Rapport

Audit d’optimisation des ressources – Protection des données confidentielles

25 mars 2022

Présenté à :

Raymond Chabot Grant Thornton

Ville de Saint-Hyacinthe
Technopole agroalimentaire

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

25 mars 2022

Aux membres du Conseil municipal
Ville de Saint-Hyacinthe
700, avenue de l'Hôtel-de-ville
Saint-Hyacinthe (Québec) J2S 5B2

Objet : Rapport – Audit d'optimisation des ressources – Protection des données confidentielles

Mesdames, Messieurs,

Nous avons le plaisir de vous présenter notre rapport portant sur l'information relative à la protection des données confidentielles par la Ville de Saint-Hyacinthe (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 Saint-Hyacinthe (ci-après la « Ville ») collecte des données confidentielles de diverses natures dans le cadre de ses opérations. Une donnée confidentielle constitue une donnée qui ne doit être communiquée ou rendue accessible qu'aux personnes ou entités autorisées. De plus, une donnée confidentielle devient une donnée ou une information sensible lorsqu'elle a le potentiel de mettre en péril l'intégrité de la personne ou de l'entité qu'elle concerne.

La Ville étant un organisme municipal, elle est entre autres 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.

Voici quelques exemples de données confidentielles détenues par la Ville :

- 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. Les témoins (*cookies*) et les adresses IP récoltés sur les sites en ligne de la Ville;
- Informations sur les fournisseurs, les données financières et les documents confidentiels.

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

Une mauvaise protection des données confidentielles, en plus de ne pas être conforme à la loi, peut avoir comme conséquences la divulgation non autorisée des données confidentielles, l'utilisation de l'information des données confidentielles par une personne malintentionnée aux fins d'usurpation d'identité, l'atteinte à la réputation de la Ville, la 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 confidentiels.

Cet audit avait pour objectif de s'assurer que les données confidentielles détenues par la Ville faisaient l'objet d'une protection adéquate afin de mitiger les risques de violation de la confidentialité, de vol ou d'accès non autorisés aux données confidentielles.

Responsabilité de la direction

La direction de la Ville est responsable de la protection des renseignements confidentiels 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 confidentiels, et ce, conformément aux règles en vigueur et aux saines pratiques en matière de protection des renseignements confidentiels.

Responsabilité de l'auditeur

Notre responsabilité consiste à fournir une conclusion sur les objectifs de l'audit. Pour ce faire, nous estimons que nous avons recueilli des 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 15 octobre 2021 au 23 novembre 2021. Nous avons toutefois tenu compte d'informations qui nous ont été transmises jusqu'en décembre 2021.

Nos travaux ont été réalisés sur un échantillon de systèmes contenant des données confidentielles et jugées critiques par la Ville et s'y sont limités. Les systèmes sélectionnés sont les suivants :

- Sport-Plus – logiciel d'inscription, de réservation et de location en ligne (géré et hébergé par un fournisseur externe);
- AccèsCité Territoire – système utilisé pour la gestion du territoire et des demandes diverses dont l'urbanisme (hébergé par la Ville);
- AccèsCité Finances (SFM) – système de paie et des ressources humaines (hébergé par la Ville);
- Première Ligne – système des gestions du service incendie (hébergé par la Ville);
- Serveur de fichiers et contrôleur de domaine – système gérant les fichiers et les utilisateurs sur le réseau (hébergé par la Ville).

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 d'encadrer les principes et les standards souhaités par la Ville et cette notion s'applique à l'ensemble des sphères d'une Ville, incluant une gestion adéquate des données confidentielles.

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 d'encadrer la gouvernance. Celles-ci établissent les attentes et les comportements attendus en matière de sécurité de l'information et de protection des renseignements confidentiels. 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 de sécurité ayant été mise à jour en février 2020 et étant disponible sur l'intranet de la Ville. De plus, une procédure est en place pour que chaque nouvel employé à la Ville prenne connaissance de la politique et accepte de s'y conformer en la signant. Cependant, nous avons relevé que la politique de sécurité n'était pas transmise aux fournisseurs ni aux consultants externes qui interagissent avec les données confidentielles et qu'il n'y a pas non plus de clause de confidentialité dans les contrats avec ceux-ci.

