Vérificateur général
MANITOBA

Rapport à l'Assemblée législative du Manitoba

Gestion de la sécurité des TI en lien avec l'accès à distance

Rapport d'assurance indépendant

VERSION DU SITE WEB

Mars 2024

Cette page a été laissée
blanche intentionnellement.

La traduction de ce rapport a été fournie par le Service de traduction du Manitoba. En cas d'incohérence, se reporter à la version anglaise.

Cette page a été laissée
blanche intentionnellement.

Table des matières

Cette page a été laissée
blanche intentionnellement.

Observations du vérificateur général

La pandémie de COVID-19 a transformé la structure des milieux de travail traditionnels. Les employés d'une panoplie de secteurs ont appris à travailler à distance ou à diviser leur temps entre la maison et le bureau. Et ils peuvent le faire grâce aux avancées technologiques, qui ont fait naître de nouvelles manières d'échanger de l'information et de collaborer à distance.

En 2021, en réponse à ce virage, la Province du Manitoba a adopté une politique en matière d'entente de travail flexible pour les employés de la fonction publique centrale. Cette politique est venue officialiser les attentes envers les employés en télétravail à temps plein et ceux qui suivent un modèle de travail hybride. Elle a également tenu compte du besoin d'établir des contrôles de sécurité informatique rigoureux dans l'environnement de travail à distance, où les menaces sont plus nombreuses. En effet, l'information devrait toujours être protégée, que ce soit au bureau ou à la maison.

Je me réjouis de constater que le Manitoba a introduit des mesures de sécurité afin de protéger l'information et les systèmes qu'utilisent les employés à distance, mais des améliorations s'avèrent nécessaires. À l'issue de cet audit, nous avons constaté que la Province protège les données en mouvement à l'aide du chiffrement, mais que certains paramètres pourraient être renforcés. L'audit a également révélé que certains employés n'ont pas suivi la formation obligatoire de sensibilisation à la sécurité. La Province doit se pencher sur ces constatations pour que l'environnement de télétravail soit plus sécuritaire.

Le présent rapport formule trois recommandations. Une lettre distincte a aussi été fournie à la direction pour lui présenter les constatations contenant des renseignements de nature délicate. J'encourage le ministère de la Protection du consommateur et des Services gouvernementaux et la Commission de la fonction publique à donner suite aux recommandations contenues dans le présent rapport et dans la lettre afin d'éliminer les risques cernés dans cet audit.

Je tiens à remercier le personnel et les représentants du gouvernement provincial que nous avons rencontrés pendant l'audit pour leur coopération et leur aide. Je souhaite également saluer mon équipe d'audit pour son travail.

Original signé par :

Tyson Shtykalo, CPA, CA
Vérificateur général

Cette page a été laissée
blanche intentionnellement.

Points saillants

Motifs de l'audit

- En juin 2021, la Province du Manitoba (la Province) a introduit une politique en matière d'entente de travail flexible qui a mené à l'adoption d'un modèle de travail hybride, grâce auquel les employés de la fonction publique centrale peuvent travailler à distance certaines journées.
- Les systèmes d'information et les données doivent être bien protégés lors du télétravail.
- Notre objectif consistait à déterminer si la Province disposait de procédures et de contrôles pour atténuer les risques à la sécurité informatique dans l'environnement de télétravail.

Conclusion

La Province gère les risques à la sécurité informatique liés au télétravail, mais des améliorations s'imposent.

Notre rapport comprend **3 RECOMMANDATIONS**.

Nos constatations

Sécurité des données

Les données sont protégées, mais les paramètres de chiffrement doivent être améliorés

- Les données sont chiffrées dans l'environnement de télétravail, mais des paramètres de chiffrement doivent être modifiés pour renforcer la sécurité.

Authentification et correctifs sur les dispositifs

Les dispositifs sont authentifiés et les correctifs sont appliqués automatiquement

- Les travailleurs à distance doivent utiliser des dispositifs délivrés par la Province. L'accès à ces dispositifs est contrôlé par une authentification multifacteur.
- Les mises à jour relatives à la sécurité sont effectuées automatiquement sur chaque ordinateur grâce à un processus de gestion des correctifs automatisé.

Gestion des vulnérabilités et des incidents

Les vulnérabilités et les incidents de sécurité sont relevés et atténués sans délai

- La Province s'est dotée d'une procédure d'intervention en cas d'incidents de sécurité et d'interruptions relativement aux technologies qu'utilisent les travailleurs à distance.
- Les technologies de télétravail sont vérifiées régulièrement pour cerner et résoudre toute vulnérabilité.

Formation de sensibilisation à la sécurité

De nombreux employés n'ont pas suivi la formation de sensibilisation à la sécurité de l'information

- Tous les employés du gouvernement manitobain doivent suivre la formation de sensibilisation à la sécurité de l'information (SSI) dans les deux mois suivant leur embauche.
- En date du 31 mars 2023, 30 % des employés n'avaient pas achevé la formation.

Politiques et procédures

Les politiques et les procédures de sécurité sont désuètes

- Les politiques et les procédures de sécurité informatique pour le télétravail n'ont pas été révisées depuis plusieurs années.

