# 5. Logical Penetration Tests

2020 ANNUAL REPORT
Auditor General of the Ville de Montréal

# 5. Logical Penetration Tests

## 5.1. Background

Several Ville de Montréal (the City) business units and some organizations controlled by the City have systems through which critical and confidential information passes.

To have effective security measures to adequately protect information systems against cyberattacks, the industry strongly recommends that logical penetration tests be used to test the strength of controls applied in various computer environments. According to information security experts, testing information systems' resistance to internal or external penetration attempts is a key issue.

Logical penetration tests simulate real attacks on technology infrastructures. To this end, they implement, in a controlled and secure replications of malicious steps taken by hackers to break into systems and networks, either from the Internet or internally, in order to better detect potential flaws in information systems, networks or software and strengthen information security. Unlike hacker penetration attempts, logical penetration tests are legal because the target entities provide their consent before testing is started. Specialists generally use the same tools and techniques as hackers do. The difference is that they do not damage information systems, make them unavailable, or alter the information handled by them and do not steal confidential information. The attacked systems' integrity, confidentiality and availability are maintained during tests.

There are two main types of logical penetration tests:

- **External logical penetration tests:** they reveal whether a hacker could use the Internet to compromise the security of information systems to::
  - obtain confidential or privileged information;
  - alter the information handled by these systems;
  - make information systems unavailable.

- **Internal logical penetration tests:** they can determine whether a person could use the internal system with his usual access rights to compromise the security of the information systems and perform the same three actions defined for external tests. Internal testing is also used to access and test information systems that are invisible from the Internet.

## 5.2. Purpose and Scope of the Logical Penetration Tests

We performed two logical penetration testing missions tests throughout 2020. The main objective of these engagements was to test the security of IT environments considered critical in order to qualify their resistance to certain levels of attacks.

For obvious security reasons, in this annual report we cannot disclose the details of the targeted systems and the results of our logical penetration tests. Moreover, the business units concerned would have implemented appropriate action plans to address any deficiencies we would have noted and recommendations we would have made.