Recommandations

- Nous recommandons à la Ville de communiquer les politiques aux consultants et fournisseurs ayant accès à des données confidentielles dans le cadre de leur mandat.
- Nous recommandons à la Ville d'inclure des clauses relatives à la confidentialité dans ces contrats avec des fournisseurs de services.

3.1.2. Classification et inventaire des données confidentielles

Les organismes publics se doivent d'établir et de maintenir à jour un inventaire de leurs fichiers contenant des données confidentielles. Par ailleurs, la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (article 76) 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 données confidentielles permettent de mieux maîtriser les actifs informationnels de l'organisation pour ainsi déployer les mesures nécessaires pour leur protection. On peut ainsi bien déterminer les objectifs en matière de sécurité de l'information et de protection des données confidentielles.

Dans le cadre de notre audit, nous avons observé que la Ville est dotée d'un plan de classification des documents papier municipaux, d'un calendrier de conservation et d'une politique relative à la gestion des documents et des archives, la dernière mise à jour datant de janvier 2011. La Ville est aussi dotée d'un plan d'intervention en cas d'urgence, mis à jour en février 2020, et qui détaille le processus à suivre en cas d'incident mineur ou majeur. Le plan donne un résumé de différents scénarios ainsi qu'un portrait général des dépôts d'archives dans les différentes chambres fortes de la Ville.

Nous avons également constaté qu'un plan directeur de la gestion des documents électroniques (GED) a été rédigé en 2010 avec la collaboration d'un fournisseur externe. Toutefois, nous avons relevé lors de nos rencontres et de l'observation du plan directeur que plusieurs étapes ne sont pas encore réalisées et qu'il n'y avait aucune politique en place au préalable pour la gestion intégrée des documents électroniques à la Ville.

Recommandations

- Nous recommandons à la Ville de mettre à jour son inventaire et de procéder à la classification de ses données électroniques, 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 de déterminer les renseignements personnels et les données confidentielles 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 données électroniques, incluant les données confidentielles.
- Nous recommandons à la Ville de communiquer les politiques et les attentes à la direction des différents services afin qu'ils participent au maintien de l'inventaire et à la classification des renseignements, incluant les données confidentielles.

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, de par leur manque de connaissance à ce sujet.

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 données confidentielles. Un programme de sensibilisation performant contient des formations sur la sécurité des TI et sur la protection des données confidentielles, des simulations d'hameçonnage et d'autres exercices afin d'informer les utilisateurs sur les façons de se prémunir contre des menaces comme l'hameçonnage, le harponnage, les rançongiciels, l'ingénierie sociale, etc.

Dans le cadre de notre audit, nous avons constaté que le service des technologies de l'information déploie des avertissements sur les bonnes pratiques concernant la confidentialité des mots de passe et l'hameçonnage via l'intranet. De plus, nous avons observé qu'une formation en continu a démarré en juillet 2021 pour l'ensemble des employés ayant comme thème « les cybercomportements à risque ».

Recommandation

- Nous recommandons à la Ville de poursuivre la mise en place de son processus visant à s'assurer que tous les employés suivent les formations en sécurité et cybersécurité et de varier les formations obligatoires chaque année.

3.2. CONSERVATION ET DESTRUCTION DES DONNÉES CONFIDENTIELLES

La Ville doit prendre les mesures de sécurité nécessaires afin d'assurer la protection des données confidentielles collectées, utilisées, communiquées, conservées ou détruites 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 données confidentielles, et ce, autant en ce qui concerne les données sur support papier et support électronique. En effet, la capacité et le désir de conserver d'importantes quantités de données confidentielles augmentent les risques relatifs à leur protection. 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 ses 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 tous les fichiers de sauvegarde.