Contexte

Le télétravail est de plus en plus populaire et viable grâce aux avancées technologiques, à l'Internet haute vitesse et au changement de la nature de plusieurs emplois, qui peuvent maintenant se faire numériquement. Le 28 juin 2021, la Commission de la fonction publique (CFP) du Manitoba a fait des démarches pour multiplier les possibilités de télétravail en introduisant la politique en matière d'**entente de travail flexible**, qui autorise les employés de la **fonction publique centrale** à travailler hors du bureau, soit à la maison ou ailleurs.

En vertu de la politique de la CFP, le télétravail est une « entente de travail flexible selon laquelle l'employé est autorisé à exécuter la totalité ou une partie de ses tâches à un autre endroit », généralement sa résidence principale, « de façon récurrente ou continue ». Dans le cadre d'une entente de travail à distance, l'employé peut travailler à distance à temps plein ou partager son temps entre le bureau central et un autre endroit.

Une **entente de travail flexible** est une entente conclue entre la direction et un employé pour modifier les heures et le lieu de travail d'un employé de façon récurrente ou continue.

Source : Section 1.2.4 des politiques de la Commission de la fonction publique

La **fonction publique centrale** est composée du greffier du Conseil exécutif, des autres sous-ministres et des employés occupant un poste au sein d'un ministère du gouvernement.

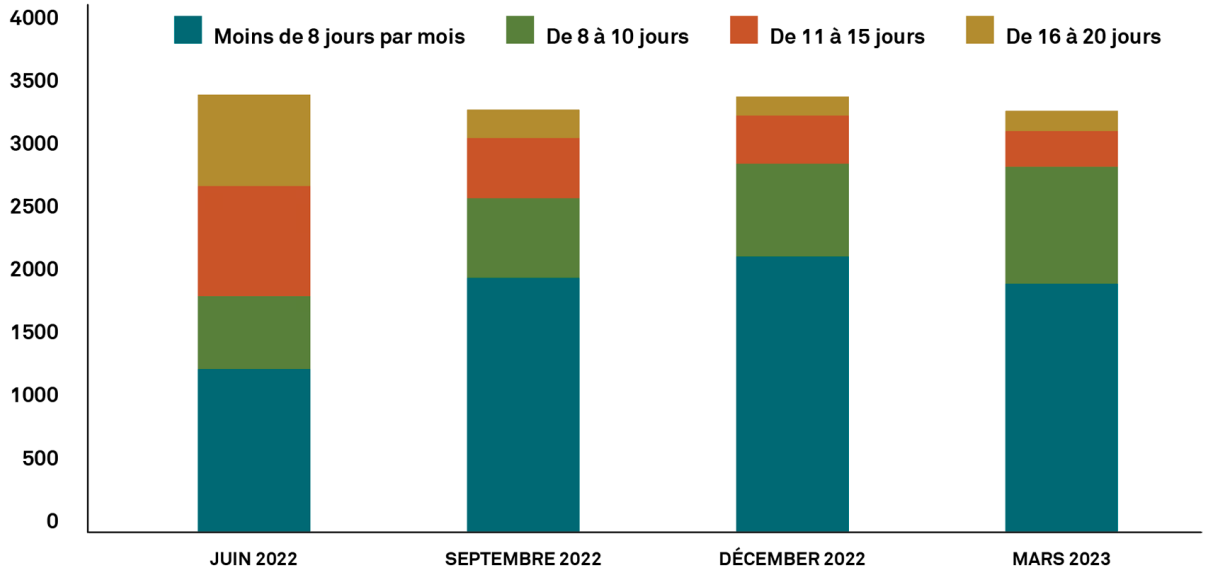
Source : Loi sur la fonction publique du Manitoba

Pendant la plus récente urgence de santé publique, l'entente de travail flexible a été utilisée comme outil pour assurer la continuité des fonctions gouvernementales essentielles. Quoique la pandémie de COVID-19 soit maintenant terminée, le télétravail est toujours bien présent dans les milieux professionnels. Selon une étude réalisée en mars 2021 par la Banque de développement du Canada, 54 % des employés interrogés ont affirmé que l'accès au télétravail est un facteur déterminant pour postuler ou accepter un nouvel emploi. De plus, dans un sondage plus récent effectué par l'Angus Reid Institue en avril 2023, la moitié des employés interrogés ont dit qu'ils changeraient d'emploi si leur employeur leur demandait de revenir au bureau à temps plein. De ce fait, en autorisant le travail à distance, les employeurs ont accès à un bassin de talents plus vaste et ont plus de chances de maintenir leur personnel en poste.

Avant la pandémie, le télétravail était limité dans le secteur public en raison de contraintes technologiques et de la réticence à briser les normes établies. D'ailleurs, au Manitoba, moins de 1 000 membres de la fonction publique centrale travaillaient à distance. Toutefois, avec l'arrivée de la pandémie et la mise en place des restrictions de santé publique et des confinements, la Province a dû s'adapter rapidement pour pouvoir continuer à servir les citoyens en autorisant la fonction publique centrale à travailler à distance. La pandémie a stimulé les investissements dans les technologies de travail à distance pour répondre aux besoins émergents.

Le nombre de journées de télétravail varie selon les semaines de travail, mais la quantité de travailleurs à distance a augmenté et a oscillé autour de 3 500 de juin 2022 à mars 2023. Consultez le **FIGURE 1** ci-dessous.

