Bureau du vérificateur général

V.10. Tests d'intrusion physique

TABLE DES MATIÈRES

1. INTRODUCTION....375

2. PORTÉE DE LA MISSION....376

3. CONSTATATIONS, RECOMMANDATIONS ET PLANS D'ACTION....378

3.1. Constatations....378

3.2. Recommandations....382

3.3. Plans d'action des unités d'affaires concernées....383

4. ANNEXE....384

4.1. Description des niveaux d'impact....384

V.10. TESTS D'INTRUSION PHYSIQUE

1. INTRODUCTION

La Ville de Montréal (la Ville) et ses organismes contrôlés possèdent de nombreux actifs essentiels et vitaux localisés, entreposés ou détenus dans divers bâtiments, édifices et locaux.

Étant donné leur importance, ces actifs doivent être adéquatement protégés, d'une part, pour maintenir un niveau de protection suffisant garantissant la sécurité des personnes et des biens et, d'autre part, pour offrir la continuité des services essentiels au fonctionnement, au bien-être et à la prospérité de la société montréalaise.

La sécurité physique est le premier moyen de défense qui doit être mis en place afin de gérer les risques liés à la protection des actifs de la Ville, puisque l'intrusion physique est l'une des premières avenues envisagées par les personnes malintentionnées dont le dessein est de perpétrer des actes visant à dérober, à détruire ou à détériorer les actifs ou encore les informations hébergées par ces actifs.

Afin de prévenir les actes de vol ou de sabotage, des mécanismes de protection, de surveillance et de contrôle d'accès efficaces doivent être mis en place.

Dans l'optique d'obtenir un niveau de confiance raisonnable sur la qualité des contrôles en place pour assurer la protection physique des actifs, les meilleures pratiques en sécurité préconisent d'effectuer des tests d'intrusion physique en conditions réelles.

Le Bureau du vérificateur général de la Ville (BVG) a donc décidé de réaliser une mission de vérification comportant des tests d'intrusion physique. Contrairement aux procédures habituellement appliquées par le BVG, il s'avérait nécessaire de ne pas aviser, au préalable, les propriétaires des actifs ciblés par notre vérification. Cette démarche a été utilisée afin que les contrôles relatifs à la sécurité physique soient testés en conditions réelles et pour qu'ils ne soient pas momentanément renforcés au moment de nos visites.

Sécurité physique et mécanismes de contrôle

La sécurité physique consiste à protéger les actifs par des mécanismes de contrôle d'accès physique. Les mécanismes de contrôle peuvent être, par exemple, la présence de clôtures, de

portes d'accès munies de serrures mécaniques ou électroniques, de guérites de sécurité, de caméras de surveillance ou la présence humaine (p. ex. gardiens de sécurité). Ces moyens de contrôle sont nécessaires afin de prévenir les actes non autorisés, intentionnels ou non, pouvant compromettre la sécurité des actifs.

Le niveau de protection physique nécessaire doit être défini en fonction de l'importance des actifs et répondre proportionnellement aux risques et aux menaces qui leur sont inhérents. Les mécanismes de sécurité doivent prendre en compte l'emplacement géographique, le type de bâtiment et l'aménagement physique des lieux où se trouvent ces actifs.

Les exigences en matière de sécurité physique varieront selon les rôles et les responsabilités des unités d'affaires et l'importance de leurs activités pour desservir les citoyens. Par exemple, une unité d'affaires telle que le SPVM nécessite un très haut niveau de protection physique, alors qu'il serait moindre pour d'autres unités d'affaires, telles que les ateliers municipaux. Cependant, les concepts de contrôle de la périphérie, les contrôles d'accès physique et les mesures de protection des équipements sont universellement applicables lorsqu'ils sont conçus et prévus avec une interprétation adéquate qui tient compte du principe de proportionnalité.

