Rapport

Audit d’optimisation des ressources – Protection des renseignements personnels

18 janvier 2022

Présenté à :

Raymond Chabot Grant Thornton

Notre-Dame-de-l’Île-Perrot

Raymond Chabot
Grant Thornton

Raymond Chabot
Grant Thornton S.E.N.C.R.L.
Bureau 2000
Tour de la Banque Nationale
600, rue De La Gauchetière Ouest
Montréal (Québec)
H3B 4L8

T 514 878-2691

Le 18 janvier 2022

Aux membres du conseil municipal
Ville de Notre-Dame-de-l'Île-Perrot
21, rue de l'Église
Notre-Dame-de-l'Île-Perrot (Québec) J7V 8P4

Objet : Rapport – Audit d'optimisation des ressources – Protection des renseignements personnels

Mesdames, Messieurs,

Nous avons le plaisir de vous présenter notre rapport portant sur l'information relative à la protection des renseignements personnels par la Ville de Notre-Dame-de-l'Île-Perrot (ci-après la « Ville »).

Ce mandat a été réalisé en vertu des dispositions de la Loi sur les cités et villes, et le présent rapport doit être déposé à la première séance du conseil municipal qui suit sa réception par la direction de la Ville. Celui-ci doit également être publié sur le site Web de la Commission municipale du Québec.

Nous tenons à souligner l'excellente collaboration de toutes les personnes rencontrées au cours de la réalisation du mandat.

Nous vous prions de recevoir, Mesdames, Messieurs, nos salutations les plus distinguées.

Raymond Chabot Grant Thornton S.E.N.C.R.L.[1]

[1] CPA auditeur, CA permis de comptabilité publique nº A129112

Table des matières

1. Contexte et objectifs

1.1. CONTEXTE

La Ville de Notre-Dame-de-l'Île-Perrot (ci-après la « Ville ») collecte et traite des renseignements personnels (« RP ») afférents à la vie privée de ses employés et des citoyens. La Ville compte plus de 11 000 citoyens, plus de 50 employés permanents et plus de 55 employés temporaires dans la haute saison. Les informations détenues par la Ville sont nécessaires afin de servir adéquatement les citoyens et consistent en ce qui suit :

- Dossiers d'employés, leurs dossiers médicaux ainsi que leurs coordonnées bancaires;
- Candidatures aux fins de recrutement;
- Informations personnelles des citoyens pour utilisation des services en lignes comme les demandes permis et la taxation.

La Ville de Notre-Dame-de-l'Île-Perrot étant un organisme municipal, il est donc assujetti à la loi pour le secteur public, soit la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

Cette loi s'applique à tous les documents, peu importe leur format : écrit, graphique, sonore, visuel, informatisé ou autre.

Les renseignements personnels sont définis par les RP qui portent sur une personne physique et permettent de l'identifier. Ils sont confidentiels. Sauf exception, ils ne peuvent être communiqués sans le consentement de la personne concernée.

Des exemples de RP :

- Nom, prénom, pseudonyme, date de naissance, NAS;
- Photos, enregistrements sonores de voix;
- Numéro de téléphone fixe ou portable, adresse postale, adresse courriel;
- Adresse IP, identifiant de connexion informatique ou identifiant de *cookie*;
- Numéro de plaque d'immatriculation, numéro d'une pièce d'identité, coordonnées bancaires;
- Les données relatives à la santé des individus;
- Les données concernant la vie sexuelle ou l'orientation sexuelle;
- Les données qui révèlent une prétendue origine raciale ou ethnique.

Certaines données sont de nature publique comme le rôle d'évaluation et de taxation, où on trouve les informations des propriétaires (nom, prénom, adresse), et le rôle d'évaluation du terrain et bâtiment.

Les conséquences d'une mauvaise protection des RP, en plus de ne pas être conforme à la loi, peuvent être de permette la divulgation non autorisée des RP, qu'une personne malintentionnée utilise l'information des RP aux fins d'usurpation d'identité, d'atteinte à la réputation de la Ville, une perte de confiance des citoyens envers la Ville ainsi que des poursuites judiciaires.

2. Objectif de l’audit et portée des travaux

2.1. OBJECTIF DE L’AUDIT

En vertu des dispositions de la Loi sur les cités et villes, nous avons réalisé une mission d’audit de l’optimisation des ressources portant sur la protection des renseignements personnels.

Cet audit avait pour objectif de s’assurer que les renseignements personnels détenus par la Ville faisaient l’objet d’une protection adéquate afin de mitiger les risques de bris de confidentialité, de vol ou d’accès non autorisés aux RP.

Responsabilité de la direction

La direction de la Ville est responsable de la protection des renseignements personnels qu’elle détient. Elle est également responsable de la mise en place des systèmes, des procédures et des contrôles lui permettant d’identifier, de gérer et de protéger les renseignements personnels, et ce, conformément aux règles en vigueur et aux saines pratiques en matière de protection des renseignements personnels.

Responsabilité de l’auditeur

Notre responsabilité consiste à fournir une conclusion sur l’objectif de l’audit. Pour ce faire, nous estimons que nous avons recueilli les éléments probants suffisants et appropriés pour fonder notre conclusion et pour obtenir un niveau d’assurance raisonnable. Notre évaluation est basée sur les critères que nous avons jugés valables dans les circonstances. Ces derniers sont exposés à la section 5.2.

Nous avons planifié et réalisé notre mission d’assurance raisonnable conformément à la norme canadienne de missions de certification (NCMC) 3001, Missions d’appréciation directe, du Manuel de CPA Canada – Certification. Cette norme requiert que nous planifiions et réalisions la mission de façon à obtenir une assurance raisonnable à l’égard de notre conclusion sur l’objectif de l’audit.

L’assurance raisonnable correspond à un niveau élevé d’assurance, qui ne garantit toutefois pas qu’une mission réalisée conformément à cette norme permettra toujours de détecter tout cas important de non-conformité ou les déficiences significatives qui pourraient exister. Les cas de non-conformité ou déficiences significatives aux critères peuvent résulter de fraudes ou d’erreurs et ils sont considérés comme significatifs lorsqu’il est raisonnable de s’attendre à ce que, individuellement ou collectivement, ils puissent influer sur les décisions des utilisateurs de notre rapport. Une mission d’assurance raisonnable visant la délivrance d’un rapport de l’auditeur implique la mise en œuvre de procédures en vue d’obtenir des éléments probants suffisants et appropriés pour fonder raisonnablement une conclusion et obtenir un niveau d’assurance élevé. La nature, le calendrier et l’étendue des procédures d’audit choisies relèvent de notre jugement professionnel, et notamment

de notre évaluation des risques de non-conformités ou de déficiences significatives, que celles-ci résultent de fraudes ou d'erreurs.