Figure 1 – Nombre d'employés de la fonction publique centrale travaillant à distance, de juin 2022 à mars 2023



Source : Commission de la fonction publique

D'une part, le télétravail a permis de protéger les employés pendant la pandémie de COVID-19. D'autre part, il a fait augmenter les menaces informatiques pouvant compromettre les systèmes et les données. Selon un bulletin publié en mars 2020 par l'Information Technology Laboratory du National Institute of Standards and Technology (NIST) des États-Unis, « les technologies de télétravail et d'accès à distance nécessitent bien souvent une protection supplémentaire, car, de par leur nature, elles sont plus exposées aux menaces externes que les technologies utilisées uniquement à l'intérieur d'un organisme » [traduction]. Voici les menaces ou les préoccupations en matière de sécurité qui ont été cernées relativement au télétravail pendant la période d'audit de juin 2021 à 2023 :

1. Les données stockées et transmises avec les dispositifs utilisés à distance ne sont pas protégées contre l'accès non autorisé.	L'accès non autorisé à de l'information sensible peut se traduire par une fuite de données et mener à l'exposition de données confidentielles, notamment les renseignements personnels et financiers des Manitobains et Manitobaines. Ce type de fuites peuvent engendrer des coûts énormes en matière de redressement et endommager la réputation de la Province.
2. Les correctifs nécessaires ne sont pas appliqués aux dispositifs avant que les employés obtiennent l'accès au réseau de la Province.	Les dispositifs des travailleurs à distance pourraient contenir des logiciels malveillants. Lorsque les dispositifs se connectent au réseau de la Province et qu'aucun mécanisme n'est en place pour détecter les menaces, mettre les fichiers douteux en quarantaine et nettoyer les dispositifs, les logiciels malveillants ont alors la possibilité de s'attaquer à d'autres biens informatiques (ordinateurs, réseaux, applications, etc.).

3. Les vulnérabilités et les incidents de sécurité en télétravail ne sont pas relevés ni atténués sur-le-champ.	S'ils sont ignorés, les vulnérabilités et les problèmes de sécurité peuvent dégénérer en incidents tentaculaires et destructeurs. Par exemple, un dispositif compromis d'un travailleur à distance peut à lui seul être utilisé pour lancer des attaques contre d'autres parties du réseau de la Province.
4. Les employés ne suivent pas régulièrement une formation de sensibilisation sur les risques du télétravail et les pratiques d'atténuation.	Sans formation adéquate sur les risques à la sécurité en télétravail, les employés ont plus de chances d'être victimes d'hameçonnage, de logiciels malveillants et d'autres cybermenaces. Ils sont également plus vulnérables à la manipulation visant à les forcer à révéler de l'information sensible ou à poser des gestes qui compromettent la sécurité. Tous ces risques peuvent être évités avec une formation adéquate et un programme de sensibilisation à la sécurité.

Compte tenu des menaces à la sécurité susmentionnées, il est essentiel que les environnements de télétravail (comme la maison) disposent de contrôles de sécurité informatique afin de protéger les systèmes d'information et les données au même degré qu'au bureau.

Dans le cadre de cet audit, nous nous sommes penchés sur les contrôles mis en place pour atténuer les risques à la sécurité informatique en télétravail. Nous avons ainsi examiné les procédures, politiques et pratiques de sécurité informatique; les mesures de protection des systèmes d'information et des données; ainsi que les directives et la formation sur la sécurité offertes aux employées.

Cette page a été laissée
blanche intentionnellement.

Division des solutions numériques et technologiques

Le General Manual of Administration établit la Division des solutions numériques et technologiques (anciennement la Division de la technologie et de la transformation opérationnelle) en tant qu'organisme central de la Province responsable de la gestion des technologies de l'information et de la communication (TIC). Pour ce qui est de la gestion de la sécurité informatique en télétravail, la Division est chargée :

- d'établir les politiques et procédures provinciales qui régissent les ententes de travail à distance;
- de déployer des dispositifs et des technologies qui facilitent le télétravail des employés de la fonction publique;
- de mettre en œuvre des contrôles afin de prévenir et de détecter les incidents de sécurité touchant les dispositifs et les technologies de télétravail;
- d'aider la CFP à mettre sur pied un programme de sensibilisation à la sécurité pour les employés de la fonction publique.

La Division dirige également le travail visant à protéger les données, les systèmes et les réseaux électroniques du gouvernement manitobain, tout en harmonisant les politiques et les pratiques de sécurité informatique aux priorités et à la tolérance au risque de la Province.

Commission de la fonction publique

La CFP est un organisme indépendant et impartial chargé de la gestion efficace des ressources humaines et des relations de travail au sein du gouvernement. Elle représente l'intérêt public dans la mise en œuvre de *la Loi sur la fonction publique* et de ses règlements d'application.

La Loi exige que la Province élabore et mette en œuvre des politiques sur les ententes de travail flexible. En réponse, la CFP a créé une politique en matière d'entente de travail flexible en collaboration avec le Service central de la paye, la Direction de l'assurance et de la gestion des risques, la Division des services des installations, la Division des solutions numériques et technologiques, la Direction des services juridiques et le comité consultatif sur le télétravail. La politique, entrée en vigueur le 28 juin 2021, s'applique à quelque 13 000 membres de la fonction publique centrale.

