Comment accompagner et améliorer la cybersécurité des PME ?

Les paysages informatique et économique ont été marqués par de nombreuses attaques de ramsomwares ces derniers mois : Wannacry et NotPetya, pour ne citer qu'eux, ont touché des milliers d'entreprises à travers le monde.

En France, 92% des entreprises déclarent avoir subi une ou plusieurs attaques en 2017, contre 80% l'année précédente. Mais si les grands groupes et les TPE-PME sont confrontés aux mêmes menaces, les dégâts engendrés par une cyberattaque restent plus destructeurs pour ces dernières. Les PME représentent 50 000 victimes en France chaque année et près d'un tiers d'entre elles font état d'un impact financier contre seulement 7,2% des grandes entreprises. En effet, sur le terrain de la cybersécurité, les entreprises ne se battent pas toutes avec les mêmes armes. Plus vulnérables et moins préparées aux attaques, les PME constituent une cible de choix pour les cybercriminels. Comment expliquer ce décalage entre les PME et les grands groupes ? Quelles solutions mettre en place pour aider les PME à mieux appréhender les failles de sécurité ?

Le coût conséquent des solutions de sécurité

Actuellement, de profondes disparités entre les entreprises marquent le paysage de la cybersécurité et les raisons sont, avant tout, d'ordre budgétaire. En effet, les plus petites structures n'ont généralement pas capacité à dégager des ressources financières dédiées pour adresser les problématiques de protection, généralement par manque de moyen ou à cause d'une mauvaise évaluation des risques. Or, les solutions existantes contre les cybermenaces représentent un coût important. A titre d'exemple, un grand groupe qui souhaite évaluer son niveau de sécurité s'oriente généralement vers un cabinet de conseil, prend le temps de réaliser un audit, attend les résultats et choisit les mesures adéquates (et souvent onéreuses) pour se mettre à niveau. Une démarche que peu de petites entreprises peuvent mettre en place.

Etant moins flexibles en termes de coûts et de temps que les grandes entreprises, les PME ont une vision beaucoup plus pragmatique de leur activité et se concentrent d'abord sur leurs tâches opérationnelles et la satisfaction de leurs clients. La sécurité de leur infrastructure informatique et la protection de leurs données n'intervient qu'en second temps, car ces mesures ne sont pas primordiales au développement immédiat de l'entreprise.

Le manque de compréhension des menaces

L'autre facteur qui explique le retard des PME est leur manque de maturité et de connaissances sur le sujet de la cybersécurité. Les petites entreprises semblent avoir bien du mal à se protéger correctement contre ces risques, avec 29 % des entrepreneurs en TPE-PME qui déclarent n'avoir rien changé à leur politique de sécurité à la suite d'une attaque.

En effet, à l'inverse des grands groupes, les PME ont rarement de postes et les ressources dédiés à

la gestion de leur parc informatique et de leur sécurité. Responsable informatique, Chief Data Officer etc, ne font pas partie de leur paysage et cela ne facilite pas leur travail de compréhension des menaces.

En conséquence, 23% d'entre elles se retrouvent avec une équipe de sécurité occupée par des tâches de maintenances et de gestion des outils de sécurité, plutôt qu'à effectuer des analyses révélatrices de l'état de santé de leurs infrastructures. 53% des équipes de cybersécurité existantes perdent un temps considérable à s'occuper d'opérations de routines (incident, mises à jour, etc.). L'enjeu actuel est donc double : aider les entreprises à évaluer leur niveau de sécurité et informer correctement les équipes opérationnelles sur la manière dont elles peuvent se protéger correctement des menaces. Car si les lois européennes sur la protection des données comme la RGPD par exemple, imposent aux entreprises de savoir exactement où se trouvent leurs données sensibles et comment elles sont protégées, la régulation ne donne cependant aucune piste sur la manière dont les entreprises peuvent financer leur cybersécurité par exemple ou savoir si elles sont suffisamment protégées. Difficile donc pour des PME de prévenir les autorités en cas de failles si elles ne disposent d'une visibilité précise de leur niveau de protection

La solution : sensibiliser tout en s'adaptant aux contraintes des petites entreprises

En réponse à cette problématique, l'Anssi a initié des démarches pour démocratiser l'information aux PME sur tout le territoire, avec la mise en place entre autres, d'un site Internet complet sur la question : cybermalveillance.gouv.fr. Notre ministre de l'Intérieur a également insisté sur la nécessité de développer la lutte à l'échelle européenne afin de construire la résilience des PME dans les années à venir. ?

Aujourd'hui, il est urgent de poursuivre ce travail de sensibilisation, en apportant des solutions clés en main pour équiper les PME avec les bases de la sécurité. Le but n'est pas de couvrir toutes les fonctions mais d'instaurer une « première brique » de sécurité pour évoluer petit à petit vers une protection plus poussée, le temps d'identifier les besoins propres à l'entreprise et de s'adapter à son budget. Au fur et à mesure que l'entreprise se développe et gagne en maturité, des solutions de sécurité supplémentaires peuvent être ajoutées. Des tests de vulnérabilités peu couteux peuvent par exemple être initiés et permettre ainsi un suivi régulier de la surface d'attaque.

Externaliser le travail de protection auprès de prestataires comme les opérateurs de télécommunication est une option à envisager pour filtrer les menaces en contrôlant et en décontaminant le flux de données entrant sur le réseau de l'entreprise par exemple. Ce type de solution pensée pour l'entreprise dans son ensemble est à même de sécuriser les échanges que peuvent avoir les utilisateurs sur Internet ou avec leurs collaborateurs au sein de l'entreprise.

Apporter des protections basiques de sécurité aux PME tout en les éduquant, est une première étape vers la réduction des dégâts causés par les cyberattaques qui menacent profondément notre économie. Car au-delà de l'impact sur le chiffre d'affaires, c'est l'activité même de l'entreprise et sa chaîne de production qui sont en jeu, sans oublier bien sûr les préjudices humains (division des salariés, incertitude du dirigeant, faillite, etc.), les conséquences sur l'image de l'entreprise et sur l'aspect légal, à l'approche de la date butoir du devoir de conformité au RGPD, le 25 mai 2018.