Direction générale adjointe

DE LA CYBERSÉCURITÉ
ET DE L'INFONUAGIQUE (DGACI)

CYBERSÉCURITÉ

Directive sur la cybersécurité

MSSS-DIR03

2023-11-20

Votre gouvernement

Ministère de la Santé et des Services sociaux
Québec

Table des matières

Contexte

L'infonuagique, l'intelligence artificielle, la mobilité, l'Internet des objets ainsi que les nouvelles technologies de stockage et de transmission sont au cœur de l'utilisation quotidienne du numérique au ministère de la Santé et des Services sociaux (MSSS) ainsi que pour les établissements et organismes constituant le réseau de la Santé et des Services sociaux (RSSS).

La stratégie de transformation numérique, initiée par le gouvernement et appuyée par le Plan de modernisation technologique du MSSS, permettra à terme de bonifier la prestation de services au citoyen. Elle suscite néanmoins des préoccupations à considérer en lien avec la cybersécurité, particulièrement pour une organisation qui détient des renseignements sociaux et médicaux extrêmement sensibles.

Dans un contexte de prolifération des cyberattaques, l'exploitation d'une vulnérabilité d'un actif informationnel pourrait entraîner des conséquences plus que significatives sur les activités du MSSS ou du RSSS dans son ensemble, mais également sur la population québécoise ou sur l'image du gouvernement.

Le MSSS et le RSSS doivent donc anticiper les menaces, faire évoluer leurs mesures de cybersécurité et corriger les vulnérabilités présentes dans l'écosystème de sécurité afin de réduire les risques d'atteinte à la disponibilité, à l'intégrité et à la confidentialité de cette information sensible.

Objectifs

Les objectifs de la présente directive se déclinent comme suit :

- intervenir de façon proactive en anticipant les cybermenaces et en adaptant constamment les moyens de s'en protéger;
- mobiliser l'ensemble des acteurs de l'écosystème de cybersécurité du MSSS et du RSSS.

Champs d'application

Cette directive s'applique aux entités suivantes :

- au MSSS;
- aux organismes publics visés au paragraphe 5 de l'article 2 de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G 1.03)*, ci-après appelés « RSSS ».

Elle concerne et vise également :

- tous les domaines d'activités de ces organisations;
- toute information détenue par ces entités, native ou confiée, le support numérique sur lequel elle se trouve ou sa localisation, et ce, durant tout son cycle de vie.

Cadre légal et administratif

Cette directive s'inscrit dans une perspective qui s'inscrit, sans s'y limiter, en respect des exigences de :

- la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., chap. A-2.1);
- la politique gouvernementale de cybersécurité - SCT mars 2020;
- la Politique provinciale de la sécurité de l'information - MSSS-POL01;
- le Cadre de gestion de la sécurité de l'information - MSSS-CDG01;
- la Règle particulière sur la sécurité organisationnelle - 2017-06-27;
- la Directive Élaboration et évolution d'un plan de reprise informatique – MSSS-DIR11.

La sécurité de l'information à un niveau organisationnel doit être considérée comme un écosystème. Par conséquent, les exigences de cybersécurité spécifiées dans les divers documents d'encadrement en la matière s'additionnent et se complètent.

Définitions

Pour l'application de la présente directive, les termes suivants signifient :

Terme	Description
Actif informationnel	Actif qui peut être un système, une banque d'information, un réseau de télécommunication, une infrastructure technologique ou un ensemble de ces éléments. Ce peut également être une composante informatique d'un équipement médical spécialisé.
Actif informationnel critique	Actif informationnel qui est nécessaire à l'exécution d'un processus critique et dont un bris de disponibilité, d'intégrité ou de confidentialité pourrait, de façon significative, porter préjudice à la vie, à la santé ou au bien-être du citoyen, ou nuire à la mission ou à la prestation de service de l'organisation.
Cyberattaque	Ensemble coordonné d'actions malveillantes réalisées par l'intermédiaire du cyberespace et qui visent à endommager, à forcer ou à détourner un réseau ou un système informatique afin de commettre un acte préjudiciable.
Cyberdéfense	Ensemble des moyens mis en place par une organisation pour défendre dans le cyberespace les systèmes d'information jugés d'importance critique et qui contribuent à assurer la cybersécurité. Dans le présent document, la notion d'importance critique réfère notamment à la valeur de l'information établie selon la disponibilité, l'intégrité et la confidentialité.

