Rapport

Audit d’optimisation des ressources – Protection des renseignements personnels

6 octobre 2022

Présenté à :

Raymond Chabot Grant Thornton

Bécancour

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 6 octobre 2022

Aux membres du conseil municipal
Ville de Bécancour
1295, av. Nicolas-Perrot
Bécancour (Québec) G9H 1A1

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 Bécancour (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 Bécancour (ci-après la « Ville ») collecte et traite des renseignements personnels afférents à la vie privée de ses employés et des citoyens. La Ville compte plus de 14 000 citoyens et plus de 100 employés. 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 ligne, comme les demandes de permis et la taxation.

La Ville étant un organisme municipal, elle est donc assujettie à la loi pour le secteur public : 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 comme les renseignements personnels 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 renseignements personnels :

- 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 témoin *(cookie)*;
- Numéro de plaque d'immatriculation, numéro d'une pièce d'identité, coordonnées bancaires;
- Données relatives à la santé des individus;
- Données concernant la vie sexuelle ou l'orientation sexuelle;
- Données qui révèlent une origine raciale ou ethnique.

Certaines données sont de nature publique, comme le rôle d'évaluation et taxation, où l'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 renseignements personnels, en plus de ne pas être conformes à la loi, peuvent être de permettre la divulgation non autorisée des renseignements personnels; qu'une personne malintentionnée utilise l'information des renseignements personnels 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 violation des données, de vol ou d'accès non autorisé aux renseignements personnels.

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-conformité 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 22 décembre 2021 au 11 février 2022. Cependant, nous avons tenu compte des informations reçues jusqu'en septembre 2022.

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

- Suite financière (SFM) – système financier et de taxation;
- AccèsCité Territoire – système utilisé entre la gestion des permis;
- Target 911 – système de gestion du Service incendie;
- Activitek – système de gestion des loisirs permettant de gérer les différentes activités offertes aux citoyens. Il permet également aux citoyens de procéder à des inscriptions en ligne;
- Serveur de fichiers et contrôleur de domaine – système gérant les fichiers et les utilisateurs sur le réseau.

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 renseignements personnels.

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

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 informatique, 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 officiellement 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 y avait une *Politique d'utilisation des systèmes informatiques* en place et disponible sur le réseau de la Ville. La politique décrit ce que l'employé est autorisé à faire ainsi que les usages interdits avec les systèmes TI, les contrôles et la surveillance de l'utilisation par les employés des ressources informatiques ainsi que les mesures disciplinaires en cas de non-conformité à la politique. Cependant, celle-ci ne traite pas des critères de sécurité ni de la protection des renseignements personnels, et la dernière mise à jour remonte à mai 2010.

Une procédure est également en place afin que chaque nouvel employé de la Ville prenne connaissance de la politique et accepte de s'y conformer en la signant. Cependant, nous avons relevé que la politique n'était pas diffusée aux fournisseurs ni aux consultants externes qui interagissent avec les renseignements personnels et qu'il n'y a pas de clause de confidentialité détaillée dans les contrats avec ceux-ci.

Recommandations

- Nous recommandons à la Ville de mettre en place une politique à l'égard de la sécurité des TI et de la protection de l'information (ci-après la « politique de sécurité des TI »). Des procédures devront par la suite être élaborées pour venir opérationnaliser la politique. De plus, cette nouvelle politique de sécurité des TI, la *Politique d'utilisation des systèmes informatiques* ainsi que les procédures élaborées devront être revues et mises à jour périodiquement.
- Nous recommandons à la Ville de communiquer les politiques de sécurité aux consultants et fournisseurs de services ayant accès à des renseignements personnels dans le cadre de leur mandat.
- Nous recommandons à la Ville d'inclure des clauses relatives à la confidentialité dans les contrats conclus avec des consultants ou fournisseurs de services ou de leur faire signer une entente de confidentialité.

3.1.2. Classification et inventaire des renseignements personnels

Les organismes publics se doivent d'établir et de maintenir à jour un inventaire de leurs 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 renseignements personnels 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 renseignements personnels.

