Vérificateur général
de la Ville de Montréal

Report of the Auditor General of the Ville de Montréal
to the City Council and to the Urban Agglomeration Council

For the Year Ended December 31, 2013

5.5

Penetration Tests

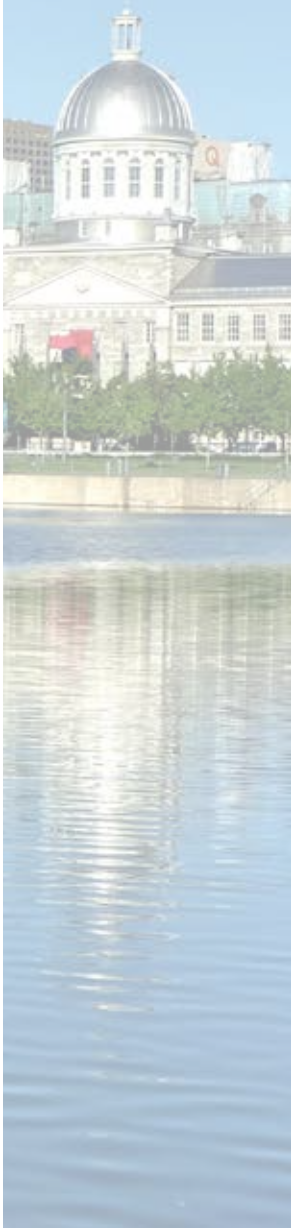

Table of Contents

5.5. Penetration Tests

1. Background

Several business units of Ville de Montréal and some bodies controlled by the city have systems through which they transmit critical and confidential information. Most of these systems are housed on common or individual networks that can sometimes be accessed through the Internet.

In order to ensure effective safeguards are in place to adequately protect the information systems from cyberattacks, the industry strongly recommends that penetration tests be done to verify the strength of the controls applied to the various computer environments. According to the information security experts, testing the resistance of information systems to internal or external threats is of paramount importance.

The term “penetration testing” refers to simulating, in a controlled and secure manner, malicious actions carried out by computer hackers to penetrate systems and networks, either through the Internet or internally, in an effort to identify any potential vulnerabilities in the computer systems, networks or software and enhance the information security. In opposition to penetration attempts by computer hackers, penetration testing is ethical because it is done with the prior consent of the entities involved. Specialists generally use the same tools and techniques as computer hackers, except that they do not cause damage to the information systems, make them unavailable, alter the information processed by these systems, or steal confidential information. The integrity, confidentiality and availability of the systems being attacked are maintained during the penetration testing.

There are two main categories of penetration tests:

- **External penetration tests:** these tests make it possible to know whether a malicious individual could, using the Internet, breach the security of the information system in order to:
  - obtain confidential or privileged information;
  - change information processed by these systems;
  - make the systems unavailable.
- **Internal penetration tests:** these tests make it possible to determine whether an individual could, internally and using his usual access, compromise the security of the information system in order to carry out the same three actions mentioned under the

external tests. Internal tests also allow access to and testing of information systems that are invisible from the Internet.

2. Purpose and Scope of the Audit

In an effort to ensure a reasonable level of confidence in the quality of existing controls and to reduce to an acceptable level the risks of cyberattacks on the information systems of some of the city's business units and bodies controlled by the city, we continued during 2013 a program of penetration testing that we initiated in 2012. This program is continuing in 2014.

The main objective is to test the security of computer environments that have been deemed critical and assess their resistance to a certain level of cyberattack originating externally and internally.

3. Results

For obvious security reasons, we are unable to disclose, in the current annual report, the results of the penetration tests carried out in 2013. Besides, it is important to stress out that the concerned business units have prepared appropriate action plans to address the deficiencies we have identified.