Terme	Description
Cybersécurité	Pratique qui consiste à protéger les systèmes, les réseaux et les programmes contre les cyberattaques. Ce type d'attaque vise généralement à accéder à de l'information sensible, à la modifier ou à la détruire, à extorquer de l'argent aux utilisateurs, ou à interrompre les processus normaux de l'organisation, et ainsi porter atteinte à la disponibilité, à l'intégrité et à la confidentialité de l'information que cette dernière détient.
Événement de sécurité de l'information	Événement lié à la sécurité de l'information, indésirable ou inattendu, présentant une forte probabilité de compromettre les opérations liées à l'activité d'une organisation et de menacer la disponibilité, l'intégrité ou la confidentialité de l'information détenue par cette dernière. Dans le contexte de cybersécurité, un événement de sécurité de l'information est généralement lié à l'utilisation des technologies de l'information.
Immotique	Ensemble de techniques englobant les ressources électroniques, informatiques et de télécommunications et qui vise à améliorer l'habitat et le milieu de travail dans un bâtiment ou un immeuble.
Menace	Événement potentiel appréhendé qui est susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité de l'information d'un système ou de l'information que ce système traite, stocke ou transmet. Ce peut également être un événement qui constitue une violation ou une menace imminente notamment de violation des politiques, des règles ou des procédures de sécurité.
Mesure de sécurité	Moyen concret qui assure, en tout ou en partie, la protection de l'actif informationnel contre une ou plusieurs menaces informatiques, et dont la mise en œuvre vise à réduire la probabilité de concrétisation de ces menaces ou à minimiser les pertes qui en résultent.
Restauration de données	Action de régénérer des données qui ont été perdues ou contaminées.
Vulnérabilité	Faille d'un actif ou d'une mesure de sécurité qui peut être exploitée par une menace, par exemple : ➜ un manque d'entretien du matériel informatique; ➜ un antivirus non mis à jour; ➜ une formation insuffisante du personnel; ➜ l'absence de séparation de tâches incompatibles[1].

[1] Certaines tâches sont incompatibles parce que si elles sont assumées par la même personne, elles mettent cette dernière en position de commettre une fraude ou une erreur et de la dissimuler. La séparation de tâches vise à réduire les possibilités de manipulation ou d'utilisation abusive ou non autorisée des actifs informationnels.

Obligations

Mesures de sécurité à mettre en place

Les mesures précisées dans cette section permettent de renforcer la protection des actifs informationnels de l'organisation dans un contexte de cybersécurité.

1. Inventaire des actifs informationnels

L'organisation doit inclure dans sa stratégie de cybersécurité une cartographie des actifs informationnels qu'il détient. À cet effet, il doit :

- détenir un inventaire complet et à jour de ces actifs ainsi que de ceux liés à l'infrastructure technologique : postes de travail, serveurs, appareils biomédicaux, équipement immotique (systèmes de contrôles et de sécurité du bâtiment) ainsi que tout équipement connecté au réseau;
- préciser, pour chaque actif informationnel, le nom du système et celui de son détenteur, le nom et la version du système d'exploitation, les composantes physiques de base, le résumé de ses fonctions principales et des actifs informationnels critiques qu'il supporte, ainsi que les coordonnées de l'hébergeur, le cas échéant.

