3.1.

Gestion des technologies de l'information utilisées pour le télétravail

Service des technologies de l'information

Le 19 janvier 2022

RAPPORT ANNUEL 2021
Bureau du vérificateur général de la Ville de Montréal

3.1. Gestion des technologies de l'information utilisées pour le télétravail

Gestion des technologies de l'information utilisées pour le télétravail

Mise en contexte

Le télétravail est un mode d'organisation du travail qui a progressé au cours des dernières décennies. La technologie a permis aux employés d'effectuer une partie de leur travail régulier à domicile tout en étant reliés au bureau. C'est ce qu'on appelle souvent « télétravail » ou « travail à distance ».

Le 13 mars 2020, les directives gouvernementales pour contrôler les risques de contamination ont imposé le télétravail comme configuration de l'emploi qui s'est substituée à toute autre forme.

Bien que cette pratique existe déjà au sein de la Ville de Montréal (la Ville), elle a dû basculer vers le télétravail dans une plus large mesure. Jusqu'à 4 500 employés en simultané travaillent de la maison en mode télétravail accédant ainsi au réseau de la Ville à distance.

Objectif de l'audit

Déterminer si les mécanismes de contrôle, mis en place pour la gestion des technologies de l'information utilisées pour le télétravail au sein de la Ville, permettent de fournir l'équipement nécessaire et les accès à distance sécurisés aux actifs informatiques de la Ville afin que les employés maintiennent leur prestation de travail.

Résultats

Nous concluons que la Ville a mis en place les mécanismes de contrôle assurant une saine gestion des technologies de l'information utilisées pour le télétravail.

En effet, malgré l'urgence sanitaire due à la crise COVID-19, le Service des technologies de l'information (STI) de la Ville a déployé rapidement dans un contexte exceptionnel tous les efforts nécessaires pour mettre en place l'environnement technologique ainsi que les mécanismes de sécurité requis pour permettre à tous ses télétravailleurs de poursuivre leurs activités professionnelles de la maison sans interruption de services.

Ces mécanismes touchent l'encadrement du STI sur les technologies de l'information (TI) utilisées pour le télétravail, la stratégie de sensibilisation et de formation sur le télétravail, les mécanismes de protection entourant les accès aux données de la Ville ainsi que la gestion des opérations entourant les équipements corporatifs des télétravailleurs.

Principaux constats

Encadrement du télétravail

- Plusieurs encadrements sur les saines pratiques à adopter par les employés en mode télétravail ont été développés au sein de l'organisation. Ils ont été approuvés et diffusés à l'ensemble des employés à travers l'intranet de la Ville.
- Ces encadrements fournissent l'information requise aux employés afin que ces derniers puissent utiliser les TI pour le télétravail de façon sécuritaire.

Formation sur le télétravail

- Une sensibilisation et une formation appropriées sur le télétravail et ses composantes ont été mises en place depuis mars 2020.

Protection des accès aux données

- Des mécanismes d'authentification adéquats sont utilisés par les employés pour accéder aux données localisées dans le réseau de la Ville conformément aux saines pratiques de sécurité. Le verrouillage de l'écran des ordinateurs portables corporatifs est automatiquement activé après une période d'inactivité définie centralement.
- Un logiciel adéquat est installé et maintenu à jour sur tous les appareils corporatifs connectés à distance au réseau de la Ville pour les protéger contre les attaques malveillantes.

Gestion des opérations

- Afin de permettre aux employés d'être en télétravail, le STI a mis en place des mécanismes sécuritaires pour que les employés ne disposant pas d'un ordinateur corporatif puissent utiliser leur ordinateur personnel. Depuis le début de l'année 2021, près de 2 200 ordinateurs portables ont été distribués aux employés leur permettant ainsi de travailler à distance. Le STI a fourni un support informatique adéquat aux télétravailleurs.

  Les infrastructures en place permettent une redondance appropriée des composantes clés et comportent un environnement sécuritaire pour le télétravail.

Lexique

Authentification à deux facteurs ou forte : combine quelque chose que l'on sait (mot de passe, code confidentiel) avec une autre chose qui peut être un élément biométrique, un objet que l'on possède ou une action que l'on sait faire.

Espiogiciel : désigne un logiciel espion qui collecte des données personnelles afin de les envoyer à un tiers.

Maliciel : ou logiciel malveillant, désigne un logiciel destiné à nuire à l'utilisateur qui peut prendre la forme par exemple un virus informatique.