Dans le cadre de notre audit, nous avons pris en considération les données confidentielles conservées ou détruites. Pour conserver et par la suite détruire les données confidentielles 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 données confidentielles. Cependant, le plan de classification ne tient pas compte des données électroniques, puisqu'il n'y a pas de recueil pour les données électroniques ni de délai de conservation défini.

Les archives papier sont quant à elles conservées à l'hôtel de ville dans des chambres fortes verrouillées par un code et celui-ci est connu par un nombre restreint d'employés à la Ville, soit les employés de la gestion documentaire. Cependant, nous avons relevé que le code n'avait pas été modifié depuis plus de 20 ans.

De plus, la gestion par code est moins efficace qu'une gestion par cartes d'accès magnétiques. En effet, le nombre de cartes magnétiques ainsi que leurs détenteurs peuvent être facilement analysés et validés sur une base périodique, et ce, grâce à des rapports du système de gestion des cartes d'accès. La gestion par cartes permet également une reddition des actions qui n'est pas possible avec les accès par code.

Concernant la conservation des données électroniques à la Ville, nous avons audité les 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 de conservation des données des sauvegardes et qu'il n'y avait pas non plus de tests de restauration pour valider l'intégrité des sauvegardes. De plus, nous avons noté que les sauvegardes ne sont pas chiffrées. Il est recommandé de chiffrer les sauvegardes afin de s'assurer qu'elles ne sont pas lues par des personnes non autorisées si jamais un incident survenait.

Concernant la destruction des archives papier, celle-ci est confiée à une entreprise spécialisée dans le domaine qui détruit les archives dont le délai de conservation est expiré. L'organisme émet un certificat de destruction des informations. Nous avons observé le dernier certificat de destruction d'octobre 2021, celui-ci détaille les travaux effectués et le fournisseur certifie que tous les documents confidentiels ont été détruits de manière à rendre impossible toute reconstitution. Concernant les données électroniques, il n'y a aucune politique d'élimination des disques durs qui doivent être détruits ou effacés.

Pour les données gérées par les tiers, les contrats ne précisent pas les paramètres quant à la conservation et 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 données confidentielles conservées 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.
- Nous recommandons à la Ville d'inclure, dans les contrats avec les fournisseurs hébergeant des données confidentielles, des clauses sur les durées de conservation et la destruction des données, et ce, harmonisées au plan de classification de la Ville.
- Nous recommandons à la Ville 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 de standardiser 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 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 données confidentielles. Les mesures de protection sont les procédures et contrôles mis en place par la Ville afin de protéger contre l'accès non autorisé aux données confidentielles. 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 données confidentielles ou aux données 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 les 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 données confidentielles pour les systèmes inclus dans la portée de nos travaux, soit les systèmes Sport-Plus, AccèsCité Territoire, AccèsCité Finances (SFM), Première Ligne ainsi que le serveur de fichiers et 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 assurer que lors du départ d'un employé ou 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 pour la création ou la modification d'un compte utilisateur passe via un système de billetterie. Un formulaire de besoins informatiques est rempli par un employé des ressources humaines ou par le superviseur immédiat du nouvel employé. Ensuite, le formulaire est joint à une requête à la billetterie C2 Enterprise pour être traité par un employé responsable au service des technologies de l'information. Un formulaire supplémentaire est rempli et transmis avec la requête pour Sport-Plus, indiquant la liste des accès à autoriser au niveau applicatif.

Lorsque la requête est acheminée au service des TI, l'analyste responsable prend en charge le billet et s'assure que le formulaire est dûment rempli et signé. Par la suite, un compte réseau est créé et les accès sont octroyés selon le titre du nouvel employé. Pour les applications Sport-Plus, AccèsCité Territoire et AccèsCité Finances (SFM), les accès sont gérés par une ou des personnes du service responsable de l'application au service des TI. En revanche, pour les applications Sport-Plus et AccèsCité Territoire, nous avons relevé que certains utilisateurs n'étant pas du service des TI avaient des droits permettant de gérer les accès, ce qui ne constitue pas une séparation adéquate des tâches.

