Rapport du Vérificateur général du Québec
à l'Assemblée nationale pour l'année 2021-2022

Novembre 2021

CHAPITRE 7

Cybersécurité

Étude

EN BREF

Au fil des ans, le Vérificateur général a observé que des améliorations pourraient être apportées aux mesures de cybersécurité mises en place par un grand nombre d'entités gouvernementales pour assurer la sécurité des renseignements personnels et confidentiels et des autres actifs informationnels qu'elles possèdent. Nous avons donc mené une étude auprès de trois entités qui détiennent des renseignements personnels et confidentiels sur les Québécois.

Au cours de notre étude, nous avons validé l'existence de mesures recommandées par des référentiels reconnus de bonnes pratiques en matière de cybersécurité au sein des trois entités. Pour ce faire, nous avons procédé à une collecte de données par l'entremise de questionnaires et d'entrevues comportant plus de 400 questions. Nous n'avons toutefois pas testé l'efficacité de ces mesures.

La cybersécurité demeure un défi pour ces trois entités, et ce, malgré les mesures qu'elles ont mises en place. En effet, leur niveau de préparation demande à être amélioré continuellement étant donné l'augmentation constante des risques de cyberattaques ainsi que du niveau de sophistication de ces dernières. Les entités demeurent donc exposées à des risques liés à la sécurité de l'information. Par conséquent, elles doivent continuer à appliquer et à améliorer leurs mesures de cybersécurité.

La cybersécurité constitue un enjeu prioritaire pour le Vérificateur général. Nos travaux ont mené à la formulation d'observations importantes qui pourraient permettre aux entités visées et au gouvernement du Québec d'améliorer leurs mesures et ainsi de mieux gérer les risques de cybersécurité. Pour des raisons évidentes de sécurité, nous ne divulguons pas le détail de nos observations. Enfin, le but de cette étude n'est pas de prendre connaissance de l'existence de contrôles visant à compenser les faiblesses des mesures qui pourraient être améliorées. D'ailleurs, ces contrôles compensatoires ne sauraient aussi bien mitiger les risques que les mesures ayant fait l'objet de notre étude.

Il est important de noter que nos travaux n'ont pas permis de déceler des erreurs ou des cas de fraude liés aux observations que nous avons effectuées.

Les commentaires que le Secrétariat du Conseil du trésor a formulés en son nom et au nom des trois entités étudiées et qui sont présentés dans ce rapport démontrent l'importance qu'ils accordent à cette question. Le Secrétariat du Conseil du trésor indique qu'il va intégrer les observations du Vérificateur général dans un plan d'action visant l'amélioration de la gestion de la cybersécurité au sein de l'appareil gouvernemental.

OBSERVATIONS

1. Les mesures de cybersécurité mises en place par les entités étudiées en vue de se protéger d'éventuelles cyberattaques sont à améliorer.

2. Les mesures de cybersécurité mises en place par les entités étudiées afin de détecter les cyberattaques sont à améliorer.

3. L'absence de certaines activités liées à la gouvernance des entités étudiées nuit à la mise en place de mesures de cybersécurité visant l'identification des risques de cyberattaques.

4. Les mesures de cybersécurité mises en place par les entités étudiées afin de réduire leur temps de réponse et de récupération en cas de cyberattaque sont à améliorer.

ÉQUIPE

Alain Fortin
Directeur général d'audit

Patrice Watier
Directeur d'audit informatique
et d'intelligence d'affaires

Rachel Ladouceur
Frantz Christelle Montès
Lyne Roberge

TABLE DES MATIÈRES

MISE EN CONTEXTE

1 La cybersécurité se définit comme un processus de protection des actifs informationnels fondé principalement sur la prévention et la détection des cyberattaques.

Actifs informationnels

Il s'agit de l'ensemble des éléments contenant de l'information (ex. : information numérique, banque d'information numérique, système ou support d'information, documentation, technologie de l'information, installation) acquis ou constitués par une organisation.

Cyberattaque

Il s'agit d'un acte malveillant envers un système informatique, un réseau ou tout autre matériel des technologies de l'information (ex. : téléphone intelligent, portable, tablette), ayant notamment pour but de compromettre la sécurité de l'information.

Pourquoi avons-nous fait cette étude ?

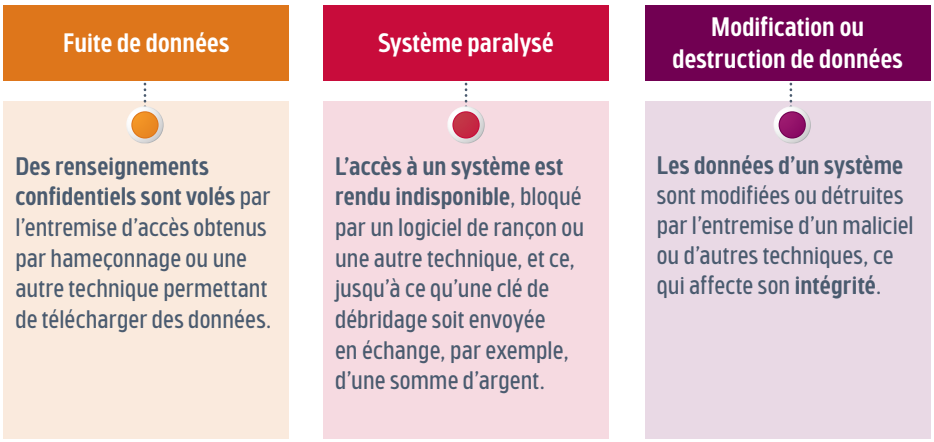
2 Bien que nos travaux aient commencé avant la pandémie de COVID-19, la cybersécurité est un sujet qui a pris de l'importance avec l'augmentation significative du télétravail, et ainsi des risques liés à la sécurité de l'information.

3 Le vol de renseignements personnels et confidentiels s'avère fort lucratif pour les pirates informatiques, et les tentatives risquent de se multiplier au cours des prochaines années. Plusieurs grandes entreprises en ont d'ailleurs été victimes, tout comme certains organismes du gouvernement et organismes publics. D'ailleurs, selon le Centre canadien pour la cybersécurité, il est probable que les cyberattaques contre les ministères, les universités et les hôpitaux persistent étant donné la nature essentielle des services qu'ils offrent et la sensibilité de l'information qu'ils gèrent.

4 Les trois entités étudiées détiennent des renseignements personnels et confidentiels sur les Québécois et les entreprises québécoises, et ont la responsabilité de les protéger adéquatement. Les principaux rôles et responsabilités des entités sont présentés dans la section Renseignements additionnels.

5 Des lacunes en matière de cybersécurité exposent les organisations à plusieurs risques liés à la sécurité de l'information. Tous ces risques peuvent porter atteinte à la confidentialité, à la disponibilité et à l'intégrité de l'information (figure 1).

FIGURE 1 Exemples de risques liés à la cybersécurité



6 Si les organisations sont mal protégées contre les cyberattaques, ces risques peuvent se matérialiser et entraîner des conséquences à court et à long termes (figure 2).