Dans le cadre de notre audit, nous avons observé que la Ville a finalisé l'élaboration de son plan de classification des documents papier et électroniques municipaux ainsi que d'un calendrier de conservation. Ceux-ci ont été soumis à la Bibliothèque et Archives nationales du Québec (BAnQ) et approuvés par celle-ci.

En ce qui concerne l'établissement et le maintien de l'inventaire des renseignements personnels, nous avons constaté qu'il n'y avait pas d'inventaire à jour des renseignements personnels conservés sur support papier ni d'inventaire des données conservées sur support électronique malgré le fait que la Ville s'est dotée d'un logiciel de catégorisation des actifs informationnels. En effet, nous avons relevé que le logiciel était utilisé par peu de services au sein de la Ville.

Recommandations

- Nous recommandons à la Ville de maintenir à jour son inventaire des renseignements personnels 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 une politique visant à assurer le maintien et la mise à jour de l'inventaire et de la classification des renseignements, incluant les renseignements personnels. Cette politique et les attentes à l'égard de celle-ci devront être communiquées à l'ensemble des services afin qu'ils soient impliqués dans le processus de maintien de l'inventaire et de la classification des données.

3.1.3. Programme de sensibilisation

La sensibilisation à la sécurité des TI est indispensable pour protéger une organisation de personnes malveillantes et 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 connaissances 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 pour protéger l'organisation et ses renseignements personnels. Un programme de sensibilisation performant contient des formations sur la sécurité des TI et sur la protection des renseignements personnels, 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'une campagne de sensibilisation sur la cybersécurité a été suivie par les employés de la Ville. Cependant, cette campagne était demandée par les assurances et ne faisait pas partie intégrante d'un programme de sensibilisation officiel.

Recommandations

- Nous recommandons à la Ville de mettre en place un programme de sensibilisation officiel, visant à sensibiliser sur une base périodique les employés de la Ville par l'entremise de campagnes de sensibilisation à l'égard de différents sujets en matière de cybersécurité (i.e. confidentialité des données, protection des renseignements personnels, utilisation de mots de passe sécuritaire, etc.)

3.2. CONSERVATION ET DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

La Ville doit prendre les mesures de sécurité nécessaires pour assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits, comme l'exige 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 renseignements personnels, 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 les reconstituer 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 renseignements personnels conservés ou détruits. Pour conserver et par la suite détruire les renseignements personnels au bon moment, un calendrier de conservation doit être instauré. La Ville a finalisé l'élaboration et fait approuver par la BAnQ son plan de classification, qui contient le recueil des délais de conservation des données, dont les renseignements personnels. Le plan de classification tient en compte les données papier et électroniques. Actuellement, le processus de conservation et de destruction des données est informel.

Conservation des données

Les archives papier sont conservées dans plusieurs locaux répartis dans différents bâtiments de la Ville. Les accès à ces bâtiments requièrent une carte d'accès, et les archives sont conservées derrière des portes verrouillées par clé ou par code. Seulement quelques employés possèdent une copie des clés. Par ailleurs, à la suite de nos rencontres, nous avons relevé que les codes permettant les accès à certaines archives papier n'ont pas été changés depuis de nombreuses années.

La gestion par clés est plus complexe que la 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 cartes permet également une imputabilité des actions qui n'est pas présente avec les accès par clé.

Concernant la conservation des données électroniques à la Ville, nous avons observé le processus relatif aux sauvegardes informatiques. Un outil est utilisé pour sauvegarder les serveurs, dont le serveur de fichiers. Nous avons constaté qu'il n'y avait pas de politique officielle de conservation des données des sauvegardes et qu'il n'y avait pas de tests de restauration afin de valider l'intégrité des sauvegardes.

Destruction des données

Concernant la destruction des archives, la Ville possède une déchiqueteuse industrielle pour procéder elle-même à la destruction des documents papier. Il arrive que la Ville sous-traite le processus de destruction à des entreprises spécialisées dans le domaine lorsqu'il s'agit d'un lot important de documents. De plus, la Ville exige de l'entreprise un certificat de destruction suivant les travaux effectués. Nous avons obtenu le dernier certificat de destruction, datant de février 2019. Concernant les données électroniques, il n'y a aucune politique de mise au rebut des disques durs qui doivent être éliminés ou effacés.