Pour l'application Première Ligne, les accès sont gérés par des personnes-ressources au sein du service incendie, soit le directeur adjoint, le chef d'équipe ou l'adjointe administrative. Ainsi, nous avons constaté que la même personne peut remplir une demande, l'approuver et donner les accès à l'application.

En ce qui concerne les accès confidentiels sur le serveur de fichiers, toutes les demandes sont acheminées au service des technologies de l'information via une requête. Ceux-ci doivent être approuvés par un gestionnaire du service en question avant l'octroi des accès.

Les accès à distance sont quant à eux autorisés à même le contrôleur de domaine par l'entremise d'un groupe de sécurité. Les autorisations sont faites via des requêtes par les gestionnaires au service de technologie de l'information en fonction des besoins des utilisateurs. La Ville utilise un VPN qui est lié aux comptes du contrôleur de domaine et, par conséquent, les accès en VPN 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 est centralisé au service des technologies de l'information à l'exception des applications Première Ligne, Sport-Plus et AccèsCité Territoire. Un formulaire de cessation d'emploi est rempli par le gestionnaire ou par les ressources humaines et acheminé par requête via la billetterie et par courriel pour les trois applications qui sont gérées par le responsable applicatif lorsque pertinent. Il arrive que la demande soit acheminée par courriel lors de départs précipités. Nous avons constaté que les droits d'accès sont retirés en temps opportun autant au niveau applicatif que pour le contrôleur de domaine.

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 la reddition des actions commises. Dans le contexte des données confidentielles, il peut aussi y avoir des comptes génériques avec de moindres privilèges, mais possédant des accès en lecture ou écriture aux données confidentielles. Cela peut rendre difficile la reddition des actions ou des accès aux données en cas de violation de confidentialité avec ces comptes génériques.

Dans le cadre de notre audit, nous avons relevé l'existence de comptes génériques sur le réseau et dans les applications incluses à la portée de l'audit. Pour le réseau, les comptes sont principalement des comptes de service étant utilisés pour des outils ou des applications dont les mots de passe sont connus par les TI uniquement. Dans AccèsCité Finances (SFM), un compte générique PG Admin est utilisé par le fournisseur. Pour Première Ligne, le compte « admin » est présent et le mot de passe est connu par le directeur adjoint du service de prévention.

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 définis en fonction de leurs rôles et responsabilités au sein de l'organisation. La gestion par groupe permet de gérer plus facilement les processus d'octroi, de modification ou de révision des accès. Nous avons relevé que les accès sont gérés par groupe uniquement pour le réseau. En effet, toutes les applications testées n'ont pas de rôles assignés et ont des accès octroyés à la pièce. Voici ce que nous avons constaté :

- Sport-Plus et Première Ligne : Nous avons noté que plusieurs comptes utilisateurs n'ont pas de rôles assignés ou ont des accès octroyés à la pièce. De plus, il n'est pas possible de générer 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 données confidentielles.
- AccèsCité Territoire et AccèsCité Finances (SFM) : Les accès sont gérés à la pièce et non par groupe, ce qui complexifie la gestion des accès et la restriction des accès aux données confidentielles.

Accès aux bases de données

Les accès aux bases de données sont réservés aux employés du service des TI ou aux fournisseurs selon les applications auditées.