FIGURE 2 Exemples de conséquences engendrées par les cyberattaques

Introduction aux cyberattaques

7 Une cyberattaque provient essentiellement de l'exploitation de deux principales faiblesses, soit les vulnérabilités humaines, qui ouvrent la porte au piratage psychologique (ex. : hameçonnage), et les vulnérabilités des systèmes, comme une faille technique dans une application Web, un réseau informatique ou une base de données.

Piratage psychologique

Il s'agit d'une pratique de manipulation psychologique utilisée par les pirates informatiques pour obtenir les renseignements personnels d'une personne dans le but d'usurper son identité.

Exemple d'une technique de piratage psychologique

Lors d'une tentative d'hameçonnage, le pirate informatique envoie un message (ex. : courriel, message texte) frauduleux à ses victimes en se faisant passer pour une institution ou une entreprise. Généralement, ce message contient un hyperlien qui redirige les victimes vers une copie conforme du site Internet officiel de cette institution ou de cette entreprise, et les incite à y saisir certains renseignements personnels et confidentiels (ex. : nom d'utilisateur, mot de passe, numéro de carte de crédit), qui sont ensuite récupérés par le pirate informatique.

8 De plus, les cyberattaques peuvent provenir autant de l'intérieur que de l'extérieur d'une organisation. Les attaques internes, résultant d'actes volontaires ou non, sont particulièrement dommageables puisque leurs auteurs ont déjà accès aux réseaux informatiques. Ils n'ont alors pas besoin d'intermédiaire (ex. : courriel) pour accomplir leurs méfaits. Les organisations doivent donc mettre en place des mesures de cybersécurité efficaces pour faire face à ces risques, même si leurs systèmes sont hébergés par un tiers, puis s'assurer qu'elles sont mises en œuvre de façon adéquate.

9 La pandémie de COVID-19 a poussé de nombreuses organisations à privilégier le télétravail pour maintenir leurs activités, ce qui a augmenté de ce fait la vulnérabilité de leurs systèmes informatiques et a ainsi ouvert de nouvelles portes aux pirates informatiques. Toutefois, certaines mesures de cybersécurité spécialement mises en place en contexte de télétravail ont pu réduire les risques liés à cette vulnérabilité.

10 Le gouvernement du Québec a publié, en 2020, sa politique gouvernementale de cybersécurité, dans laquelle il prône une ouverture sur le partage et la mise en commun des connaissances, de l'expertise et des bonnes pratiques en matière de cybersécurité. Il a également mis sur pied, en 2019, le Centre gouvernemental de cyberdéfense au sein du Secrétariat du Conseil du trésor. Cette structure spécialisée en sécurité de l'information est soutenue par des centres opérationnels de cyberdéfense établis dans les ministères et les organismes publics. Le Centre gouvernemental de cyberdéfense joue le rôle d'entité de confiance au sein du réseau gouvernemental de cyberdéfense. Il a notamment comme responsabilités de coordonner les efforts en cybersécurité des organismes publics et des centres opérationnels de cyberdéfense, d'assurer la prise en charge des incidents de sécurité à portée gouvernementale et de jouer un rôle collaboratif dans l'écosystème de cybersécurité québécois, national et international.

Bonnes pratiques en matière de cybersécurité

Les mesures de cybersécurité se trouvent notamment dans des référentiels internationaux tels que ceux produits par le Center for Internet Security (CIS)[1], l'International Organization for Standardization (ISO)[2] et le National Institute of Standards and Technology (NIST)[3]. Ces référentiels sont un ensemble structuré de bonnes pratiques qui s'adressent à toutes les organisations, tant gouvernementales que privées. Ces bonnes pratiques doivent être adaptées aux objectifs de chaque organisation et à ses risques liés à la sécurité de l'information.

1. Le CIS est un organisme américain qui a pour objectif de promouvoir de bonnes pratiques permettant aux individus, organisations et entités étatiques de se protéger des cyberattaques.
2. L'ISO est une organisation internationale de normalisation composée de représentants d'organisations nationales de normalisation de 165 pays. Elle produit des normes internationales, utiles aux organisations industrielles et économiques de tout type, et aux gouvernements.
3. Le NIST est une agence du département du Commerce des États-Unis. Il a pour but de promouvoir l'économie en développant, de concert avec l'industrie, des technologies, la métrologie et des normes.

Quels sont l'objectif de l'étude et la portée des travaux ?

11 Nos travaux visaient à déterminer si les trois entités étudiées appliquent les mesures de cybersécurité nécessaires afin de contrer le plus efficacement possible les cyberattaques. Pour ce faire, nous avons analysé divers documents. Nous avons également réalisé des entrevues ainsi qu'une collecte de données par l'entremise de questionnaires comportant plus de 400 questions basées sur des référentiels reconnus de bonnes pratiques en matière de cybersécurité.

12 Nos travaux portent principalement sur la dernière année financière, qui s'est terminée le 31 mars 2021. Toutefois, certaines observations peuvent avoir trait à des situations antérieures ou postérieures à cette période.

13 Nos travaux nous ont permis de formuler des observations importantes qui pourraient permettre aux entités visées ainsi qu'au gouvernement du Québec de mieux gérer les risques de cybersécurité auxquels ils font face. Pour des raisons évidentes de sécurité, nous ne divulguons pas le détail de nos observations. Le but de cette étude n'était pas de prendre connaissance de l'existence de contrôles visant à compenser les faiblesses des mesures qui pourraient être améliorées. D'ailleurs, ces contrôles compensatoires ne sauraient aussi bien mitiger les risques que les mesures ayant fait l'objet de notre étude. Enfin, cette étude a pour but de couvrir un large éventail d'éléments concernant la cybersécurité pour sensibiliser l'ensemble des entités gouvernementales aux bonnes pratiques en matière de cybersécurité. Elle pourrait également servir de base à des travaux plus détaillés dans le cadre d'un futur audit.

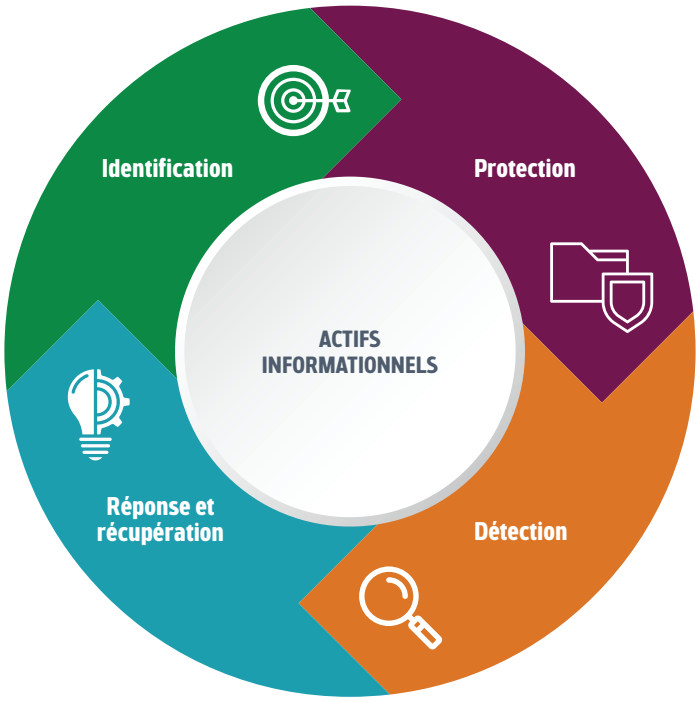
14 L'objectif de l'étude et la portée des travaux sont présentés en détail dans la section Renseignements additionnels.

