Des cybermenaces bien réelles

Au cœur de la révolution numérique, les municipalités du Québec sont de plus en plus dans le viseur des cybercriminels. Une menace croissante, qui soulève des questions cruciales sur la cybersécurité et la vulnérabilité des données municipales, peu importe la taille de l'organisation, peu importe sa situation géographique. Plus il y a de failles dans les outils numériques ou de manque de méfiance des employés, plus le risque d'être une cible des cybercriminels est élevé.

Les conséquences d'une attaque réussie vont au-delà de la simple perturbation des opérations. La compromission des données sensibles et les demandes de rançon engendrent des dommages financiers et réputationnels considérables, en plus de causer du tort aux citoyens. Les services à la population sont interrompus et, élément non négligeable, l'équipe administrative est paralysée.

En matière de cybercriminalité, personne n'est à l'abri. La Ville de Lac-Mégantic l'a d'ailleurs réalisé avec consternation le 30 novembre dernier quand une cyberattaque a paralysé l'écocentre, l'hôtel de ville, le centre sportif et la station touristique Baie-des-Sables.

« Les cyberattaques sont de plus en plus fréquentes et complexes. Malgré toutes les mesures qui sont mises en place, les organismes publics n'échappent malheureusement pas à cette réalité », pouvait-on lire dans le communiqué émis par la Ville au lendemain de la cyberattaque.

Quand des outils de surveillance spécifiques sont déployés en prévention, certaines attaques peuvent être contrées. Lorsque c'est impossible, on peut au moins intervenir rapidement et limiter les dégâts.

– **Véronica Romero-Rosales**
Coordonnatrice à la cybersécurité à la Direction des projets spéciaux de la FQM

Investir dans la protection et la formation

Cette inévitable confrontation avec le cybercrime met en lumière l'urgence d'une préparation minutieuse de la part de toutes les administrations municipales. Selon la Fédération québécoise des municipalités (FQM), le nombre de campagnes d'hameçonnage visant les organismes municipaux a augmenté de 13 % de 2021 à 2022. Comme 91 % des cyberattaques ont pour point de départ un courriel, chaque employé côtoie le danger.

Ainsi, au-delà des dimensions techniques, la cybersécurité nécessite une transformation profonde de l'attitude organisationnelle et humaine. « Nos données démontrent clairement que le facteur humain demeure la principale porte d'entrée des cyberattaques », indique Nadine Dodeman, souscriptrice principale en analyse de risques au Fonds d'assurance des municipalités du Québec (FAMQ), géré par la FQM.

Les campagnes d'hameçonnage visant les organismes municipaux ont augmenté de 13 % de 2021 à 2022. 91 % des cyberattaques ont comme point de départ un courriel.

– **Lila Beddar**
Directrice du Service de la soumission du FAMQ

Elle a constaté que les municipalités sont de plus en plus conscientisées aux risques et, bonne nouvelle, qu'il existe une foule d'outils simples et efficaces à mettre en place. Ces outils pourraient même faire économiser quelques dollars en primes d'assurance.

« Par exemple, une politique de mots de passe est un moyen peu coûteux et efficace. Lors de l'analyse, l'assureur regarde tout ce qui a été fait par la municipalité pour mieux se protéger; si elle a un plan de relance en cas de cyberattaque, si les employés ont reçu une formation, s'il y a des outils de protection comme des pare-feu, un VPN ou l'identification à deux facteurs », énumère Mme Dodeman.

« Pour un assureur, c'est vraiment important que de telles mesures soient en place, que l'organisation utilise des réseaux sécurisés, des logiciels à jour. Encore une fois, on considère toutes les politiques ou les mécanismes internes qui auront été déployés pour protéger l'organisation », ajoute sa collègue Lila Beddar, directrice du Service de la soumission du FAMQ.

Les réseaux organisés de la cybercriminalité

L'image du jeune *geek* dans son sous-sol est révolue. Le Centre canadien pour la cybersécurité, autorité reconnue sur le sujet qui est pilotée par le gouvernement du Canada, mentionne que le cybercrime est aujourd'hui l'apanage d'entreprises très bien organisées, d'hacktivistes ou encore de cybercriminels parrainés par des États.

« Ça n'ira pas en s'améliorant ! La technologie change à une vitesse effarante, et les méthodes employées par les cybercriminels se raffinent. Ce sont des réseaux internationaux. Il faut être conscient que les risques existent, se méfier et mettre en place des procédures pour mobiliser les équipes et éviter de tomber dans un piège », explique Véronica Romero-Rosales, coordonnatrice à la cybersécurité à la Direction des projets spéciaux de la FQM.