Pare-feu : dispositif qui protège la totalité du trafic réseau et a la capacité d'identifier et de bloquer le trafic de données indésirables.

Remote Desktop Protocol (RDP) : protocole de bureau à distance

Réseau privé virtuel (VPN) : méthode qui permet de relier deux ordinateurs distants par une seule et même connexion privée, ou tunnel, tout en utilisant une infrastructure réseau de plus grande taille, comme le web ou un réseau étendu. Une fois activé, un VPN fait office de connexion directe à un réseau privé.

STI : Service des technologies de l'information

Système centralisé de gestion des événements et des informations de sécurité (SIEM) : sert à effectuer la collecte, le suivi, la corrélation des logs ainsi que la génération de tableaux de bord et de rapports.

Système de détection d'intrusion (IDS) : protège les entreprises contre les cyberattaques en surveillant le trafic réseau pour détecter les activités suspectes.

Système de prévention d'intrusion (IPS) : permet de prendre des mesures afin de diminuer les impacts d'une attaque.

TI : technologies de l'information

Table des matières

1. Contexte **41**
1.1. Définition du terme télétravail 41
1.2. Description des technologies de l'information utilisées pour le télétravail 42
1.3. Principaux avantages du télétravail 42
1.4. Principaux enjeux du télétravail 42

2. Objectif de l'audit et portée des travaux **43**

3. Résultats de l'audit **44**
3.1. Encadrement sur le télétravail 44
3.2. Formation sur le télétravail 46
3.3. Protection des accès aux données 47
3.3.1. Mécanismes d'authentification 47
3.3.1.1. Réseau privé virtuel – utilisé sur les postes de la Ville de Montréal 47
3.3.1.2. Bureau à distance – utilisé sur les ordinateurs personnels 48

3.3.2. Verrouillage de l'écran 48
3.3.3. Logiciel anti-maliciel 48

3.4. Gestion des opérations 49
3.4.1. Approvisionnement de portables 49
3.4.2. Support informatique 50
3.4.3. Surveillance du lien Réseau privé virtuel 50
3.4.4. Redondance d'équipements 51

4. Conclusion 52

5. Annexe 54
5.1. Objectif et critères d'évaluation 54

3.1. Gestion des technologies de l'information utilisées pour le télétravail

1. Contexte

Le télétravail est un mode d'organisation du travail qui a progressé au cours des dernières décennies. Grâce aux nouvelles technologies, le télétravail est possible, voire indispensable au maintien des activités des entreprises.

Le 13 mars 2020, les directives gouvernementales pour contrôler les risques de contamination ont imposé le télétravail comme une configuration de l'emploi qui s'est substituée à toute autre forme. À la fin du mois de mars, 39,1 % des travailleurs canadiens étaient en mode télétravail. Bien que cette pratique existe déjà au sein de la Ville de Montréal (la Ville), elle a dû également basculer vers le télétravail dans une plus large mesure. Jusqu'à 4 500 employés en simultané travaillent de la maison en mode télétravail accédant ainsi au réseau de la Ville à distance. Ces ressources proviennent des différentes unités d'affaires.

L'essor généralisé du télétravail multiplie les échanges et les portes d'accès aux données sensibles des entreprises. Également, les réseaux personnels peuvent être moins bien protégés face aux cyberattaques que les réseaux privés d'entreprise.

Il est donc indispensable de limiter au maximum les risques en mettant en place les bons outils et en instaurant des pratiques sécurisées afin d'assurer une saine gestion des technologies de l'information utilisées pour le télétravail.

1.1. Définition du terme télétravail

Il est de plus en plus fréquent pour les gens d'effectuer au moins une partie de leur travail régulier à domicile plutôt qu'au bureau. La technologie a permis aux travailleurs de rester à la maison tout en étant reliés au bureau par téléphone, Internet ou courrier électronique. C'est ce qu'on appelle souvent « télétravail » ou « travail à distance ».

Il n'existe pas de définition officielle au Québec. Les études sur ce sujet le définissent à partir de deux principales dimensions[1] :

- Un lieu de travail à distance hors du lieu conventionnel de travail;
- Un travail à distance accompli à l'aide de technologies de l'information (TI) et des communications (TIC)[2].

C'est pourquoi les organisations doivent définir le télétravail par l'élaboration d'une politique ou directive interne.