Sujet de l'étude : cybersécurité

15 Les mesures de cybersécurité mises en place par les entités étudiées ont été divisées selon quatre fonctions (figure 3). Les principales mesures de cybersécurité sont présentées dans la section Renseignements additionnels.

16 Le présent rapport est divisé en quatre grandes parties, soit une partie pour chacune des fonctions présentées à la figure 3. Ces fonctions visent à protéger les actifs informationnels des organisations.

FIGURE 3 Fonctions des mesures de cybersécurité



OBSERVATION 1

Les mesures de cybersécurité mises en place par les entités étudiées en vue de se protéger d'éventuelles cyberattaques sont à améliorer.

Qu'avons-nous observé ?

17 Certaines des mesures de cybersécurité mises en place par les entités étudiées afin de se protéger le plus efficacement possible des cyberattaques pourraient être améliorées pour réduire les risques liés à la sécurité de l'information. Ces améliorations concernent :

Identifiant générique

Il s'agit d'un identifiant n'appartenant pas à une personne en particulier et qui peut être employé par plusieurs personnes. Après la création de l'identifiant, des accès aux systèmes lui sont attribués.

- le processus de gestion des identités et des accès (ex. : utilisation d'identifiants génériques) ;
- les règles de sécurité appliquées lors du cycle de développement des systèmes (ex. : utilisation de renseignements personnels et confidentiels réels lors de la phase de mise à l'essai) ;
- l'utilisation de logiciels et de matériel informatique désuets et l'application de correctifs de sécurité ;
- les coupe-feu ;
- la protection contre la fuite massive de données et le suivi de l'utilisation des médias amovibles (ex. : clé USB).

Pourquoi cette observation est-elle importante ?

18 Les identifiants génériques sont souvent utilisés par des personnes ayant des accès privilégiés. Celles-ci partagent les mêmes accès ainsi que le même mot de passe. Il est donc difficile d'imputer chacune des actions à son véritable responsable. Ces identifiants sont des cibles de choix pour les pirates informatiques, car une fois en leur possession, ils représentent un moyen de compromettre les réseaux et systèmes informatiques d'une organisation[1].

Accès privilégiés

Il s'agit d'accès réservés généralement à un nombre restreint d'employés, tels que les administrateurs de réseau, de base de données ou de la sécurité informatique. Les accès privilégiés permettent, par exemple, de modifier la sécurité des systèmes, d'attribuer et de modifier des accès aux systèmes informatiques, ainsi que d'installer et de configurer des logiciels (ex. : coupe-feu).

19 Les organisations doivent établir des règles de sécurité lors du cycle de développement ou de la refonte majeure d'un système, et ce, afin de minimiser les risques de failles ainsi que d'erreurs de conception et de programmation. Cela permet de réduire les risques de cyberattaques pouvant mener au vol de données ou à l'arrêt non planifié des systèmes. De plus, l'utilisation de renseignements personnels et confidentiels réels lors de la mise à l'essai présente un risque pour la sécurité et la confidentialité de ces renseignements.

20 L'utilisation de systèmes désuets et l'application tardive des correctifs de sécurité par les organisations augmentent le risque que les pirates informatiques s'infiltrent dans les systèmes vulnérables, d'autant plus que lorsque les fournisseurs des systèmes publient de nouveaux correctifs visant à éliminer certaines vulnérabilités, les pirates informatiques en sont aussi informés.

Ce qui appuie notre observation

Processus de gestion des identités et des accès à améliorer

21 Deux des trois entités pourraient resserrer leurs mesures de cybersécurité liées à la gestion des accès privilégiés. En effet, les deux entités utilisent des identifiants génériques. Selon les bonnes pratiques en matière de cybersécurité, l'utilisation de ce genre d'identifiant devrait être limitée, et un identifiant unique devrait être créé pour chaque administrateur des technologies de l'information, notamment les administrateurs de réseau, de base de données ou de la sécurité informatique.

22 Par ailleurs, deux des entités effectuent la révision des accès privilégiés à une fréquence qui, selon les bonnes pratiques, devrait être plus élevée. Pour sa part, la troisième entité ne fait pratiquement jamais la révision des accès privilégiés à certains de ses systèmes, mais l'effectue périodiquement pour d'autres.

1. Ce sujet a été traité dans le rapport intitulé *Gestion des identités et des accès informatiques* déposé à l'Assemblée nationale en juin 2020.

23 Dans deux des trois entités, d'autres éléments à améliorer ont été relevés, dont la vérification concernant la création d'identifiants non autorisés, ainsi que le cumul d'accès, qui implique que les utilisateurs ont accès à des systèmes dont ils n'ont pas besoin dans le cadre de leurs fonctions. Un manque de séparation des accès incompatibles a également été observé. Il convient de séparer les accès incompatibles pour limiter les possibilités de modification ou de mauvais usage des données de l'organisation, que ce soit volontaire ou non.

24 Les trois entités ont affirmé avoir entrepris des actions pour améliorer la situation.

Règles de sécurité appliquées lors du cycle de développement des systèmes à améliorer

25 Les trois entités auraient avantage à améliorer leurs mesures de cybersécurité liées au développement de systèmes ou à la maintenance de logiciels.

26 En effet, les personnes qui développent les systèmes des entités étudiées n'utilisent pas toujours un logiciel spécialisé destiné au repérage d'erreurs de programmation. Enfin, des renseignements personnels et confidentiels sont utilisés lors de la mise à l'essai des systèmes, ce qui est non recommandé selon les bonnes pratiques et à éviter sous l'angle de l'utilisation et de la protection des renseignements personnels.

Utilisation de logiciels et de matériel informatique désuets et application tardive des correctifs de sécurité

27 Les trois entités étudiées utilisent des logiciels et du matériel informatique désuets (ex. : serveurs, postes de travail).

28 Les entités affirment avoir mis en place des mesures de mitigation (ex. : déconnexion d'Internet, isolement du réseau par l'installation de coupe-feu) visant à réduire les risques d'accès non autorisé. Des travaux seraient également en cours pour mettre à niveau les logiciels désuets ainsi que remplacer plusieurs appareils.

29 Par ailleurs, l'une des entités tarde à appliquer certains correctifs de sécurité visant à éliminer les vulnérabilités connues de ses systèmes.

Mise à profit des coupe-feu à améliorer

30 L'utilisation de coupe-feu est l'une des pierres angulaires de la sécurité des réseaux informatiques. En effet, les coupe-feu protègent les réseaux internes des organisations, dans lesquels les données sont stockées, en permettant le passage sélectif des flux d'information entre ces réseaux internes et Internet, et neutralisent les tentatives de cyberattaques.

31 Les entités étudiées disposent de coupe-feu, mais auraient avantage à apporter des améliorations pour répondre aux bonnes pratiques et bénéficier d'une protection plus efficace. Pour des raisons évidentes de sécurité, nous ne présentons pas le détail des améliorations qui sont souhaitables.