Notre indépendance et notre contrôle qualité

Nous nous sommes conformés aux règles ou au code de déontologie pertinents applicables à l'exercice de l'expertise comptable et se rapportant aux missions de certification, qui sont publiés par les différents organismes professionnels comptables, lesquels reposent sur les principes fondamentaux d'intégrité, d'objectivité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

Le cabinet applique la Norme canadienne de contrôle qualité (NCCQ) 1, *Contrôle qualité des cabinets réalisant des missions d'audit ou d'examen d'états financiers et d'autres missions de certification*, et, en conséquence, maintient un système de contrôle qualité exhaustif qui comprend des politiques et des procédures documentées en ce qui concerne la conformité aux règles de déontologie, aux normes professionnelles et aux exigences légales et réglementaires applicables.

2.2. PORTÉE DES TRAVAUX

Nos travaux d'audit ont porté sur la période du 10 juin 2021 au 30 août 2021. Nous avons toutefois tenu compte d'informations qui nous ont été transmises jusqu'en septembre 2021.

Nos travaux se sont limités et ont été réalisés sur un échantillon de systèmes contenant des RP jugés critiques par la Ville. Les systèmes sélectionnés sont les suivants :

- COBA – système de paie (hébergé par la Ville)
- ACCEO Municipal – système financier et de taxation (hébergé par la Ville)
- AccèsCité Territoire – système utilisé pour la gestion du territoire et des demandes diverses (hébergé par la Ville)
- Permis en ligne – système de gestion des demandes de permis (géré et hébergé par un fournisseur externe)
- ACCEO Transphere – système de paiement en ligne (géré et hébergé par un fournisseur externe)
- AccèsCité Loisirs – système de réservation en ligne pour les citoyens (géré et hébergé par un fournisseur externe)
- Serveur de fichiers et contrôleur de domaine – systèmes gérant les fichiers et les utilisateurs sur le réseau (hébergé par la Ville)

Bien qu'il s'agisse d'un audit, notre mission ne constitue pas en soi un exercice de conformité à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels ni aux autres lois et normes auxquelles la Ville pourrait se référer en ce qui concerne les RP.

À la fin de nos travaux, un rapport préliminaire comprenant nos constats a été présenté aux instances concernées de la Ville, et ce, aux fins de discussions. Par la suite, le rapport final a été transmis aux mêmes instances pour l'obtention d'un plan d'action et d'un échéancier pour la mise en œuvre des recommandations les concernant.

3. Résultats de l'audit

3.1. GOUVERNANCE

La gouvernance est un élément important pour la Ville, car elle vient établir et officialiser les orientations prises par la direction et le conseil municipal. Elle jette les bases des attentes de la Ville envers ses employés, les consultants ainsi que les fournisseurs avec qui elle collabore. Une bonne gouvernance permet de venir encadrer les principes et les standards souhaités par la Ville et cette notion s'applique à l'ensemble des sphères d'une Ville, incluant le respect des renseignements personnels.

Plus précisément, la gouvernance à l'égard des technologies de l'information (TI) s'entend de la gestion et du contrôle de l'environnement TI, notamment les données utiles à une organisation et à ses parties prenantes. La gouvernance des TI exige un leadership, des structures organisationnelles, des politiques, des processus et des contrôles internes afin que les TI respectent la stratégie et les objectifs de la Ville et de ses parties prenantes. Elle englobe les efforts des employés et les processus qui soutiennent la prise de décisions relatives aux initiatives technologiques. Lorsqu'elle est mise en œuvre avec efficacité, cette gouvernance permet d'atteindre un équilibre entre la création de valeur et l'atténuation des risques pour la Ville.

3.1.1. Politiques

La mise en place de politiques des TI permet de venir encadrer la gouvernance. Celles-ci établissent les attentes et les comportements attendus en matière de sécurité de l'information et de protection des renseignements personnels.

Ces politiques doivent être formellement autorisées par la direction, revues périodiquement et diffusées à l'ensemble des employés, consultants et fournisseurs.

Dans le cadre de notre audit, nous avons constaté qu'il n'y a aucune politique de sécurité ni de procédure en place.

Recommandations

- Nous recommandons à la Ville de mettre en place, minimalement, une politique à l'égard de la sécurité des TI et de la protection de l'information ainsi qu'une procédure d'utilisation des technologies de l'information TI. Des procédures devront par la suite être élaborées afin d'opérationnaliser ces politiques. De plus, les politiques et procédures devront être revues périodiquement.
- Nous recommandons à la Ville que les politiques soient entérinées par la direction et le conseil municipal et par la suite diffusées à l'ensemble des employés, consultants et fournisseurs. Les nouveaux employés devront en prendre connaissance à leur arrivée et tous les employés devraient en prendre connaissance annuellement.
- Nous recommandons à la Ville que les politiques définissent les responsabilités en matière de protection des RP.

3.1.2. Classification et inventaire des renseignements personnels

Les organismes publics se doivent d'établir et de maintenir à jour un inventaire de ses fichiers contenant des renseignements personnels. Cela est requis par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. L'article 76 de cette loi indique ce que doit contenir l'inventaire :

- La désignation de chaque fichier, les catégories de renseignements qu'il contient, les fins pour lesquelles les renseignements sont conservés et le mode de gestion de chaque fichier;
- La provenance des renseignements versés à chaque fichier;
- Les catégories de personnes concernées par les renseignements versés à chaque fichier;
- Les catégories de personnes qui ont accès à chaque fichier dans l'exercice de leurs fonctions;
- Les mesures de sécurité prises pour assurer la protection des renseignements personnels.

Une classification et un inventaire des RP permettent de mieux maîtriser les actifs informationnels de l'organisation pour ainsi déployer les mesures nécessaires pour la protection de ceux-ci. Cela permet de bien déterminer les objectifs en matière de sécurité de l'information et de protection des RP.

Dans le cadre de notre audit, nous avons observé que la Ville s'est dotée d'un plan de classification des documents municipaux, d'un calendrier de conservation et d'une politique relative à la gestion des documents et des archives, ceux-ci datant de 2019. Cependant, nous pouvons conclure à la suite des rencontres effectuées dans le cadre du mandat que le plan de classification n'a pas été mis en application par les différents services de la Ville en raison de la pandémie de la COVID-19. La Ville prévoit déployer le plan à tous ses employés en lançant son calendrier de formation dans les prochains mois.

Nous avons également constaté qu'une entente de services a été signée en novembre 2019 avec un fournisseur externe pour la gestion intégrée des documents sur support électronique. Toutefois, nous avons relevé lors de nos rencontres que les services avec le fournisseur n'ont pas débuté et qu'il n'y avait aucune politique en place au préalable pour la gestion intégrée des documents à la Ville. Aussi, l'entente de services ne spécifie pas le traitement des documents contenant des renseignements personnels comme indiqué par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

Nous avons également constaté qu'il n'y avait pas d'inventaire à jour des RP conservés sur support papier ni d'inventaire des données conservées sur support électronique.