Pour ce qui est de la gestion de la sécurité informatique en télétravail, la CFP est chargée :

- d'établir des politiques et procédures qui régissent les ententes de travail à distance pour la Province;
- de déployer le programme de sensibilisation à la sécurité (créé par la Division des solutions numériques et technologiques) sur sa plateforme de formation;
- de veiller à la conformité des ministères à l'achèvement de la formation obligatoire de sensibilisation à la sécurité.

Cette page a été laissée
blanche intentionnellement.

Objectif, portée et approche, critères

Objectif

Notre objectif consistait à déterminer si la Province disposait de procédures et de contrôles pour atténuer les risques à la sécurité informatique dans l'environnement de télétravail.

Portée et approche

L'audit comprenait l'inspection des documents, des procédures, des normes, des rapports et d'autres documents de la Province portant sur la gestion des risques à la sécurité informatique en télétravail. Nous avons interrogé des propriétaires de processus et des intervenants clés de la Division des solutions numériques et technologiques et de la CFP afin de comprendre les procédures et les activités en place pour gérer la sécurité informatique du travail effectué à l'extérieur des locaux du gouvernement.

L'audit porte sur les pratiques et les contrôles appliqués pendant la période de juin 2021 à juin 2023. Étant donné que la politique en matière d'entente de travail flexible ne s'applique qu'aux membres de la fonction publique centrale de la Province, nous avons uniquement interrogé des personnes qui font partie de la fonction publique centrale conformément à la définition de *la Loi sur la fonction publique*. Nous avons également interrogé des entrepreneurs utilisés pour le renforcement des effectifs au sein de ces ministères.

Les membres des fonctions publiques élargie et alliée ont été exclus de cet audit. Conformément à la Loi, ces membres comprennent :

- la fonction publique élargie – premier dirigeant et employés des organismes suivants :
  - sociétés d'État,
  - Shared Health Inc.,
  - offices régionaux de la santé,
  - universités,
  - districts scolaires,
- la fonction publique alliée – personnel des bureaux de l'Assemblée et des bureaux de circonscription des députés à l'Assemblée, personnel des hauts fonctionnaires et personnel politique.

Le présent audit exclut les entrepreneurs qui ne sont pas utilisés pour le renforcement des effectifs, comme ceux utilisés pour la sous-traitance (p. ex., Kyndryl, DXC).

Critères d'audit

Nous avons utilisé les critères suivants pour déterminer si la Province disposait de procédures et de contrôles pour atténuer les risques à la sécurité informatique dans l'environnement de télétravail :

Critères	Sources
Critère 1 : Les données stockées et transmises avec les dispositifs utilisés à distance doivent être protégées contre l'accès non autorisé.	Cadre de cybersécurité du NIST • Sécurité des données (PR.DS) • Technologie de protection (PR.PT)
Critère 2 : Les dispositifs utilisés pour le télétravail doivent être authentifiés et les correctifs nécessaires doivent y être appliqués avant que les employés obtiennent l'accès au réseau de la Province.	Cadre de cybersécurité du NIST • Contrôle d'accès (PR.AC) • Maintenance (PR.MA) • Surveillance constante de la sécurité (DE.CM)
Critère 3 : Les vulnérabilités et les incidents de sécurité en télétravail doivent être relevés et atténués sans délai.	Cadre de cybersécurité du NIST • Atténuation (RS.MI)
Critère 4 : Les employés doivent suivre régulièrement une formation de sensibilisation sur les risques du télétravail et les pratiques d'atténuation.	Cadre de cybersécurité du NIST • Gouvernance (ID.GV) • Sensibilisation et formation (PR.AT)

La Province gère les risques à la sécurité informatique liés au télétravail, mais des améliorations s'imposent

La pandémie de COVID-19 a amorcé la transition du travail traditionnel au bureau aux ententes de travail à distance. Même si le télétravail était possible avant la pandémie, il est devenu plus commun et accepté après que les gouvernements du monde entier ont exigé aux travailleurs non essentiels de rester à la maison pendant les confinements. Maintenant que la COVID-19 n'est plus considérée comme une urgence de santé publique mondiale, la politique en matière d'entente de travail flexible de la Province garantit un soutien aux employés qui choisissent une **entente de travail hybride**. La Division des solutions numériques et technologiques s'est alors retrouvée à devoir déployer rapidement des contrôles de sécurité dans un périmètre élargi pour protéger les divers lieux de travail à distance.

Une **entente de travail hybride** est un modèle de travail qui combine le travail au bureau et le travail à distance.

Nous avons conclu que la Province avait mis en place des contrôles pour gérer les risques à la sécurité informatique en télétravail, mais que des améliorations s'imposaient pour renforcer ces mesures. Notre conclusion s'appuie sur les constatations suivantes :

- Les données stockées et transmises avec les dispositifs de travail à distance sont protégées, mais les paramètres de chiffrement doivent être améliorés **(SECTION 1)**.
- Les dispositifs utilisés pour le télétravail sont authentifiés et les correctifs nécessaires y sont appliqués **(SECTION 2)**.
- Les vulnérabilités et les incidents de sécurité en télétravail sont relevés et atténués sans délai **(SECTION 3)**.
- De nombreux employés n'ont pas suivi la formation obligatoire de sensibilisation à la sécurité **(SECTION 4)**.
- Les politiques et les procédures de sécurité sont désuètes **(SECTION 5)**.

