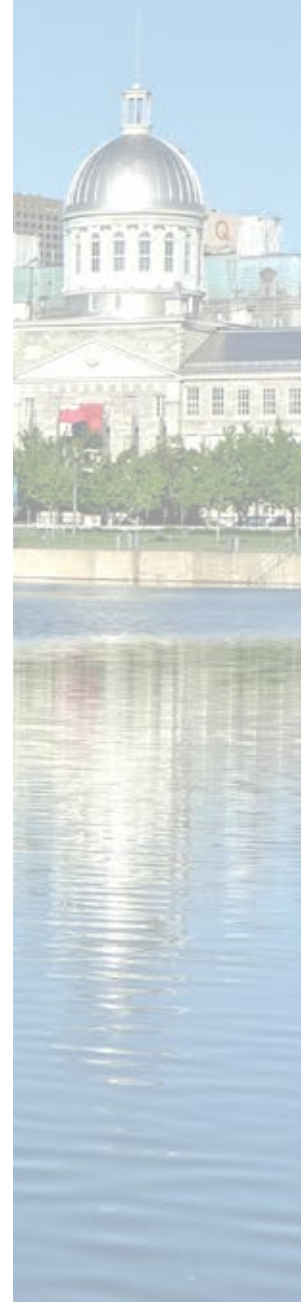


## **Sécurité des réseaux sans fil**





## Table des matières

1. Introduction .....	183
2. Objectif de l'audit et portée des travaux.....	184
3. Sommaire des constatations.....	185
4. Constatations détaillées et recommandations .....	185
4.1. Processus de détection des réseaux sans fil non autorisés.....	185
4.2. Points d'accès sans fil.....	186
4.3. Protocoles de sécurité.....	187
4.4. Imprimantes avec accès sans fil .....	188
5. Conclusion générale .....	189
6. Annexe.....	190
6.1. Description des niveaux d'impact.....	190

## Liste des sigles

MAC	<i>Medium Access Control</i>	WPA	<i>Wi-Fi Protected Access</i>
NIST	<i>National Institute of Standards and Technology</i>	WPA2	<i>Wi-Fi Protected Access 2</i>
STI	Service des technologies de l'information	WPS	<i>Wi-Fi Protected Setup</i>

## 5.4. Sécurité des réseaux sans fil

### 1. Introduction

L'essor des équipements de communication et d'informatique nomades est à l'origine de l'omniprésence des réseaux sans fil. Ces réseaux permettent de connecter toutes sortes d'équipements (p. ex. des ordinateurs portables, des tablettes électroniques, des téléphones intelligents) à des réseaux corporatifs tels que celui de la Ville de Montréal (la Ville).

Les réseaux sans fil sont largement utilisés pour leur commodité d'accès au réseau informatique interne des entreprises et des organisations tout en évitant les coûts importants d'une infrastructure filaire. Chaque réseau sans fil contient un nombre varié de points d'accès sans fil selon le nombre de connexions et la superficie des locaux.

Pour desservir sa population, la Ville utilise un réseau informatique complexe par lequel se branchent des milliers d'employés. Pour y accéder, en plus des connexions filaires, les utilisateurs peuvent se connecter au réseau par l'intermédiaire de points d'accès sans fil. Ainsi, les utilisateurs bénéficient d'une plus grande flexibilité, n'étant pas limités à leur poste de travail fixe.

Contrairement à un réseau filaire, le sans-fil ne permet pas d'avoir un périmètre géographique circonscrit puisque son signal est diffusé bien au-delà des limitations physiques des lieux de travail (bureaux et bâtiments). Par conséquent, le sans-fil est souvent vulnérable à des attaques de personnes malveillantes qui tentent d'accéder à des renseignements confidentiels sans qu'elles soient obligées d'être physiquement présentes au sein de l'entreprise.

Tout comme le réseau filaire, l'infrastructure des réseaux sans fil doit être adéquatement protégée afin d'empêcher des accès non autorisés. Ces points d'entrée sont tout aussi importants, car ils donnent accès à des renseignements confidentiels concernant les citoyens, les élus et les employés.

C'est dans ce contexte que nous avons jugé opportun de réaliser la mission d'audit sur la sécurité des réseaux sans fil.

