Complémentarité technologique et souveraineté : l'âge de maturité

Plus que jamais, la cybersécurité est un enjeu stratégique et réglementaire pour l'ensemble des ETI, PME, secteur public, associations… Tout le monde est concerné et peut être amené à gérer une attaque. Dans ce contexte, si faire évoluer sa gouvernance cybersécurité est une évidence, il convient également de s'équiper de solutions adaptées à son organisation. Mais lesquelles choisir et comment élever au mieux son niveau de sécurité pour réduire au maximum son exposition au risque cyber ?

Cartographier son organisation et ses processus

Avant de parler d'outils, il est important de connaitre précisément son entreprise, d'identifier tous ses processus de communication et d'échanges, les acteurs internes et externes et de parfaitement identifier la place qu'occupe le numérique. Cette vision précise doit permettre d'avoir une vue d'ensemble exhaustive pour ensuite de se poser la question des outils à mettre en place. Attention donc de bien prendre le temps de réaliser cette tâche de fond.

À qui confier les clés de la sécurisation de son système d'information ?

Une tentation de nombre d'organisations est d'utiliser une solution unique pour gérer leur sécurité. Dans les faits, si cette approche peut répondre à des besoins fondamentaux, elle trouve rapidement ses limites. C'est en ce sens qu'il est intéressant et nécessaire d'avoir une approche basée sur la complémentarité technologique. Pour ce faire, choisir des fournisseurs qui affichent une politique de partenariat volontariste avec d'autres concepteurs de solutions de confiance est un gage de succès.

Cette notion de confiance est également à étudier sous différents aspects. Sur ce point, l'approche souveraine prend alors tout son sens. En effet, en matière de sécurité IT, les éditeurs, intégrateurs, et sociétés de conseil françaises occupent une place de choix et sont largement reconnus à l'international pour leur expertise et la qualité de leurs offres. De plus, travailler avec des entreprises souveraines permet d'accéder à d'autres bénéfices concrets comme la proximité des équipes (notamment support) tout en s'appuyant sur des solutions qui respectent la législation française et européenne. Sur ce point, les aspects liés à la confidentialité des données sont alors préservés.

Au regard de ces éléments, les organisations
pourront donc s'adosser à un schéma directeur et adapté à leurs enjeux. Bien sûr, comme tous les projets de cybersécurité, il n'existe pas de réponse à 100 %, mais une telle mise en œuvre permet d'atteindre une certaine sérénité contre le risque cyber. Il appartient donc aux entreprises comme aux concepteurs de technologies français de travailler en proximité pour associer le meilleur de leurs expertises afin de créer des espaces numériques de confiance.

Par Christophe BOUREL, CEO de Kub Cleaner