Enfin, pour les données gérées et hébergées par des tiers, les contrats ne spécifient pas les paramètres de conservation et de 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 renseignements personnels, conservés dans les différents systèmes de la Ville.
- Nous recommandons à la Ville de mettre en place un processus officiel 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 dans les contrats avec les fournisseurs hébergeant des renseignements personnels des clauses sur les durées de conservation et sur la destruction des données, selon le plan de classification de la Ville.
- Nous recommandons à la Ville d'établir une politique de sauvegarde des données électroniques, de chiffrer les sauvegardes des données électroniques à l'externe et de faire des tests de restauration périodiquement pour tester l'efficacité des sauvegardes.
- Nous recommandons à la Ville de rédiger et d'officialiser le processus de destruction des données électroniques et de documenter le processus chaque fois que des données sont effacées. Cela implique de documenter le détail des médias détruits (comme les disques), la procédure de destruction et la mise au rebut et également 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 renseignements personnels. Les mesures de protection sont les procédures et contrôles mis en place par la Ville afin de protéger contre l'accès non autorisé aux renseignements personnels. 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 de la relève informatique;
- 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 renseignements personnels ou aux renseignements personnels directement sont restreints au personnel approprié en fonction de ses 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 de restreindre l'accès aux renseignements personnels pour les systèmes inclus dans la portée de nos travaux, soit les systèmes SFM, Activitek, Target 911 et AccèsCité Territoire, 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 officiellement autorisés et restreints en fonction de ses rôles et responsabilités. De plus, ces mesures visent à s'assurer qu'au départ ou au changement de fonction d'un employé, ses accès 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 de la modification de comptes n'était pas officialisé. Le Service des ressources humaines avise par téléphone ou courriel le responsable des TI lors de l'arrivée ou du départ d'un employé.

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 SFM, les personnes qui gèrent les accès sont la trésorière et l'assistant-trésorier. À l'arrivée de l'employé, le responsable des 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. En ce qui concerne les accès confidentiels sur le serveur de fichiers, toutes les demandes sont acheminées par un gestionnaire, souvent de manière informelle, soit par courriel, téléphone ou billetterie.

Les accès à distance sont quant à eux autorisés à même le contrôleur de domaine par l'intermédiaire d'un groupe de sécurité. Les autorisations sont faites via des requêtes par les gestionnaires au Service des TI en fonction des besoins des utilisateurs. Les utilisateurs sont ajoutés au groupe de sécurité par le responsable des TI. La Ville utilise un réseau privé virtuel (VPN) qui est lié aux comptes du contrôleur de domaine et, par conséquent, les accès en réseau privé virtuel restent les mêmes que si la personne était physiquement dans les locaux de la Ville.

Retrait des accès

Nous avons noté que le processus en place pour le retrait des accès n'était pas officialisé. Le responsable des TI est informé par un courriel, téléphone ou via la billetterie lorsqu'il doit désactiver les accès. Il prend en charge la demande et procède au retrait des accès au réseau de l'employé en question. Cependant, le responsable des TI n'a pas de procédure ni d'étapes à suivre pour s'assurer que l'ensemble des accès ont été retirés ni si ceux-ci ont été retirés en temps opportun.

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 renseignements personnels, il peut aussi y avoir des comptes génériques avec de moindres privilèges, mais possédant des accès en lecture ou écriture aux renseignements personnels. Cela peut rendre difficile l'imputation des actions ou des accès aux renseignements personnels en cas de violation des données avec ces comptes génériques.

Dans le cadre de notre audit, nous avons relevé l'existence de certains comptes génériques. Cependant, il s'agit de comptes utilisés par les fournisseurs des applications ou uniquement par le responsable des TI en ce qui concerne le domaine de serveur.

