser les bonnes pratiques en matière de sécurité informatique. Cette annonce est intervenue quelques mois seulement après le lancement de la plateforme cybermalveillance.gouv.fr, également destinée à la sensibilisation des publics vulnérables, dont les PME.
Malgré ces efforts, moins de 50% des décisionnaires au sein des petites et moyennes entreprises sont informés des efforts de sensibilisation et de protection mis en place par les organisations officielles (CNIL, ANSSI, gouvernement, etc.).

Cette situation est regrettable car les PME sont devenues une cible prioritaire pour les cyber-criminels. Au cours des 12 derniers mois, 21% d'entre elles ont été victimes d'une cyber-attaque. La plupart du temps, le coût de ces attaques ne dépasse pas les 10 000 € (64%), bien qu'il soit parfois beaucoup plus élevé. 14% des répondants admettent que les attaques leur ont coûté plus de 51 000 €, et même plus de 100 000 € pour 6% d'entre eux.

Les 5 risques informatiques qui inquiètent le plus les responsables sont :

- Les e-mails frauduleux (52%),
- Le piratage de données (51%),
- Les malwares (41%),
- La perte ou le vol de matériel informatique (26%)
- La fraude / malversation / escroquerie (24%).

Si les risques sont multiples et variés, leurs conséquences le sont tout autant. Suite à une attaque ou une fuite de données, les dirigeants sont particulièrement préoccupés par :

- La divulgation d'informations confidentielles (63%),
- L'impact négatif sur la réputation de l'entreprise (38%),
- Les pertes d'exploitation / de chiffre d'affaires (30%),
- Les pertes financières directes (28%)
- La cyber extorsion (17%).

« *Trois conséquences du top 5 font directement référence à un impact financier. Les PME françaises ont compris que leur trésorerie est en première ligne, mais prennent-elles les dispositions nécessaires pour se protéger ? La perte financière liée à une fraude ou une cyber-attaque est assurable, ce qui signifie que les entreprises n'ont pas à en supporter le préjudice. Pourtant, le choix de l'assurance reste minoritaire : moins d'une PME sur deux est assurée contre ces risques. Les PME sont conscientes de leur exposition, mais pas des moyens qui existent pour la réduire* », **explique Sébastien Hager, Responsable de la souscription assurance fraude chez Euler Hermes France.**

Révélateur du manque de sensibilisation des PME aux évolutions réglementations et les obligations qui les accompagnent, seuls **9%** des répondants craignent le versement d'une ou plusieurs amendes. Le risque est pourtant bien réel, lorsque l'on sait qu'en 2018, la CNIL a enregistré près de **10 000** plaintes (dont **6 000** depuis le 25 mai et la mise en application du RGPD), soit **35%** de plus qu'en 2017.

Le secteur du commerce, un exemple à suivre

Le secteur du commerce s'illustre par une bonne maitrise des technologies et une compréhension aigue des enjeux de sécurité. **62%** des dirigeants de PME travaillant dans le secteur du commerce jugent « bon » le niveau de maturité technologique de leur entreprise. Convaincus que la cybersécurité est un sujet de préoccupation pour leurs clients (**73%**, contgre **54%** en moyenne) et leurs employés (**69%**, contre **53%** en moyenne), les dirigeants de PME sont **89%** à s'inquiéter des questions de sécurité. Il n'y a donc rien de surprenant à ce qu'ils aient été les plus promptes à prendre des mesures concrètes lors de la mise en place du RGPD (**71%** contre **55%** en moyenne).

Malgré tous ces efforts, le commerce est le secteur le plus touché par les cyber-attaques (**35%** contre **21%** en moyenne).

Méthodologie :
Etude IFOP pour Kaspersky Lab réalisée en ligne auprès d'un panel de 702 décideurs de PME en France, du 5 au 9 novembre 2018

À propos de Kaspersky Lab
Kaspersky Lab est une société de cybersécurité mondiale qui est active sur le marché depuis plus de 20 ans. L'expertise de Kaspersky Lab en matière de « Threat Intelligence » et sécurité informatique vient perpétuellement enrichir la création de solutions et de services de sécurité pour protéger les entreprises, les infrastructures critiques, les gouvernements et les consommateurs à travers le monde. Le large portefeuille de solutions de sécurité de Kaspersky Lab comprend la protection avancée et complète des terminaux et un certain nombre de solutions et de services de sécurité dédiés afin de lutter contre les menaces digitales sophistiquées et en constante évolution. Les technologies de Kaspersky Lab aident plus de 400 millions d'utilisateurs et 270 000 clients à protéger ce qui compte le plus pour eux. Pour en savoir plus : www.kaspersky.fr

A propos d'Euler Hermes
Prévoir les risques commerciaux et d'impayés aujourd'hui, c'est protéger la trésorerie demain
Euler Hermes est le leader mondial des solutions d'assurance-crédit et un spécialiste reconnu dans les domaines du recouvrement et de la caution. Avec plus de 100 années d'expérience, Euler Hermes offre une gamme complète de services pour la gestion du poste clients. Son réseau international de surveillance permet d'analyser la stabilité financière de PME et de grands groupes actifs dans des marchés représentant 92% du PNB global. Basée à Paris, la société est présente dans 52 pays avec plus de 6 050 employés. Membre du groupe Allianz, Euler Hermes est noté AA par Standard & Poor's. La société a enregistré un chiffre d'affaires consolidé de 2,6 milliards d'euros en 2017 et garantissait pour 894 milliards d'euros de transactions commerciales dans le monde fin 2017. Plus d'informations : eulerhermes.com

Contacts presse :
Euler Hermes
Maxime Demory +33 (0)1 84 11 35 43
maxime.demory@eulerhermes.com

Hotwire Global pour Kaspersky Lab
KasperskyFrance@hotwireglobal.com
Marion Delmas/ Séverine Randjelovic / Noémie Minster/ Aliénor Gamerdinger
01 43 12 55 55