1 Le télétravail – Chaire BMO – Université de Montréal.

2 Les téléphones intelligents, les tablettes, les ordinateurs portables et de bureau.

1.2. Description des technologies de l'information utilisées pour le télétravail

Les TI utilisées pour le télétravail sont, entre autres, les ordinateurs distants de la Ville configurés avec des solutions d'accès à distance. De plus, des équipements de télécommunications sont en place pour assurer une saine gestion des transferts de données entre les ordinateurs distants et le réseau informatique de la Ville.

La Ville utilise la technologie de Bureau à distance (RDP) (c.-à-d. le protocole « *Remote Desktop Protocol* ») pour les ordinateurs personnels ainsi que la technologie du Réseau privé virtuel (VPN) pour les ordinateurs de la Ville comme méthode d'authentification pour accéder aux données et applications de l'organisation.

1.3. Principaux avantages du télétravail

Les principaux avantages du télétravail pour toute organisation autres que l'économie au pied carré et les gains de productivité se listent comme suit :

- Accélération du maintien ou de la reprise des opérations en cas de sinistre (panne d'électricité ou tempête de verglas);
- Préparation aux risques de pandémie (réduire les risques de contagion, gérer le niveau de stress collectif);
- Offre d'accommodement aux personnes handicapées ou à mobilité réduite (sur une base temporaire ou permanente);
- Augmentation de ses atouts de recrutement et de fidélisation du personnel.

1.4. Principaux enjeux du télétravail

Les principaux enjeux associés au télétravail auxquels s'expose une organisation sont les suivants :

- Une croissance de fraudes en ligne (p. ex. l'exploitation de connexions réseau non sécurisées pour surveiller le trafic ainsi que l'envoi de faux rappels de réinitialisation de mots de passe);
- Des vols de données;
- Une surcharge de connexion;
- Une mauvaise gestion des accès logiques, dont la sécurité non renforcée des mots de passe;
- Une utilisation inappropriée de l'équipement par une personne tierce dans le domicile privé;
- Des outils, logiciels et applications non homologués;

- Un déploiement non progressif ou inexistant des mises à jour;
- Des équipes de services d'assistance informatique surchargés et des employés bénéficiant d'un soutien moindre de ces équipes.

2. Objectif de l'audit et portée des travaux

En vertu des dispositions de la *Loi sur les cités et villes*, nous avons réalisé une mission d'audit de performance portant sur la Gestion des technologies de l'information utilisées pour le télétravail. Nous avons réalisé cette mission conformément à la *Norme canadienne de missions de certification* (NCMC) 3001 du *Manuel de CPA Canada – Certification*.

Cet audit avait pour objectif de déterminer si les mécanismes de contrôle, mis en place pour la Gestion des technologies de l'information utilisées pour le télétravail au sein de la Ville, permettent de fournir l'équipement nécessaire et les accès à distance sécurisés aux actifs informatiques de la Ville afin que les employés maintiennent leur prestation de travail.

La responsabilité du vérificateur général de la Ville consiste à fournir une conclusion sur l'objectif de l'audit. Pour ce faire, 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 l'Annexe 5.1.

Le vérificateur général de la Ville applique la *Norme canadienne de contrôle qualité* (NCCQ 1) du *Manuel de CPA Canada – 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. De plus, il se conforme aux règles sur l'indépendance et aux autres règles de déontologie du *Code de déontologie des comptables professionnels agréés*, lesquelles reposent sur les principes fondamentaux d'intégrité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

L'objet de notre audit a porté uniquement sur la gestion des technologies de l'information utilisées pour le télétravail permettant de fournir l'équipement nécessaire et les accès à distance sécurisés aux actifs informatiques de la Ville afin que les employés maintiennent leur prestation de travail.

Afin de réaliser nos travaux d'audit, nous avons audité le STI responsable de la gestion des technologies de l'information utilisées pour le télétravail.

Nous avons exclu de notre portée le Service de Police de la Ville de Montréal (SPVM), car ses critères de gestion des technologies de l'information diffèrent grandement à ceux de la Ville. En effet, le SPVM doit respecter des règles de sécurité propres à son service afin de protéger les accès au Centre de renseignements policiers du Québec. C'est une banque de données que les policiers utilisent quotidiennement.

Nos travaux d'audit ont porté sur la période s'échelonnant de février 2021 à octobre 2021. Ils ont consisté à effectuer des entrevues auprès du personnel, à examiner divers documents et à réaliser les sondages que nous avons jugés appropriés en vue d'obtenir l'information probante nécessaire. Nous avons toutefois tenu compte d'informations qui nous ont été transmises jusqu'au 19 janvier 2022.

