Lapierre, Marie-Ève

De: Responsable Acces
Envoyé: 1 avril 2021 13:01
À: [redacted]
Objet: Demande d'information
Pièces jointes: PJ_Tableau.pdf; Liste des articles.pdf; Avis de recours.pdf

Québec, le 1er avril 2021

[redacted]

[redacted]

[redacted],

La présente donne suite à votre demande d'accès à l'information reçue le 10 mars 2021, laquelle est rédigée ainsi :

> « En vertu de l'article 9 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, je désire obtenir copie du ou des document(s) suivant(s) :
>
> - Tous rapports ou autres documents sur l'état de préparation du ministère des Finances pour faire face aux cyberattaques ou aux atteintes à la protection des données, du 1er janvier 2017 à aujourd'hui.
> - Tous rapports ou autres documents relatifs à toute atteinte à la protection des données qui ont eu lieu depuis le 1er janvier 2018. »

En vertu de l'article 47 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1) (« Loi sur l'accès »), nous vous informons que le ministère des Finances détient des renseignements relativement à votre demande.

En ce qui concerne le premier point de votre demande, vous trouverez ci-joint un document faisant état des renseignements détenus par le Ministère. Notez que certaines informations dans le document sont caviardées conformément à l'article 29 de la Loi sur l'accès.

De même, d'autres documents recensés ne peuvent être transmis car certains renseignements visés en forme la substance et la divulgation de certains renseignements aurait pour effet de réduire l'efficacité des programmes de sécurité du Ministère. Ils sont donc protégés en vertu des articles 14 et 29 de la Loi sur l'accès.

En ce qui concerne le deuxième point de votre demande, le Ministère n'a relevé aucun incident relativement à la protection de données pour les années 2018, 2019 et 2020.

Si vous désirez contester cette décision, il vous est possible de le faire en vous adressant à la Commission d'accès à l'information. Vous trouverez ci-joint une note explicative concernant l'exercice de ce recours.

Je vous prie de recevoir, [redacted], l'expression de mes sentiments distingués.

David St-Martin
Directeur général de l'organisation du budget, de l'administration et du secrétariat
Responsable de l'accès aux documents et de la protection des renseignements personnels

Direction générale de l'organisation du budget, de l'administration et du secrétariat
390, boulevard Charest Est, 8e étage
Québec (Québec) G1K 3H4
Tél. : 418 643-1229 / Téléc. : 418 646-0923
Courriel : david.st-martin@finances.gouv.qc.ca

