Sécurité informatique et petites entreprises : un dialogue de sourds ?

Télés, radios, presse écrite, on parle aujourd'hui partout de cybersécurité, comme de même des malwares, de la cyber-malveillance, des hackers. Certains sont même devenus des mots familiers du grand public et des entreprises. Et pourtant, très régulièrement, la presse se fait l'écho d'études et de sondages qui montrent qu'une grande partie, pour ne pas dire la majorité des petites entreprises françaises sont peu ou mal sécurisées, voire pas sécurisées du tout.

Comment expliquer ce phénomène ?

Les médias ne rapportent le plus souvent que les cas d'attaques ayant ciblé de grandes entreprises médiatisées et connues. Tout d'abord parce que leur nom parle au plus grand nombre. Ensuite parce qu'elles sont plus « regardées » au vu de leur poids économique. Et enfin parce que les journalistes suivent plus volontiers l'actualité des entreprises à rayonnement national ou international.

On parle donc beaucoup de cybersécurité, mais par le biais d'attaques très ciblées.

Malheureusement les petites et moyennes entreprises ne se reconnaissent pas dans le profil de ces sociétés prises pour cible et mises en avant par les médias. Cela résulte en un manque cruel d'intérêt pour ces problématiques de leur part. Une entreprise de 15 personnes pense ne présenter aucun intérêt pour des cybercriminels contrairement à une entreprise de 4000 personnes. Cette analyse est sans doute vraie, mais le problème réside ailleurs. Il existe de très nombreux groupes de pirates, et autant de variété de types d'attaques dont le but demeure le même : faire du profit illégalement. La petite entreprise ne sera pas ciblée de la même manière qu'une grande, la méthode de piratage utilisée sera différente. L'attaque ne se fera peut-être pas sur une entreprise précisément mais sur un ensemble. Ces attaques massives cherchent à toucher et infecter le plus grand nombre de machines.

L'homme apprend par sa propre expérience ou celle de ses pairs. Si les nombreux cas d'attaques touchant les petites entreprises étaient plus souvent mis en lumière, on peut légitimement se demander si les entreprises de la même typologie se sentiraient davantage concernées ?

Des fournisseurs de sécurité peu concernées

Autre point, les sociétés de sécurité, celles qui apportent la protection, s'intéressent-elles, à ces petites entreprises, ou en tous cas, suffisamment ? Notoriété, chiffre d'affaires, développement, concurrence, toutes les entreprises doivent répondre à ces enjeux. Compter de grands groupes parmi ses clients est un gage de réussite et de qualité.

Si la vocation d'une société de sécurité est d'apporter une protection, elle devrait s'adresser à tous les segments de marché, et adapter son discours à chaque problématique. Certaines entreprises de petite taille sont tenues, par leur activité, à protéger des données très sensibles. La problématique est la même pour une mairie, quelle que soit sa taille. Elle aussi a la nécessité de garantir la protection des données de ses citoyens, surtout à l'heure du RGPD. Le manque de sécurité dans les TPE et PME est, peut-être aussi, de la responsabilité des fournisseurs de protection informatique.

Des petites entreprises mal informées

Ce sont les revendeurs en région, présent sur le terrain et rencontrant ces entreprises, qui doivent bien souvent insister auprès de ces entreprises pour installer des outils de sécurité. Et cela vaut même le premier d'entre eux, celui qui semble évident en 2019 : l'antivirus. Inconscience ou manque d'intérêt et de temps, de nombreux dirigeants de TPE ou de PME ne se préoccupent pas de la sécurité. Il même encore fréquent d'entendre encore des rumeurs disant que ce sont les entreprises de sécurité qui créent les virus

Inquiétant, car si ce mythe est depuis bien longtemps dépassé, il est clair que l'ensemble des maillons de la chaîne qui sensibilise, informe, équipe et suit les utilisateurs a failli quelque part. Editeurs et chercheurs en sécurité le répètent sans cesse, et avec eux les médias sérieux et les pouvoirs publics, la menace induite par la cybercriminalité n'est pas une légende. Personne ne brandit de menace fictive pour inquiéter les utilisateurs et les entreprises ou pour vendre des produits.

L'homme apprend par l'expérience. Faut-il alors attendre de se retrouver avec l'intégralité de ses données chiffrées pour réagir ? Libre à chacun et à chacune de répondre à cette question et d'interroger sa responsabilité face à ses clients, fournisseurs et partenaires