1 Les données sont protégées, mais les paramètres de chiffrement doivent être améliorés

La Province recourt au chiffrement pour protéger les données stockées et transmises par les travailleurs à distance. Selon le Center for Internet Security (CIS), le chiffrement est une opération cryptographique qui transforme l'information lisible (texte brut) en information illisible (texte chiffré) pour renforcer la sécurité et protéger les données électroniques. Le CIS est une entité sans but lucratif qui crée, valide et promeut des solutions exemplaires opportunes pour aider les individus, les entreprises et les gouvernements à se protéger contre les cybermenaces.

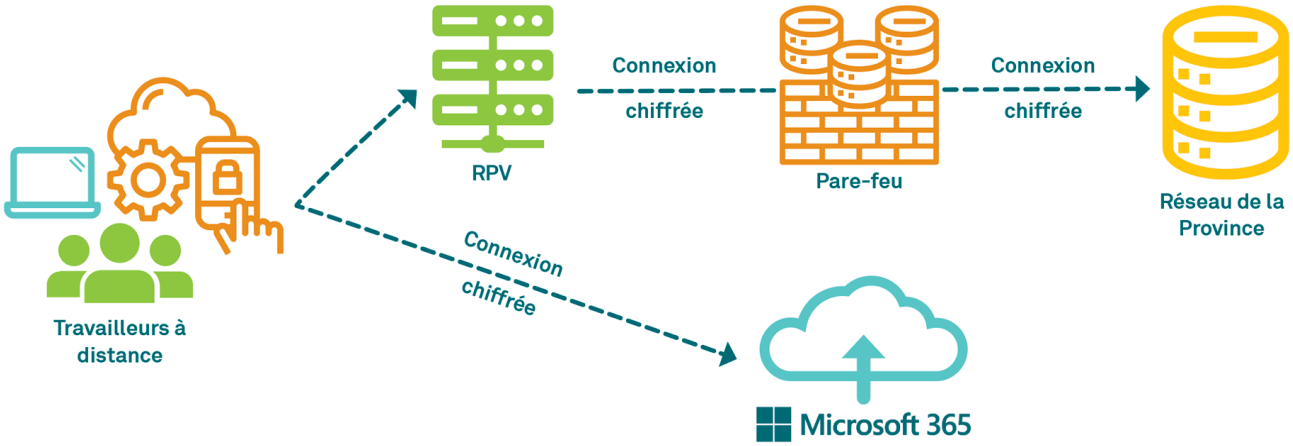
Les postes informatiques, y compris les ordinateurs portables et les ordinateurs de bureau, sont chiffrés pour prévenir toute divulgation de données non autorisée. Le transfert sécurisé de fichiers par courriel peut être utilisé pour envoyer de l'information sensible en format chiffré. Les données transmises entre le réseau de la Province et l'ordinateur d'un travailleur à distance connecté à un réseau domestique sont également protégées par un réseau privé virtuel (RPV). Selon la définition du Centre canadien pour la cybersécurité, un RPV « est une connexion sécurisée entre deux points ». Il agit comme un tunnel par lequel des données peuvent être envoyées et reçues en toute sécurité sur un réseau physique existant.

L'**infonuagique** est un modèle qui offre un accès sur demande à des ressources informatiques (réseaux, serveurs, mémoires, applications, services) et nécessite peu de gestion ou d'interaction de la part du fournisseur.

Source : Publication spéciale 800-145 du NIST

La Division des solutions numériques et technologiques a déployé Microsoft Office 365 (y compris son outil de collaboration Microsoft Teams) pour favoriser la productivité des travailleurs à distance. Il s'agit d'une suite logicielle par abonnement que Microsoft héberge dans le **nuage**. Les utilisateurs n'ont pas besoin de se connecter au RPV pour utiliser les applications de Microsoft Office 365. Cependant, ils doivent tout de même se connecter à leur compte gouvernemental pour avoir accès à ces ressources infonuagiques. Même si un RPV n'est pas nécessaire, les connexions à Microsoft Office 365 ne sont pas moins sécuritaires. Notamment, Microsoft offre une connexion chiffrée entre l'utilisateur et ses applications.

Figure 2 – Ce diagramme montre que les connexions à Microsoft 365 sont envoyées directement au service. Le reste du trafic passe par le RPV.



Si le chiffrement est une méthode de protection efficace, nous avons constaté que des configurations et des paramètres de chiffrement pourraient être renforcés pour améliorer la sécurité de ces connexions.

Notamment, nous avons remarqué des cas où un chiffrement insuffisant semblait être utilisé pour les données en mouvement des travailleurs à distance. Dans ces cas, le chiffrement ne respectait pas les normes de TIC du Manitoba. Ces normes établissent les pratiques exemplaires en matière de protection des données et des systèmes, et contiennent des recommandations et des exigences pour prévenir la compromission grâce à un chiffrement infaillible.

Si un pirate informatique interceptait une communication mal chiffrée, il pourrait user de techniques pour déchiffrer et lire les données, ce qui exposerait des données sensibles et confidentielles à un accès non autorisé.

Étant donné la nature délicate de nos observations sur la sécurité, nous avons présenté en détail nos constatations et nos recommandations dans une lettre interne à l'intention de la Division des solutions numériques et technologiques.

Recommandation 1

Nous recommandons que la Division revoie et actualise les paramètres de chiffrement conformément aux normes provinciales en suivant nos recommandations dans la lettre adressée à la direction.