Protection contre la fuite massive de données à améliorer

32 L'utilisation d'outils spécifiques de protection contre la fuite massive de données permet aux organisations de détecter d'éventuelles fuites de données importantes hors du périmètre de leurs réseaux, qu'elles aient lieu par l'entremise de leurs sites Web, d'une clé USB ou de tout autre canal de transmission. Or, certaines des mesures de cybersécurité de deux des entités pourraient être améliorées pour offrir une protection plus efficace contre la fuite massive de données. Pour des raisons évidentes de sécurité, nous ne présentons pas le détail des améliorations qui sont souhaitables.

OBSERVATION 2

Les mesures de cybersécurité mises en place par les entités étudiées afin de détecter les cyberattaques sont à améliorer.

Qu'avons-nous observé ?

33 Les mesures de cybersécurité mises en place par les entités étudiées pour détecter les cyberattaques pourraient être améliorées en ce qui a trait :

- aux alertes de sécurité automatisées et aux journaux ;
- à la surveillance des événements liés à la sécurité des systèmes ;
- à la modification directe de données ;
- à la gestion de la configuration de sécurité des systèmes ;
- à la documentation des délais de réponse aux notifications de sécurité.

Journaux

L'utilité des journaux est d'assurer une traçabilité des événements en les enregistrant. Ces événements comprennent entre autres les activités des utilisateurs et des systèmes, notamment :

- les défaillances (ex. : actions non traitées par les systèmes) ;
- les événements liés à la sécurité (ex. : tentatives d'accès infructueuses à des données confidentielles) ;
- la découverte de vulnérabilités (ex. : logiciel devenu désuet).

Pourquoi cette observation est-elle importante ?

34 Les mesures de cybersécurité visant la détection des cyberattaques renseignent rapidement les organisations sur les événements importants qui requièrent une intervention. Elles permettent aussi de pallier, entre autres, un manque ou une déficience dans les mesures visant à prévenir les cyberattaques.

35 Il est essentiel que les organisations surveillent leurs systèmes de façon continue afin de relever les événements suspects qui se produisent pendant leur fonctionnement.

36 Un nombre insuffisant d'alertes ou le manque de suivi de celles-ci exposent les organisations à des risques liés à la sécurité de l'information, puisque c'est le repérage et le traitement rapide des événements suspects qui permettent notamment de contrer les cyberattaques, ainsi que de réduire leur probabilité de survenue et leur impact.

37 L'enregistrement des événements doit se faire sous forme de journaux centralisés. Cette centralisation des données permet une détection, une investigation et une réponse plus rapide et efficace en cas de cyberattaque.

Ce qui appuie notre observation

Alertes de sécurité automatisées et journaux à améliorer

38 Certaines alertes automatisées n'ont pas été mises en place par les entités étudiées. De plus, nous avons observé que des améliorations concernant la collecte et la centralisation des journaux pourraient également être apportées. Pour des raisons évidentes de sécurité, nous ne présentons pas le détail des améliorations à apporter.

39 Par ailleurs, l'une des entités nous a indiqué que les journaux liés à l'un de ses systèmes critiques ne sont pas protégés contre les modifications par des personnes ayant des accès privilégiés, dont les activités se font journaliser. Cette situation pourrait empêcher la détection en temps opportun d'activités malveillantes effectuées par ces personnes.

Mesures de surveillance à améliorer

40 Les entités étudiées exercent une surveillance pour détecter les intrusions et disposent d'antivirus. Toutefois, certaines améliorations pourraient être apportées. Pour des raisons évidentes de sécurité, nous ne détaillons pas ces améliorations.

Contrôles liés aux modifications directes de données à améliorer

41 En général, ce sont les utilisateurs qui modifient des données par l'entremise d'un logiciel, mais il est également possible pour des personnes ayant des accès privilégiés d'apporter des modifications directement à partir du serveur de la base de données de ce logiciel. Il existe toutefois des risques liés à ces modifications, notamment qu'elles soient effectuées sans être enregistrées (ex. : journalisation) ou autorisées, et ainsi qu'elles ne correspondent pas aux demandes initiales.

42 Les contrôles liés aux modifications directes de données mis en place par deux des entités sont à améliorer. Par exemple, bien qu'un processus d'autorisation existe pour ces modifications, leur journalisation est incomplète. Ainsi, des modifications directes de données pourraient être effectuées, que ce soit par erreur ou par malveillance, sans être détectées.

Gestion des paramètres de configuration à améliorer

43 Des alertes peuvent être déclenchées pour aviser ceux qui surveillent les systèmes de toute modification importante non autorisée apportée à leurs paramètres de configuration. De plus, les paramètres initiaux peuvent être rétablis de façon périodique pour effacer toute modification qui aurait pu être effectuée.

44 Certaines des directions de l'une des entités ne disposent pas d'outils permettant le rétablissement automatique des paramètres de configuration initiaux. De plus, d'autres mesures de cybersécurité liées à la gestion des paramètres de configuration sont à améliorer. Pour des raisons évidentes de sécurité, nous ne présentons pas le détail des améliorations à apporter.

Configuration

Il s'agit de l'ensemble des composants matériels et logiciels déterminant les caractéristiques essentielles de fonctionnement d'un système informatique.

Documentation insuffisante des délais de réponse aux notifications de sécurité

45 Les trois entités étudiées ne documentent pas leurs délais de réponse aux notifications de sécurité. Même si, en pratique, les entités sont conscientes qu'elles doivent répondre de façon urgente à certaines de ces notifications, ce sont leurs délais de réponse qui démontrent leur capacité à réagir à l'intérieur d'un laps de temps prédéfini pour corriger les problèmes de sécurité signalés. La documentation des délais de réponse permettrait également aux entités de gérer leur performance en comparant ces délais avec leurs objectifs.

OBSERVATION 3

L'absence de certaines activités liées à la gouvernance des entités étudiées nuit à la mise en place de mesures de cybersécurité visant l'identification des risques de cyberattaques.

Qu'avons-nous observé ?

46 Les entités étudiées ne respectent pas l'ensemble des bonnes pratiques en matière de cybersécurité concernant :

- l'évaluation des menaces et des risques liés à la sécurité de l'information ;
- la mise en place d'indicateurs de gestion et l'utilisation de tableaux de bord ;
- la gestion des mesures de cybersécurité mises en place selon le niveau de criticité des actifs informationnels et l'inventaire de ces derniers ;
- le suivi des mesures de cybersécurité mises en place par les fournisseurs de services infonuagiques.

Pourquoi cette observation est-elle importante ?

47 Une évaluation des menaces et des risques liés à la sécurité de l'information doit être réalisée considérant son importance pour une gestion efficace de la cybersécurité. En effet, cette évaluation permet aux organisations de mieux comprendre les différentes menaces auxquelles elles sont confrontées et de mettre en place des mécanismes de défense pour mieux protéger leurs actifs informationnels dans un délai approprié. Elle leur permet également de cerner les risques auxquels sont exposés leurs systèmes, ainsi que d'identifier les mesures de cybersécurité appropriées pour réduire ces risques à un niveau acceptable.

48 Par ailleurs, la transmission d'une information de qualité aux instances de gouvernance permet aux organisations de surveiller l'efficacité des mesures mises en place pour contrer les cyberattaques au moment opportun. L'évaluation de l'efficacité des mesures et des processus en place s'avère particulièrement utile pour déceler des vulnérabilités et pour déterminer les besoins d'investissement prioritaires liés à la cybersécurité.