À la fin de nos travaux, un projet de rapport d'audit a été présenté, aux fins de discussions, aux gestionnaires concernés au sein de l'unité d'affaires auditée. Par la suite, le rapport final a été transmis à la direction de l'unité d'affaires concernée ainsi qu'à la Direction générale de la Ville.

3. Résultats de l'audit

3.1. Encadrement sur le télétravail

Un encadrement sur les technologies utilisées pour le télétravail consiste à développer un cadre normatif portant, notamment, sur l'utilisation d'équipements informatiques dédiés, d'un VPN, d'un pare-feu filtrant les données ainsi que sur la limitation d'ajouts d'application, la protection des réseaux et des appareils configurés de manière sécuritaire selon la *Politique de sécurité de l'information*.

De plus, cet encadrement doit être approuvé par les instances appropriées, à jour et diffusé à l'ensemble des employés de la Ville en télétravail afin de prévenir des pratiques non sécuritaires de leur part pouvant se solder en des failles de sécurité importante.

Plusieurs encadrements touchant de près ou de loin les saines pratiques à adopter par les employés en mode télétravail existent à la Ville. Ces encadrements se listent comme suit :

- La directive « *Utilisation des appareils et des technologies mis à la disposition des employés de la Ville de Montréal* » du STI, datée du 15 juin 2018, encadre l'usage des appareils informatiques et des services technologiques, afin de prévenir toute utilisation illégale, fautive, abusive ou déraisonnable par certains utilisateurs. Elle vient préciser les règles relatives à l'utilisation des services Internet, du service de courrier électronique de la Ville, des services de téléphonie cellulaire et des services d'accès à distance;

- Le formulaire de consentement cité dans la section 9.5 – Utilisation d'appareils qui n'appartiennent pas à la Ville de la directive ci-dessus stipule que « *Les utilisateurs concernés doivent préalablement signer un formulaire de consentement à l'utilisation d'un appareil personnel dans le cadre professionnel, et se soumettre aux exigences de sécurité énoncées dans ce formulaire.* ». Ce formulaire, mis à jour dans le contexte de la pandémie, comporte les liens utiles à la directive de télétravail et les capsules de cybersécurité;
- La directive « *Directive sur le télétravail des employés de la Ville de Montréal* » du Service des ressources humaines est entrée en vigueur le 13 mars 2020 en mode urgence. Cette dernière vise à encadrer la pratique du télétravail. Elle précise la nature des privilèges consentis, les conditions d'admissibilité, les rôles et responsabilités, ainsi que les règles et mesures à observer. Elle fait également référence à des encadrements complémentaires, dont la directive ci-dessus;
- Le « *Guide de sécurité de l'information pour l'employé en télétravail* » a été développé en mars 2021 par la Direction Sécurité de l'information du STI. Ce guide se trouve dans la Zone TI, Cybersécurité. Il détaille, par exemple, les bons réflexes à adopter, la configuration sécuritaire du poste de travail (incluant les portables) et la configuration sécuritaire des réseaux de connexion (c.-à-d. domestiques filaires et le sans-fil);
- L'« *Encadrement administratif sur le modèle hybride d'organisation du travail* » du Service des ressources humaines daté du 28 juin 2021 fait des référencements aux encadrements cités ci-dessus. Il mentionne, entre autres, dans la section sur les règles d'utilisation de l'équipement informatique, la directive d'utilisation du matériel technologique de la Ville et, dans la section sur la sécurité et la protection des données, le guide de sécurité de l'information pour l'employé en télétravail.

Ces encadrements ont été approuvés et diffusés à l'ensemble des employés à travers l'intranet de la Ville.

Nous considérons que les encadrements existant avant la pandémie et ceux développés subséquemment ont permis de fournir l'information requise aux employés afin que ces derniers puissent utiliser les TI pour le télétravail de façon sécuritaire.

Aucune recommandation n'est nécessaire.

3.2. Formation sur le télétravail

La formation sur le télétravail se compose normalement de formations sur la détection des courriels frauduleux et des tentatives d'hameçonnage, l'utilisation d'un mot de passe robuste et d'un réseau sans fil sécurisé, la surveillance des appareils et la communication en cas d'enjeux de sécurité. Ces formations peuvent être réalisées à travers différents médias comme des conférences, des capsules de formation ou à travers des sites Internet reconnus.

Pour accroître la vigilance et maintenir les réflexes des employés sur ces sujets clés, la répétition de messages est primordiale.