Recommandations

- Nous recommandons à la Ville d'éviter l'utilisation de comptes génériques afin d'assurer la reddition des actions commises. Dans les situations où l'utilisation de tels comptes est nécessaire, nous recommandons à la Ville de mettre en place des mesures permettant d'assurer la reddition 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.
- Nous recommandons à la Ville de restreindre au service des TI la capacité de gérer les accès aux applications Première Ligne, Sport-Plus et AccèsCité Territoire.
- Nous recommandons à la Ville, pour l'application AccèsCité Finances (SFM), de gérer l'ensemble des utilisateurs par profil ou groupe afin de faciliter le processus d'octroi, de modification et de révision des accès.
- Nous recommandons à la Ville, pour les applications Sport-Plus, Première Ligne 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 activés, qu'ils sont conformes aux rôles et responsabilités des utilisateurs et que les accès aux données confidentielles 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 données confidentielles, 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 pour Première Ligne, malgré le fait qu'il n'y ait aucune révision officiellement documentée, une révision constante des utilisateurs est effectuée, car les quarts de travail sont attitrés automatiquement par l'ancienneté d'un utilisateur activé dans l'application.

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 que l'accès aux données confidentielles, autant en lecture qu'en écriture, est restreint au personnel approprié. Le processus devrait être appliqué pour l'ensemble des applications.

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 inclus à notre portée.

Nous avons relevé que les logiciels Sport-Plus et Première Ligne ne respectent pas les 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.

Pour ce qui est d'AccèsCité Territoire et d'AccèsCité Finances (SFM), ceux-ci utilisent les paramètres d'authentification unique via le contrôleur de domaine *Single sign-on*. Nous avons constaté que les paramètres du contrôleur de domaine respectaient les bonnes pratiques en matière de mot de passe robuste.

Recommandations

- Nous recommandons à la Ville de revoir les paramètres de mots de passe pour les applications Sport-Plus et Première Ligne afin de respecter les bonnes pratiques en matière d'authentification.
- Nous recommandons à la Ville d'envisager la mise en place d'une authentification multifacteurs pour l'accès au réseau afin de renforcer le processus d'authentification.

Accès physiques

La gestion des accès physiques vise à assurer que les accès aux salles des serveurs hébergeant les systèmes contenant des données confidentielles 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 discutée à la section 3.2 – Conservation et destruction des données confidentielles.

La salle des serveurs principale est localisée au service des TI et la salle des serveurs secondaire est localisée à l'usine de traitement d'eaux usées. L'accès aux salles est protégé par une porte verrouillée par code à l'hôtel de ville et par clé physique à l'usine de traitement d'eaux usées. Ces mécanismes ne permettent pas d'identifier les personnes ayant accédé aux salles ni de journaliser les accès.

Dans une situation où de l'équipement contenant des données confidentielles est volé où 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 mettre en place des mécanismes d'accès permettant de journaliser les accès aux salles des serveurs critiques et hébergeant des données confidentielles. De plus, l'accès à ces salles devrait être restreint au personnel autorisé seulement.

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 de détecter les menaces, incluant celles reliées aux données confidentielles.

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

Mise à jour des rustines (*patchs*)

Nous avons évalué le processus de mise à jour des serveurs et des applications dans la portée de nos travaux. L'équipe du service des TI effectue des tests en local avant d'effectuer des mises à jour mineures. Pour les mises à jour majeures, une copie complète de l'environnement à mettre à jour est effectuée avant le déploiement. 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 rustines de sécurité étaient installées. Cependant lors de nos discussions avec le directeur TI, celui-ci nous confirme qu'il y a encore certains serveurs 2008 et que certains postes de travail dans le parc informatique fonctionnent avec Windows XP. Ces serveurs et ces postes de travail pourraient contenir des failles de sécurité qui ne sont plus corrigées par les fournisseurs, ce qui pourrait permettre à des personnes malintentionnées d'exploiter ces failles.

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 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 toutes les 60 minutes. L'administrateur réseau gère les antivirus via une console. Cette console contient entre autres un tableau de bord lui permettant de voir rapidement les versions des antivirus déployées sur les serveurs et les postes de travail. Une surveillance est effectuée par l'administrateur réseau, qui consulte les alertes reçues par courriel et les traite en fonction de la criticité de celles-ci. De plus, nous avons constaté que les employés étant administrateurs de leur poste de travail sont connus, autorisés et requis dans le cadre de leurs fonctions.