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 précis en fonction de leurs responsabilités. Ce processus de gestion par groupes permet de plus facilement gérer les accès autant lors de l'octroi que de la modification ou de la révision des accès. Les accès sont gérés par groupes pour l'application Target 911 et pour le réseau. Voici ce que nous avons constaté pour les autres applications :

- SFM et Activitek : Les accès sont octroyés à la pièce et non par groupes. De plus, il n'est pas possible de produire 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 renseignements personnels;
- AccèsCité Territoire : Les accès sont gérés à la pièce et non par groupes. 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 responsable des TI ou aux fournisseurs selon les 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 officiel de gestion des retraits d'accès afin qu'ils soient traités en temps opportun au départ des employés et que les démarches soient uniformes pour les différentes applications.
- Nous recommandons à la Ville de restreindre au Service des TI la capacité de gérer les accès aux applications.
- Nous recommandons à la Ville, pour les applications SFM, Activitek et AccèsCité Territoire, de valider auprès des fournisseurs la possibilité de gérer les 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 renseignements personnels 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 renseignements personnels, en lecture ou en écriture, de leurs bases de données et des systèmes de fichiers et du contrôleur de domaine.

Cependant, il est à noter que certaines applications comme Target 911 et Activitek n'ont pas beaucoup d'utilisateurs, limitant ainsi le risque d'accès non autorisés.

Recommandation

- Nous recommandons à la Ville de mettre en place un processus officiel 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 du fait que l'accès aux renseignements personnels, autant en lecture qu'en écriture, est restreint au personnel approprié. Le processus devrait être adopté pour l'ensemble des applications, incluant celles avec peu d'utilisateurs.

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 la portée.

Nous avons relevé que, pour les systèmes inclus dans la portée de nos travaux, les paramètres de mots de passe ne respectent pas les bonnes pratiques.

Recommandations

- Nous recommandons à la Ville de revoir les paramètres de mots de passe à ses systèmes afin de respecter les bonnes pratiques en matière d'authentification.
- Nous recommandons à la Ville d'envisager la mise en place d'une authentification multifacteur pour l'accès au réseau afin de renforcer le processus d'authentification.

Accès physiques

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

En ce qui concerne les salles des serveurs se situant dans des bâtiments appartenant à la Ville, l'accès aux salles est protégé par une porte verrouillée par un code mécanique pour la salle principale et par une clé pour la salle secondaire. Ce type de mécanisme ne permet pas d'identifier les personnes ayant accédé aux salles ni de journaliser quand celles-ci ont été accédées.

De plus, nous avons relevé lors de nos rencontres que l'accès aux salles n'est pas restreint au personnel TI et de l'infrastructure uniquement. Dans une situation où de l'équipement contenant des renseignements personnels est volé ou en cas d'accès non autorisé aux serveurs, il serait difficile, voire impossible, de déterminer qui a accédé aux salles.

Recommandation

- Nous recommandons à la Ville de renforcer les contrôles d'accès physique aux salles des serveurs afin de restreindre l'accès au personnel autorisé seulement et 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 pour prévenir et détecter les menaces, incluant celles reliées aux renseignements personnels.

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 *(patchs)* sur les serveurs et les applications, la mise en place d'antivirus et l'exécution de tests d'intrusion.

Mise à jour des correctifs *(patchs)*

Nous avons évalué le processus de mise à jour des serveurs et des applications dans la portée de nos travaux. Selon nos observations, il existe un processus automatisé de mise à jour des serveurs via un serveur de distribution Windows. En effet, le serveur télécharge et applique automatiquement les mises à jour de vulnérabilités et les correctifs de sécurité. Les autres sont acheminées par courriel automatique au responsable des TI qui les révise une fois par mois pour approbation. Les

postes de travail des employés, eux, sont mis à jour automatiquement. Lors de notre audit, nous avons constaté que les serveurs étaient à jour et que les correctifs de sécurité étaient tous installés.