Nous avons constaté qu'à travers des hyperliens sur l'intranet de la Ville, les télétravailleurs pouvaient s'informer sur les différentes solutions d'accès à distance mises en place par la Ville, sur les actualités et les informations importantes mises à jour liées au télétravail et sur la sensibilisation aux courriels frauduleux avec un lien qui redirige l'usager à une vidéo YouTube de la Ville diffusée en février 2019. Celle-ci s'intitule « *Cybersécurité : l'accès à distance en toute sécurité* »[3] et explique « *Comment sécuriser vos informations et vos outils avec le téléaccès de la Ville pour ceux qui travaillent à distance* ». De plus, le formulaire de « *Consentement pour l'autorisation d'utilisation d'un ordinateur personnel en télétravail* » à compléter par l'employé le redirige à des liens utiles, dont celui sur les capsules de cybersécurité accessibles dans le portail de formation de la Ville.

Nous avons aussi constaté que dans le cadre du mois d'octobre 2021[4], deux conférences ont eu lieu : la cybersécurité en télétravail et les tendances de la cybersécurité. D'autres conférences devraient être réalisées par le STI tout au long de la campagne de sensibilisation selon les besoins identifiés auprès de leurs publics cibles.

De plus, les capsules de sécurité de la Direction Sécurité de l'information du STI font l'objet d'un suivi afin de s'assurer que tous les employés connectés les visionnent et les complètent à l'intérieur d'un délai raisonnable. En cas de nécessité, un gestionnaire est avisé par le STI que son employé devrait reprendre une formation promptement.

Nous avons été informés que dans le cadre du projet – Sensibilisation et formation des employés, les capsules de formation sur différents thèmes de la cybersécurité sont en cours de révision. D'ailleurs, selon ce projet, la sortie progressive de ces capsules devrait se réaliser tout au long de la campagne de sensibilisation en cours jusqu'à l'automne 2022. Tous les employés « connectés », environ 12 000, seront obligatoirement tenus de compléter les capsules.

---

3 https://www.youtube.com/l'accès à distance en toute sécurité

4 Le mois d'octobre marque le *Mois de la sensibilisation à la cybersécurité*, une campagne d'envergure internationale visant à informer le public de l'importance de la cybersécurité.

Nous estimons qu'une sensibilisation et une formation appropriées sur le télétravail et ses composantes ont été mises en place depuis mars 2020.

Aucune recommandation n'est nécessaire.

3.3. Protection des accès aux données

La protection des accès à distance passe par plusieurs approches techniques, dont l'utilisation d'une authentification à deux facteurs ou forte[5], soit par l'entremise d'un VPN[6] sécurisé ainsi que d'un pare-feu[7] filtrant les données entrantes et sortantes. Sur les ordinateurs de la Ville offrant cet accès à distance, un verrouillage de l'écran devrait être activé automatiquement après une période d'inactivité, en plus de comporter un logiciel anti-maliciel[8] à jour.

3.3.1. Mécanismes d'authentification

Des mécanismes d'authentifications fortes sont en place pour accéder aux données de la Ville à partir des ordinateurs distants. En effet, durant nos travaux, nous avons constaté l'utilisation de deux types de mécanismes d'authentification, soit le VPN utilisé sur les postes de la Ville et le RDP utilisé sur les ordinateurs personnels. Un employé en télétravail pourrait se connecter via le VPN ou le RDP.

3.3.1.1. Réseau privé virtuel – utilisé sur les postes de la Ville de Montréal

L'accès à distance VPN clients a été implanté lors du déploiement du mode de travail à distance à grande échelle avec une authentification robuste à deux facteurs. Nous avons pris en considération, notamment, la configuration des composantes clés de l'environnement VPN, des deux facteurs utilisés lors de l'authentification de la durée de session et la documentation usager mise à la disposition des télétravailleurs.

Nous estimons que les éléments précités sont en adéquation avec ce qui est normalement attendu.

Aucune recommandation n'est nécessaire.

5 La méthode d'authentification à deux facteurs, ou forte, combine quelque chose que l'on sait (mot de passe, code confidentiel) avec une autre chose qui peut être un élément biométrique, un objet que l'on possède ou une action que l'on sait faire.

6 VPN est une méthode qui permet de relier deux ordinateurs distants par une seule et même connexion privée, ou tunnel, tout en utilisant une infrastructure réseau de plus grande taille, comme le web ou un réseau étendu. Une fois activé, un VPN fait office de connexion directe à un réseau privé.

7 Un pare-feu est un dispositif qui protège la totalité du trafic réseau et a la capacité d'identifier et de bloquer le trafic de données indésirables.