Recommandations

- Nous recommandons à la Ville de compléter l'élaboration de sa politique de gestion intégrée des documents avec son fournisseur externe. Cette politique devra être formellement approuvée.
- Nous recommandons à la Ville de mettre en place un inventaire des RP conservés autant sur support papier qu'électronique et de procéder à la classification de ses données, et ce, afin de se conformer à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. Cet inventaire devrait permettre d'identifier les renseignements personnels détenus par la Ville.
- Nous recommandons à la Ville de mettre en place un processus afin d'assurer le maintien et la mise à jour de l'inventaire et de la classification des renseignements, incluant les RP.
- Nous recommandons à la Ville de communiquer les politiques et les attentes à la direction des différents services afin qu'ils soient impliqués dans le maintien de l'inventaire et la classification des renseignements, incluant les RP.

3.1.3. Programme de sensibilisation

La sensibilisation à la sécurité des TI est indispensable afin de protéger une organisation de personnes malveillantes et de prévenir les cyberattaques potentielles. En effet, les techniques utilisées sont de plus en plus sophistiquées et les employés, consultants et fournisseurs sont souvent les premiers visés par ces cyberattaques, et ce, par leur manque de connaissance au sujet de celles-ci.

Ceux-ci ont donc tous un rôle important à jouer à l'égard de la sécurité de l'information. Il est primordial de mettre en place un programme de sensibilisation. Un tel programme permet de transmettre aux utilisateurs les connaissances nécessaires afin de protéger l'organisation et ses RP. Un programme de sensibilisation performant contient des formations sur la sécurité des TI et sur la protection des RP, des simulations d'hameçonnage et d'autres exercices afin d'informer les utilisateurs des façons pour se prémunir de menaces comme l'hameçonnage, le harponnage, les rançongiciels, l'ingénierie sociale, etc.

Dans le cadre de notre audit, nous avons constaté qu'il n'y a pas eu de campagne de sensibilisation formelle ni de formation sur la sécurité de l'information et des RP auprès de l'ensemble des employés de la Ville.

Recommandations

- Nous recommandons à la Ville de mettre en place un programme de sensibilisation formel à l'égard de la sécurité de l'information et de la protection des RP. Le programme devrait être revu annuellement et diffusé auprès de l'ensemble des employés et consultants de la Ville. Un tel programme peut prendre diverses formes telles que des courriels de rappel de sécurité, de la formation continue sur des sujets d'actualité ainsi que des simulations et exercices afin de tester le niveau de connaissance et de conscience en matière de sécurité et de protection des RP.
- Nous recommandons à la Ville de mettre en place des mesures afin de suivre les employés et consultants ayant participé ou ayant exécuté les activités reliées au programme de sensibilisation pour s'assurer que tous les employés suivent les formations.

3.2. CONSERVATION ET DESTRUCTION DES RP

La Ville doit prendre les mesures de sécurité nécessaires afin d'assurer la protection des RP collectés, utilisés, communiqués, conservés ou détruits telle qu'exigée par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels à l'article 63.1.

Une organisation doit s'assurer de définir des règles et procédures à l'égard de la conservation et de la destruction des données, dont les RP, et ce, autant en ce qui concerne les données sur support papier que sur support électronique. En effet, la capacité et le désir de conserver d'importantes quantités de renseignements personnels augmentent les risques relatifs à la protection des renseignements personnels. De ce fait, les durées de conservation doivent être clairement établies et tenir compte des exigences réglementaires applicables et de l'objectif initial ayant mené à la collecte de ces données.

En ce qui concerne la destruction de ces données lorsque la durée de conservation a été atteinte, une organisation doit définir les procédures visant à détruire irrémédiablement le support sur lequel sont stockées ses données, de sorte qu'il soit impossible de reconstituer celles-ci de quelque façon que ce soit. De plus, ces procédures doivent également tenir compte de la destruction de toutes les copies ainsi que de tous les fichiers de sauvegarde.

Dans le cadre de notre audit, nous avons pris en considération les RP conservés ou détruits. Pour conserver et par la suite détruire les RP au bon moment, un calendrier de conservation doit être instauré. La Ville a un plan de classification qui contient le recueil des délais de conservation des données, dont les RP. Cependant, le plan de classification ne tient pas compte des données sur support électronique, puisqu'il n'y a pas de recueil pour les données sur support électronique ni de délai de conservation défini.

Les archives sur support papier sont quant à elles conservées au sous-sol de l'hôtel de ville, et ce, derrière une porte verrouillée. Cependant, il n'y a pas de processus de gestion des accès physiques et les archives sont facilement accessibles par l'ensemble des employés de la Ville, puisque la clé se trouve à la réception et aucune gestion des clés n'est effectuée pour contrôler qui l'a utilisée.

De plus, la gestion par clé est plus complexe comparativement à une gestion par des cartes d'accès magnétiques. En effet, l'inventaire des cartes magnétiques, ainsi que les détenteurs de ces cartes, peut être facilement analysé et validé sur une base périodique, et ce, par l'entremise de rapports du système de gestion des cartes d'accès. La gestion par carte permet également une imputabilité des actions qui n'est pas présente avec les accès par clé.

Concernant la conservation des données sur support électronique à la Ville, nous avons audité les sauvegardes informatiques. Un outil est utilisé pour sauvegarder les serveurs, dont le serveur de fichiers. Cependant, la configuration de rétention pour l'ensemble des sauvegardes est de 12 jours et le système de réplique ne fonctionne pas actuellement entre les deux salles de serveurs. De plus, nous avons noté que les sauvegardes ne sont pas chiffrées. Il est recommandé de chiffrer les sauvegardes afin de s'assurer que les données sauvegardées ne sont pas accédées par des personnes non autorisées.

Concernant la destruction des archives, elle se fait par une entreprise spécialisée dans le domaine, qui détruit les archives qui sont arrivées au terme de leur délai de conservation. L'organisme émet un certificat de destruction des informations. Selon les informations recueillies lors de nos rencontres dans le cadre de l'audit, la dernière destruction de documents d'archives remonte à 2016, ce qui nous permet de conclure que le calendrier de conservation n'est pas respecté en ce qui concerne les données à détruire. De plus, relativement aux données sur support électronique, il n'y a aucune politique de disposition à l'égard des disques durs qui doivent être disposés ou effacés.

Pour les données gérées par les tiers, les contrats ne spécifient pas les paramètres quant à la conservation et à la destruction des données.