En ce qui concerne les actifs informationnels sur support magnétique, les mécanismes de sécurité électronique s'avéreront inadéquats et coûteux si la sécurité physique en place n'empêche pas les personnes malveillantes d'accéder aux équipements informatiques les contenant, de les voler, de les endommager ou de les détruire.

2. PORTÉE DE LA MISSION

Notre mission de vérification consistait à réaliser des tests d'intrusion physique en conditions réelles. Cette mission est la première partie d'un mandat plus global de vérification de la gestion de la sécurité physique à la Ville.

L'objectif de notre mission de vérification était d'obtenir une assurance raisonnable que les mécanismes de contrôle en place permettent de protéger adéquatement l'accès physique aux actifs de la Ville.

Cette mission de vérification porte uniquement sur les contrôles afférents à la sécurité physique et ne couvre pas ceux du domaine de la sécurité logique, tels que les contrôles d'accès aux données électroniques.

La principale méthode utilisée pour la réalisation de nos tests d'intrusion physique a été celle de l'ingénierie sociale.

L'ingénierie sociale est préconisée pour réaliser des tests d'intrusion physique lorsqu'il y a présence d'employés dans les locaux ciblés par les tests. Il s'agit d'une méthode d'escroquerie qui utilise l'art de manipuler les personnes. Elle exploite les failles procédurales et le jugement des employés de l'entité ciblée pour obtenir d'autrui un bien, un service, de l'information confidentielle, etc.

L'ingénierie sociale est fondée sur l'utilisation de la force de persuasion et l'absence de procédure appropriée afin d'exploiter la crédulité des personnes en se faisant passer, par exemple, pour un employé de la Ville. Par conséquent, les vérificateurs du BVG ont utilisé leurs connaissances, leur charisme et l'imposture pour tenter d'accéder aux lieux et aux biens de la Ville. Plus spécifiquement, nos méthodes d'ingénierie sociale se sont déroulées selon le schéma suivant :

- Une phase d'approche permettant de mettre l'employé en confiance, en se faisant passer pour un employé de la Ville (p. ex. Direction des immeubles);
- La présentation d'un motif important lié à la sécurité des personnes (p. ex. contrôle des systèmes de détection d'incendie);
- Une diversion, c'est-à-dire une phrase ou une mise en situation permettant de rassurer l'employé et d'éviter qu'il ait des soupçons.

Au moment de nos intrusions, nous avons photographié les lieux empruntés. Nous avons fait une description narrative de chacune des intrusions réalisées. Plus particulièrement, nous avons :

- noté la date et l'heure de l'intrusion;
- indiqué de façon détaillée les étapes que nous avons suivies et les approches que nous avons utilisées pour réaliser nos tests d'intrusion;
- précisé le cheminement de notre intrusion, c'est-à-dire les portes d'accès franchies, les locaux visités et les corridors empruntés;
- décrit les actifs que nous avons observés.

Avant d'appliquer notre démarche d'ingénierie sociale, nous avons effectué, pour chacun des sites visités, une reconnaissance du périmètre extérieur des lieux afin de détecter visuellement la présence d'accès non verrouillés.

L'étendue de nos tests d'intrusion physique portait sur les 31 sites et installations de la Ville et de la Société de transport de Montréal (STM) ayant été sélectionnés selon les résultats de notre analyse d'impact afférente à l'importance des actifs détenus au sein des bâtiments.

