Cédric Marécaux et Didier Lefebvre ©DR

L'IT : DES CHALLENGES AU SERVICE DE LA SÉCURITÉ

PAULINE JANS

Après 30 ans dans le secteur marchand, c'est au SeGEC que Didier Lefebvre a décidé de poser ses valises, apportant avec lui son expertise du monde de l'IT. Coup d'œil sur le directeur du Service informatique et sur l'un de ses chevaux de bataille : la sécurité avec la stratégie *Zero Trust*.

« *Lorsque je suis arrivé, c'était chaotique* », confie Didier. C'est ainsi qu'il a pris ses fonctions en janvier 2023 : à partir d'une page blanche. « *Il a fallu définir les missions du service au sein du SeGEC mais surtout, en déterminer les priorités importantes à mener.* » Un challenge que Didier s'est donné pour mission de relever.

Un changement de paradigme

La sécurité informatique est devenue primordiale avec l'évolution du modèle de travail. Avant la pandémie de 2020, les travailleurs effectuaient leurs tâches principalement au sein du bâtiment, et donc là où se trouvaient les serveurs. Tout était cloisonné. Mais avec la crise sanitaire, le travail s'est ouvert. « *Les serveurs sont donc maintenant dans des infrastructures "cloud"* (NDLR : nuages). *On ne travaille plus uniquement sur son ordinateur. Il y a donc une multiplication des routes possibles pour s'introduire* », explique Didier.

Didier Lefebvre ©DR

Le saviez-vous ? « *Les domaines de l'éducation et de la recherche sont les domaines les plus ciblés par les hackeurs car ce sont les moins bien gardés puisque ce sont ceux qui ont les budgets les plus serrés.* »

Mais pour quelles raisons attaquer le SeGEC ? « *Souvent, c'est pour faire du rebond : nous attaquer pour attaquer quelqu'un d'autre.* »

Lorsque Didier est arrivé parmi nous, le SeGEC était confronté à 700 attaques par jour. « *Pour chacune d'entre elles, il a fallu agir. Cela signifie qu'il a fallu prendre le temps de les classifier et de bloquer les adresses malicieuses* », décrit le directeur du Service IT. Aujourd'hui, grâce aux efforts fournis, le SeGEC n'en connait plus qu'une cinquantaine.

« *Nous avons couru au feu et mis en place des défenses de bastions* », poursuit-il. Ces actions permettent maintenant à l'équipe IT de se concentrer sur d'autres aspects de la sécurité.

Une stratégie *Zero Trust*

« *La cybersécurité, c'est quelque chose de très complexe et en constante évolution. C'est la raison pour laquelle on a adopté la solution Zero Trust. Elle repose sur le principe de ne jamais faire confiance par défaut, même à ceux à l'intérieur du réseau* », explique Didier. Parmi les mesures mises en place, la connexion à double authentification est essentielle : « *Il est nécessaire de mettre en place un système de vérification explicite de l'identité de l'utilisateur.* »

Cependant, Didier et son équipe font face à divers obstacles pour développer leur stratégie, notamment ceux liés aux utilisateurs. « *Je pense que l'IT est parfois difficile à comprendre. Imposer de nouvelles pratiques n'est pas simple. C'est un processus qui demande un changement de comportement. Et changer le comportement des utilisateurs pose parfois des problèmes.* » Il rappelle qu'il n'est plus possible de faire « *comme avant* » et qu'il est crucial de se protéger. « *Nous devons être des pares-feux humains.* »

Un travail d'équipe

Comme le souligne Didier, ce travail n'est pas celui d'un seul homme. Il est entouré d'une équipe de choc. Une équipe qui se dit prête à relever les nouveaux défis qui s'annoncent.

Pour conclure cet entretien, Didier s'est penché sur l'avenir du numérique au sein du SeGEC : « *Il faut reconstruire beaucoup de choses pour être aptes à utiliser les nouvelles technologies, comme l'intelligence artificielle. En parallèle, de grands chantiers, comme ceux liés à la durabilité, vont nous être imposés. Nous devrons réfléchir à une utilisation du numérique à bon escient, ce qui engendrera de nouveaux changements.* »

Affaire à suivre donc ! ▪