Recommandations

- Nous recommandons à la Ville de maintenir à jour son plan de classification contenant le recueil des délais de conservation et d'y inclure les données informatiques, incluant les RP, conservées dans les différents systèmes de la Ville.
- Nous recommandons à la Ville de mettre en place un processus formel afin de gérer les accès aux divers sites d'archives et de restreindre l'accès au personnel approprié uniquement.
- Nous recommandons à la Ville d'inclure, pour les contrats avec les fournisseurs hébergeant des RP, des clauses sur les durées de conservation et la destruction des données, et ce, en ligne avec le plan de classification de la Ville.
- Nous recommandons à la Ville de procéder au chiffrement des sauvegardes des données sur support électronique conservées à l'externe et de s'assurer que la période de rétention des sauvegardes répond aux besoins de la Ville.
- Nous recommandons à la Ville de mettre en place un mécanisme de suivi des délais de conservation afin de s'assurer que le calendrier de destruction des documents est respecté.
- Nous recommandons à la Ville de rédiger et de formaliser le processus de destruction des données sur support électronique (par exemple, les disques durs ou autres supports électroniques) et de documenter le processus chaque fois que des données sont effacées. Cela implique de documenter le détail des médias détruits, la procédure de destruction et la mise au rebut ainsi que de conserver une confirmation que les données ont été effacées et qu'elles ne sont plus lisibles.

3.3. MESURES DE PROTECTION

Comme indiqué précédemment et selon l'article 63.1 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, l'organisme public doit prendre les mesures propres à assurer la protection des RP. Les mesures de protection sont les procédures et contrôles mis en place par la Ville afin de protéger contre l'accès non autorisé aux RP. Nous avons évalué les procédures et contrôles en lien avec les activités suivantes :

- Gestion des accès logiques et physiques;
- Gestion des vulnérabilités;
- Gestion des incidents et de la surveillance;
- Gestion des fournisseurs.

3.3.1. Gestion des accès logiques et physiques

Accès logiques

La gestion des accès logiques vise à assurer que les accès aux systèmes contenant des RP ou aux RP directement sont restreints au personnel approprié en fonction de leurs rôles et responsabilités. La mise en place de contrôles d'accès vise à :

- Gérer et contrôler les accès logiques aux systèmes et aux données;
- Détecter des accès non autorisés;
- Définir les règles en matière d'identification, d'authentification et d'autorisation d'accès.

Nous avons évalué les mesures en place afin de contrôler et restreindre l'accès aux RP pour les systèmes inclus dans la portée de nos travaux, soit les systèmes COBA, AccèsCité Territoire, ACCEO Municipal, Permis en ligne, ACCEO Transphere, AccèsCité Loisirs ainsi que le serveur de fichiers et le contrôleur de domaine.

Gestion des octrois, modifications et retraits d'accès

La mise en place de mesures de contrôle relatives à l'octroi, à la modification et au retrait d'accès vise à assurer que les accès octroyés à un employé sont formellement autorisés et restreints en fonction des rôles et responsabilités de celui-ci. De plus, ces mesures visent à assurer que lors du départ d'un employé ou lors d'un changement de fonction, les accès de l'employé sont retirés ou modifiés, et ce, en temps opportun.

Octroi et modification des accès

Nous avons noté que le processus en place dans le cadre de la création ou modification de compte n'était pas formalisé. Le fournisseur de services de TI est avisé directement par le directeur des services financiers et trésorier. Celui-ci a été averti au préalable par les ressources humaines de l'arrivée ou du départ d'un employé par courriel ou verbalement.

En ce qui concerne les arrivées, un compte réseau est créé et les accès sont octroyés selon le titre du nouvel employé. Les accès aux applications sont gérés par une ou des personnes du service responsable de l'application (désigné comme responsable des accès à l'application). Par exemple, pour l'application ACCEO Municipal pour les finances, les personnes qui gèrent les accès sont le directeur des services financiers et une analyste comptable. À l'arrivée de l'employé, le fournisseur de services de TI va créer le compte réseau. Du côté des applications, le responsable de chaque application va octroyer les accès en fonction du rôle de l'employé au sein de la Ville.

De plus, les responsables des applications peuvent recevoir les demandes d'accès en provenance des directeurs des autres services, mais cela est informel et non documenté. Ce sont les responsables des accès qui vont généralement déterminer le type d'accès requis pour la personne.

Pour les accès confidentiels sur le serveur de fichiers, il n'existe aucun processus formalisé. Les demandes sont acheminées, par courriel ou téléphone, au directeur des services financiers et trésorier. Si ce dernier juge la demande adéquate, il l'achemine au fournisseur de services de TI pour déployer les accès.

En ce qui concerne les accès à distance, tous les utilisateurs ont désormais la possibilité d'accéder au réseau de la Ville à distance, la pandémie forçant ce choix. La Ville utilise un VPN qui est lié aux comptes du contrôleur de domaine. Par conséquent, les accès en VPN restent les mêmes que si la personne était physiquement dans les locaux de la Ville.

Le processus de gestion des accès à la Ville est généralement informel et non documenté. Les responsables des applications vont eux-mêmes octroyer les rôles et fonctions de chaque employé. Il n'y a pas de propriétaire de données qui vient approuver les demandes.

Retrait des accès

Nous avons noté que le processus en place de retrait des accès n'était pas formalisé. Le fournisseur de services de TI est informé par le directeur des services financiers et trésorier du départ d'un employé, et le fournisseur procède au retrait des accès au réseau de l'employé en question. Cependant, le fournisseur ne reçoit pas toujours l'information donc dans certaines situations, le fournisseur de services de TI ne peut pas retirer les droits d'accès en temps opportun.

C'est le même constat pour les applications, les responsables ne sont pas toujours avisés des départs. Lors de notre audit, nous avons relevé des comptes d'anciens employés qui étaient toujours actifs dans les systèmes.

Comptes génériques à hauts privilèges

Un compte générique est un compte n'appartenant pas à un utilisateur en particulier et pouvant être utilisé par plusieurs utilisateurs. Un tel compte possède généralement des accès privilégiés et ne permet pas l'imputabilité des actions commises. Dans le contexte des RP, il peut aussi y avoir des comptes génériques avec de moindres privilèges, mais possédant des accès en lecture ou écriture aux RP. Cela peut rendre difficile l'imputation des actions ou des accès aux RP en cas de bris de confidentialité avec ces comptes génériques.

