2.7.

Gestion de la résilience face aux rançongiciels

LE 23 AVRIL 2026

Rapport annuel 2025

Bureau du vérificateur général
de la Ville de Montréal

2027

2.7. Gestion de la résilience face aux rançongiciels

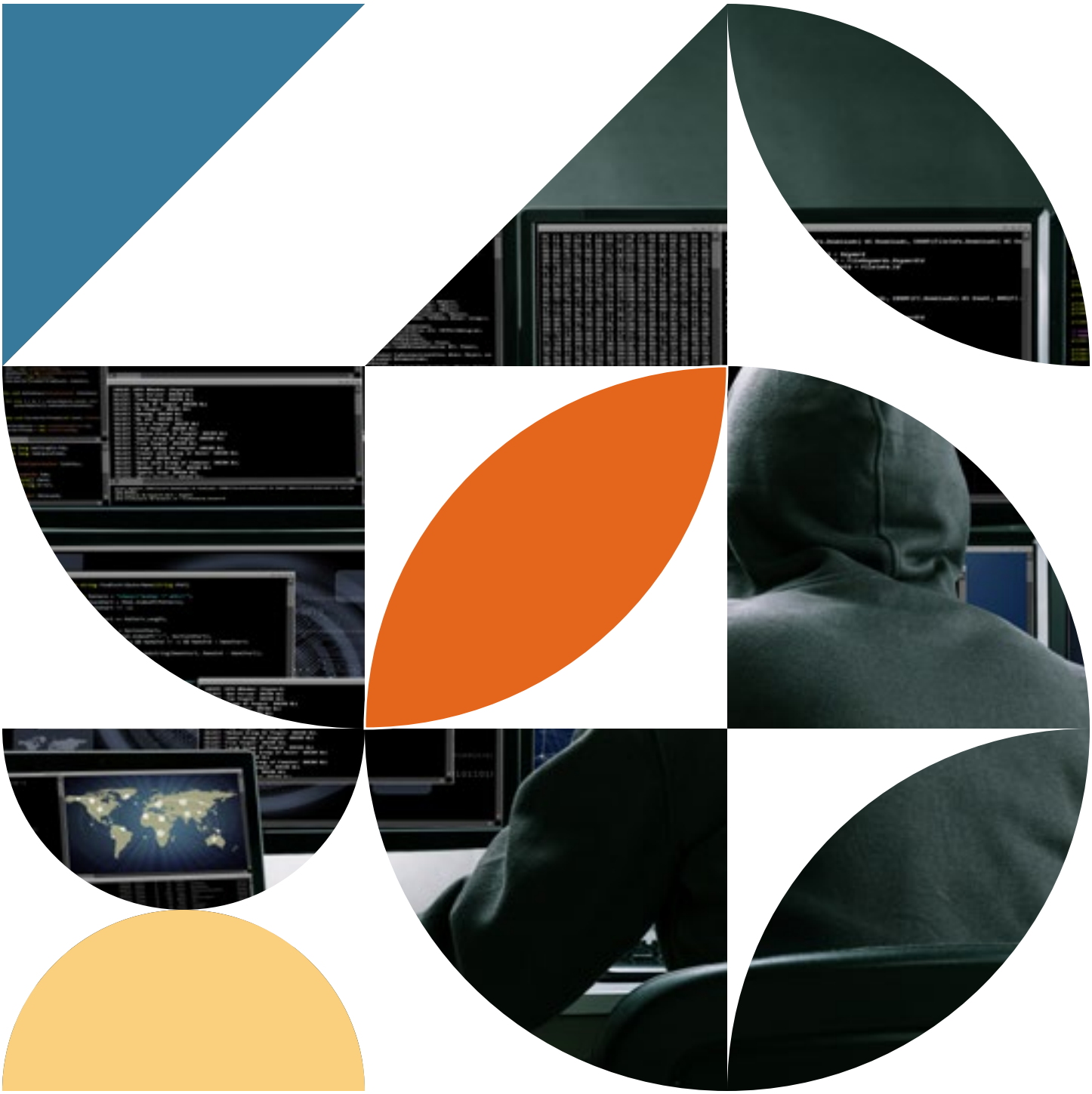
2.7.1. Mise en contexte

De nos jours, à l'échelle mondiale, les rançongiciels représentent l'une des menaces les plus sérieuses tant pour les organisations du domaine publique que du domaine privé. Il s'agit de programmes malveillants qui chiffrent les données d'une organisation en exigeant une rançon en échange de leur déverrouillage. Les villes et les municipalités, en raison de la richesse de leurs données, de la diversité de leurs systèmes et de leur rôle dans la prestation de services essentiels à la population, figurent parmi les cibles privilégiées des cybercriminels.

Dans ce contexte, une attaque réussie peut paralyser des services critiques comme les systèmes de transport, les services d'urgence et les services essentiels. Outre les conséquences opérationnelles, les impacts financiers, juridiques et réputationnels peuvent être majeurs. À cela s'ajoute la perte de confiance des citoyennes et citoyens lorsque des services numériques deviennent inaccessibles ou que des données sensibles, comme les renseignements personnels, sont exposées.

Face à ces enjeux, il est essentiel que la Ville de Montréal (la Ville) mette en place une gestion robuste de la cybersécurité et des mécanismes efficaces de prévention, de détection, de réponse et de rétablissement. Une gestion efficace de la résilience face aux rançongiciels permet non seulement de réduire les risques d'interruption de services, mais aussi d'assurer la continuité des opérations municipales et la protection des informations personnelles des citoyennes et citoyens.

2.7.2. Objectif et résultats

Cette mission avait pour objectif d'évaluer dans quelle mesure la Ville a mis en place des mécanismes de contrôle pour faire face aux risques liés aux attaques par rançongiciel, afin de réduire à un niveau acceptable, les risques d'indisponibilité des services critiques offerts aux citoyennes et citoyens.

Pour des raisons manifestes de sécurité, nous ne pouvons pas 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.