Vérificateur général
de la Ville de Montréal

Rapport du vérificateur général de la Ville de Montréal
au conseil municipal et au conseil d'agglomération

Pour l'exercice terminé le 31 décembre 2013

5.5

Tests d'intrusion logique

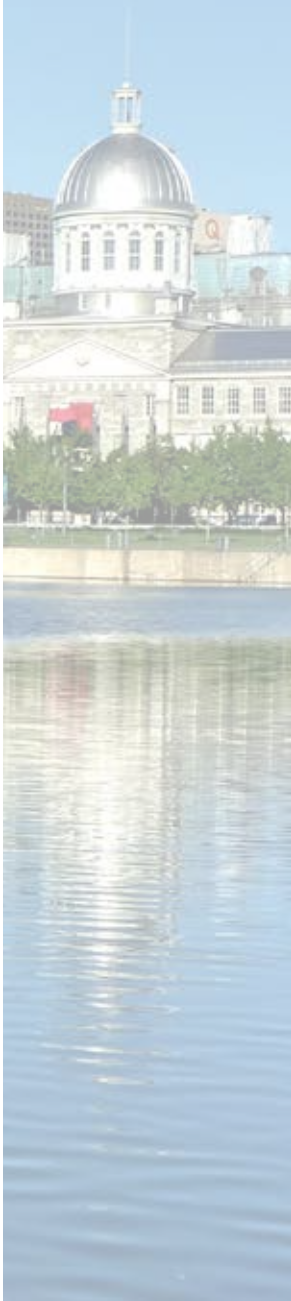

Table des matières

5.5. Tests d'intrusion logique

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. La plupart de ces systèmes résident sur des réseaux communs ou individuels qui peuvent parfois être accessibles depuis Internet.

Afin de disposer de mesures de sécurité 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 experts dans le domaine de la sécurité de l'information.

Les tests d'intrusion logique désignent la mise en application, de façon contrôlée et sécuritaire, des actions malveillantes réalisées par les pirates informatiques (communément appelés *hackers*) pour 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 sécurité de l'information. Contrairement aux tentatives d'intrusion des pirates informatiques, les tests d'intrusion logique sont licites puisqu'il y a consentement des entités auditées 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 sécurité 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 sécurité 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.

2. Objectif de l'audit et portée des travaux

Dans l'optique d'obtenir un niveau de confiance raisonnable quant à la qualité des contrôles en place pour réduire, à un niveau acceptable, les risques d'attaque des systèmes d'information de certaines unités d'affaires de la Ville et d'organismes contrôlés par celle-ci, nous avons poursuivi au cours de 2013 un programme entrepris en 2012 pour réaliser des missions de tests d'intrusion logique. Ce programme se poursuit en 2014.

Le principal objectif de ces missions est de mettre à l'épreuve la sécurité d'environnements informatiques jugés critiques pour qualifier leur résistance à un certain niveau d'attaques provenant tant de l'externe que de l'interne.

3. Résultats des tests d'intrusion

Pour des raisons évidentes de sécurité, nous ne pouvons divulguer dans le présent rapport annuel les résultats de nos tests d'intrusion logique qui ont été effectués en 2013. Par ailleurs, soulignons que les déficiences que nous avons constatées ont fait l'objet de plans d'action appropriés par les unités d'affaires concernées.