49 Afin de bien gérer les risques liés à la sécurité de l'information, les organisations doivent mettre en place des mesures de cybersécurité en fonction de la classification de leurs actifs informationnels. Un inventaire à jour de ces actifs est donc requis pour qu'une protection adéquate soit mise en place selon leur niveau de criticité.

Classification des actifs informationnels

Cette classification permet d'établir les priorités de traitement des risques en fonction du niveau de criticité des actifs informationnels en matière de disponibilité, d'intégrité et de confidentialité.

50 Les organisations qui font appel à des fournisseurs de services infonuagiques demeurent les premières responsables de la sécurité de l'information, et ce, malgré l'impartition. En effet, elles doivent convenir avec leurs fournisseurs des mesures de cybersécurité à adopter. Les organisations doivent ensuite consulter des rapports d'auditeurs externes indépendants permettant de faire le suivi de l'application de ces mesures.

Ce qui appuie notre observation

Évaluation des menaces et des risques à améliorer

51 Aucune des trois entités étudiées n'a formalisé le processus d'évaluation des menaces et des risques liés à la sécurité de l'information. Une documentation stratégique élaborée selon une méthodologie harmonisée de gestion des menaces et des risques permettrait aux entités d'avoir un portrait global de leur capacité à contrer les cyberattaques. L'une des entités nous a remis de la documentation sur les risques associés à quatre actifs informationnels critiques revus annuellement, mais elle ne tient pas de registre intégré documentant l'ensemble des menaces et des risques stratégiques associés à la cybersécurité. Une autre des entités doit terminer son évaluation des risques liés à la protection des renseignements. Quant à la troisième entité, elle a élaboré sa méthodologie d'évaluation des menaces et des risques en partenariat avec le Secrétariat du Conseil du trésor. Il lui reste toutefois à la mettre en place.

Manque d'indicateurs de gestion liés à la cybersécurité

52 La mise en place d'indicateurs de gestion dans un tableau de bord fait partie des bonnes pratiques en matière de cybersécurité. Ils permettent de renseigner les instances de gouvernance d'une organisation sur les risques liés à la sécurité de l'information et les faiblesses des mesures de cybersécurité en place, ainsi que sur les améliorations à apporter. Voici quelques exemples d'indicateurs de gestion pertinents :

- pourcentage du personnel et des contractuels ayant reçu une formation de sensibilisation à la cybersécurité ;
- pourcentage d'applications dont les vulnérabilités ont été évaluées ;
- nombre d'incidents dus à des accès non autorisés et au manque de séparation des tâches incompatibles ;
- nombre d'appareils non autorisés détectés sur les réseaux.

53 Deux des entités disposent d'indicateurs de gestion à propos des incidents de sécurité. Les autres aspects de la cybersécurité, comme la gestion des identités et des accès, la gestion des menaces et la gestion des vulnérabilités et des risques, ne sont pas couverts par des indicateurs.

54 Quant à la troisième entité, elle n'a pas terminé de définir ses indicateurs de gestion liés à la cybersécurité, et ce, malgré l'adoption de sa stratégie de cybersécurité en 2019. Toutefois, elle a amorcé les travaux pour la mise en place de son centre opérationnel de cyberdéfense et travaille actuellement sur un projet concernant la mise en place d'indicateurs de gestion supplémentaires en cybersécurité basés sur un référentiel reconnu.

55 En conséquence, les instances de gouvernance des trois entités étudiées sont actuellement privées de certains indicateurs de gestion qui les aideraient à mesurer et à améliorer l'efficacité des mesures de cybersécurité en place. Les entités n'ont donc pas en main toute l'information nécessaire pour évaluer adéquatement leur capacité à réduire les risques de cyberattaques.

Gestion des mesures de cybersécurité et de l'inventaire des actifs informationnels à améliorer

56 Aucune des entités étudiées n'a mis en place de mesures de cybersécurité correspondant au niveau de criticité de ses actifs informationnels. Par exemple, l'une des entités doit ajuster ses mesures en fonction de la nouvelle classification de ses actifs effectuée en 2020. Pour ce qui est des deux autres entités, elles ont établi leurs mesures de cybersécurité en fonction d'un référentiel reconnu, mais ces dernières ne sont pas encore appliquées. Elles affirment avoir entrepris des actions pour améliorer la situation.

57 Par ailleurs, l'une des entités n'a pas encore terminé son projet visant à centraliser l'inventaire de ses actifs, ce qui pourrait rendre plus difficile la protection de tous ses actifs critiques. De plus, l'entité n'a établi aucun mécanisme automatisé servant à détecter l'utilisation du réseau par des appareils non autorisés. Néanmoins, un projet est en cours à cet égard.

Suivi des mesures de cybersécurité des fournisseurs de services infonuagiques à améliorer

58 Deux des entités n'obtiennent pas ou ne consultent pas les rapports d'auditeurs indépendants sur la conception et l'efficacité des mesures de cybersécurité de l'ensemble de leurs fournisseurs de services infonuagiques. Même si les exigences de sécurité sont convenues dans un contrat avec chaque fournisseur, il n'en demeure pas moins que les entités n'ont aucune assurance que ces exigences sont appliquées adéquatement.

Rapport d'audit sur les mesures de cybersécurité

Il s'agit d'un rapport qui fournit l'assurance raisonnable que les mesures de cybersécurité sont appliquées par le fournisseur de services visé par le rapport. L'auditeur y exprime une opinion concernant l'efficacité des mesures et leur capacité à assurer la disponibilité, l'intégrité et la confidentialité des actifs informationnels.

OBSERVATION 4

Les mesures de cybersécurité mises en place par les entités étudiées afin de réduire leur temps de réponse et de récupération en cas de cyberattaque sont à améliorer.

Qu'avons-nous observé ?

59 Nous avons observé des possibilités d'amélioration des mesures de cybersécurité mises en place par les entités étudiées afin de réduire leur temps de réponse et de récupération en cas de cyberattaque. Ces améliorations sont liées :

- aux simulations de cyberattaques ;
- aux tests d'intrusion ;
- aux plans de continuité des services et de reprise informatique ;
- à la documentation du processus de gestion des incidents.

Pourquoi cette observation est-elle importante ?

60 Les mesures de cybersécurité visant à minimiser le temps de réponse et de récupération en cas de cyberattaque sont essentielles pour la prise en charge efficace des incidents ou l'évaluation rapide des menaces. Elles permettent également l'amélioration en continu des processus et des plans en matière de cybersécurité.

61 Les faiblesses des mesures de cybersécurité sont mises en évidence lors de simulations, de tests d'intrusion et à la suite du traitement des incidents. Il est donc fondamental que les organisations mettent à l'épreuve leurs mesures pour s'assurer de leur efficacité et de leur amélioration continue. Pour ce faire, des équipes spécialisées sont mandatées pour effectuer des simulations afin d'évaluer la capacité des organisations à contrer d'éventuelles cyberattaques. Des tests d'intrusion sont également réalisés dans le but de découvrir les faiblesses liées aux équipements réseau, aux applications ainsi qu'aux comportements des employés et des consultants sur le réseau.