Coupe-feu

Nous avons observé l'existence de coupe-feu aux différents points d'entrée du réseau de la Ville qui sont munis d'un IPS (*Intrusion Prevention System*). Les coupe-feu sont maintenus à jour et les règles sont révisées périodiquement. De plus, un mécanisme d'alerte IPS a été développé à l'interne afin de détecter les menaces et un rapport périodique des alertes est révisé par un responsable au service des TI.

Tests d'intrusion

Nous avons constaté que des tests d'intrusion ont été effectués par une firme externe spécialisée en 2020. Nous avons obtenu une copie du rapport et discuté des différentes vulnérabilités critiques déjà corrigées par le service des TI de la Ville.

Recommandations

- Nous recommandons à la Ville de mettre à jour les versions des serveurs et des postes de travail à des versions supportées par les fournisseurs pour s'assurer qu'il n'y a pas de faille de sécurité sur le réseau. Si cela n'est pas réalisable, nous recommandons d'isoler ces serveurs du réseau et d'en restreindre l'accès.
- 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 dans les données et les processus.

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 données confidentielles, 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 à l'interne par le service des TI.

Nous avons constaté que la Ville n'a pas de processus officiel concernant les incidents de sécurité. La Ville utilise l'outil C2 Enterprise pour gérer les incidents et les problèmes. Les demandes peuvent être reçues directement de l'interface Web, par téléphone ou par courriel. Une fonctionnalité de C2 convertit les courriels directement en billets, qui sont par la suite remplis par la technicienne. La priorisation des billets est déterminée selon le jugement de la personne de garde qui les assigne aux techniciens responsables.

De plus, il n'y a pas de processus officiel de détection et d'escalade en cas d'incident de sécurité et de violation de la confidentialité de données confidentielles. Un tel processus permet d'être prêt à l'éventualité d'un incident de sécurité ou de violation de la confidentialité de données confidentielles, d'être en mesure de répondre rapidement lors de l'incident et de ne pas oublier d'étapes primordiales pour résoudre l'incident dans les meilleurs délais.

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-feu et du VPN ne sont pas révisés et les validations sont faites de façon réactive et non proactive. Ainsi, une tentative d'accès ou même une intrusion sur leur infrastructure pourrait être détectée uniquement après les faits.

Recommandations

- Nous recommandons à la Ville de mettre en place un processus officiel de gestion des incidents de sécurité, des violations de la confidentialité 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 des alertes permettant de détecter en temps réel les tentatives d'accès ou des incidents de sécurité.

3.3.4. Gestion de la relève informatique

La relève informatique permet de ramener la situation à la normale rapidement en cas d'incident majeur dans les salles de serveurs. La Ville a dressé un plan de relève informatique qui couvre l'ensemble des applications et des infrastructures. Le plan établit une stratégie basée sur la virtualisation et la réplication fréquente des données entre les deux sites et prévoit une stratégie de recouvrement. Cependant, nous avons relevé que le plan a été testé une seule fois lors de son implantation en 2019 et celui-ci n'a pas été mis à jour depuis.

Recommandation

- Nous recommandons à la Ville de créer un calendrier de tests pour couvrir la stratégie de recouvrement du plan de relève, d'effectuer les tests périodiquement et de maintenir son plan de relève TI à jour.

3.3.5. Gestion des fournisseurs

La Ville collabore avec des fournisseurs qui peuvent héberger des données confidentielles qui ont été collectées pour le bénéfice de la Ville. Nous avons constaté qu'il n'existe aucun processus officiel d'évaluation des fournisseurs. Dans le cas de Sport-Plus, d'AccèsCité Territoire et d'AccèsCité Finances (SFM), les bases de données sont gérées par les fournisseurs.