2 Les dispositifs sont authentifiés et les correctifs sont appliqués automatiquement

Un **jeton** est une chose qu'un utilisateur possède et contrôle qui lui sert à valider son identité. Il peut s'agir, par exemple, d'un dispositif qui génère et affiche des mots de passe ponctuels que l'utilisateur entre manuellement. Même s'il est désigné comme un « dispositif », l'authentifiant peut être un dispositif physique distinct ou bien une application s'exécutant sur un dispositif universel, comme un téléphone intelligent.

Source : Federal Information Processing Standards 201-3 du NIST (définition) et Publication spéciale 800-63B du NIST (exemple)

Le RPV n'est pas la seule couche de sécurité en place pour l'accès aux ressources du réseau de la Province. Outre posséder un compte réseau, les travailleurs à distance doivent avoir un dispositif contrôlé, un RPV et un **jeton** pour l'authentification multifacteur. Les dispositifs contrôlés comprennent les ordinateurs formatés et délivrés par la Province. La Province s'occupe également des correctifs de ces ordinateurs.

Un processus de gestion des correctifs est en place pour l'application des correctifs de sécurité à ces dispositifs contrôlés. Un correctif est une modification ou une mise à jour appliquée pour corriger un dysfonctionnement ou une lacune en matière de sécurité. Les correctifs sont automatiquement installés sur les dispositifs contrôlés utilisés en télétravail lorsqu'une connexion à Internet est établie, soit par une connexion filaire ou un RPV. Les erreurs survenant lors du déploiement des correctifs sont surveillées. Les messages d'erreur sont passés en revue, puis les correctifs sont renvoyés si nécessaire.

3 Les vulnérabilités et les incidents de sécurité sont relevés et atténués sans délai

Un centre de services gère et résout les incidents de sécurité et les interruptions dans l'environnement informatique de la Province, ce qui englobe les technologies qu'utilisent les travailleurs à distance. Son personnel utilise un système de gestion des incidents qui consigne et surveille les incidents signalés par les employés, qu'ils soient survenus au bureau ou à un poste de télétravail.

Il y a également un processus de gestion des vulnérabilités. Ce dernier est régi par la norme de gestion des vulnérabilités de la Division des solutions numériques et technologiques. La norme exige des cycles de vérification régulière des vulnérabilités dans l'environnement informatique de la Province, y compris les serveurs à distance, les postes informatiques et les dispositifs de réseau. Le processus sert à détecter les vulnérabilités dans les dispositifs susceptibles d'être exploités par les pirates désirant s'en servir pour entrer dans le réseau et le compromettre. Une vulnérabilité est une faiblesse qu'un pirate peut exploiter pour compromettre un système d'information. La Division surveille les sources de sécurité pour rester au fait des menaces et des annonces de vulnérabilité concernant un matériel ou un logiciel couramment utilisé au gouvernement.

La Division évalue les vulnérabilités pour déterminer leur incidence et cerner les mesures correctives à prendre. Pendant la période d'audit, nous avons soulevé les trois mesures correctives principales qu'elle utilise : l'installation d'un correctif logiciel, l'ajustement des paramètres de configuration ou la suppression du logiciel compromis.

4 De nombreux employés n'ont pas suivi la formation de sensibilisation à la sécurité de l'information

La Province, par l'intermédiaire de la CFP, oblige tous ses employés à suivre la formation obligatoire du Manitoba sur la SSI. Cette formation renseigne les utilisateurs sur la **compromission de messagerie d'entreprise**, notamment sur les tactiques d'hameçonnage et de piratage psychologique, et sur les risques liés aux clés USB. Dans le contexte du télétravail, la formation aborde des sujets comme les risques liés aux réseaux publics, l'utilisation du RPV de la Province et le chiffrement de l'information sensible. Tous les fonctionnaires doivent suivre cette formation obligatoire de base, qui leur démontre les compétences et les connaissances qu'ils doivent posséder. La formation doit avoir été achevée dans les deux mois suivant l'embauche.

La **compromission de messagerie d'entreprise** est un type de cybercrime par lequel un escroc utilise des courriels pour inciter une personne à envoyer de l'argent ou à divulguer des renseignements d'entreprise confidentiels.

Source : Sécurité Microsoft

La CFP surveille l'achèvement de cette formation et envoie des rapports trimestriels de non-conformité aux ministères par l'entremise d'un tableau de bord numérique. Ces statistiques sont passées en revue par les sous-ministres et intégrées aux rapports des tableaux de bord équilibrés des ministères. De même, les ministères peuvent produire leurs propres rapports, indiquant les employés qui ont fait la formation obligatoire. Les rapports de la CFP et des ministères servent à veiller à ce que chaque employé ait suivi la formation.

D'après l'examen de la CFP, en date du 31 mars 2023, 3 843 employés (31,17 %) n'avaient pas achevé la formation obligatoire du Manitoba sur la SSI. Pour notre part, nous avons sélectionné un échantillon de 67 travailleurs à distance pour déterminer s'ils avaient suivi cette formation obligatoire. Nous avons alors constaté que cinq d'entre eux, qui étaient tous en poste depuis plus de 12 mois, ne l'avaient pas terminée.