8 Un maliciel ou logiciel malveillant désigne un logiciel destiné à nuire à l'utilisateur qui peut prendre la forme par exemple d'un cheval de Troie ou d'un virus informatique.

3.3.1.2. Bureau à distance – utilisé sur les ordinateurs personnels

Pour accélérer la mise en place du télétravail et suivant les délais de livraison des ordinateurs portables, l'authentification RDP a été permise sur les ordinateurs personnels aux employés autorisés de se connecter sur leurs postes de travail du bureau et accéder aux données de la Ville. Toutefois, la Ville pouvait révoquer en tout temps ce privilège.

Nous avons examiné la configuration de l'environnement RDP, le processus de changement de mot de passe, le processus de connexion, le processus d'authentification à multiples facteurs, la durée des sessions RDP, les fonctionnalités au niveau de la copie ou la sauvegarde des données, ainsi que la documentation usager et technique de cette solution.

Nous estimons que les éléments précités sont adéquats et permettent un environnement d'authentifications multiples sécuritaire.

Aucune recommandation n'est nécessaire.

3.3.2. Verrouillage de l'écran

Nous avons été informés que les ordinateurs portables de la Ville utilisés par les travailleurs sont configurés avec un verrouillage d'écran automatique après une période d'inactivité de la session Windows qui varie si l'actif informationnel est critique ou non.

Nous avons constaté que la session Windows sur ces ordinateurs portables se verrouille conformément au standard – Gestion des accès logiques en date du 2 novembre 2020. Nous estimons que cela est adéquat.

Aucune recommandation n'est nécessaire.

3.3.3. Logiciel anti-maliciel

Nous avons été informés que tous les postes de travail et les ordinateurs portables de la Ville sont équipés d'un logiciel de gestion des anti-maliciels. Cet outil est utilisé notamment pour le filtrage des courriels et des pages Web consultées par les employés.

Nous avons constaté que la configuration de l'environnement de cet anti-maliciel est conforme aux saines pratiques, avec notamment, la mise à jour toutes les heures des composantes du serveur hébergeant ce logiciel et des agents de sécurité (c.-à-d. les signatures virus, les espiogiciels[9], etc.), l'analyse intelligente des signatures anti-programmes malveillants et anti-espiogiciels, l'évaluation de la réputation des sites Web[10] automatique et l'apprentissage automatique

---

9 Le terme espiogiciel désigne un logiciel espion qui collecte des données personnelles afin de les envoyer à un tiers.

10 La fonction de réputation de sites Web évalue le risque que présente une URL demandée pour la sécurité.

prédictif[11]. De surcroît, la détection des connexions suspectes malveillantes et la surveillance des comportements des programmes malveillants sont activées sur le serveur.

Nous avons été informés également qu'un durcissement des agents de sécurité installés sur tous les postes de travail, dont les ordinateurs portables, est en cours de réalisation et qu'une augmentation du niveau de sécurité de sa composante de pare-feu est planifiée selon les bonnes pratiques, les recommandations du fournisseur ainsi que les besoins d'affaires et opérationnels de la Ville. Cela s'imbrique dans une des initiatives du projet – Acquisition d'infrastructures technologiques de sécurité en cours de réalisation.

Nous considérons que cette solution avec ses différentes couches est adéquate.

Aucune recommandation n'est nécessaire.

3.4. Gestion des opérations

Une saine gestion des opérations vise l'approvisionnement d'équipements corporatifs avec des outils de communications pour les télétravailleurs. Cela englobe le support informatique mis à la disposition de ces derniers afin de répondre aux incidents de sécurité liés à l'accès à distance ainsi que la surveillance du lien où transigent les données entre l'ordinateur utilisé par l'employé et le réseau de la Ville.

La redondance des différents types de serveurs d'authentification avec une réplication des données est primordiale afin de maintenir le service disponible et un équilibre de la charge des demandes d'accès à distance. Une segmentation réseautique[12] entre les postes de travail au bureau et les ordinateurs distants devrait être préconisée afin d'éviter des communications douteuses de s'infiltrer dans le réseau informatique de la Ville.

3.4.1. Approvisionnement de portables

Dans le contexte actuel de la pandémie, le STI a déployé progressivement des mesures permettant d'élargir le télétravail. A priori, le STI n'avait pas assez d'ordinateurs portables de disponibles pour tous les télétravailleurs. Ainsi, il a été permis aux employés sans ordinateurs portables de la Ville, requérant d'accéder au réseau informatique, d'utiliser leurs ordinateurs personnels pour effectuer leur prestation de travail. Cette utilisation d'ordinateurs personnels suit un processus rigoureux de demande d'autorisation auprès du gestionnaire de l'employé. La Ville pouvait révoquer en tout temps le privilège d'utiliser un appareil personnel pour accéder à son environnement technologique.

