Physical Penetration Tests

4.


10101
10
10101
10

4. Physical Penetration Tests

4.1. Background

The City of Montréal (the City) and the bodies it controls have many vital and essential assets located, stored or held in various buildings and premises.

Given the importance of these assets, they must be adequately protected — on the one hand, to maintain a level of protection sufficient to ensure the safety of people and property and, on the other hand, to provide the continuity of services that are essential to the functioning, well-being and prosperity of Montréal as a society.

Physical security is the first line of defence that must be implemented to manage the risks associated with protecting the City's assets, as physical penetration is one of the first avenues considered by ill-intentioned people whose objective is to perpetrate acts aimed at stealing, destroying or damaging the assets — or the information housed within those assets.

To prevent acts of theft or sabotage, effective protection, surveillance and access control mechanisms must therefore be put in place.

In order to obtain a reasonable level of confidence in the quality of the controls in place to physically protect the assets, performing physical penetration tests in real-life conditions is what security best practices recommend.

The social engineering method is the main method used for physical penetration tests.

Social engineering is recommended for performing physical penetration tests when employees are present in the premises targeted by the tests. This method uses the art of manipulating people. It exploits procedural loopholes and the judgment of the targeted entity's employees to obtain goods, services, confidential information and so forth from others.

Social engineering is a method of manipulation based on the use of persuasive force. Physical penetration test specialists use their knowledge, charisma and deception to attempt to gain access to the City's premises and property.

More specifically, the social engineering method works as follows:

- An approach phase to win the employee's trust by, for example, posing as a City employee;
- An important reason given that has to do with personal safety (e.g., to monitor the fire detection systems);
- A diversion, i.e., a phrase or situation conceived to reassure the employee and avoid suspicion.

Prior to applying social engineering, a perimeter scan of the exterior of the premises is conducted for each of the targeted buildings to detect possible gaps in access control (e.g., unlocked doors or absence of a security guard).

4.2. Objective and Results of the Physical Penetration Tests

In 2022, we conducted a physical penetration test mission. The main objective of this mission was to test the access control mechanisms to buildings considered critical and to assess their resistance to certain levels of attacks.

For obvious security reasons, we can disclose neither the details of the buildings that were targeted nor the results of our physical penetration tests in this annual report. Furthermore, in the event that we had noted any deficiencies, recommendations would have been made and the recommendations would have been the subject of appropriate action plans by the business units concerned.