En outre, quatre de ces cinq employés étaient des directeurs ou des directeurs généraux. Les employés à ces échelons sont ceux qui donnent le ton à un organisme et à sa culture, y compris en matière de cybersécurité. En participant à la formation sur la sécurité informatique, ils démontrent un engagement à l'égard de la sécurité et montrent l'exemple à leurs collègues.

La CFP avise les ministères lorsque leurs employés n'ont pas fait la formation à temps. Les ministères doivent envoyer des rappels à leurs employés pour veiller à ce qu'ils suivent la formation du Manitoba

sur la SSI (cela inclut les travailleurs sur place et à distance). Outre les rappels, ceux qui n'achèvent pas la formation dans les délais prescrits ne subissent aucune conséquence importante.

La formation du Manitoba sur la SSI est essentielle, car elle renseigne les employés sur les menaces, les pratiques sûres et l'importance d'avoir des procédures de sécurité. Cette formation permet aux employés, particulièrement à ceux à distance :

- d'apprendre comment bien utiliser le réseau du gouvernement;
- de reconnaître les menaces et d'y répondre convenablement;
- d'éviter les cyberattaques causées par l'erreur humaine.

L'erreur humaine est une grave menace pour la cybersécurité. D'ailleurs, un rapport de 2022 du Forum économique mondial indique que 95 % des problèmes de cybersécurité sont attribuables à l'erreur humaine. De ce fait, les travailleurs à distance qui ne suivent pas la formation sur la sécurité sont plus susceptibles d'être victimes de courriels d'hameçonnage et d'autres tactiques de piratage psychologique. Cela peut mener à la compromission de données d'accès, à l'intrusion de logiciels malveillants et à des fuites de données.

Recommandation 2

Nous recommandons que la CFP élabore, en collaboration avec les ministères, des procédures d'escalade pour garantir que les employés suivent la formation obligatoire, y compris la formation du Manitoba sur la SSI. Les procédures doivent prévoir des conséquences, comme la désactivation de l'accès au système, dans les cas où la formation n'est pas achevée à temps.

5 Les politiques et les procédures de sécurité sont désuètes

Les ententes de travail flexible ont introduit de nouvelles menaces à la sécurité de la Province et ont rapidement accéléré l'utilisation de biens technologiques pour le travail à distance. Il faut impérativement que les politiques et les procédures soient révisées afin d'y intégrer les menaces et les technologies relatives au télétravail. Notamment, la Province a augmenté son utilisation de cellulaires et de tablettes pour effectuer certaines tâches, mais les appareils mobiles ne sont pas inclus explicitement comme bien de TIC dans la norme sur les mots de passe du Manitoba. Par conséquent, les appareils mobiles semblent non conformes à la norme.

Les politiques, procédures et lignes directrices suivantes sont désuètes :

Document	Dernière mise à jour
Pratiques exemplaires de gestion de la sécurité informatique	Janvier 2003
Normes et procédures du Manitoba sur l'élimination du contenu électronique	Novembre 2005
Guide de classification des données	Décembre 2012
Politique sur les technologies de l'information et des communications	Juillet 2013
Lignes directrices sur la protection des technologies de l'information et de la communication pendant les déplacements	Juin 2014
Norme sur les mots de passe du Manitoba	Juin 2015
Contrôles de sécurité de base du Manitoba	Juin 2016
Norme sur la gestion des vulnérabilités	Novembre 2016

Les politiques, procédures et lignes directrices sur la sécurité informatique aident la Province à s'adapter aux changements et à orienter son personnel à l'égard des pratiques de sécurité. Ces documents sont importants, car ils établissent et maintiennent une position de sécurité informatique robuste. Leur actualisation permettrait de répondre aux menaces à la sécurité actuelles et encouragerait une culture d'amélioration continue.

Voici d'autres audits contenant des constatations sur des politiques et des procédures désuètes :

- *Accès privilégiés aux systèmes d'information*, octobre 2022
- *Vieillissement des systèmes d'information*, février 2022
- *Bureau de l'état civil*, septembre 2020

Les politiques désuètes peuvent semer la confusion chez le personnel quant aux pratiques de sécurité adéquates et mener à des brèches de sécurité indues. Enfin, si les formations reposent sur des documents désuets, les employés seront mal informés et les formations s'avéreront ultimement inutiles.

Pendant notre travail sur le terrain, nous avons découvert que la direction et les analystes des politiques de la Division des solutions numériques et technologiques sont tenus de réviser ces documents chaque année en vertu d'une procédure opérationnelle normalisée adoptée en mai 2023. La direction de la Division nous a informés que cette exigence a été établie pour garantir la mise à jour des politiques.

Recommandation 3

Nous recommandons que la Division :

a. révise tous les ans les politiques, procédures et lignes directrices désuètes afin de tenir compte des pratiques exemplaires et des exigences réglementaires en vigueur, conformément à la procédure opérationnelle normalisée;
b. forme et sensibilise les employés au sujet des documents révisés et des nouvelles mesures de sécurité.

Renseignements supplémentaires sur l'audit

Ce rapport de certification indépendant sur la gestion de la sécurité informatique dans un milieu de travail à distance a été préparé par le Bureau du vérificateur général du Manitoba. Notre responsabilité consistait à fournir des renseignements objectifs, des conseils et une assurance pour aider l'Assemblée législative à examiner la gestion des ressources et des programmes du gouvernement et à déterminer si la Division des solutions numériques et technologiques et la CFP se conforment, à tous les égards importants, aux critères applicables.