11 Cet apprentissage est une technologie avancée qui permet de détecter les nouveaux risques de sécurité inconnus dans des processus ou des fichiers suspects à faible prévalence.

12 Une segmentation réseautique consiste à diviser un réseau en plusieurs sous-réseaux.

Nous avons constaté que depuis le début de l'année 2021, une distribution d'ordinateurs portables corporatifs est en cours dont près de 2 200 ordinateurs portables ont déjà été distribués aux employés en télétravail.

Aucune recommandation n'est nécessaire.

3.4.2. Support informatique

Les équipes du STI ont prêté main-forte au Centre de services TI pour accélérer la mise en place du télétravail en mars 2020. Les employés étaient invités à fournir du support téléphonique pour aider les télétravailleurs à se connecter à distance au réseau informatique de la Ville. Cette situation a perduré durant les premières semaines de la situation d'urgence. Après une stabilisation, le Centre de services TI a repris la gestion des appels.

Le Centre de services TI compte 20 agents dédiés au support pour la Ville dont 5 agents ont été engagés depuis mars 2020 pour répondre aux besoins. Pour les demandes de soutien concernant les outils technologiques en contexte de télétravail, l'usager peut ouvrir un incident sur le libre-service informatique ou les appeler.

Nous avons constaté que le processus de soutien aux télétravailleurs comporte l'envoi de courriels comportant des documents usagers en ligne sur les méthodes de connexions VPN et RDP avec des liens et vidéos afin de les guider dans l'utilisation de celles-ci. De plus, les appels sont redirigés vers les techniciens TI spécialisés dans ces domaines afin de résoudre les situations complexes.

Nous avons analysé la liste des incidents du 20 mars 2020 au 14 septembre 2021. Il en ressort qu'elle ne contient aucun incident lié aux accès à distance.

Nous estimons que le Centre de services TI a la capacité en ressources et les outils pour fournir un support informatique aux télétravailleurs liés à l'accès à distance.

Aucune recommandation n'est nécessaire.

3.4.3. Surveillance du lien Réseau privé virtuel

Nous avons constaté qu'un accès administrateur à la console de la passerelle VPN demeure ouvert durant les heures de bureau. Cette console surveille en permanence la performance des disques durs et des ressources utilisées de cette passerelle. Ainsi, l'administrateur procède à des vérifications ponctuelles.

Le système centralisé de gestion des événements et des informations de sécurité (SIEM)[13] a été implanté et une formation a été donnée à l'administrateur des réseaux de télécommunications. De plus, la surveillance à travers le SIEM est en cours de configuration au niveau des alertes automatisées et de l'analyse des données de sécurité avec l'intégration des journaux de sécurité.

---

13 Un SIEM sert à effectuer la collecte, le suivi, la corrélation des logs ainsi que la génération de tableaux de bord et de rapports.

Actuellement, les alertes sont journalisées et envoyées vers l'application de gestion des journaux (Graylog) et aucune alerte n'est envoyée aux administrateurs. Le SIEM viendra adresser ce point.

Nous considérons que l'implantation et la configuration du SIEM en cours permettront la réalisation d'une surveillance en continu à travers la collecte, le stockage et l'analyse en temps réel des événements du lien où transigent les données entre l'ordinateur utilisé par l'employé et le réseau de la Ville (c.-à-d. le lien VPN pour l'accès à distance).

Nous avons déjà émis une recommandation à cet égard lors d'un précédent audit. Aucune nouvelle recommandation n'est nécessaire.

3.4.4. Redondance d'équipements

Nous avons obtenu de la documentation sur les solutions de télétravail. Un document détaille à haut niveau les solutions d'accès à distance – RDP et VPN – avec des schémas d'infrastructures. Un autre document présente un schéma plus détaillé de l'environnement RDP. Nous avons constaté à partir de la documentation et des ressources rencontrées qu'une redondance est bel et bien en place au niveau des équipements.

Nous considérons que les différents types de serveurs d'authentification avec une réplication des données entre eux sont en place et que toutes les composantes clés font l'objet d'une redondance adéquate.

Aucune recommandation n'est nécessaire.