Dans le cadre de notre audit, nous avons relevé l'existence des comptes génériques suivants :

- Active Directory : Compte « Administrateur », celui-ci étant utilisé par plusieurs personnes chez le fournisseur de services de TI. Cependant, il est à noter que le fournisseur possède son propre compte administrateur, mais il utilise parfois le compte « Administrateur » pour certaines tâches spécifiques et pour se connecter à certains serveurs;
- COBA – Paie : Compte « SA » pour la base de données. Le mot de passe du « SA » se trouve sur le bureau du serveur sous un fichier Note qui n'est pas protégé. L'accès au serveur est limité au fournisseur de services.
- AccèsCité Territoire : Compte générique « Formation (superviseur) », mais ce compte est inutilisé. D'après nos rencontres, nous avons constaté qu'aucun employé n'y avait accès.
- ACCEO Municipal : Compte « Conseil » utilisé uniquement par le directeur des services financiers pour approuver des factures de 10 000 $ ou plus. Il existe aussi le compte « Supervisor », mais aucun employé à la Ville ne connaît son utilisation.
- AccèsCité Loisirs : Compte « campdejours » utilisé par les responsables du camp de jour. Le compte donne accès à tous les paramètres administrateurs d'AccèsCité Loisirs.

Gestion des rôles des utilisateurs

Une bonne pratique dans la gestion des droits d'accès est d'utiliser des groupes bien définis et d'octroyer aux utilisateurs des groupes spécifiques en fonction de leurs responsabilités. Ce processus de gestion par groupe permet de plus facilement gérer les accès autant lors de l'octroi que de modification ou de révision des accès. Les accès sont gérés par groupe pour les applications et pour le réseau sauf pour les applications ACCEO Transphere, qui n'a cependant pas beaucoup d'utilisateurs, et pour AccèsCité Territoire. Voici ce que nous avons constaté :

- ACCEO Municipal : Nous avons noté que plusieurs comptes n'ont pas de rôles assignés et ont des accès octroyés à la pièce, ce qui complexifie la gestion des accès et la restriction des accès aux RP.
- ACCEO Transphere : Les accès sont également octroyés à la pièce et non par groupe. De plus, il n'est pas possible de sortir une liste des utilisateurs et de leurs accès à partir de l'application, rendant difficile l'exercice de validation de la séparation de tâches et des accès aux RP.
- AccèsCité Territoire : Les accès sont gérés à la pièce et non par groupe. On donne un accès lecture ou écriture à certains modules de l'application.

Accès aux bases de données

Les accès aux bases de données sont réservés au fournisseur de services de TI ou aux fournisseurs des applications auditées.

Recommandations

- Nous recommandons à la Ville de formaliser le processus d'octroi d'accès et de modification d'accès pour les applications et les serveurs de fichiers. Le processus doit comprendre une autorisation du propriétaire des données avant d'octroyer un accès. Ce processus doit être documenté et appliqué à toutes les applications aussi bien qu'au niveau du réseau.
- Nous recommandons à la Ville de mettre en place un processus formel afin d'aviser le fournisseur de service de TI et de retirer les accès en temps opportun lors du départ des employés. Le processus pourrait être automatisé par l'entremise du logiciel COBA ou manuel.
- Nous recommandons à la Ville d'éviter l'utilisation de comptes génériques afin d'assurer l'imputabilité des actions commises. Dans les situations où l'utilisation de tels comptes est nécessaire, la Ville devra mettre en place des mesures afin d'assurer l'imputabilité des actions, comme l'instauration d'une voûte de mot de passe qui permet de journaliser les accès aux mots de passe et le moment de l'utilisation par un utilisateur. De plus, il faudrait que les comptes génériques, bien qu'ayant des accès restreints dans les applications, n'aient pas accès aux RP.
- Nous recommandons à la Ville, pour l'application ACCEO Municipal, de gérer l'ensemble des utilisateurs par profil ou groupe afin de faciliter le processus d'octroi et de révision des accès.
- Nous recommandons à la Ville, pour les applications ACCEO Transphere et AccèsCité Territoire, de valider avec les fournisseurs s'il est possible de mettre en place la gestion des accès par groupes de sécurité.

Révision périodique des accès

Une révision périodique des accès permet au responsable d'un système de confirmer que seuls les accès autorisés sont actifs, que les accès sont conformes aux rôles et responsabilités des utilisateurs et que les accès aux RP sont restreints au personnel approprié.

Nous avons noté qu'il n'y a présentement pas de processus défini à la Ville en ce qui concerne la révision périodique des accès. Il n'y a aucune révision des accès aux applications, incluant la juste séparation des tâches et l'accès aux RP, en lecture ou écriture, de leurs bases de données et des serveurs de fichiers et du contrôleur de domaine.

Cependant, il est à noter que certaines applications comme COBA – Paie, ACCEO Transphere ainsi que les bases de données n'ont pas beaucoup d'utilisateurs, limitant ainsi le risque d'accès non autorisés.

Recommandations

- Nous recommandons à la Ville de mettre en place un processus formel de révision périodique des accès. Ce processus doit comprendre la revue complète des utilisateurs et de leurs rôles pour s'assurer de la juste séparation des tâches et que l'accès aux RP, autant en lecture qu'en écriture, est restreint au personnel approprié. Le processus devrait être appliqué pour l'ensemble des applications, incluant celles avec peu d'utilisateurs.

  En ce qui concerne les accès aux bases de données et aux systèmes d'exploitation, cette révision devrait être effectuée conjointement avec le fournisseur de services de TI.

Authentification et gestion des mots de passe

L'authentification, soit la combinaison d'un code d'utilisateur et d'un mot de passe, doit être assez robuste afin de limiter les risques d'accès non autorisés. Dans le cadre de nos travaux, nous avons évalué les paramètres de mots de passe des systèmes dans notre portée.

Nous avons relevé que l'ensemble des logiciels ne répondent pas aux bonnes pratiques en ce qui concerne la longueur, la complexité, le changement périodique des mots de passe, le verrouillage automatique après un nombre de tentatives infructueuses et le verrouillage automatique après une période d'inactivité. Nous avons constaté la même situation pour le contrôleur de domaine à l'exception de la longueur minimale qui respectait les bonnes pratiques.

Recommandations

- Nous recommandons à la Ville de revoir ses paramètres de mots de passe au contrôleur de domaine et à l'ensemble des applications, soit COBA, ACCEO Municipal, AccèsCité Territoire, Permis en ligne, ACCEO Transphere et AccèsCité Loisirs, afin de répondre aux bonnes pratiques en matière d'authentification.

  La Ville devrait également envisager la mise en place d'une authentification multifacteur afin de renforcer le processus d'authentification, et ce, en complément de la mise en place de paramètres de mots de passe plus robustes.

Accès physiques

La gestion des accès physiques vise à assurer que les accès aux salles des serveurs hébergeant les systèmes contenant des RP sont restreints au personnel approprié en fonction de leurs rôles et responsabilités. Il est à noter que la gestion des accès aux salles d'archives a été abordée à la section 3.2 – Conservation et destruction des RP.

En ce qui concerne les salles des serveurs (salles principale et secondaire), l'accès aux salles est protégé par une porte verrouillée à clé. Ce type de mécanisme ne permet pas d'identifier les personnes ayant accédé aux salles ni de journaliser quand celles-ci ont été accédées.

