4.11.

GESTION DES INCIDENTS DE CYBERSÉCURITÉ

MISE EN CONTEXTE

La Ville de Montréal (la Ville) utilise de nombreux systèmes d'information qui traitent une quantité très importante de données dont certaines sont confidentielles, comme les renseignements personnels, qui doivent être protégées afin d'éviter qu'elles soient utilisées à mauvais escient. Actuellement, toutes les grandes organisations sont connectées d'une manière ou d'une autre à l'ensemble du globe et sont exposées à des cybermenaces ayant une croissance exponentielle.

La cybersécurité est l'action de se protéger de ces cybermenaces qu'elles viennent de l'extérieur ou de l'intérieur de l'organisation. Les moyens utilisés peuvent comprendre, sans s'y limiter, l'ensemble des encadrements, les outils techniques, les concepts de sécurité, les mécanismes de sécurité, les démarches de gestion des risques et les programmes de sensibilisation et de formation qui permettent de protéger les données de ses citoyens et de ses employés, les utilisateurs et les actifs informationnels de l'organisation. Ces derniers comprennent, principalement, les applications, les serveurs, les bases de données et les équipements de télécommunication et de réseaux.

Les cyberattaques se font de plus en plus nombreuses et elles augmentent de façon exponentielle. La question n'est plus à savoir si la Ville va être attaquée, mais bien à quel moment elle le sera.

Un incident de cybersécurité peut causer des torts importants, par exemple :

- des coûts financiers importants lorsqu'une cyberattaque perdure trop longtemps;
- le vol et la diffusion d'informations confidentielles (p. ex. des renseignements personnels, des informations stratégiques);
- entacher la réputation de la Ville;
- une perte de confiance des citoyens;
- des poursuites judiciaires.

Si la Ville n'est pas préparée adéquatement, un incident risque d'avoir un impact néfaste sur ses processus d'affaires. Afin de réduire significativement les impacts d'une cyberattaque, une gestion adéquate des incidents de cybersécurité est primordiale et doit comprendre, entre autres, les éléments suivants :

- Une documentation adéquate des politiques et des procédures;
- L'assignation formelle de la responsabilité de la gestion des incidents de cybersécurité à des gens d'expérience;
- Un programme de sensibilisation et de formation à la cybersécurité;
- Des mécanismes de détection technologique et administrative afin de prévenir et de déjouer des cyberattaques;

- La catégorisation des incidents de cybersécurité afin de prioriser ceux ayant le plus d'impacts et de probabilités;
- Un processus de coordination, de communication et de suivi d'incidents dans le but de diminuer le temps d'attaque et d'améliorer l'ensemble de la gestion des incidents de cybersécurité.

OBJECTIF ET RÉSULTATS DE L'AUDIT

L'audit avait pour objectif d'évaluer le processus mis en place pour assurer une gestion adéquate des incidents de cybersécurité par la Ville qui permet de les traiter en temps opportun, d'en limiter les impacts et d'empêcher qu'ils ne se reproduisent.

Pour des raisons évidentes de sécurité, nous ne pouvons divulguer dans le présent rapport annuel l'objectif et les résultats de cet audit. Par ailleurs, advenant des déficiences que nous aurions constatées, celles-ci auraient fait l'objet de plans d'action appropriés par les unités d'affaires concernées.