## 2. Objectif de l'audit et portée des travaux

L'objectif de notre mission d'audit était de déterminer si les contrôles mis en place permettent que seuls les réseaux sans fil dûment autorisés soient présents à la Ville et que leurs mécanismes de sécurité empêchent les accès illicites au réseau corporatif de la Ville.

Nos travaux d'audit ont porté sur les réseaux sans fil gérés par le Service des technologies de l'information (STI), par la Division des ressources informationnelles relevant de la Direction des services administratifs et du greffe de l'arrondissement de Saint-Laurent et par la Division de l'informatique relevant de la Direction des services administratifs de l'arrondissement de Saint-Léonard.

Nos travaux d'audit ont été réalisés avec la participation d'un spécialiste reconnu dans le domaine de la sécurité de l'information et nos conclusions reposent sur les bonnes pratiques de l'industrie, notamment les suivantes :

- *Recommandations de sécurité relatives aux réseaux WiFi*, Agence nationale de la sécurité des systèmes d'information, Secrétariat général de la défense et de la sécurité nationale, ministère français de la Défense;
- *Establishing Wireless Robust Security Networks: A Guide to IEEE802.11i*, Special Publication 800-97, National Institute of Standards and Technology (NIST)<sup>1</sup>.

D'après les résultats de notre analyse de risques, nous avons sélectionné huit édifices en fonction de leur importance stratégique au sein de la Ville, du type de renseignements traités et du nombre de réseaux sans fil implantés.

Au sein de ces édifices, nous avons effectué les étapes suivantes :

- Étape 1 : visite complète des locaux afin de détecter tous les réseaux sans fil présents dans l'édifice;
- Étape 2 : visite de chacune des salles de communication de l'édifice pour recenser, le cas échéant, les équipements sans fil non autorisés;
- Étape 3 : obtention des adresses MAC<sup>2</sup> du réseau local de l'édifice afin de les comparer avec les adresses MAC des réseaux sans fil (détectés à la première étape) pour recenser les réseaux sans fil non autorisés.

De plus, nous avons évalué les encadrements administratifs et la gestion de l'inventaire des réseaux sans fil.

---

<sup>1</sup> Organisme du Département américain du commerce. Son but est de promouvoir l'économie en développant des technologies, la métrologie et des standards, de concert avec l'industrie.

<sup>2</sup> Identifiant physique stocké dans une carte réseau et utilisé pour attribuer mondialement une adresse unique.

Notre mission d'audit a été réalisée d'août à décembre 2013.

### 3. Sommaire des constatations

Le tableau 1 présente les lacunes que nous avons relevées au cours de nos travaux d'audit.

**Tableau 1 – Sommaire des constatations**

Section du rapport	Constatation	Détails	Niveau d'impact
4.1	Absence de processus de détection des réseaux sans fil	s.o.	Élevé
4.2	Points d'accès sans fil non sécurisés	3 points d'accès sans fil répartis dans 2 édifices	Élevé
4.3	Protocoles de sécurité inadéquats	9 points d'accès sans fil répartis dans 5 édifices	Modéré
4.4	Imprimantes avec accès sans fil non protégées	2 imprimantes présentes dans 1 édifice	Modéré

## 4. Constatations détaillées et recommandations

### 4.1. Processus de détection des réseaux sans fil non autorisés

#### 4.1.A. Contexte et constatations

Au sein d'une organisation telle que la Ville, il est essentiel qu'un processus récurrent de détection des réseaux sans fil non autorisés soit en place au sein du STI.

Un tel processus permet de détecter et de retirer, en temps opportun, tout réseau sans fil mis en place sans avoir été dûment autorisé. De plus, cela permet de supprimer les possibles failles de sécurité introduites par ces réseaux sans fil.

Nous avons constaté que le STI n'avait pas mis en place un processus de détection des réseaux sans fil non autorisés. Par exemple, au cours de nos tests d'audit, nous avons trouvé un point d'accès sans fil caché au sein d'un édifice de la Ville pour lequel il a été impossible de déterminer le propriétaire. Selon les informations obtenues, ce point d'accès n'est pas connecté sur le réseau corporatif de la Ville.