Nous avons relevé lors de nos rencontres que les portes des salles des serveurs ne sont pas verrouillées lors des heures de bureau et que la salle située aux ateliers municipaux est un bureau avec des fenêtres et sert aussi de salles pour effectuer des photocopies, donc avec un haut achalandage.

Dans une situation où de l'équipement contenant des RP est volé où en cas d'accès non autorisé aux serveurs, il serait difficile, voire impossible, de déterminer qui a accédé aux salles. De plus, à la suite de nos rencontres nous avons constaté que la clé est conservée à la réception de l'hôtel de ville et qu'aucun registre n'a été instauré afin de faire le suivi des accès à la salle des serveurs. De plus, la direction ignore s'il existe des copies de cette clé.

Recommandations

- Nous recommandons à la Ville de renforcer leurs contrôles d'accès physique aux salles des serveurs afin de restreindre l'accès au personnel autorisé seulement et de s'assurer de mettre en place une journalisation des accès aux salles de serveurs.

3.3.2. Gestion des vulnérabilités

La gestion des vulnérabilités est un processus qui vise la découverte proactive de menaces, la surveillance en continu des actifs informationnels d'une organisation ainsi que la mise en place de mesures afin de prévenir et détecter les menaces, incluant celles reliées aux RP.

La gestion des vulnérabilités comprend la mise en place de contrôles relatifs à l'évaluation des vulnérabilités de sécurité, la mise à jour des correctifs (*patches*) sur les serveurs et les applications, la mise en place d'antivirus et l'exécution de tests d'intrusion.

Mise à jour des correctifs (*patches*)

Nous avons évalué le processus de mise à jour des serveurs et des applications dans la portée de nos travaux. L'équipe du fournisseur de services de TI a des tâches récurrentes à l'agenda pour faire les mises à jour des serveurs régulièrement. Les postes de travail des employés sont quant à eux mis à jour automatiquement. Lors de notre audit, nous avons constaté que les serveurs étaient à jour et que les correctifs de sécurité étaient installés. Cependant, nous avons constaté que l'application COBA et le contrôleur de domaine sont hébergés sur des serveurs Windows 2008 R2, ceux-ci n'étant plus supportés par le fournisseur depuis juin 2021. Cela implique que les mises à jour de sécurité ne se font plus sur ces serveurs, ce qui augmente le risque d'accès non autorisés à ces serveurs.

Antivirus

Les postes de travail et les serveurs sont tous protégés par un antivirus qui est mis à jour automatiquement. De plus, le fournisseur de services de TI fait une revue mensuelle des postes de travail et des serveurs pour s'assurer que les mises à jour ont été effectuées sur l'ensemble du parc informatique.

L'administrateur gère les antivirus via une console qui contient entre autres un tableau de bord lui permettant de voir rapidement les versions des antivirus déployés sur les serveurs et les postes de travail. Aucune alerte n'est envoyée au fournisseur de services de TI, qui est avisé par courriel ou par téléphone par les utilisateurs lorsqu'une anomalie survient et celui-ci applique les correctifs nécessaires de façon réactive. Les utilisateurs sont administrateurs de leur poste de travail; ceci est en raison d'une limite des logiciels de PG Solutions qui requiert que le poste soit administrateur pour effectuer les mises à jour. Ceci n'est pas une bonne pratique, car les utilisateurs pourraient installer d'autres logiciels non autorisés par la Ville. En revanche, ils ne sont pas en mesure de désactiver l'antivirus.

Coupe-feu

Nous avons observé l'existence de coupe-feu aux différents points d'entrées du réseau de la Ville qui sont munis d'un IPS (*Intrusion Prevention System*). Les coupe-feu ne sont pas maintenus à jour et les règles ne sont pas révisées périodiquement. Cependant, les serveurs Web sont installés dans une zone séparée du réseau interne. Il n'y a pas de diagramme de réseau permettant de visualiser la façon dont les divers équipements communiquent entre eux. Le diagramme de réseau permettrait à la Ville de documenter son environnement réseau et de faciliter la compréhension de celui-ci par les différents intervenants amenés à intervenir en cas de problème, de changement à l'infrastructure, afin de renforcer la sécurité ou aux fins de conformité.

Tests d'intrusion

Nous avons constaté qu'aucun test d'intrusion n'a été effectué depuis de nombreuses années à la Ville.

Recommandations

- Nous recommandons à la Ville de mettre à jour son infrastructure réseau avec des versions de systèmes d'exploitation supportées par les fournisseurs pour réduire le risque d'attaque sur le réseau.
- Nous recommandons à la Ville de valider périodiquement les règles de coupe-feu pour s'assurer qu'elles sont toujours à jour et utiles et qu'elles protègent adéquatement le réseau.
- Nous recommandons à la Ville de réaliser des tests d'intrusion sur le réseau interne et d'effectuer, annuellement, des tests d'intrusion par l'entremise d'une firme de sécurité externe. Les vulnérabilités à corriger doivent être suivies et priorisées en fonction de leur criticité.
- Nous recommandons à la Ville de documenter et de maintenir à jour un diagramme de réseau.
- Nous recommandons à la Ville de mettre en place un processus d'autorisation visant l'installation de logiciels sur les postes de travail et de vigie des logiciels installés sur les postes de travail.

3.3.3. Gestion des incidents et de la surveillance

Un processus de gestion des incidents vise à identifier les incidents de sécurité, incluant les incidents afférents aux RP, et permet de s'assurer que des mesures de mitigation appropriées sont mises en place afin d'éviter qu'un incident se reproduise.

La gestion des incidents de sécurité se fait par le fournisseur de services de TI.

Nous avons constaté que la Ville n'a aucun processus formalisé concernant la gestion des incidents. Lorsqu'il y a un problème urgent, un employé de la Ville a la possibilité de contacter le service à la clientèle du fournisseur de services de TI. Pour tout autre incident, un technicien se présente une fois par mois à l'hôtel de ville.

De plus, il n'y a pas de processus formel de détection et d'escalade en cas d'incident de sécurité et de bris de confidentialité de RP. Un tel processus permettrait d'être prêt à intervenir dans l'éventualité d'un incident de sécurité ou de bris de confidentialité de RP, d'être en mesure de répondre rapidement lors de l'incident et de ne pas oublier les étapes critiques permettant de résoudre celui-ci dans les meilleurs délais, le cas échéant.

Les actions sur l'infrastructure du réseau, les coupe-feu ainsi que le VPN sont journalisés et celles-ci peuvent être consultées en cas d'incident. Cependant, les journaux (*logs*) ne sont pas formellement analysés et révisés périodiquement par le fournisseur de service de TI.

