Anticiper la menace cyber : un impératif pour chaque entreprise

Julien LOPIZZO
Président Directeur Général
Semkel

Quelle que soit leur taille, les entreprises doivent faire de l'investissement dans la protection de leur patrimoine numérique et informationnel une priorité absolue. Avec la mise en application imminente de la directive NIS 2 pour tous les états européens à horizon mi-octobre, cette mise en conformité des organisations au niveau européen va devenir une obligation. Pour se protéger efficacement, la capacité d'anticipation de la menace s'avère la méthode la plus efficace.

Pourtant, beaucoup d'entreprises considèrent encore aujourd'hui que cet investissement ne les concerne pas, une erreur qui peut coûter cher.

Enjeux de la cybersécurité face à l'augmentation de la menace

La cybersécurité est devenue l'un des défis majeurs du XXIe siècle. Le dernier rapport de Davos la place dans le top cinq des risques majeurs en 2024 et les chiffres continuent de pointer du doigt l'augmentation croissante du nombre de cyberattaques alors que les craintes autour des Jeux Olympiques ne cessent de raviver le spectre d'une paralysie globale des systèmes.

En 2021 déjà, 54% des entreprises françaises déclaraient avoir été attaquées. Ransomware, phishing, attaque par déni de services, arnaque au président, deepfake… La diversification et la sophistication de la menace résultent en partie de l'accès facilité à l'intelligence artificielle mais aussi de la professionnalisation globale du cybercrime qui largement profité de l'instabilité géo-économique des états au cours des dernières années. Ce niveau de complexification des attaques est un paramètre essentiel à mesurer pour se protéger efficacement car aucune organisation n'est à l'abri aujourd'hui.

Les grandes entreprises doivent exiger de leurs prestaires, fournisseurs et partenaires d'accès, qu'ils se plient de plus en plus au même niveau de protection que leurs propres systèmes d'informations/exploitation.
Une cyberattaque peut en effet être dévastatrice pour une entreprise et l'interconnexion des organisations entre elles est un facteur multiplicateur de risques pour les entreprises. Elle peut en compromettre la croissance, aller jusqu'à provoquer un arrêt d'exploitation de plusieurs jours à plusieurs mois, voire menacer leur existence. Au-delà de l'atteinte à sa pérennité économique et financière, une cyberattaque est un coup puissant porté à son image. Elle peut menacer sa réputation si certaines données sensibles ou confidentielles sont révélées.

Anticiper la menace, c'est déjà se protéger

Pour limiter ces risques, il existe une règle d'or : anticiper en créant une première ligne de défense efficace. Ce "premier kilomètre" de la cybersécurité, appelé *Threat Intelligence*, peut prendre plusieurs formes. Parmi elles, l'évaluation des vulnérabilités et de la surface d'attaque, la mise en place d'outils de surveillance et de détection avancée des menaces... Il est aussi crucial de se doter de solutions d'investigation et de défense suffisamment performantes et à la pointe de la technologie pour éviter à des réseaux entiers d'être paralysés en cas d'attaques.

Grandes entreprises, TPE, PME, ETI : toutes sont sur un pied d'égalité face aux menaces en ligne. C'est en investissant communément, et de manière proactive, sur ces outils et les mesures de défense adaptées que les organisations pourront renforcer leur résilience face aux cybermenaces toujours plus nombreuses et sophistiquées.