Plan d'action en rehaussement de la sécurité - Ministère des finances

Mesure	Actions	Précisions et étapes de réalisation
1.1	**Inventaire :** l'organisation possède un inventaire à jour de ses actifs informationnels.	Pour l'instant, nous avons un inventaire décentralisé de nos actifs, composé de : postes de travail [redacted]), serveurs [redacted], pour nos logiciels nous avons une application maison qui se nomme [redacted]. Nous sommes en train de mettre en place notre inventaire centralisé [redacted]) dans la solution [redacted] la mise-en-production devrait être pour la fin mars 2021.
1.2	**Serveurs désuets :** un plan de rehaussement ou délestage des systèmes d'exploitation désuets est défini et sera réalisé.	Nos serveurs sont à des versions supportées dans plus de 95% des cas. Nous avons [redacted] serveurs [redacted] : rehaussement du système applicatif [redacted] est en cours et la fin est prévu le 2021-03-31. Nous avons [redacted] serveurs [redacted] : rehaussement du système de l'Intranet est en cours et la fin est prévu le 2021-03-31
1.3	**Mitigation des serveurs désuets :** un plan de mitigation des vulnérabilités des systèmes d'exploitation désuets en attendant leur rehaussement/délestage est défini et sera réalisé.	Nous sommes en train de préparer la coupure d'internet des tous nos serveurs. Nous sommes présentement en train d'établir la planification pour sortir les besoins des différents systèmes. Nous sommes en contrat avec les porteurs de systèmes pour arriver avec une planification.
1.4	**Postes de travail désuets :** un plan de rehaussement ou délestage des systèmes d'exploitation désuets est défini et sera réalisé.	Quelques postes sont encore en [redacted] leur migration vers [redacted] ayant été retardée. Nous allons catégoriser les postes [redacted] et planifier leur migrations d'ici juin 2021.
1.5	**Mitigation des postes de travail désuets :** un plan de mitigation des vulnérabilités des systèmes d'exploitation désuets en attendant leur rehaussement/délestage est défini et sera réalisé.	L'accès aux mises à jour de sécurité est assurée via un contrat de support étendu avec [redacted] pour ces postes. Ces postes sont scannés régulièrement.
1.6	**Appareils mobiles désuets :** un plan de mise à jour ou de remplacement des appareils pour avoir recours à des versions supportées par les manufacturiers est défini et sera réalisé.	Les appareils mobiles du ministère sont presque tous encore supportés par le manufacturier. Seuls [redacted] vieux [redacted] qui sont très rarement utilisés seraient à retirer de la circulation d'ici la fin du printemps. Le processus qui s'assure du respect du cycle de vie pour les mobiles sera renforcé d'ici juin 2021.
1.7	**Équipements de télécom désuets :** un plan de mise à jour ou de remplacement des équipements (ex. : pare-feux, commutateurs, etc.) pour avoir recours à des versions supportées par les manufacturiers est défini et sera réalisé.	Nous planifions la mise à jour ou le remplacement des commutateurs et des pare-feux en suivant les phases de support des manufacturiers, de manière à avoir des équipements supportés en tout temps. Pour nos bornes sans-fils sont sous contrat de service par l'ITQ, donc ce n'est pas nous qui gérons les équipements.
2.1	**Détection des vulnérabilités :** un plan de détection des vulnérabilités est défini et pris en charge, pour nos actifs internes.	Notre detection des vulnérabilités est effectué en 3 étapes : 1-Nous avons nos outils de mise-à-jour qui nous indique si nous avons des vulnérabilités relié à des [redacted] 2-Nous avons un service de SOC qui es [redacted] qui surveille nos journaux de tous nos serveurs, télécommunications, anti-virus et pare-feu en temps réel. Ainsi que des scan de vulnérabilité sur des actifs critiques ciblés une fois par mois. 3-Nous sommes aussi des participants du projet pilote avec le CGCD pour les scans de vulnérabilité avec [redacted] (Outil du SCT [redacted] fois par semaine.
2.2	**Correctifs sur les serveurs :** un plan d'application des correctifs est défini et appliqué sur les systèmes d'exploitation et logiciels.	Tous nos serveurs [redacted] ont été mis à jour avec les mises-a-jour de Janvier : Nous avons un plan de mise-à-jour des serveurs [redacted] qui revient 3 fois par année, Janvier, Avril et Septembre. Nos serveurs [redacted] et [redacted] ont été mis-à-jour en Janvier. Nous avons un plan de mise-à-jour des serveurs [redacted] qui revient 3 fois par année, Janvier, Avril et Septembre. Les logiciels des utilisateurs sont à jour pour [redacted]. Pour les outils bureautiques, ils sont mis à jour en fonction des migrations de système d exploitation (compatibilité), lors de vulnérabilités détectées (CERTAQ), en fonction des besoins de la clientèle (nouvelles fonctionnalités). Les versions de progiciels sont mis à jour au fur et à mesure de leur diffusion selon les disponibilités des clients. Les mises à niveau majeurs des versions sont en fonction du support du fournisseur ou lors d un projet applicatif qui en permet l évolution. La téléphonie est un service géré obtenu via les offres de l'ITQ qui est mise à jour par le fournisseur TELUS. Un accent particulier est mis sur les progiciels importants, tels [redacted] et [redacted], en consolidation avec les fournisseurs et les clientèles concernées au Ministère.
2.3	**Correctifs sur les postes de travail :** un plan d'application des correctifs est défini et appliqué sur les systèmes d'exploitation et logiciels.	Nous utilisons [redacted] pour déployer les correctifs de sécurité sur les postes de travail chaque mois. Notre plan inclut des phases d'essais avec la clientèle. Le processus peut être accéléré si les correctifs corrigent des failles critiques.
2.4	**Correctifs sur les appareils mobiles :** un plan d'application des correctifs, dès leur disponibilité, est défini et appliqué.	Un plan d'application de correctifs sera mis en place d'ici juin 2021, suite au déploiement du volet MDM de [redacted] prévu pour mai.
2.5	**Télétravail :** une stratégie de mise à jour automatisée des postes de travail hors site existe et est appliquée.	Même stratégie que la mesure 2.3, mais avec une planification sur plusieurs soirées. Nous utilisons [redacted] pour gérer les postes, via notre infrastructure. Comme nous avons une solution de [redacted] tous nos postes informatiques sont toujours connectés à notre réseau. Les applications courantes (ex.: Chrome, Acrobat) sont configurées pour se mettre à jour de façon automatisée.
2.6	**Télétravail :** une stratégie de validation de la conformité des postes non gérés qui se connectent à l'infrastructure VPN est en place.	Seuls les postes qui sont joints au domaine du ministère peuvent se connecter à distance par [redacted] L'utilisation de postes non gérés est possible seulement via le portail du MFQ, et et le poste est alors utilisé simplement comme un terminal.
3.1	**Antivirus EDR sur les serveurs :** un antivirus moderne est en fonction sur tous les serveurs.	Nous avons le produit [redacted] qui comprends une solution EDR pour nos serveurs autant Windows que Linux.
3.2	**Antivirus EDR sur les postes :** un antivirus moderne est en fonction sur tous les postes de travail.	Côté solution antivirus pour les postes, nous utilisons actuellement une combinaison des solutions [redacted] et [redacted] gérée dans le Cloud (EDR)