Considérant que des données confidentielles collectées pour la Ville sont hébergées 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 respectent les standards établis en matière de sécurité et de protection des données confidentielles. De plus, la Ville doit mettre en place des mesures de surveillance afin d'évaluer la conformité de ces fournisseurs aux standards établis. De plus, nous avons noté que la Ville n'a pas mis en place un 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 de découvrir quels fournisseurs sont les plus à risque selon les données confidentielles hébergées et 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.

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 afin 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 données confidentielles.
- 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 données confidentielles ainsi qu'aux divulgations nécessaires en cas de violation de confidentialité. Voici une liste non exhaustive de clauses à considérer :
    - Accès aux données confidentielles restreint au personnel autorisé du fournisseur;
    - Confidentialité des données confidentielles hébergées;
    - Sous-traitants du fournisseur (si applicable) devant se conformer aux mêmes standards de sécurité que le fournisseur selon le contrat;
    - Durée de conservation des données confidentielles et méthodes de destruction;
    - Etc.

4. Conclusion

La Ville collecte et détient une multitude de données confidentielles, incluant des données sensibles, dont certaines à l'égard des employés et des citoyens de la Ville. La Ville doit donc s'assurer de mettre en place un environnement de contrôle adéquat permettant de maintenir la confidentialité des données et de les protéger.

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

Gouvernance

La Ville est dotée d'une politique de sécurité des TI regroupant des politiques d'utilisation de l'informatique et une politique de la protection de l'information qui vient établir la gouvernance et qui décrit les lignes directrices de la sécurité des TI et de la protection des données confidentielles au sein de la Ville. Cependant, bien que les employés doivent attester de se conformer à la politique en signant celle-ci, ce n'est pas le cas pour les consultants et les fournisseurs ayant accès à des données confidentielles.

De plus, en vertu de la législation en vigueur, la Ville se doit d'établir et de maintenir à jour un inventaire de ses fichiers contenant des données confidentielles. 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 étaient présents et suivis par les différents services. Le registre d'inventaire est à jour et permet de trouver les données confidentielles conservées sur support papier. Cependant, nous avons relevé qu'il n'y avait pas de politiques et de classification officielle en ce qui concerne les données électroniques. En effet, un plan de gestion des données électroniques a débuté en 2015 et est toujours en cours en date du présent rapport.

Enfin, en ce qui concerne la sensibilisation des employés, il y a eu des campagnes de sensibilisation et une formation sur la sécurité de l'information et des données confidentielles 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. La Ville doit donc s'assurer que tous les employés suivent les formations.

Conservation et destruction des données confidentielles

La Ville a un plan de classification des documents municipaux qui contient le recueil des délais de conservation des données. Cependant, nous avons noté que ce plan de classification ne tient pas compte des données électroniques ni des délais de conservation définis.

En ce qui concerne les archives papier, elles sont conservées dans des chambres fortes à l'hôtel de ville protégées par des portes verrouillées par code. Bien que le code ne soit pas connu par plusieurs employés, celui-ci n'a pas été modifié depuis plus de 20 ans, rendant difficile pour la Ville de savoir quels employés ont accès à ces salles et ainsi d'assurer une reddition des actions.

Concernant les sauvegardes informatiques, celles-ci sont mises sur cassettes à l'extérieur de la salle des serveurs principale. Cependant, nous avons noté qu'il n'existe pas de politique relativement à la hiérarchie des sauvegardes. De plus, les sauvegardes ne sont pas chiffrées, ce qui augmente le risque que des sauvegardes contenant des données confidentielles soient lues par des personnes non autorisées. Également, le processus de destruction des données informatiques n'est pas officiel, ce qui permettrait de s'assurer que les équipements informatiques mis au rebut ne contiennent pas de données confidentielles.