Recommandations

- Nous recommandons à la Ville, par l'entremise de son fournisseur de services de TI, de mettre en place d'un processus de gestion des incidents de sécurité et bris de confidentialité de RP ainsi qu'un processus d'escalade.
- Nous recommandons à la Ville, par l'entremise de son fournisseur de services de TI, de mettre en place un processus visant à analyser les journaux afin d'identifier et d'intervenir en temps opportun s'il y a des tentatives d'accès ou des incidents de sécurité.

3.3.4. Gestion des fournisseurs

La Ville collabore avec des fournisseurs qui peuvent héberger des RP, et ce, collectés pour le bénéfice de la Ville. Dans le cas d'AccèsCité Loisirs, Permis en ligne et ACCEO Transphere, il s'agit d'applications hébergées et gérées par le fournisseur. Les RP se trouvent donc chez ces fournisseurs. De plus, les serveurs et les bases de données sont gérés par le fournisseur de services de TI Trilogie. Celui-ci a accès aux RP de COBA, ACCEO Municipal, AccèsCité Territoire ainsi qu'au contrôleur de domaine.

AccèsCité Loisirs

Nous pouvons trouver les RP suivants sur l'application :

Ouverture du compte citoyen : adresse de courriel, nom, prénom, téléphone et sexe sont obligatoires. La date de naissance, le rôle familial, l'adresse complète sont optionnels.

Mise à jour du profil de chaque membre de la famille : nom, prénom, adresse, code postal, téléphone. Les informations suivantes sont facultatives : numéro d'assurance maladie et NAS.

De plus, pour les enfants, les renseignements suivants sont facultatifs : allergies, médicaments et troubles de comportement.

Permis en ligne

Les demandes de permis en ligne doivent avoir au minimum les informations sur l'adresse complète, le courriel du citoyen et son téléphone. Les paiements ne sont pas pris électroniquement, mais via un terminal de paiement.

ACCEO Transphere

Plateforme de paiements des fournisseurs et pour recevoir les paiements des citoyens provenant d'AccèsCité Loisirs et Permis en ligne. Nous pouvons trouver les RP suivants dans l'application :

- Lors de la consultation d'une fiche d'un fournisseur : nom, adresse, courriel
- Lors de la consultation d'une fiche d'un citoyen : nom, prénom, adresse, courriel
- L'application détient aussi les informations bancaires de la Ville qui permet de procéder à des virements en ligne.

Trilogie

Trilogie est le fournisseur de services de TI pour la Ville. Il n'héberge aucun RP sur ses systèmes internes. En revanche, les techniciens attitrés au mandat de support technique de la Ville sont en mesure d'accéder à l'ensemble des bases de données entreposées à l'interne sur les serveurs de la Ville. Nous pouvons trouver les RP suivants :

- COBA : nom, prénom, adresse, date de naissance, sexe, langue maternelle, information bancaire et numéro d'assurance sociale.
- ACCEO Municipal : nom, prénom et adresse des citoyens et courriel.
- AccèsCité Territoire : nom, prénom, adresse, courriel et téléphone.

Considérant que des RP collectés pour la Ville sont hébergés chez des fournisseurs et que des RP sont accessibles par le fournisseur Trilogie, il est important pour la Ville de mettre en place un processus formel de gestion des fournisseurs afin de s'assurer que les fournisseurs avec qui la Ville collabore répondent aux standards établis en matière de sécurité et de protection des RP. De plus, la Ville doit mettre en place des mesures de surveillance afin d'évaluer la conformité de ces fournisseurs aux standards établis. Nous avons noté que la Ville n'a pas élaboré de processus formel de gestion des fournisseurs permettant de s'assurer que les bonnes pratiques de sécurité sont prises en compte dans les contrats.

Aussi, la Ville ne procède pas à une évaluation périodique de ses fournisseurs afin d'identifier les fournisseurs les plus à risque, et ce, en fonction des RP hébergés ou des services rendus, afin d'évaluer la sécurité par l'entremise d'un questionnaire ou l'obtention d'une attestation externe démontrant leur conformité à un cadre de référence reconnu en matière de sécurité de l'information.

Recommandations

- Nous recommandons à la Ville de mettre en place un processus formel de gestion des fournisseurs afin de définir le processus lors de la sélection d'un nouveau fournisseur et d'évaluer périodiquement la performance et la conformité de celui-ci aux standards de sécurité établis et attendus. L'évaluation périodique doit être effectuée en fonction du risque associé au fournisseur afin de s'assurer qu'il respecte les clauses contractuelles et les standards établis en matière de sécurité et de protection des RP.
- Nous recommandons à la Ville d'intégrer des clauses au contrat de service auprès des fournisseurs relativement aux attentes en matière de sécurité et de protection des RP ainsi qu'aux divulgations nécessaires en cas de bris de confidentialité. Voici une liste non exhaustive de clauses à considérer :
    - Accès aux RP restreint au personnel autorisé du fournisseur;
    - Confidentialité des RP hébergés;
    - Sous-traitants du fournisseur (si applicable) devant se conformer aux mêmes standards de sécurité que le fournisseur selon le contrat;
    - Durée de conservation des RP et méthodes de destruction;
    - Etc.

4. Conclusion

La Ville possède plusieurs RP autant sur ses employés que sur ses citoyens. La Ville doit donc s'assurer de mettre en place un environnement de contrôle adéquat permettant de maintenir la confidentialité des RP et de protéger ceux-ci.

Gouvernance

La Ville ne s'est pas dotée d'une politique de sécurité des TI et de politiques d'utilisation de l'informatique ni d'une politique de la protection de l'information qui viennent établir la gouvernance et qui décrivent les lignes directrices de la sécurité des TI et de la protection des RP au sein de la Ville. Ces politiques devraient être formellement approuvées par la direction et par le conseil municipal.

Tel qu'il est requis dans la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, la Ville se doit d'établir et de maintenir à jour un inventaire de ses fichiers contenant des renseignements personnels. Nos travaux nous ont permis de constater qu'un plan de classification des documents municipaux, qu'un calendrier de conservation et qu'une politique relative à la gestion des documents et des archives sont en place depuis 2019. Cependant, ceux-ci ne sont pas suivis par les différents services.

En date du présent rapport, le registre d'inventaire n'était pas à jour pour les documents sur support papier et il n'y a pas de registre en place pour les données sur support électronique. De plus, il n'y a pas de classification des fichiers permettant d'identifier les RP. La Ville se devra de poursuivre son projet de classification et de mettre à jour son registre d'inventaire, et ce, périodiquement.

En ce qui concerne la sensibilisation des employés, il n'y a pas eu de campagnes de sensibilisation formelle ou de formation sur la sécurité de l'information et des RP auprès de l'ensemble des employés de la Ville. Les employés sont un point névralgique de la sécurité de l'information et ils doivent être sensibilisés et formés afin de détecter les menaces éventuelles.