2. Gestion des vulnérabilités

Le MSSS et le RSSS doivent demeurer vigilant face aux vulnérabilités, car elles représentent une entrée potentielle pour toute personne malveillante qui tente de les exploiter. De façon préventive, l'organisme doit donc réaliser les interventions suivantes :

Balayages de vulnérabilités :

- s'inscrire au service du centre d'opérationnalisation de cyberdéfense (COCD) de balayage des vulnérabilités afin d'accéder ainsi à une surveillance centralisée et conséquemment plus efficace;
- réaliser des balayages régulièrement sur les actifs informationnels critiques ainsi que sur ceux exposés sur Internet;
- les effectuer lors de l'implantation d'un nouvel actif, lors de son rehaussement ou de changements majeurs apportés à sa configuration ou à son environnement;
- identifier les risques liés aux vulnérabilités découvertes, les évaluer et y apporter les correctifs nécessaires, dans le respect du processus de gestion des menaces, des vulnérabilités et des incidents (GMVI).

Correctifs de sécurité :

- appliquer les correctifs les plus récents fournis par le manufacturier;
- s'assurer qu'ils proviennent d'une source authentifiée, dont la provenance est formellement établie;
- le faire le plus tôt possible, dans le respect des orientations ministérielles et du processus GMVI.

Si le MSSS ou le RSSS héberge des actifs dont les fournisseurs n'offrent pas de correctifs à des vulnérabilités identifiées (les appareils biomédicaux par exemple), il doit :

- isoler ces actifs du réseau (physiquement ou logiquement) ou mitiger le risque à l'aide de l'outil recommandé par le COCD;
- en détenir une liste à jour;
- exercer une surveillance accrue de ces actifs.

Enfin, pour tout rehaussement ou toute acquisition d'un nouvel actif, il faut s'assurer de la capacité du fournisseur à fournir les correctifs à des vulnérabilités identifiées, et que ce dernier puisse les corriger à l'intérieur des délais respectant les standards du COCD.

3. Gestion de la désuétude

L'organisation doit élaborer et mettre en œuvre un processus de gestion de la désuétude afin que tous les actifs informationnels qu'il détient soient rehaussés et maintenus à des versions récentes qui permettront de réduire le risque de cyberattaque. Ce processus doit également prévoir les modalités de retrait des actifs qui ne sont plus requis ou utilisés.

4. Tests d'intrusion

L'organisation doit effectuer des tests d'intrusion sur tout actif informationnel exposé sur Internet qui :

- a été mis à jour;
- dont la configuration ou l'environnement ont subi des changements majeurs;

Par ailleurs, des tests d'intrusion doivent être planifiés par l'organisme lors de toute nouvelle acquisition ou de tout rehaussement d'actif informationnel exposé sur Internet. L'organisme peut utiliser le service de tests d'intrusion offert par le COCD, réaliser ces tests lui-même ou mandater une tierce partie[2].

5. Gestion des menaces

L'organisation doit s'assurer d'une gestion efficace des menaces, car elles peuvent causer des préjudices sérieux aux actifs informationnels qu'il détient. À cet effet, il doit notamment :

- déployer et configurer la solution provinciale antivirale moderne sur tous les postes de travail et les serveurs;
- se connecter aux deux consoles provinciales antivirales du MSSS, soit celle dédiée aux serveurs et celle dédiée aux postes de travail;
- procéder au filtrage des accès à Internet, en excluant notamment par défaut la catégorie « Non catégorisé » (*unrated*)[3], le cas échéant;

[2] Si elle choisit de le faire elle-même ou de mandater une tierce partie, l'organisation doit présenter les résultats de ces tests au COCD dans les meilleurs délais afin que ce dernier puisse fournir ses recommandations.

[3] Ce type de catégorie représente un risque plus élevé de cybersécurité, étant donné qu'elle représente, de prime abord, une « boîte noire » dont on ne connait pas la légitimité.

- s'assurer que ses spécialistes en cybersécurité suivent les formations spécifiques dispensées par le COCD afin qu'ils puissent gérer efficacement les outils de sécurité qui sont mis à leur disposition par ce dernier, notamment ceux générant des alertes système.

6. Stratégie de sauvegarde des données et plan de reprise informatique

L'organisation doit s'assurer d'avoir une stratégie de sauvegarde des données afin de pouvoir recouvrir rapidement l'accès aux données à la suite d'une cyberattaque. Il doit donc :

- effectuer une sauvegarde au moins une fois par jour de l'ensemble de ses actifs informationnels critiques;
- isoler son infrastructure de sauvegarde;
- tester la restauration des données afin de s'assurer que les copies de sauvegarde sont fonctionnelles, dans le respect de la stratégie retenue par l'organisme et à une fréquence minimale d'une fois par année.