62 Un plan de continuité des services permet d'éviter ou de minimiser toute interruption des services essentiels en cas de cyberattaque. Partie intégrante du plan de continuité, le plan de reprise informatique comprend les procédures à suivre et les ressources nécessaires à la remise en service des systèmes dans les délais requis.

63 Par ailleurs, il est aussi indispensable que les organisations révisent régulièrement leur processus de gestion des incidents de cybersécurité. Ce processus permet aux organisations de détecter les incidents et d'y réagir rapidement afin de réduire la durée de la non-disponibilité de leurs systèmes, ainsi que de minimiser les dommages à l'intégrité et à la confidentialité de leurs données. Par ailleurs, une analyse rétrospective de chaque incident permet de réduire les probabilités de récidives et d'améliorer les interventions.

Équipes spécialisées

Ces équipes, l'une offensive et l'autre défensive, ont pour objectif de réduire le niveau de vulnérabilité de l'organisation. Pour ce faire, l'équipe offensive utilise une technique qui consiste à adopter l'état d'esprit des pirates informatiques pour mieux tester les mesures de cybersécurité appliquées par l'équipe défensive.

Exemples d'incidents

- Exploitation d'une ou de plusieurs vulnérabilités connues, comme l'utilisation d'un identifiant générique
- Courriel non autorisé contenant des données confidentielles acheminé à l'extérieur de l'organisation
- Défaillance d'une mesure de cybersécurité, comme un coupe-feu non fonctionnel

Ce qui appuie notre observation

Simulations inexistantes ou inadéquates

64 Aucune des trois entités étudiées n'a mandaté d'équipe spécialisée pour effectuer des simulations de cyberattaques. Ces simulations permettent pourtant de mettre en lumière les forces et les faiblesses des mesures de cybersécurité en place et d'évaluer leur capacité à répondre à certaines cyberattaques potentielles. L'absence de ce type de simulation nuit donc à l'identification de certaines faiblesses importantes à corriger.

65 Bien que l'une des entités ait indiqué avoir réalisé des simulations de cyberattaques en 2020, ces dernières avaient seulement pour objectif de trouver les failles de sécurité dans les systèmes. La capacité des mesures de cybersécurité en place à répondre à certaines cyberattaques n'a donc pas été évaluée. L'entité déclare toutefois avoir commencé à en effectuer véritablement en 2021, ce qui devrait lui permettre de se conformer aux bonnes pratiques en matière de cybersécurité.

66 Les deux autres entités projettent éventuellement d'effectuer des simulations en ayant recours aux services du Centre gouvernemental de cyberdéfense.

Tests d'intrusion à améliorer

67 L'une des entités établit une planification annuelle des tests d'intrusion. Selon cette entité, le nombre de tests exécutés demeure toutefois insuffisant depuis 2019. Elle n'est donc pas à même de détecter certaines vulnérabilités et d'évaluer avec exactitude dans quelle mesure chacune d'elles représente une menace pour la sécurité de l'information. L'entité a mentionné vouloir augmenter la fréquence de ces tests.

68 Les tests d'intrusion effectués par une autre des entités au cours des dernières années étaient incomplets puisqu'ils n'étaient menés que sur les systèmes nouvellement mis en œuvre ou ayant subi des changements importants. Ainsi, un système ne faisant pas partie des deux dernières catégories, et n'ayant donc fait l'objet d'aucun test, est plus susceptible d'être vulnérable aux nouvelles menaces. Au sein de cette entité, aucune planification n'existe pour les tests d'intrusion. Elle indique toutefois vouloir en élaborer une prochainement. Elle nous a tout de même mentionné que, depuis 2020, des tests d'intrusion sont effectués en collaboration avec le Centre gouvernemental de cyberdéfense.

Plan de continuité des services incomplet et tests à améliorer

69 Les plans de continuité des services de deux des entités ne contiennent pas de stratégie de continuité liée aux cyberattaques. Pourtant, l'absence de cette stratégie en cas de panne ou de dégradation des systèmes provoquées par une cyberattaque pourrait retarder le rétablissement de ces derniers et empêcher la minimisation des dommages occasionnés. Selon l'une de ces deux entités, la révision de son plan de continuité des services est en cours. Pour sa part, l'autre entité nous a indiqué que sa stratégie de continuité était en cours de rédaction.

70 En ce qui a trait à la reprise informatique, l'une des trois entités n'a pas réalisé les tests qu'elle avait planifiés pour l'année 2020. En l'absence de ces tests, il lui est difficile de s'assurer que son plan de reprise informatique atteint les objectifs fixés et permet de respecter les délais requis.

71 Par ailleurs, le plan de reprise informatique de l'une des entités ne priorise pas la reprise de certains mécanismes de sécurité essentiels à la protection des systèmes. Toutefois, l'entité nous a mentionné travailler actuellement sur un projet qui lui permettra de corriger la situation.

72 Cette même entité a également mis en place un plan de continuité des services et un plan de reprise informatique en lien avec un système critique bénéficiant d'une infrastructure technologique indépendante. Cependant, les deux plans sont incomplets et il est donc difficile de tester leur efficacité. De ce fait, l'entité n'a pas la certitude qu'elle pourrait rétablir ce système et maintenir la continuité des services essentiels en cas de cyberattaque.

Processus de gestion des incidents à améliorer

73 Chacune des entités étudiées a mis en place un processus de gestion des incidents. Cependant, les processus s'avèrent incomplets et méritent d'être mieux documentés, d'autant plus que les bonnes pratiques en matière de cybersécurité recommandent que les étapes du processus soient documentées et mises en pratique pour permettre aux intervenants d'agir rapidement et avec précision en cas d'incident.

74 Des critères qui aident à signaler, dans les meilleurs délais, les événements liés à la sécurité de l'information gagneraient à être documentés et mis à jour régulièrement. D'autres critères qui permettent de décider si ces événements doivent être classés comme des incidents à traiter rapidement doivent être précisés.

75 En raison de ce manque d'information, les entités pourraient ne pas être en mesure de réduire efficacement les risques d'incidents ou de les contrer.

RECOMMANDATIONS

76 Le Vérificateur général a formulé des recommandations à l'intention des trois entités étudiées. Celles-ci sont présentées ci-dessous. Nous invitons l'ensemble des entités gouvernementales à s'en inspirer étant donné que ces recommandations peuvent s'appliquer à plusieurs d'entre elles.

1 Renforcer leurs mesures de cybersécurité afin de se protéger efficacement contre d'éventuelles cyberattaques.

2 Améliorer leurs mesures de cybersécurité de façon à détecter efficacement les cyberattaques.

3 Veiller à ce que leurs activités de gouvernance permettent un meilleur encadrement de l'évaluation des risques et de la reddition de comptes.

4 Améliorer leurs mesures de cybersécurité afin de réduire leur temps de réponse et de récupération en cas de cyberattaque.

COMMENTAIRES DES ENTITÉS

Le Secrétariat du Conseil du trésor a eu l'occasion de transmettre ses commentaires en son nom et au nom des trois entités étudiées. Nous tenons à souligner que le Secrétariat et les entités étudiées ont adhéré à toutes nos recommandations.

