PG Solutions

David Champmartin
Directeur du développement des affaires

Chronique informatique

Cybersécurité : votre ville est-elle bien outillée ?

Les villes et municipalités comptent parmi les cibles les plus vulnérables aux cyberattaques; un danger encore tabou et pourtant en très forte expansion. Face à cette menace complexifiée, la protection optimale des données et des infrastructures municipales n'est vraiment plus une option.

La multiplication des cyberattaques est un phénomène en inexorable croissance, orchestré par de véritables organisations le plus souvent automatisées, nombreuses, et en recherche avide et constante de toute faille informatique dans les infrastructures les plus vulnérables, soit celles qui sont les moins bien protégées.

Notre ère numérique est clairement propice à l'expansion de cette cybercriminalité, et le monde municipal n'y échappe pas. Alors que les données recueillies et stockées abondent, qu'elles sont migrées vers des infrastructures tierces et que de plus en plus d'employés travaillent à distance, les organisations municipales n'ont pas forcément adapté leurs pratiques et leurs ressources pour détecter les cyberattaques, quelle que soit leur nature, et s'en prémunir efficacement.

Rappelons qu'il suffit d'un clic malencontreux d'un(e) employé(e) pour ouvrir la porte à une intrusion malveillante complexe qui compromettra les systèmes de l'organisation si celle-ci n'est pas adéquatement protégée.

Les conséquences sont souvent sous-estimées, surtout dans un contexte de renforcement législatif sérieux et récent. L'organisation est notamment impactée par les rançons et les frais de justice encourus ainsi que par le temps requis pour mettre en place en urgence des mesures de sécurité. De plus, sa crédibilité se retrouve lourdement affaiblie.

D'autant que les nouvelles abondent concernant des cyberattaques, et que la récente législation relative à la protection des renseignements personnels impose désormais aux organisations de déclarer à l'autorité compétente tout incident de confidentialité survenu, selon une procédure spécifique, entre autres mesures obligatoires.

Face à cette nouvelle réalité, l'organisation municipale doit impérativement se munir dès à présent d'une solution de cybersécurité qui lui fournira une protection robuste de surveillance, de détection et de réponse contre les menaces portées à son infrastructure informatique.

Et pour protéger l'ensemble de l'infrastructure informatique, une solution unique et complète est nécessaire. Cela permet notamment une surveillance en continu (24/7) et évite la gestion de plusieurs fournisseurs en cybersécurité.

L'embauche d'une personne experte en cybersécurité dans l'équipe municipale serait un défi coûteux. L'organisation préférera ainsi se munir d'une solution à la pointe de l'expertise en cybersécurité, qui inclut notamment l'accès à des analystes experts en cybersécurité pour un soutien personnalisé comme des conseils techniques, mais aussi des recommandations stratégiques en la matière. Elle a également tout intérêt à gagner du temps pour réaliser l'installation de cette solution, en optant par exemple pour le *plug & play* et un système simple d'utilisation.

Face à la multiplication des attaques visant les organisations municipales et à la pression législative encadrant la protection des données, qui ajoute nombre de responsabilités et mesures applicables, les villes et municipalités de toutes envergures doivent sans attendre s'assurer d'être protégées.

Quelle que soit la complexité de leur réseau, il leur est désormais crucial de se doter dans les meilleurs délais d'une solution qui les protègera complètement et selon les meilleures pratiques de l'industrie.

David Champmartin, directeur du développement des affaires, en collaboration avec Sonia Maatem.