Mise à jour applicative

Nous avons évalué le processus de mise à jour des applications lorsque les fournisseurs proposent des mises à jour. Nous avons noté que les mises à jour sont appliquées directement en production sans que celles-ci fassent l'objet de tests avant la mise à jour. Des tests dans un environnement de préproduction permettent de s'assurer que la mise à jour applicative n'entraînera pas de problèmes en matière de compatibilité ou d'intégrité des données.

Antivirus

Les postes de travail et les serveurs sont tous protégés par un antivirus qui est mis à jour automatiquement toutes les six heures avec une fréquence de distribution aux postes de travail toutes les 60 minutes. Le responsable des TI gère les antivirus via une console. Cette console contient entre autres un tableau de bord permettant de voir rapidement les versions des antivirus déployées sur les serveurs et les postes de travail. Une surveillance est exercée par le responsable des TI, qui consulte les alertes reçues par courriel et les traite en fonction de leur criticité. Aucun utilisateur n'est administrateur de son poste de travail, les empêchant ainsi d'installer des logiciels non autorisés.

Coupe-feu

Nous avons observé l'existence de coupe-feux aux différents points d'entrée du réseau de la Ville qui sont munis d'un IPS *(Intrusion Prevention System).* Les coupe-feux sont maintenus à jour et les règles sont révisées lors des activités de maintenance. De plus, les serveurs Web sont installés dans une zone séparée du réseau interne.

Tests d'intrusion

À la suite de nos rencontres, nous avons constaté que la Ville n'effectue pas de tests d'intrusion, et ce, sur une base périodique.

Recommandations

- Nous recommandons à la Ville de tester les mises à jour applicatives évaluées comme étant critiques dans un environnement de préproduction avant la mise en production de la version afin de s'assurer que celles-ci ne causent pas de problème touchant les données et les processus.
- Nous recommandons à la Ville de réaliser, sur une base périodique, des tests d'intrusion sur les réseaux interne et externe par l'intermédiaire d'une firme de sécurité externe. Les vulnérabilités à corriger doivent être suivies et priorisées en fonction de leur criticité, le cas échéant.

3.3.3. Gestion des incidents et de la surveillance

Un processus de gestion des incidents vise à découvrir les incidents de sécurité, incluant les incidents afférents aux renseignements personnels, 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 Service des TI de la Ville.

Nous avons constaté que la Ville n'a pas de processus officialisé concernant les incidents de sécurité. La Ville utilise le logiciel Octopus pour gérer les incidents et les problèmes. Les demandes peuvent être reçues directement de l'interface Web et la priorisation des billets est déterminée selon le jugement du responsable des TI. Cependant, nous avons constaté que plusieurs employés communiquent directement par courriel ou téléphone pour rapporter un incident.

Concernant la surveillance, les journaux *(logs)* de l'infrastructure du réseau ne sont pas analysés périodiquement par le responsable au Service des TI. Les journaux des serveurs, des coupe-feux et du réseau privé virtuel ne sont pas revus. Les validations sont faites de façon réactive, alors que celles-ci devraient se faire de manière proactive.

Recommandations

- Nous recommandons à la Ville de mettre en place un processus officiel de gestion des incidents de sécurité, des violations de données confidentielles ainsi qu'un processus d'escalade.
- Nous recommandons à la Ville de mettre en place un processus d'analyse des journaux et d'alerte permettant de détecter en temps réel les tentatives d'accès ou les incidents de sécurité.

3.3.4. Gestion de la relève informatique

La relève informatique permet de rétablir la situation à la normale rapidement en cas d'incident majeur dans les salles de serveurs. Un plan de relève permet également de remonter plus rapidement l'environnement informatique sans négliger la sécurité de l'information.

La Ville n'a pas de plan de relève informatique qui couvrirait l'ensemble des applications et des infrastructures.

Recommandation

- Nous recommandons à la Ville de concevoir un plan de relève informatique pour l'infrastructure et les applications critiques ainsi qu'un calendrier de tests périodiques pour s'assurer que la stratégie de relève est valide et qu'elle permet de maintenir son plan de relève informatique à jour.

