3.

Tests d’intrusion logique

Rapport annuel 2025

Bureau du vérificateur général
de la Ville de Montréal

3. Tests d'intrusion logique

3.1. Mise en contexte

Plusieurs unités d'affaires de la Ville de Montréal et certains organismes contrôlés par celle-ci possèdent des systèmes par lesquels transitent des informations critiques et confidentielles.

Afin de disposer de mesures de cybersécurité efficaces pour protéger adéquatement les systèmes d'information contre des cyberattaques, l'industrie recommande fortement de procéder à des tests d'intrusion logique mettant à l'épreuve la robustesse des mécanismes de contrôle appliqués sur les différents environnements informatiques. En effet, tester la résistance des systèmes d'information à l'encontre des tentatives d'intrusion, internes ou externes, est un enjeu primordial selon les expertes et experts dans le domaine de la cybersécurité.

Les tests d'intrusion logique simulent de véritables attaques contre les infrastructures technologiques. À cet effet, ils mettent en application, de façon contrôlée et sécuritaire, des actions malveillantes réalisées par les pirates informatiques (communément appelés « pirates »). Les tests permettent de s'introduire dans les systèmes et les réseaux, soit depuis Internet, soit de l'interne, afin de mieux découvrir les failles éventuelles des systèmes d'information, des réseaux ou des logiciels, et ce, dans le but de renforcer la cybersécurité. Contrairement aux tentatives d'intrusion des pirates informatiques, les tests d'intrusion logique sont licites puisqu'il y a consentement des unités d'affaires avant le début des tests. À cette fin, les spécialistes utilisent généralement les mêmes outils et techniques que les pirates informatiques, à la différence qu'ils n'endommagent pas les systèmes d'information, ne les rendent pas indisponibles, n'altèrent pas les informations manipulées par ces derniers et ne dérobent pas d'informations confidentielles. Ainsi, l'intégrité, la confidentialité et la disponibilité des systèmes attaqués sont maintenues durant les tests.

Il existe principalement deux catégories de tests d'intrusion logique :

— **Tests d'intrusion logique externes** : ils permettent de savoir si une personne malveillante pourrait, à partir d'Internet, compromettre la cybersécurité des systèmes d'information pour :

  - s'approprier de l'information confidentielle ou privilégiée;
  - modifier les informations manipulées par ces systèmes;
  - rendre les systèmes d'information indisponibles.

— **Tests d'intrusion logique internes** : ils permettent de déterminer si une personne pourrait, de l'interne et avec ses accès habituels, compromettre la cybersécurité des systèmes d'information pour y effectuer les mêmes trois actions énoncées pour les tests externes. Les tests internes permettent également d'atteindre et de mettre à l'épreuve des systèmes d'information qui sont invisibles depuis Internet.

3.2. Objectif et résultats des tests d'intrusion logique

Nous avons réalisé une mission de tests d'intrusion logique. Le principal objectif de cette mission était de mettre à l'épreuve la cybersécurité d'environnements informatiques jugés critiques pour qualifier leur résistance à certains niveaux d'attaques.

Pour des raisons manifestes de sécurité, nous ne pouvons pas divulguer, dans le présent rapport annuel, le détail des systèmes ciblés et les résultats de nos tests d'intrusion logique. 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 l'unité d'affaires concernée.