Nous estimons que le niveau d'impact est **élevé**, car la Ville fait face au risque potentiel suivant : sans processus récurrent de détection, il est difficile de découvrir et de localiser des points d'accès sans fil non autorisés. L'installation de tels points d'accès pourrait permettre

à un employé malveillant ou à un attaquant externe d'avoir un accès caché au réseau corporatif de la Ville, et ainsi de pouvoir accéder à de l'information confidentielle.

#### 4.1.B. Recommandation

**Nous recommandons au Service des technologies de l'information de mettre en place un processus récurrent de détection des réseaux sans fil non autorisés et, le cas échéant, de prendre les actions correctives nécessaires pour les supprimer.**

#### Réponse de l'unité d'affaires :

Le plan d'action proposé par le STI répond à notre recommandation et devrait permettre, à terme, de solutionner la problématique en cause. Les détails de ce plan ne peuvent toutefois être divulgués compte tenu des impératifs de confidentialité liés à la sécurité.

## 4.2. Points d'accès sans fil

#### 4.2.A. Contexte et constatations

Un réseau sans fil non sécurisé donne accès à l'ensemble des données qui y sont échangées. Si des données confidentielles transitent par ce réseau, une personne, sans avoir de connaissance particulière, peut aisément les intercepter avec des outils accessibles librement sur Internet.

Au cours de nos travaux d'audit, nous avons découvert plusieurs points d'accès sans fil ouverts et non sécurisés dans deux des huit édifices de notre échantillon.

Nous estimons que le niveau d'impact est **élevé**, car la Ville fait face aux risques potentiels suivants :

- Un point d'accès sans fil non sécurisé utilisé pour naviguer sur Internet sans restriction ne bénéficie pas de la protection de l'infrastructure de sécurité de la ville. Ainsi, un poste de travail d'une personne connectée à ce point d'accès pourrait être infecté par un logiciel malveillant qui pourrait compromettre la sécurité du réseau corporatif de la Ville;
- Une personne malintentionnée pourrait utiliser certains points d'accès sans fil pour intercepter d'éventuelles données confidentielles y transitant et pourrait tenter de compromettre la sécurité du réseau corporatif de la Ville.

#### 4.2.B. Recommandation

**Nous recommandons au Service des technologies de l'information de s'assurer que tous les points d'accès sans fil sont configurés avec un protocole de sécurité robuste.**



### Réponse de l'unité d'affaires :

Le plan d'action proposé par le STI répond à notre recommandation et devrait permettre, à terme, de solutionner la problématique en cause. Les détails de ce plan ne peuvent toutefois être divulgués compte tenu des impératifs de confidentialité liés à la sécurité.

## 4.3. Protocoles de sécurité

### 4.3.A. Contexte et constatations

Les réseaux sans fil diffusent leurs signaux bien au-delà des barrières physiques des locaux des organisations. Il est donc nécessaire que des protocoles de sécurité soient implantés afin d'empêcher que des personnes non autorisées s'y connectent et interceptent les données échangées.

Le *Wi-Fi Protected Access* (WPA) est un protocole de sécurité pour les réseaux sans fil qui a été implanté au début des années 2000 et qui a été une solution temporaire pour remplacer l'ancien protocole *Wired Equivalent Privacy* (WEP), lequel n'était plus considéré comme sécuritaire.

En 2004, le *Wi-Fi Protected Access 2* (WPA2) succède au WPA. Il est considéré comme un protocole complètement sécurisé dont le chiffrement protège les données qui transitent sur les réseaux sans fil. Le WPA2 a été approuvé par le NIST et est certifié par l'organisation *Wi-Fi Alliance*<sup>3</sup>.

Un autre protocole existe, le *Wi-Fi Protected Setup* (WPS), qui est utilisé pour simplifier le paramétrage de la sécurité d'un réseau sans fil. Le WPS est destiné avant tout aux particuliers et ne convient pas à des organisations telles que la Ville, car il contient une vulnérabilité de sécurité importante.

Au cours de notre audit, nous avons découvert neuf points d'accès sans fil configurés pour utiliser le WPA2, mais ils permettaient aussi l'utilisation de protocoles moins robustes, dont le WPA et le WPS (répartis dans cinq édifices).

Nous estimons que le niveau d'impact est **modéré**, car la Ville fait face au risque potentiel suivant : une personne malveillante serait capable de déchiffrer la clé d'authentification en quelques heures et pourrait accéder au réseau corporatif de la Ville. Ainsi, elle pourrait avoir accès à de l'information confidentielle.