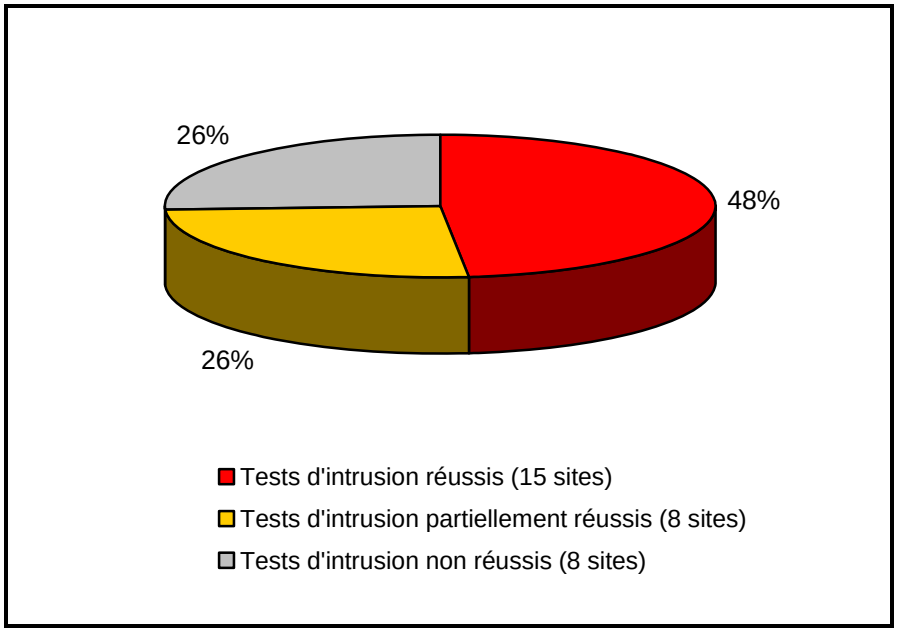
Étant donné la nature sensible de ces sites, nous préférons conserver la liste de ceux-ci confidentielle.

3. CONSTATATIONS, RECOMMANDATIONS ET PLANS D'ACTION

3.1. CONSTATATIONS

Dans l'ensemble, nous avons réussi, en totalité ou en partie, nos tests d'intrusion physique pour 23 des 31 sites ciblés, soit **74 %** de l'ensemble des sites. Les résultats sont présentés au graphique 1.

Graphique 1 – Sommaire des résultats



Tests d'intrusion réussis : les tests d'intrusion physique se sont avérés concluants pour 15 des 31 sites ciblés. Nous avons réussi à accéder à plusieurs zones critiques et aux actifs de ces sites sans être interceptés ou inquiétés.

Tests d'intrusion partiellement réussis : les tests d'intrusion physique se sont avérés partiellement réussis pour 8 des 31 sites ciblés. Nous avons réussi à accéder à certaines zones et à certains actifs de ces sites sans être interceptés.

Tests d'intrusion non réussis : les tests d'intrusion physique ont été vains ou mis en échec pour 8 des 31 sites ciblés. Soit nous avons été incapables d'accéder aux sites à cause des mesures de protection mises en place, soit nous avons été rapidement interceptés et reconduits à l'extérieur du site. C'est donc dire que seulement 26 % des sites ciblés ont démontré un niveau de protection physique adéquat visant à contrer l'ingénierie sociale.

Les trois tableaux ci-dessous présentent le détail des résultats des tests d'intrusion par unités d'affaires, sites et niveaux d'impact (voir l'annexe 4.1 pour la définition des niveaux d'impact).

Précisons que, en aucun temps, tant pour les tests d'intrusion réussis ou partiellement réussis, nous n'avons pris ou consulté quelque document que ce soit appartenant à l'entité vérifiée.

Tableau 1 – Tests d'intrusion réussis

Niveau d'impact	Nombre d'unités d'affaires	Nombre de sites*
Majeur	3	9
Élevé	2	2
Modéré	2	4
Total	**7**	**15**

* Une unité d'affaires peut avoir plusieurs sites.

Tableau 2 – Tests d'intrusion partiellement réussis

Niveau d'impact	Nombre d'unités d'affaires	Nombre de sites*
Majeur	2	2
Élevé	1	1
Modéré	5	5
Total	**8**	**8**

* Une unité d'affaires peut avoir plusieurs sites.

Tableau 3 – Tests d'intrusion non réussis

Niveau d'impact	Nombre d'unités d'affaires	Nombre de sites*
Majeur	3	6
Élevé	1	1
Modéré	1	1
Total	**5**	**8**

* Une unité d'affaires peut avoir plusieurs sites.