Commentaires du Secrétariat du Conseil du trésor

« Le Secrétariat du Conseil du trésor (SCT) et les entités étudiées accueillent favorablement les recommandations du Vérificateur général portant sur la gestion de la cybersécurité. Celles-ci sont cohérentes avec les priorités du gouvernement et les actions que les entités étudiées ont entreprises au cours des dernières années en la matière.

« La protection des renseignements confidentiels et la sécurité de l'information revêtent une très grande importance considérant l'augmentation constante des risques de cyberattaques ainsi que du niveau de sophistication de ces dernières. Pour cette raison, le SCT va intégrer les observations du Vérificateur général dans un plan d'action visant l'amélioration de la cybersécurité pour l'ensemble des organisations gouvernementales du Québec. L'objectif du SCT est que l'ensemble de l'appareil gouvernemental soit mieux protégé et puisse mieux détecter d'éventuelles cyberattaques. »

RENSEIGNEMENTS ADDITIONNELS

Objectif de l'étude et portée des travaux

Rôles et responsabilités des entités étudiées

Principales mesures de cybersécurité

Objectif de l'étude et portée des travaux

Objectif de l'étude

La présente étude fait partie du tome de novembre 2021 du *Rapport du Vérificateur général du Québec à l'Assemblée nationale pour l'année 2021-2022.*

Nous avons réalisé une étude s'appuyant sur des critères d'appréciation basés sur des référentiels reconnus de bonnes pratiques en matière de cybersécurité (CIS, ISO/CEI 27 002, NIST 800-53). Pour ce faire, nous avons recueilli les éléments probants suffisants et appropriés pour formuler nos observations.

Notre étude est basée sur les critères que nous avons jugés valables dans les circonstances et qui sont exposés ci-après.

Objectif de l'étude	Critères d'appréciation
Déterminer si les mesures nécessaires pour contrer le plus efficacement possible les risques de cyberattaques existent dans les trois entités étudiées.	1. Les entités ont mis en place des mesures de cybersécurité visant l'**identification** des risques de cyberattaques, notamment : ■ une planification stratégique de la cybersécurité ; ■ un cadre normatif ; ■ une évaluation des menaces et des risques revue périodiquement ; ■ une gestion des actifs informationnels, incluant leur classification ; ■ une reddition de comptes aux instances concernées. 2. Les entités ont mis en place des mesures de cybersécurité pour assurer leur **protection** contre les cyberattaques. Ces mesures concernent : ■ la gestion des accès externes et des accès privilégiés, y compris l'authentification ; ■ la sécurité des données ; ■ la sécurité des applications ; ■ la gestion des vulnérabilités et des correctifs ; ■ la gestion des paramètres de configuration ; ■ la sécurité des réseaux ; ■ la gestion, la sensibilisation et la formation des ressources humaines. 3. Les entités ont mis en place des mesures de cybersécurité visant la **détection** des cyberattaques, comme : ■ l'examen des journaux et des alertes de sécurité ; ■ la surveillance continue des systèmes. 4. Les entités ont mis en place des mesures de cybersécurité visant à **répondre** et à **récupérer** efficacement en cas de cyberattaque, comme : ■ les tests réguliers des plans de reprise informatique ; ■ les simulations périodiques de cyberattaques avec des équipes spécialisées.

Nos travaux ont été menés en vertu de la *Loi sur le vérificateur général*.

Le Vérificateur général applique la Norme canadienne de contrôle qualité 1. Ainsi, il maintient un système de contrôle qualité 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. Au cours de ses travaux, le Vérificateur général s'est conformé aux règles sur l'indépendance et aux autres règles de déontologie prévues dans son code de déontologie.

Portée des travaux

Le présent rapport a été achevé le 24 septembre 2021.

Il porte sur les mesures de cybersécurité mises en place par trois entités.

Nos travaux concernent principalement la conception, la mise en œuvre et le maintien des mesures mises en place par les trois entités. Nos travaux ne remettent pas en cause l'efficacité de ces mesures et les niveaux de criticité des actifs informationnels convenus dans le registre de classification. Nous n'avons pas effectué de tests d'intrusion ni de balayage de vulnérabilités. De plus, le but de cette étude n'était pas de prendre connaissance de l'existence de contrôles visant à compenser les faiblesses des mesures qui pourraient être améliorées.

Nous avons réalisé des entrevues auprès de gestionnaires et de professionnels des entités. Nous leur avons également fait remplir un questionnaire. De plus, nous avons analysé divers documents ainsi que des données provenant de différents systèmes d'information des entités.

Nos travaux se sont déroulés d'octobre 2020 à mars 2021 et portent principalement sur la dernière année financière. Toutefois, certains travaux peuvent avoir trait à des situations antérieures ou postérieures à cette période.

Rôles et responsabilités des entités étudiées

Les principaux rôles et responsabilités des entités étudiées à l'égard des enjeux liés à la cybersécurité sont présentés ci-après.

Règlement sur la diffusion de l'information et sur la protection des renseignements personnels	■ Mettre sur pied un comité sur l'accès à l'information et la protection des renseignements personnels ; ■ Veiller à la sensibilisation et à la formation des membres de son personnel et de son personnel de direction ou d'encadrement sur les obligations et les pratiques en matière d'accès à l'information et de protection des renseignements personnels.
Directive sur la sécurité de l'information gouvernementale	■ Adopter et mettre en œuvre une politique et un cadre de gestion de la sécurité de l'information, les maintenir à jour et assurer leur application ; ■ Déposer au dirigeant principal de l'information, selon une périodicité bisannuelle : — une planification des actions de sécurité de l'information, — un bilan de sécurité de l'information ; ■ S'assurer de la mise en œuvre des processus formels de sécurité de l'information permettant, notamment, d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents ; ■ Déclarer au dirigeant principal de l'information les risques de sécurité de l'information à portée gouvernementale ; ■ Déclarer à l'équipe de réponse aux incidents de sécurité de l'information de l'Administration québécoise les incidents de sécurité de l'information à portée gouvernementale ; ■ S'assurer de la réalisation d'un audit de sécurité de l'information, selon une périodicité bisannuelle ou à la suite d'un changement majeur susceptible d'avoir des conséquences sur la sécurité de l'information gouvernementale, et en dégager les priorités d'action ainsi que les échéanciers afférents ; ■ S'assurer de la réalisation de tests d'intrusion et de vulnérabilité chaque année ; ■ S'assurer de la mise en place d'un registre d'autorité de la sécurité de l'information ; ■ Définir et mettre en place un programme formel et continu de formation et de sensibilisation du personnel en matière de sécurité de l'information.
Cadre gouvernemental de gestion de la sécurité de l'information	■ Assigner les principales responsabilités (ex. : responsable organisationnel de la sécurité de l'information, responsable de l'architecture de sécurité de l'information, responsable de l'accès à l'information et de la protection des renseignements personnels, administrateur des accès).
Politique gouvernementale de cybersécurité	■ Gouverner la cybersécurité par une vision globale et concertée ; ■ Placer le personnel au cœur de la cybersécurité ; ■ Assurer la protection et la résilience des services publics et des échanges électroniques gouvernementaux ; ■ Être proactif à l'égard des menaces émergentes ; ■ Miser sur les forces d'un réseau gouvernemental de cyberdéfense ; ■ Tirer profit d'une expertise de pointe en cybersécurité ; ■ Préserver la confiance des citoyennes et citoyens à l'égard de la sécurité de leurs données.