4.1	**MFA :** l authentification multifacteur est implantée pour l'accès aux systèmes exposés sur internet.	Le MFA est déployé pour se connecter à distance aux applications cloud[redacted] Nous évaluons le déploiement du MFA à l'ouverture d'une session réseau. Un inventaire est en cours pour identifier les modes d'authentification aux applicatifs utilisés par une clientèle externe.
5.1	**Prise de copies :** l'infrastructure de sauvegarde est isolée au maximum pour protéger les données des attaques provenant du réseau (ex. : rançongiciel).	Nous utilisons[redacted] comme solution de sauvegarde dans notre infrastructure. Tous nos copies de sauvegarde mensuel sont conservées hors site pour une durée de[redacted] ans.
5.2	**Prise de copies :** un plan de reprise informatique est documenté, connu et mis à jour en continu.	Tous nos systèmes de mission et dépôt de données et fichiers sont en [redacted] Des tests au site de relève sont mensuels, ainsi que des tests en télétravail. Les tests d'infrastructures sont sur une base annuelle , à définir en fonction du contexte (arrêt des infrastructures centrales pour basculer sur les infrastructures de relève). Un Plan de Reprise Informatique (PRI), faisant partie du plan de continuité des services essentiels, est en révision, date de livraison prévue: juin 2021.
5.3	**Prise de copies :** une stratégie de prise de copies quotidienne est en fonction.	Nos environnements de production sont pris en back-up chaque jour ([redacted] Copie de fin de mois et de fin d'année conservée[redacted] L'utilisation de la copie est fréquente dans le cadre des services courant (boîte de courrier, répertoires, serveurs). Ceci nous démontre le bon fonctionnement autant pour les récupérations court terme que moyen terme (sur bande).
5.4	**Prise de copies :** des exercices de recouvrement sont effectués périodiquement, entre autres pour valider que les copies sont fonctionnelles.	Pour l'instant, nous n'avons pas de plan de test pour les restores des copies de sécurité. C'est un système que nous utilisons à plusieurs fins et ça plusieurs fois par semaine. Nous avons des procédures de restore pour les fichiers,courriels ou serveurs virtuels complets, mais sans de plan de test structuré.
6.1	**Données confidentielles :** une solution de courriel sécurisé est disponible.	La mission de notre organisme ne nécessite pa l'échange de données nominatives. Certains employés doivent échanger des données nominatives dans le cadre de leurs fonctions. Aucune solution de courriels sécurisés n'est présentement déployée.
6.2	**Données confidentielles :** sensibiliser et former les employés sur les échanges de données confidentielles.	Lors du dépôt du budget ou d'une mise à jour économique, soit deux fois par année, nous rappelons aux employés l'importance d'utiliser notre plateforme[redacted] qui permet d'échanger des données avec l'extérieur, chiffrées. Un guide et une assistance leur est founi pour faciliter leur formation. De plus, dans l'intranet du Ministère, un document d'orientation technologique informe les employés des moyens disponibles au ministère pour le transferts de données confidentielles.[redacted] plateformes sont offertes, soit les sites de[redacted] tel que mentionné ci-dessus ou d[redacted] pour les documents de hauts volumes et hautement sécurisés . En 2021, nous prévoyons dans notre plan de formation en SI, de sensibiliser d'avantage les employés à ce sujet.
7.1	**Balayage de vulnérabilités externes :** notre organisme est inscrit au service de balayage de vulnérabilités du Centre gouvernemental de cyberdéfense.	Le MFQ est inscrit sur le service. Le ROCD exécute un balayage sur une base mensuelle, ce service est également offert et utilisé par les organismes du portefeuille (ISQ, TAMF).
7.2	**Balayage de vulnérabilités externes :** définir un processus de travail pour corriger les lacunes découvertes en continu.	Un processus périodique de déploiement des correctifs de sécurité est en place, et les vulnérabilités critiques sont traitées en urgence.