Nous énumérons dans cette section les principales constatations relevées pour l'ensemble des unités d'affaires. Cependant, à cause de la criticité des sites pour lesquels les intrusions ont réussi ou partiellement réussi, nous avons décidé de garder confidentiels le détail et les résultats des tests d'intrusion pour chacun des sites. Un rapport de vérification spécifique a cependant été remis sous le sceau de la confidentialité aux personnes responsables de chaque unité d'affaires qui ont validé les constatations qui leur étaient spécifiques ainsi que les recommandations proposées.

CONSTATATION

Pour un site disposant d'informations extrêmement sensibles, nous avons pu sans aucune contrainte circuler à l'intérieur de celui-ci. Nous aurions pu consulter ou même emporter plusieurs documents sans que personne ne s'en rende compte.

CONSTATATION

Pour plusieurs unités d'affaires ayant un niveau d'impact élevé ou majeur, entre autres sur le plan de la sécurité civile, nous avons pu accéder au bâtiment en déclinant une fausse identité et un faux motif. De plus, pour d'autres unités d'affaires, nous avons pu entrer sans avoir rencontré une personne responsable. Pour certaines de celles-ci, nous avons même été laissés à nous-mêmes, c'est-à-dire que nous pouvions, en toute liberté, circuler à l'intérieur du bâtiment sans être accompagnés. Ainsi, nous avons accédé à des salles de contrôle qui gèrent des équipements hautement critiques pour la sécurité et le bien-être des citoyens. Nous avons également pu accéder en toute impunité :

- **à des informations confidentielles;**
- **à du matériel ou des équipements hautement critiques sur le plan de la sécurité civile ou du confort à la population;**
- **à des actifs stratégiques pour la Ville.**

CONSTATATION

Plusieurs portes d'entrée principales ou secondaires permettant d'accéder à des zones critiques de certaines unités d'affaires n'étaient pas verrouillées ou surveillées. Nous avons pu aisément nous introduire dans certains sites en utilisant ces portes d'accès. À l'intérieur de plusieurs sites, nous avons ainsi pu circuler sans être interceptés par des employés, même si, dans plusieurs cas, ceux-ci remarquaient notre présence.

CONSTATATION

À l'intérieur de plusieurs sites, nous avons pu accéder à des locaux critiques qui étaient laissés sans surveillance et dont les portes étaient déverrouillées.

Nous pouvons ainsi conclure que, pour plusieurs unités d'affaires :

- il n'y a pas de procédures appliquées :
  - pour contrôler l'identité des visiteurs,
  - pour identifier formellement avec un badge les visiteurs,
  - pour valider le motif de la visite,
  - pour accompagner en tout temps les visiteurs;
- il y a absence d'un registre des visiteurs indiquant :
  - le nom du visiteur,
  - le service ou la compagnie où travaille le visiteur,
  - la personne devant être rencontrée,
  - le motif de la visite,
  - la date et l'heure d'entrée,
  - l'heure de sortie,
  - la présence de la signature d'une personne responsable;
- la plupart des employés n'interceptent pas et ne questionnent pas les personnes non autorisées qui circulent librement dans les locaux;
- il y avait présence de caméras de surveillance dans certains endroits critiques. Toutefois, en aucun cas, un gardien de sécurité n'a remarqué notre présence et n'est venu à notre rencontre.

Ces faiblesses de sécurité physique, pour plusieurs unités d'affaires vérifiées, sont, à notre avis, extrêmement préoccupantes, car les menaces suivantes pourraient se réaliser :

- Sabotage d'équipements ayant une importance critique en matière de sécurité civile et de confort à la population;

- Vol de documents hautement sensibles pouvant avoir des conséquences sur l'intégrité et la sécurité des personnes;
- Vol d'équipements stratégiques;
- Vol d'équipements de valeur;
- Acte terroriste sur des équipements ayant une importance critique en matière de sécurité civile;
- Vol d'uniformes pour ensuite procéder à de l'usurpation d'identité.