En complément à cette stratégie, l'organisation doit :

- être muni d'un plan de reprise informatique défini, connu et mis à jour périodiquement pour chaque actif informationnel critique;
- réaliser des exercices de simulation périodiques de ce plan;
- en définir les critères et les conditions d'activation.

7. Gestion des accès aux actifs

Une saine gestion des accès permet de contrôler l'accès à une ressource par des mécanismes de contrôle, empêchant ainsi les accès non autorisés, sources potentielles d'évènements de sécurité de l'information. Dans ce contexte, l'organisation doit donc :

- appliquer le principe du moindre privilège en évitant l'octroi de comptes à privilèges élevés à des utilisateurs (ex. : de type administrateur);
- rendre disponible uniquement l'information que les utilisateurs ont besoin de connaitre pour accomplir leurs tâches;
- réviser ces accès de façon régulière.

8. Surveillance des accès aux actifs

La surveillance demeure un rempart efficace contre les actions malveillantes. L'organisation doit donc :

- surveiller les accès aux actifs informationnels exposés sur Internet, notamment en :
  - journalisant les accès à ces actifs;
  - détectant les tentatives de connexion anormales et les bloquant automatiquement.
- réaliser une surveillance accrue des accès accordés aux employés, notamment ceux dotés de privilèges élevés et de l'utilisation qu'ils en font.

9. Services d'authentification des actifs exposés sur Internet

L'authentification permet à l'organisation de s'assurer qu'elle communique avec la bonne personne. Elle doit donc s'assurer de :

- recourir à l'authentification à facteurs multiples :
  - pour les accès des citoyens et des employés aux actifs informationnels critiques exposés sur Internet;
  - pour tous les accès à privilèges élevés.
- mettre en place un ou des mécanismes assurant l'authentification en personne, un dispositif de type CAPTCHA[4] par exemple.

10. Services Web au citoyen

Le citoyen est un acteur important dans une stratégie de cybersécurité d'un organisme. L'organisation doit donc :

- l'aviser de tout accès ou de tout changement à son compte;
- mettre à sa disposition un service de communication sécurisée autre que le courriel afin qu'il puisse en tout temps échanger de façon sécuritaire avec l'organisation pour ses besoins, une page Web sécurisée par exemple.

11. Communications au citoyen

Les communications adressées au citoyen par messagerie ou par courriel ne doivent pas :

- lui demander ou lui transmettre des renseignements personnels ou confidentiels;
- contenir d'hyperlien, sauf exception[5].

12. Utilisation sécuritaire des outils de travail

L'organisation doit élaborer et diffuser de la documentation qui informe son personnel des consignes à respecter lors de l'utilisation du courriel, d'Internet et des outils technologiques.

13. Sensibilisation et formation du personnel

Un plan de sensibilisation à la sécurité de l'information doit être mis en place pour permettre aux employés de réagir adéquatement face à une possible menace et ainsi réduire les risques d'évènements de sécurité de l'information.

[4] Programme qui protège les sites Web et les applications contre les robots logiciels en générant des tests qui ne peuvent être accomplis que par des humains.

[5] Consulter le document *MSSS-EXI-009 Exigence encadrant les communications numériques avec les citoyens* pour toute exception à cette obligation.

Ce plan doit inclure :

- des capsules de formation sur la sécurité de l'information, et plus particulièrement sur la cybersécurité;
- des campagnes de simulation à l'hameçonnage de façon continue.

Entrée en vigueur et révision

Cette directive entre en vigueur à la date de son adoption. Une révision doit être effectuée tous les trois ans ou en cas de besoin.

Approuvée par le chef délégué de la sécurité de l'information :	Reno Bernier
Date d'adoption :	Le 7 mars 2022
Date de révision :	Le 20 novembre 2023