Certains cas de cyberattaques vécus par des municipalités et analysés par des experts en cybersécurité ont révélé que des informations sensibles circulaient depuis un moment sur le *Dark Web*. Armés de ces informations, les cybercriminels observent les façons de faire de l'organisation, amassent des données et ciblent les maillons faibles de la sécurité ou des membres du personnel.

« Quand des outils de surveillance spécifiques sont déployés en prévention (voir autre texte), certaines attaques peuvent être contrées. Lorsque c'est impossible, on peut au moins intervenir rapidement et limiter les dégâts », explique Mme Romero-Rosales, qui précise qu'en général, la somme investie en prévention représente environ 1 % de ce que coûterait une cyberattaque.

Le Fonds d'assurance des municipalités du Québec, anciennement la Mutuelle des municipalités du Québec, assure les cyberrisques depuis une quinzaine d'années. « Autrefois, seules les bases de données étaient assurées. Aujourd'hui, ce sont tous les produits d'assurance liés aux cyberrisques qui connaissent la plus forte croissance, et l'une des raisons est que du moment où on traite des données, on devient à risque », rappelle Nadine Dodeman.

Autrefois, seules les bases de données étaient assurées. […] Les grandes organisations ont commencé à s'en prévaloir, mais ce n'est plus le cas aujourd'hui puisque du moment où on traite des données, on devient à risque.

– **Nadine Dodeman**
Souscriptrice principale en analyse de risques au Fonds d'assurance des municipalités du Québec *(FAMQ)*, géré par la FQM

Avec toutes les obligations qui découlent de la Loi 25 et des responsabilités en matière de protection des données, les municipalités, qu'elles desservent 500 ou 100 000 habitants, doivent poursuivre le même objectif : intervenir de façon proactive en prévention et se doter d'outils efficaces pour réagir en cas de cyberattaques.

Si on a déjà entrevu la cybersécurité comme un luxe réservé aux grandes entités, il faut désormais la considérer comme une nécessité pour toutes les administrations locales. Et à l'ère du numérique actuelle, chaque membre du personnel municipal a son rôle à jouer dans la protection contre le cybercrime.

Un service sur mesure pour les municipalités

La Fédération québécoise des municipalités, en partenariat avec le gouvernement du Québec et VARS, une division de Raymond Chabot Grant Thornton, a développé un service de cybersécurité adapté aux municipalités qui comprend des protections efficaces pour diminuer les cyberrisques. Lorsque le pire survient, une intervention rapide peut grandement amoindrir les conséquences sur les opérations des municipalités touchées.

1. Accès à une équipe de cyberspécialistes en tout temps

Même si la municipalité possède des ressources en TI, elles ne sont pas nécessairement disponibles hors des heures de travail régulières. L'équipe externe de spécialistes en cybersécurité assure la surveillance 24/7. Si un cyberincident ou des activités inhabituelles ont lieu, des logiciels de surveillance interviennent. Au besoin, l'équipe de cybersécurité passe à l'action, et le responsable de la municipalité est rapidement prévenu.

2. Logiciel de surveillance des courriels

La grande majorité des cyberattaques (91 %) a comme point de départ un simple courriel. Un logiciel tel Perception Point peut détecter un courriel frauduleux ou une fausse facture d'un fournisseur. Dans le doute, l'équipe de cybersécurité fera une analyse plus approfondie pour éclaircir le cas.

3. Surveillance et analyse du *Dark Web*

Les cybercriminels utilisent le *Dark Web* pour acheter des mots de passe et des identifiants. Ainsi, ils peuvent s'infiltrer et même compromettre les comptes administrateurs de vos infrastructures. Une analyse sérieuse du *Dark Web* par des experts en cybersécurité permet de diminuer considérablement les risques liés à l'usurpation d'identité et autres informations sensibles pour votre organisation.

4. Logiciel qui analyse les activités des principaux points d'entrée de l'organisation

Les cybercriminels peuvent extirper des données en pénétrant dans le réseau et les ordinateurs de votre municipalité. Il existe fort heureusement des logiciels spécialisés permettant de détecter notamment la présence de virus dormants et toute tentative d'exfiltration d'informations ou de données de l'organisation.

5. Formation des utilisateurs

Le manque de vigilance des utilisateurs est l'un des grands risques qui exposent les organisations aux cybercriminels. Grâce à une plateforme de formation en continu, il est possible de former et de tester vos utilisateurs en cybersécurité afin qu'ils soient plus alertes et se posent davantage de questions avant de cliquer sur un lien suspect.

Source : Fédération québécoise des municipalités.