3.3.5. Gestion des fournisseurs

La Ville collabore avec des fournisseurs qui peuvent héberger des renseignements personnels qui ont été collectés au bénéfice de la Ville. Nous avons constaté qu'il n'y avait aucun processus officiel d'évaluation des fournisseurs.

Les appels d'offres de la Ville incluent une clause à l'égard des informations confidentielles. Cependant, les documents ne détaillent pas les exigences ni l'étendue des critères à respecter en matière de sécurité et de protection des renseignements personnels exigés par la Ville.

Considérant que des renseignements personnels collectés pour la Ville sont hébergés chez des fournisseurs, il est important pour la Ville de mettre en place un processus officiel 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 renseignements personnels. 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 mis en place un processus officiel de gestion des fournisseurs permettant de s'assurer que les bonnes pratiques de sécurité de l'information sont prises en compte dans les contrats.

Aussi, la Ville ne procède pas à une évaluation périodique de ses fournisseurs visant à découvrir les fournisseurs les plus à risque selon les renseignements personnels hébergés et à évaluer la sécurité grâce à un questionnaire ou à l'obtention d'une attestation externe démontrant leur conformité à un cadre de référence reconnu.

Recommandations

- Nous recommandons à la Ville de mettre en place un processus officiel de gestion des fournisseurs afin de définir le processus lors de la sélection d'un nouveau fournisseur et d'évaluer périodiquement sa performance et sa conformité 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 renseignements personnels.
- Nous recommandons à la Ville d'intégrer des clauses aux contrats de service avec des fournisseurs relativement aux attentes en matière de sécurité et de protection des renseignements personnels ainsi qu'aux divulgations nécessaires en cas de violation de données. Voici une liste non exhaustive de clauses à considérer :
    - Accès aux renseignements personnels restreint au personnel autorisé du fournisseur;
    - Confidentialité des renseignements personnels 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 renseignements personnels et méthodes de destruction;
    - Etc.

4. Conclusion

La Ville possède plusieurs renseignements personnels 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 renseignements personnels et de les protéger.

En conclusion, bien que la Ville ait mis en place plusieurs mesures visant la protection des renseignements personnels, celles-ci pourraient, à notre avis, faire l'objet d'améliorations et d'optimisations des ressources de la Ville.

Gouvernance

La Ville s'est dotée d'une politique d'utilisation des systèmes informatiques. Cependant, cette politique n'a pas été mise à jour depuis 2010 et celle-ci ne traite pas des critères de sécurité ni de la protection des renseignements personnels. De plus, bien que les employés doivent attester de se conformer à la politique en la signant, ce n'est pas le cas pour les consultants et les fournisseurs ayant accès à des données confidentielles.

De plus, 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. Nous avons constaté qu'un plan de classification ainsi qu'un calendrier de conservation ont été élaborés et approuvés par la BAnQ. Cependant, en date du présent rapport, le registre d'inventaire des données de la Ville n'est pas à jour et il n'y a pas de classification des fichiers permettant d'identifier les renseignements personnels.

Enfin, en ce qui concerne la sensibilisation des employés, nous avons constaté qu'une campagne de sensibilisation sur la cybersécurité a été suivie par les employés de la Ville. Cependant, cette campagne ne faisait pas partie intégrante d'un programme de sensibilisation officiel. Les employés sont un point névralgique de la sécurité de l'information et ils doivent être sensibilisés et formés sur une base périodique afin de reconnaître les menaces éventuelles.

Conservation et destruction des renseignements personnels

La Ville a finalisé l'élaboration et fait approuver par la BAnQ un plan de classification des documents municipaux qui contient le recueil des délais de conservation des données et celui-ci traite autant des documents papier qu'électroniques.

Concernant les archives papier, celles-ci sont conservées dans différents locaux répartis à travers les bâtiments de la Ville, derrière des portes verrouillées par clé ou par code. Cependant, nous avons relevé que les codes permettant d'accéder aux salles des archives n'ont pas été changés depuis de nombreuses années. Il est donc difficile pour la Ville de savoir quels employés ont accès à ces salles et ainsi 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 que les sauvegardes ne sont pas chiffrées, ce qui augmente le risque que des sauvegardes contenant des renseignements personnels soient lues par des personnes non autorisées. De plus, le processus de destruction des données informatiques n'est pas officialisé afin de s'assurer que les équipements informatiques mis au rebut ne contiennent plus de renseignements personnels.