Enfin, en ce qui concerne les données gérées par les tiers, les ententes avec ces tiers ne précisent pas 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 officiel et bien documenté, et ce, tant dans l'octroi des accès aux applications que dans leur retrait à la suite du départ d'un employé. Cependant, nous avons noté les éléments suivants relativement à la gestion des accès :

- La gestion des accès n'est pas restreinte au service des TI pour certaines applications;
- Des comptes génériques sont utilisés, ce qui ne permet pas d'assurer la reddition des actions commises, principalement en ce qui concerne les accès aux données confidentielles;
- Il n'y a aucun processus formel de révision périodique des accès en place, et ce, autant pour le réseau que les applications;
- Certaines applications 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 les éléments suivants : les rustines étaient à jour sur les postes de travail et sur les serveurs, ceux-ci étaient protégés par un antivirus, le réseau de la Ville est protégé par des coupe-feu aux différents points d'entrée du réseau de la Ville et ceux-ci sont munis d'un IPS (*Intrusion Prevention System*), et la Ville a réalisé des tests d'intrusion au cours des dernières années. Nous avons cependant noté les éléments suivants :

- La Ville possède des serveurs et des postes de travail fonctionnant avec des versions non supportées de Windows, ce qui augmente le risque de failles de sécurité non corrigées;
- Le processus de mise à jour des applications évaluées comme étant critiques ne passe pas par une série de tests en préproduction avant l'implantation en production;

Pour ce qui concerne la gestion des incidents, il n'y a pas de processus officiel de détection et d'escalade en cas d'incident de sécurité et de violation de la confidentialité de données confidentielles. De plus, les incidents ou problèmes découverts par le service des TI ne sont pas officiellement journalisés dans le système de billetterie, ce qui ne permet pas d'avoir une vue globale des incidents et d'isoler les tendances ou les incidents récurrents.

Concernant la relève informatique en cas de problème majeur, la Ville s'est dotée d'un plan de relève informatique, mais celui-ci n'a pas été mis à jour ni testé depuis son instauration en 2019.

Enfin, en ce qui concerne la gestion des fournisseurs, nous avons noté que ceux-ci peuvent héberger des données confidentielles, celles-ci étant collectées pour le 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 leur performance et leur conformité 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 avec des fournisseurs relativement aux attentes en matière de sécurité et de protection des données confidentielles ainsi qu'aux divulgations nécessaires en cas de violation de la confidentialité.

5. Objectif et critères d'audit

5.1. OBJECTIF

S'assurer que les données confidentielles détenues par la Ville faisaient l'objet d'une protection adéquate afin de mitiger les risques de violation de la confidentialité, de vol ou d'accès non autorisés aux données confidentielles.

5.2. CRITÈRES D'AUDIT

- Gouvernance :
  - La Ville dispose de politiques définissant les exigences quant à la gestion des données confidentielles, et ce, pour l'ensemble des services de la Ville;
  - La Ville maintient un inventaire des données confidentielles, lui permettant d'avoir un portrait global des données à protéger;
  - Les employés de la Ville sont sensibilisés quant aux enjeux et aux risques liés à la gestion des données confidentielles afin de respecter les politiques ou mesures visant la sécurité de ces données;
- Conservation et destruction des données confidentielles :
  - Les données confidentielles sont conservées selon un calendrier préétabli et, lorsque celles-ci ne sont plus requises, elles sont détruites de manière à ce qu'elles ne puissent plus être reconstituées;
- Mesures de protection à l'égard des données confidentielles :
  - Les accès sont accordés de manière à ce que les accès aux données confidentielles 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 données confidentielles;
  - 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 données confidentielles 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 données confidentielles afin de minimiser les impacts réels d'un tel incident et de prendre les mesures nécessaires afin de le résoudre;
  - Les données confidentielles transmises, gérées ou hébergées par de tierces parties (fournisseurs) sont protégées afin d'en préserver la confidentialité.

rcgt.com

Raymond Chabot Grant Thornton

Certification | Fiscalité | Conseil