<sup>3</sup> Consortium mondial qui teste et certifie les produits et la technologie Wi-Fi.

#### 4.3.B. Recommandation

**Nous recommandons au Service des technologies de l'information et aux arrondissements concernés de s'assurer que les équipements des réseaux sans fil utilisent uniquement les protocoles de sécurité les plus robustes.**

#### Réponse des unités d'affaires :

Les plans d'action proposés par les unités d'affaires répondent à notre recommandation et devraient permettre, à terme, de solutionner la problématique en cause. Les détails de ces plans ne peuvent toutefois être divulgués compte tenu des impératifs de confidentialité liés à la sécurité.

### 4.4. Imprimantes avec accès sans fil

#### 4.4.A. Contexte et constatations

Certaines imprimantes possèdent des fonctionnalités sans fil qui permettent aux postes de travail de se connecter directement à celles-ci sans qu'il soit nécessaire d'être connecté au réseau corporatif. Ces imprimantes, tout comme n'importe quel équipement sans fil, doivent être protégées afin que les documents imprimés, pouvant contenir des renseignements sensibles, ne puissent pas être interceptés.

À la suite de nos tests, nous avons découvert, au sein d'un édifice, deux imprimantes dont la fonctionnalité sans fil était activée, mais non protégée. Ces imprimantes sont utilisées par des employés traitant de l'information confidentielle.

Nous estimons que le niveau d'impact est **modéré**, car la Ville fait face au risque potentiel suivant : une personne malveillante serait capable d'intercepter, dans un rayon de 100 mètres, tout document confidentiel envoyé aux imprimantes.

#### 4.4.B. Recommandation

**Nous recommandons au Service des technologies de l'information de désactiver l'accès sans fil de ces imprimantes si celui-ci n'est pas absolument nécessaire. Dans le cas contraire, nous recommandons d'activer l'utilisation d'un protocole de sécurité robuste.**

**Réponse de l'unité d'affaires :**

Le plan d'action proposé par le STI répond à notre recommandation et devrait permettre, à terme, de solutionner la problématique en cause. Les détails de ce plan ne peuvent toutefois être divulgués compte tenu des impératifs de confidentialité liés à la sécurité.

## **5. Conclusion générale**

Sur la base des résultats de nos travaux d'audit, nous concluons que, globalement, les réseaux sans fil sont adéquatement protégés. Cependant, la gestion de la sécurité des réseaux sans fil nécessite certaines améliorations. En effet, l'absence d'un processus de détection des réseaux sans fil non autorisés a permis, d'une part, l'installation de quelques points d'accès sans fil potentiellement interdits, dont certains sont cachés. D'autre part, certains points d'accès sans fil non sécurisés ou utilisant des protocoles de sécurité non robustes ne répondent pas aux exigences de sécurité de la Ville.

En conséquence, la Ville encourt le risque que des personnes malveillantes accèdent à de l'information confidentielle en profitant de la sécurité inadéquate de certains réseaux sans fil. La Ville devrait prendre les mesures nécessaires pour contrer les lacunes découvertes dans les meilleurs délais.

La mise en place de nos recommandations devrait permettre à la Ville de disposer de réseaux sans fil adéquatement sécurisés.

## 6. Annexe

### 6.1. Description des niveaux d'impact

**Tableau A – Définition des niveaux d'impact**

Niveaux d'impact	Définitions des niveaux d'impact
Critique	Conséquences directes sur la sécurité des données et des systèmes du réseau corporatif de la Ville : atteinte majeure à la réputation de la Ville, paralysie générale des systèmes du réseau corporatif et divulgation massive de données confidentielles.
Élevé	La présence de lacunes de sécurité permettrait à des personnes non autorisées d'avoir accès à de l'information confidentielle sur les élus, les citoyens ou les employés. Cela nuirait de façon importante à la réputation de la Ville.
Modéré	La présence de certaines lacunes de sécurité nuirait modérément aux opérations des systèmes du réseau corporatif et à la réputation de la Ville et certaines informations confidentielles seraient divulguées.
Faible	Répercussions négligeables sur les opérations et les services de la Ville. Perte de confiance improbable des citoyens envers la Ville.