Enfin, en ce qui concerne les données gérées par des tiers, les ententes avec ceux-ci devraient spécifier les exigences quant à la conservation et à la destruction des données.

Mesures de protection

Nous avons noté dans nos travaux que le processus de gestion des accès logiques était bien documenté pour l'octroi des accès aux applications lors de l'arrivée d'un employé. Cependant, nous avons noté les éléments suivants relativement à la gestion des accès :

- La création des accès lors de l'embauche d'un employé est un processus généralement informel et non documenté;
- Le processus de retrait des accès lors du départ d'un employé n'est pas officiellement documenté et les accès ne sont pas toujours retirés en temps opportun;
- La gestion des accès n'est pas restreinte au Service des TI pour l'ensemble des applications;
- Il n'y a aucun processus officiel de révision périodique des accès en place, et ce, autant pour le réseau que les applications;
- Les applications et le réseau ne forcent pas les utilisateurs à utiliser des paramètres de mot de passe robustes.

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. Le réseau de la Ville est également protégé par des coupe-feux à ses différents points d'entrée et ceux-ci sont munis d'un IPS *(Intrusion Prevention System).* De plus, les coupe-feux sont mis à jour régulièrement et leurs règles sont révisées lors de déploiements. Cependant, la Ville ne réalise pas de tests d'intrusion sur une base périodique, et ce, autant pour les périmètres externes qu'internes.

Relativement à la gestion des incidents, il n'y a pas de processus officiel de détection et d'escalade en cas d'incident de sécurité ou de violation de renseignements personnels. Cependant, les incidents ou problèmes relevés par le responsable des TI sont journalisés dans le système de billetterie, ce qui permet d'avoir une vue globale des incidents et dégager les tendances ou les incidents récurrents.

Finalement, considérant que certains fournisseurs collectent et hébergent des renseignements personnels au bénéfice de la Ville, il est donc primordial de mettre en place un processus officiel de gestion des fournisseurs afin de définir le processus lors de la sélection d'un nouveau fournisseur et d'évaluer périodiquement sa performance et sa conformité aux standards de sécurité établis et attendus. De plus, nous avons noté qu'il n'y avait pas systématiquement de clauses dans les contrats de services avec les fournisseurs relativement aux attentes en matière de sécurité et de protection des renseignements personnels, ainsi qu'aux divulgations nécessaires en cas de violation de données.

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 violation de données, de vol ou d'accès non autorisé aux renseignements personnels.

5.2. CRITÈRES D'AUDIT

- Gouvernance :
  - La Ville dispose de politiques définissant les exigences quant à la gestion des renseignements personnels, et ce, pour l'ensemble des services de la Ville;
  - La Ville tient un inventaire des renseignements personnels lui permettant d'avoir un portrait global des renseignements à protéger;
  - Les employés de la Ville sont sensibilisés aux enjeux et risques liés à la gestion des renseignements personnels afin qu'ils respectent les politiques ou mesures visant la sécurité de ces renseignements;
- Conservation et destruction des renseignements personnels :
  - Les renseignements personnels sont conservés selon un calendrier préétabli et, lorsqu'ils 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 renseignements personnels :
  - Les accès sont accordés de manière à ce que les accès aux renseignements personnels 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 renseignements personnels;
  - La Ville a mis en place des mesures de surveillance afin de prévenir et de 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 renseignements personnels 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 renseignements personnels afin de réduire les impacts réels d'un tel incident et de prendre les mesures nécessaires afin de le résoudre;
  - Les renseignements personnels transmis, gérés ou hébergés par des tiers (fournisseurs) sont protégés afin d'en préserver la confidentialité.

rcgt.com

Raymond Chabot Grant Thornton

Certification | Fiscalité | Conseil