8.1	**Surveillance :** les accès aux systèmes exposés sur internet sont journalisés.	Les accès au portail sont journalisés dans l'extranet du CF,[redacted]
8.2	**Surveillance :** une stratégie est en place pour détecter et bloquer les tentatives de connexion anormales aux systèmes exposés sur internet.	Nous avons de la journalisation dans[redacted] pour la connexion et l'authentification ainsi que sur les serveurs web.
9.1	**Captcha :** l'authentification aux services externes est protégée par un dispositif captcha.	Un dossier d'opportunité est en cours de réalisation concernant un service commun de gestion des identités et des accès pour le MFQ. Ce dossier d'opportunité va tenir compte du besoin d'ajouter un Captcha.
10.1	**Notifications :** transmettre des notifications avisant le citoyen des accès ou des changements à son compte.	Il y a envoie de courriel à l'utilisateur lors d'une création de compte, d'une demande de changement ou de mot de passe pour l'extranet du CF (utilisateurs = ministères ou organismes). Note: le ministère ne fait pas affaire directement avec les citoyens.
11.1	**Transmissions sécuritaires :** mettre à la disposition des citoyens un service leur permettant de transmettre des informations de façon sécuritaire, autre que le courriel.	Un système maison [redacted] permet d'échanger des données avec l'extérieur, chiffrées. N/A car le ministère ne fait pas affaire directement avec les citoyens
12.1	**Hameçonnage :** des campagnes de simulation à l hameçonnage sont menées de façon continue et engageante auprès des employés.	Notre organisme effectue une fois par année par le biais d'un fournisseur externe une simulation d'hameçonnage, celle-ci a eu lieu à l'automne dernier. Le Ministère vise que d'ici le 2021-03-31 tous les employés auront suivi la formation de l'ATN et dans cette formation une capsule vise la sensibiliation à l'hameçonnage De plus, des formations supplémentaires de la firme Teranova qui traitent, en autre, des menaces par hameçonnage sont actuellement offertes aux nouveaux employés. Le Ministère vise de l'offrir à l'ensemble de ses employés durant la prochaine année.
13.1	**Directives :** une directive interne indique aux employés la marche à suivre lors de la réception de courriels malicieux, la détection de virus ou autres menaces.	Une nouvelle directive sur la sécurité de l'information sera émise au printemps 2021. Elle s'inspirera de la politique gouvernementale sur la sécurité de l'information, prévue au printemps 2021. D'ici là, le Ministère dispose de la Politique ministérielle de la sécurité de l'information, d'un cadre de gestion de la SI, d'une directive ministérielle sur l'utilisation des actifs informationnels. Cette dernière définit les bonnes pratiques d'utilisation des actifs, dont les obligations en termes d'utilisation des informations, de leur diffusion et du respect de la confidentialité.
14.1	**Gestion des accès :** un processus d'ajout, de révision et de retrait des accès est implanté pour la gestion du mouvement du personnel.	Un processus de mouvement de personnel est en place au MFQ, processus qui inclut la révision des accès. Des révisions ponctuelles sont faites à la demande des détenteurs d'actifs.
14.2	**Gestion des accès :** un processus d'ajout et de retrait des accès de privilèges élevés/administrateur est implanté et est révisé périodiquement.	Le processus d'octroi des privilèvesest fait selon le principe des privilège minimum. Un processus de révision des authentifiants avec privilèges, est effectué une fois l'an.
14.3	**Gestion des accès :** un outil de journalisation des accès est implanté.	Nous avons un contrat d'un SOC,[redacted] qui gère un SIEM pour les gestions des vulnérabilités et la journalisation des accès pour l'ensemble de notre parc des serveurs.

