2.7.

Gestion de la surveillance de cybersécurité

LE 31 MARS 2025

Rapport annuel 2024

Bureau du vérificateur général
de la Ville de Montréal

2.7. Gestion de la surveillance de cybersécurité

2.7.1. Mise en contexte

Les menaces de cybersécurité, auxquelles est exposée toute organisation, incluent notamment les rançongiciels, le vol de données et la perte de disponibilité de ses systèmes. Le volume de ces menaces au Canada a augmenté de 30 % entre 2022 et 2023. Elles ont touché environ 16 % des entreprises et les coûts de récupération, à la suite des incidents, ont doublé entre 2021 et 2023, passant de 600 M$ à 1,2 G$. Toutefois, les dépenses en prévention sont globalement restées stables pendant cette même période.

La mise en place d'une saine gestion de la surveillance de cybersécurité contribue à protéger la Ville de Montréal (la Ville) contre d'éventuelles cyberattaques perpétrées par des individus ou des groupes organisés qui tenteraient de prendre le contrôle de ses systèmes informatiques et par la suite de :

- voler des données confidentielles ou stratégiques, afin de les revendre ou de les divulguer au public;
- détruire une grande quantité de données de la Ville dans un but strictement malsain;
- bloquer l'accès à ces systèmes et exiger le paiement d'une rançon avant de redonner le contrôle à la Ville.

Une telle surveillance requiert notamment la présence de processus adéquats, d'outils technologiques performants ainsi que des ressources humaines compétentes et suffisantes.

Essentiellement, la surveillance de cybersécurité consiste à :

1. colliger des événements de sécurité pertinents provenant des systèmes les plus importants (ex. : des systèmes d'exploitation, des logiciels de télécommunication, des bases de données, des logiciels d'opération, des applications informatiques);
2. envoyer automatiquement les événements de sécurité à des outils de surveillance;
3. déterminer, avec des outils de surveillance, si un événement ou une combinaison d'événements de sécurité devrait se transformer en une alerte de sécurité;
4. confirmer le niveau d'importance de l'alerte ainsi que sa pertinence et apporter les actions requises afin d'en mitiger le risque;
5. documenter dans l'outil de surveillance, le détail des actions prises afin de conserver une trace des interventions réalisées.

Par conséquent, il est important de s'assurer que des mécanismes de contrôle adéquats sont en place quant à la gestion de la surveillance de cybersécurité, afin de réduire les risques liés aux menaces de cybersécurité telle que les cyberattaques.

2.7.2. Objectif et résultats

Cette mission avait pour objectif d'évaluer dans quelles mesures la Ville a mis en place des mécanismes de contrôle pour la gestion de la surveillance de cybersécurité qui répondent aux saines pratiques de l'industrie et qui permettent de réduire les risques de perte de disponibilité, d'intégrité et de confidentialité à un niveau acceptable.

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