4. Conclusion

Nous concluons que la Ville de Montréal (la Ville) a mis en place les mécanismes de contrôle assurant une saine gestion des technologies de l'information utilisées pour le télétravail.

En effet, malgré l'urgence sanitaire due à la crise COVID-19, le Service des technologies de l'information (STI) de la Ville a déployé tous les efforts nécessaires pour mettre en place, dans un court délai, l'environnement technologique ainsi que les mécanismes de sécurité requis pour permettre à tous ses télétravailleurs de poursuivre leurs activités professionnelles de leur domicile sans interruption de services.

Ces mécanismes touchent l'encadrement du STI sur les technologies de l'information (TI) utilisées pour le télétravail, la stratégie de sensibilisation et de formation sur le télétravail, les mécanismes de protection entourant les accès aux données de la Ville ainsi que la gestion des opérations entourant les équipements corporatifs des télétravailleurs.

Plus précisément, voici les détails selon les critères d'évaluation suivants :

Critère d'évaluation – Encadrement du télétravail

Plusieurs encadrements sur les saines pratiques à adopter par les employés en mode télétravail ont été développés au sein de l'organisation. Ils ont été approuvés et diffusés à l'ensemble des employés à travers l'intranet de la Ville.

Ces encadrements fournissent l'information requise aux employés afin que ces derniers puissent utiliser les TI pour le télétravail de façon sécuritaire.

Critère d'évaluation – Formation sur le télétravail

Une sensibilisation et une formation appropriées sur le télétravail et ses composantes ont été mises en place depuis mars 2020 et devraient se poursuivre jusqu'à l'automne 2022.

Un suivi est réalisé par le STI sur les capsules de formation Cybersécurité afin de s'assurer que l'ensemble des employés « connectés » au réseau de la Ville réussissent ces capsules dans un délai raisonnable.

Critère d'évaluation – Protection des accès aux données

Des mécanismes d'authentification forte sont utilisés par les employés pour accéder aux données localisées dans le réseau de la Ville conformément aux saines pratiques de sécurité. Le verrouillage de l'écran des ordinateurs portables corporatifs est automatiquement activé après une période d'inactivité définie centralement.

Un logiciel anti-maliciel adéquat est installé et maintenu à jour sur tous les appareils corporatifs connectés à distance au réseau informatique de la Ville. Ce logiciel effectue notamment un filtrage des courriels et des pages Web consultées par les employés, ainsi qu'un balayage de fichiers selon la configuration des paramètres d'analyse.

Critère d'évaluation – Gestion des opérations

Afin de permettre aux employés d'être en télétravail, le STI a mis en place des mécanismes sécuritaires pour que les employés ne disposant pas d'un ordinateur corporatif puissent utiliser leur ordinateur personnel. Depuis le début de l'année 2021, près de 2 200 ordinateurs portables ont été distribués aux employés leur permettant ainsi de travailler à distance.

Le Centre de services TI a la capacité requise en ressources et les outils pour fournir un bon support informatique aux télétravailleurs.

Une redondance appropriée des composantes clés des environnements des solutions d'authentification Réseau privé virtuel et Bureau à distance est en place.

5. Annexe

5.1. Objectif et critères d'évaluation

Objectif

Déterminer si les mécanismes de contrôle, mis en place pour la gestion des technologies de l'information utilisées pour le télétravail au sein de la Ville de Montréal (la Ville), permettent de fournir l'équipement nécessaire et les accès à distance sécurisés aux actifs informatiques de la Ville afin que les employés maintiennent leur prestation de travail.

Critères d'évaluation

Nos travaux ont porté sur les critères d'évaluation suivants :

Critère 1 : Gouvernance
Un cadre normatif sur les technologies de l'information utilisées pour le télétravail a été développé par le Service des technologies de l'information (STI), approuvé et diffusé aux employés de la Ville.

Critère 2 : Formation sur le télétravail
Une formation en continu est donnée aux employés pour les sensibiliser aux enjeux de sécurité liés au télétravail, rappeler les saines pratiques et celle-ci fait l'objet d'un suivi par le STI.

Critère 3 : Protection des accès aux données
Des mécanismes d'authentification robustes sont en place pour accéder aux données. Les ordinateurs distants disposent de mécanismes de sécurité appropriés (p. ex. un logiciel anti-maliciel).

Critère 4 : Gestion des opérations
Le STI fournit des ordinateurs portables avec des outils de communication à distance en temps opportun aux télétravailleurs. Le STI assure par une surveillance des opérations de télétravail pour que celles-ci restent disponibles pour les employés (p. ex. le support informatique).