Conservation et destruction des RP

La Ville a un plan de classification des documents municipaux qui contient le recueil des délais de conservation des données, dont les RP. Cependant, nous avons noté que ce plan de classification ne tient pas compte des données sur support électronique.

En ce qui concerne les archives sur support papier, elles sont conservées au sous-sol de l'hôtel de ville derrière une porte verrouillée à clé. Cependant, la clé se trouve à la réception et aucune gestion des clés n'est effectuée pour contrôle qui prend la clé. Il est donc difficile pour la Ville d'identifier les employés ayant accès à ces salles et ainsi d'assurer une imputabilité des actions.

Concernant les sauvegardes informatiques, celles-ci sont mises sur cassette à l'extérieur de la salle des serveurs principale. Cependant, nous avons noté qu'il n'existe pas de politique de hiérarchie des sauvegardes et que la réplique à la salle secondaire n'était pas fonctionnelle lors de notre audit. De plus, les sauvegardes ne sont pas chiffrées, ce qui augmente le risque que des sauvegardes contenant des RP soient lues par des personnes non autorisées.

Finalement, en ce qui concerne les données gérées par les tiers, les ententes auprès de ces tiers devraient spécifier les exigences quant à la conservation et à la destruction des données.

Mesures de protection

Nous avons noté dans le cadre de nos travaux que le processus de gestion des accès logiques était généralement informel et non documenté, et ce, tant au niveau de l'octroi des accès aux applications qu'au retrait de ceux-ci à la suite du départ d'un employé. Ce constat augmente le risque que des accès non autorisés soient octroyés, que les accès octroyés ne soient pas en fonction des responsabilités de l'employé ou qu'un employé ne se voie pas retirer ses accès en temps opportun. De plus, nous avons noté l'existence de comptes génériques, ce qui ne permet pas d'assurer l'imputabilité des actions commises, principalement en ce qui concerne les accès aux RP. Finalement, il n'y a aucun processus de révision périodique des accès en place, ce qui permettrait au responsable d'un système de confirmer que seuls les accès autorisés sont effectifs, que les accès sont conformes aux rôles et responsabilités des utilisateurs et que les accès aux RP sont restreints au personnel approprié.

Il est important de mettre en place des mots de passe robustes pour accéder aux applications qui contiennent des RP. Nous avons remarqué que ce ne sont pas toutes les applications qui forcent les utilisateurs à utiliser des paramètres de mot de passe robustes. Cela permettrait de réduire le risque d'usurpation de compte et d'accès non autorisé aux RP.

En ce qui concerne la gestion des vulnérabilités, nous avons été en mesure de conclure que les correctifs étaient à jour sur les postes de travail ainsi que sur les serveurs et que ceux-ci étaient protégés par un antivirus. Nous avons cependant noté que les utilisateurs sont administrateurs de leurs postes de travail et que des serveurs ont des versions non supportées de Windows pour l'application COBA et le contrôleur de domaine, ce qui augmente le risque d'accès non autorisés. De plus, le réseau de la Ville est protégé par des coupe-feu aux différents points d'entrées du réseau de la Ville et ceux-ci sont munis d'un IPS (*Intrusion Prevention System*). Cependant, les coupe-feu ne sont pas mis à jour régulièrement et les règles de ceux-ci ne sont pas révisées périodiquement. Par ailleurs, la Ville n'a pas réalisé de tests d'intrusion dans les dernières années autant pour le périmètre externe qu'interne.

Pour ce qui concerne la gestion des incidents, il n'y a pas de processus formel de détection et d'escalade en cas d'incident de sécurité et de bris de confidentialité de RP. De plus, les incidents ou problèmes identifiés directement par le fournisseur qui gère le service des TI ne sont pas formellement journalisés dans le système de billetterie, ce qui permettrait d'avoir une vue globale des incidents et d'identifier les tendances ou les incidents récurrents. La révision des journaux des équipements de sécurité comme les coupe-feu n'est effectuée que lorsqu'il y a un incident. Il n'y a pas de processus permettant de détecter les menaces en temps opportun avant que le risque se matérialise.

Enfin, en ce qui concerne la gestion des fournisseurs, nous avons noté qu'ils peuvent héberger des RP, ceux-ci étant collectés pour le bénéfice de la Ville. Il est donc primordial de mettre en place un processus formel de gestion des fournisseurs afin de définir le processus lors de la sélection d'un nouveau fournisseur et d'évaluer périodiquement la performance et la conformité de celui-ci aux standards de sécurité établis et attendus. De plus, nous avons noté qu'il n'y avait pas systématiquement de clauses au contrat de service auprès des fournisseurs relativement aux attentes en matière de sécurité et de protection des RP ainsi qu'aux divulgations nécessaires en cas de bris de confidentialité.

5. Objectif et critères d'audit

5.1. OBJECTIF

S'assurer que les renseignements personnels détenus par la Ville faisaient l'objet d'une protection adéquate afin de mitiger les risques de bris de confidentialité, de vol ou d'accès non autorisés aux RP.

5.2. CRITÈRES D'AUDIT

- Gouvernance :
  - La Ville dispose de politiques définissant les exigences quant à la gestion des RP, et ce, pour l'ensemble des services de la Ville;
  - La Ville maintient un inventaire des RP, permettant à celle-ci d'avoir un portrait global des renseignements à protéger;
  - Les employés de la Ville sont sensibilisés quant aux enjeux et risques liés à la gestion des RP afin que ceux-ci respectent les politiques ou mesures visant la sécurité de ces renseignements;
- Conservation et destruction des RP :
  - Les RP sont conservés selon un calendrier préétabli et lorsque ceux-ci ne sont plus requis, ils sont détruits de manière à ce qu'ils ne puissent plus être reconstitués;
- Mesures de protection à l'égard des RP :
  - Les accès sont accordés de manière à ce que les accès aux RP soient limités aux personnes autorisées uniquement, de par leurs rôles et responsabilités. De plus, les paramètres de sécurité sont assez robustes pour prévenir des accès non autorisés aux RP;
  - La Ville a mis en place des mesures de surveillance afin de prévenir et détecter des attaques ou des vulnérabilités potentielles. De plus, la Ville procède à des tests d'intrusion qui permettent de mesurer les vulnérabilités des systèmes contenant des RP face aux cyberattaques;
  - La Ville a mis en place un processus de gestion des incidents lui permettant de réagir en temps opportun en cas d'incident majeur visant des RP afin de minimiser les impacts réels d'un tel incident et de prendre les mesures nécessaires afin de résoudre celui-ci;
  - Les RP transmis, gérés ou hébergés par des tierces parties (fournisseurs) sont protégés afin de préserver la confidentialité de ceux-ci.

rcgt.com

Raymond Chabot Grant Thornton

Certification | Fiscalité | Conseil