Les conséquences de la matérialisation de ces menaces pourraient être graves, voire catastrophiques pour la sécurité des citoyens ainsi que pour le fonctionnement des activités sociales et économiques de Montréal.

3.2. RECOMMANDATIONS

Chaque unité d'affaires a été rencontrée afin de lui exposer les résultats de nos tests d'intrusion. Nous lui avons fait part de la démarche que nous avons utilisée, de nos constatations ainsi que des recommandations suggérées pour améliorer le niveau de protection physique des sites vérifiés qui sont sous sa responsabilité. Il faut comprendre que ces constatations sont fondées uniquement sur les résultats de nos tests d'intrusion. Un travail de vérification plus poussé sur la qualité des mécanismes d'accès et de protection physique, incluant les procédures en place, est prévu en 2011.

Parmi les recommandations suggérées, qui ne s'appliquent évidemment pas à toutes les unités d'affaires à cause de leurs particularités et leurs niveaux d'impact, nous présentons dans cette section celles qui sont les plus importantes.

Afin d'empêcher les accès physiques non autorisés et afin d'assurer la protection adéquate des actifs et des informations entreposés au sein des différents sites des unités d'affaires, nous recommandons de :

- **définir des procédures strictes de contrôle des visiteurs exigeant entre autres :**
  - **de vérifier systématiquement l'identité des visiteurs,**
  - **de s'assurer de la validité du motif de la visite,**
  - **de fournir un badge d'identification des visiteurs (ce badge pourrait avoir différentes couleurs selon le type de visiteur),**

  - **d'accompagner les visiteurs pendant toute la durée de leur visite,**
  - **de sensibiliser le personnel quant à l'importance d'accoster et de questionner les personnes étrangères ou non familières du site;**
- **mettre en place un registre des visiteurs qui soit sous le contrôle d'une personne responsable. Ce registre devrait contenir les éléments suivants :**
  - **Nom du visiteur,**
  - **Service ou la compagnie où travaille le visiteur,**
  - **Motif de la visite,**
  - **Nom de la personne devant être rencontrée,**
  - **Présence de la signature d'une personne responsable,**
  - **Date et l'heure d'entrée,**
  - **Heure de sortie;**
- **contrôler et de vérifier les écrans vidéo des caméras de surveillance et de prendre les mesures nécessaires en cas de visualisation d'activités ou d'individus suspects;**
- **sensibiliser le personnel quant aux risques et aux menaces de l'ingénierie sociale et sur les mesures de sécurité à prendre;**
- **recenser les différents points d'accès de chacun des sites et de mettre en place des mesures de protection appropriées;**
- **contrôler l'accès physique en verrouillant adéquatement les portes d'entrée principales et secondaires.**

3.3. PLANS D'ACTION DES UNITÉS D'AFFAIRES CONCERNÉES

Nos recommandations ont été validées avec les unités d'affaires concernées. Elles vont nous communiquer leur plan d'action ultérieurement.

4. ANNEXE

4.1. DESCRIPTION DES NIVEAUX D'IMPACT

NIVEAUX D'IMPACT	DÉFINITIONS DES NIVEAUX D'IMPACT
Majeur	Conséquence directe sur la sécurité et la santé publique pouvant mettre en danger la sécurité des personnes. Dès qu'il y a la moindre conséquence tangible sur la sécurité civile et la santé publique, le niveau d'impact « majeur » est attribué au site ou aux installations.
Élevé	Bien qu'il y ait moins de conséquences sur la sécurité publique à cause de la présence de nombreux actifs de grande valeur et/ou d'informations hautement confidentielles et stratégiques, une intrusion nuirait de façon importante à la réputation et au fonctionnement de la Ville ou à l'activité économique de Montréal.
Modéré	À cause de la présence de certains actifs de grande valeur ou de certaines d'informations confidentielles et stratégiques, une intrusion entraverait modérément les opérations de la Ville ou nuirait à sa réputation.