Tout le travail de cet audit a été exécuté à un niveau de certification raisonnable, conformément à la Norme canadienne de missions de certification 3001 – Missions d'appréciation directe établie par les Comptables professionnels agréés du Canada (CPA Canada) dans le Manuel de CPA Canada – Certification.

Le Bureau applique la Norme canadienne de contrôle qualité 1 et, par conséquent, assure un système de contrôle de la qualité exhaustif, y compris des politiques et des procédures documentées concernant le respect des règles de déontologie, des normes professionnelles et des exigences législatives et réglementaires applicables.

Nous avons respecté les normes d'indépendance et autres règles déontologiques du code de conduite professionnelle de l'Ordre des comptables professionnels agréés du Manitoba, lesquelles reposent sur des principes fondamentaux d'intégrité, d'objectivité, de compétence et de diligence professionnelles, de confidentialité et de professionnalisme.

Conformément à notre processus d'audit habituel, nous avons obtenu de la part de la direction :

- la confirmation de la responsabilité de la direction quant à l'objet de l'audit;
- la confirmation de la validité des critères utilisés dans le cadre de l'audit;
- la confirmation que tous les renseignements connus qui ont été demandés ou qui pourraient avoir une incidence sur les constatations ou la conclusion de l'audit ont été fournis.

Période visée par l'audit

L'audit a porté sur la période comprise entre juin 2021 et juin 2023. C'est à cette période que s'applique la conclusion de l'audit.

Date du rapport d'audit

Nous avons obtenu des éléments de preuve d'audit suffisants et appropriés sur lesquels fonder notre conclusion le 9 février 2024, à Winnipeg, au Manitoba.

Cette page a été laissée
blanche intentionnellement.

Résumé des recommandations et réponses des responsables

Recommandation 1

Nous recommandons que la Division revoie et actualise les paramètres de chiffrement conformément aux normes provinciales en suivant nos recommandations dans la lettre adressée à la direction.

Réponse des responsables :

Le ministère de la Protection du consommateur et des Services gouvernementaux (le Ministère) accepte la recommandation et donnera suite aux constatations énoncées dans la lettre adressée à la direction.

Recommandation 2

Nous recommandons que la CFP élabore, en collaboration avec les ministères, des procédures d'escalade pour garantir que les employés suivent la formation obligatoire, y compris la formation du Manitoba sur la SSI. Les procédures doivent prévoir des conséquences, comme la désactivation de l'accès au système, dans les cas où la formation n'est pas achevée à temps.

Réponse des responsables :

La CFP accepte la recommandation et lancera un examen en vue d'améliorer le taux d'achèvement de la formation obligatoire de la SSI au sein des fonctionnaires, ce qui comprendra l'élaboration de procédures d'escalade. Ce faisant, elle misera sur les outils et les processus offerts par les nouvelles technologies et fonctionnalités obtenues grâce à l'intégration du nouveau système SAP et des modules SuccessFactors.

Recommandation 3

Nous recommandons que la Division :

- révise tous les ans les politiques, procédures et lignes directrices désuètes afin de tenir compte des pratiques exemplaires et des exigences réglementaires en vigueur, conformément à la procédure opérationnelle normalisée;
- forme et sensibilise les employés au sujet des documents révisés et des nouvelles mesures de sécurité.

Réponse des responsables :

a. Le Ministère accepte la recommandation et continuera à réviser régulièrement ses politiques, procédures, lignes directrices et normes pour tenir compte des pratiques exemplaires et de l'environnement.

b. Le Ministère accepte la recommandation et mettra en œuvre des procédures pour que les outils de formation et de sensibilisation demeurent actuels.

Cette page a été laissée
blanche intentionnellement.

Notre vision

Responsabilisation du gouvernement et excellence en administration publique au service des Manitobains.

Notre vission

Fournir de manière indépendante des renseignements, des conseils et des garanties concernant les activités du gouvernement et la gestion des fonds publics

Nos valeurs

Indépendance

Nous sommes indépendants du gouvernement et réalisons un travail objectif et impartial.

Intégrité

Nous agissons avec honnêteté et appliquons des normes déontologiques élevées.

Innovation

Nous mettons de l'avant l'innovation et la créativité dans nos activités et nos façons de faire.

Travail d'équipe

Nous travaillons en équipe en mettant en commun les connaissances et les compétences de chacun pour atteindre nos objectifs.

Le Bureau vérificateur général du Manitoba reconnaît avec respect que nous menons nos activités sur les terres ancestrales des nations anichinabé, anishininewuk, dakota oyate, dénésuline et nehethowuk, ainsi que sur le territoire national des Métis de la Rivière-Rouge. Nous respectons les traités conclus sur ces territoires, nous reconnaissons les préjudices et les erreurs du passé et nous nous engageons à aller de l'avant en partenariat avec les communautés autochtones dans un esprit de réconciliation et de collaboration.

VERSION DU SITE WEB

Vérificateur général
MANITOBA

Pour plus de renseignements, veuillez communiquer avec notre bureau :

Bureau du vérificateur général
330, avenue Portage, bureau 500
Winnipeg (Manitoba) R3C 0C4
Téléphone : 204 945-3790
contact@oag.mb.ca | www.oag.mb.ca/fr

@AuditorGenMB
@AuditorGenMB
@AuditorGenMB
company/manitoba-auditor-general