15.1	**Formation :** un plan de formation en cybersécurité est en place pour sensibiliser les employés de manière continue sur le sujet.	Le plan de sensibilisation du Ministère vise que d'ici le 2021-03-31 tous les employés auront suivi la formation de l'ATN sur les capsules suivantes : Cyberdéfence : L'hameçonnage Cyberdéfence : Virus et rançongiciels Cyberdéfence : Ingénierie sociale ou l'art de la manipulation Cyberdéfence : La sécurité des appareils mobiles Un suivi sera effectué auprès des secteurs et une campagne de sensibiliation sera faite en parallèle. De plus, le MFQ c'est doté d'une plateforme de sensibilisation à la sécurité de l'information de la firmeTerranova pour des formations supplémentaires. Ce logiciel-service met à la disposition des fonctions pour créer des cours et des quiz, procéder à des analyses et gérer des utilisateurs. Des formations sont actuellement offertes aux nouveaux employés, plus de 200 personnes ont été inscrites jusqu'à maintenant. Le Ministère vise à offrir ces formations à l'ensemble de ses employés.
Autre	**Autre**	Une vérification annuelle est faite sur les accès physiques aux salles de serveurs. Cette vérification sera demandée mensuellement.

chapitre A-2.1

LOI SUR L'ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

14. Un organisme public ne peut refuser l'accès à un document pour le seul motif que ce document comporte certains renseignements qu'il doit ou peut refuser de communiquer en vertu de la présente loi. Si une demande porte sur un document comportant de tels renseignements, l'organisme public peut en refuser l'accès si ces renseignements en forment la substance.Dans les autres cas, l'organisme public doit donner accès au document demandé après en avoir extrait uniquement les renseignements auxquels l'accès n'est pas autorisé.

29. Un organisme public doit refuser de confirmer l'existence ou de donner communication d'un renseignement portant sur une méthode ou une arme susceptible d'être utilisée pour commettre un crime ou une infraction à une loi. Il doit aussi refuser de confirmer l'existence ou de donner communication d'un renseignement dont la divulgation aurait pour effet de réduire l'efficacité d'un programme, d'un plan d'action ou d'un dispositif de sécurité destiné à la protection d'un bien ou d'une personne.

AVIS DE RECOURS EN RÉVISION

RÉVISION

a) Pouvoir

L'article 135 de la Loi prévoit qu'une personne peut, lorsque sa demande écrite a été refusée en tout ou en partie par le responsable de l'accès aux documents ou de la protection des renseignements personnels ou dans le cas où le délai prévu pour répondre est expiré, demander à la Commission d'accès à l'information de réviser cette décision.

La demande de révision doit être faite par écrit; elle peut exposer brièvement les raisons pour lesquelles la décision devrait être révisée (art. 137).

L'adresse de la Commission d'accès à l'information est la suivante :

QUÉBEC
Édifice Lomer-Gouin
575 rue Saint-Amable, bureau 1.10
Québec (Québec) G1R 2G4
Téléphone : (418) 528-7741
Télécopieur : (418) 529-3102

MONTRÉAL
Bureau 18.200
500, boul. René-Lévesque Ouest
Montréal (Québec) H2Z 1W7
Téléphone : (514) 873-4196
Télécopieur : (514) 844-6170

b) Motifs

Les motifs relatifs à la révision peuvent porter sur la décision, sur le délai de traitement de la demande, sur le mode d'accès à un document ou à un renseignement, sur les frais exigibles ou sur l'application de l'article 9 (notes personnelles inscrites sur un document, esquisses, ébauches, brouillons, notes préparatoires ou autres documents de même nature qui ne sont pas considérés comme des documents d'un organisme public).

c) Délais

Les demandes de révision doivent être adressées à la Commission d'accès à l'information dans les 30 jours suivant la date de la décision ou de l'expiration du délai accordé au responsable pour répondre à une demande (art. 135).

La loi prévoit spécifiquement que la Commission d'accès à l'information peut, pour motif raisonnable, relever le requérant du défaut de respecter le délai de 30 jours (art. 135).

APPEL DEVANT LA COUR DU QUÉBEC

a) Pouvoir

L'article 147 de la loi stipule qu'une personne directement intéressée peut porter la décision finale de la Commission d'accès à l'information en appel devant un juge de la Cour du Québec sur toute question de droit ou de compétence.

L'appel d'une décision interlocutoire ne peut être interjeté qu'avec la permission d'un juge de la Cour du Québec s'il s'agit d'une décision interlocutoire à laquelle la décision finale ne pourra remédier.

b) Délais

L'article 149 prévoit que l'avis d'appel d'une décision finale doit être déposé au greffe de la Cour du Québec, dans les 30 jours qui suivent la date de réception de la décision de la Commission par les parties.

c) Procédure

Selon l'article 151 de la loi, l'avis d'appel doit être signifié aux parties et à la Commission dans les dix jours de son dépôt au greffe de la Cour du Québec.