Principales mesures de cybersécurité

La figure 4 présente les principales mesures de cybersécurité réparties selon les quatre fonctions suivantes : identification, protection, détection, et réponse et récupération.

FIGURE 4 Répartition des mesures et des catégories de mesures de cybersécurité selon leur fonction[1]

Identification	Protection	Détection	Réponse et récupération
Description			
Développer une compréhension de l'environnement informatique de l'organisation pour gérer les risques de cyberattaques	Développer et implanter des mesures pour protéger l'environnement informatique de l'organisation et garantir la continuité des services essentiels à sa bonne marche	Développer et implanter les mesures appropriées pour détecter les cyberattaques	Développer et implanter les mesures appropriées : ■ pour gérer immédiatement les cyberattaques une fois détectées ■ pour maintenir un plan de continuité à la suite d'une cyberattaque
Catégories de mesures			
■ Gouvernance de la cybersécurité ■ Environnements informatiques interne et externe ■ Stratégie, évaluation et gestion des risques ■ Gestion des actifs	■ Accès et authentification ■ Sécurité des données ■ Technologies de protection ■ Maintenance ■ Procédures et processus de protection de l'information ■ Formation et sensibilisation	■ Anomalies et événements ■ Contrôle continu de la sécurité ■ Processus de détection	■ Plan de réponse aux incidents ■ Communication ■ Analyse ■ Mitigation ■ Plan de récupération après un incident ■ Amélioration
Exemples de mesures			
■ Encadrement ■ Surveillance	■ Gestion des identités et des accès ■ Sécurité des données ■ Gestion du développement applicatif sécuritaire ■ Gestion des vulnérabilités ■ Gestion des configurations ■ Sécurité des réseaux ■ Gestion des ressources humaines	■ Journalisation des activités ■ Gestion des alertes de sécurité	■ Gestion des incidents de sécurité ■ Gestion de la continuité des services

1. Le éléments présentés dans cette figure sont inspirés du référentiel sur la cybersécurité du NIST.

Les principales mesures de cybersécurité sont décrites sommairement ci-après. Ces mesures doivent être adaptées à l'environnement et aux objectifs de chaque organisation, ainsi qu'à ses risques liés à la sécurité de l'information.

Identification

Encadrement : L'encadrement est une étape particulièrement importante tout au long du processus de cybersécurité. Cette étape comprend notamment :

- une planification stratégique de la cybersécurité ;
- la mise en place d'un cadre normatif en cybersécurité (ex. : cadre de gestion, directives) ;
- une évaluation des menaces et des risques revue périodiquement ;
- une gestion des actifs informationnels, incluant leur classification ;
- une reddition de comptes aux instances concernées ;
- une gestion des actifs informationnels hébergés par des tiers.

Surveillance : La haute direction d'une organisation doit entre autres être informée des cyberattaques en temps opportun et s'assurer de l'efficacité des mesures de cybersécurité mises en place par son organisation et les fournisseurs dont elle retient les services. Elle doit également mettre en place des indicateurs de gestion et les mesurer périodiquement. Cette surveillance permet d'apporter des améliorations au processus de cybersécurité. La direction de l'audit interne de l'organisation peut être mise à contribution en menant des travaux sur la cybersécurité.

Protection

Gestion des identités et des accès : Cette mesure permet de déterminer qui a accès à quelle information pendant une période donnée. Elle vise notamment à donner l'assurance que les accès octroyés aux utilisateurs sont autorisés selon le principe de moindre privilège et ne sont pas incompatibles. Ce principe implique que les accès des utilisateurs doivent être strictement restreints aux actifs informationnels dont ils ont besoin pour effectuer leurs tâches, rien de plus. En ce qui concerne l'authentification des utilisateurs, l'authentification par simple mot de passe s'avère insuffisante de nos jours, particulièrement pour la connexion à distance ou pour le personnel des technologies de l'information. Ainsi, selon le niveau de risque, une double authentification peut s'avérer nécessaire, par exemple un mot de passe combiné à une empreinte digitale ou à une autorisation donnée à partir d'un appareil mobile. La gestion des identités et des accès informatiques a récemment été abordée plus en détail dans le *Rapport du Vérificateur général du Québec à l'Assemblée nationale pour l'année 2020-2021* publié en juin 2020.

Sécurité des données : Cette mesure vise principalement à protéger l'information confidentielle. Voici quelques exemples de méthodes pouvant être utilisées :

- Techniques de prévention des pertes et des fuites de données : techniques qui permettent de relever, de contrôler et de protéger les informations sensibles grâce à des analyses de contenu, que les informations soient en mouvement, traitées ou stockées.
- Chiffrement : opération qui consiste à remplacer un texte clair par un texte inintelligible et inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale (ex. : protocole de transfert hypertexte ou réseau privé virtuel [« *VPN* » en anglais]). Cette opération est particulièrement importante pour protéger les informations qui transitent sur le Web et qui ne devraient pas être visibles.

Gestion du développement applicatif sécuritaire : Cette mesure vise entre autres à vérifier que les développeurs ne laissent pas, intentionnellement ou involontairement, des vulnérabilités aux différentes étapes du cycle de développement d'une application. Ceux-ci doivent respecter les bonnes pratiques liées à la sécurité des applications, telles que :

- l'analyse du code de programmation et la réalisation de tests sur celui-ci pour s'assurer que les pratiques de développement sécurisé sont respectées ;
- l'identification des menaces avant la conception de l'application ;
- la séparation des environnements de développement et de tests ;
- la documentation du fonctionnement de l'application.

La gestion du développement applicatif sécuritaire vise également à déterminer si :

- les bonnes pratiques en matière de cybersécurité sont appliquées, si elles fonctionnent comme prévu et si elles ont été mises en place à tous les endroits nécessaires ;
- l'application a été développée selon les bonnes pratiques en matière de cybersécurité.

Gestion des vulnérabilités : Cette mesure vise entre autres à assurer une vigilance continue (appelée « balayage ») des failles, du code de programmation et de la configuration d'un système. Par exemple, les éditeurs de logiciels apportent des correctifs à leurs produits lorsqu'ils découvrent des failles dans ceux-ci, puis proposent une mise à jour à leurs clients. L'application des correctifs doit s'effectuer rapidement, car les pirates informatiques cherchent constamment à découvrir les vulnérabilités des systèmes.

Gestion des configurations : Cette mesure vise entre autres la mise en place de procédures qui permettent de contrôler les changements apportés aux systèmes, notamment à la suite d'incidents et d'alertes.

Sécurité des réseaux : Cette mesure vise à protéger les réseaux internes et externes d'une organisation pour assurer la protection de ses actifs informationnels. À cet effet, plusieurs outils peuvent être employés, notamment les suivants :

- Coupe-feu : logiciel ou matériel informatique qui permet de filtrer l'information circulant entre l'ordinateur, le Web et les réseaux de l'organisation, et ainsi de bloquer ou d'autoriser des connexions.
- Système de prévention d'intrusion et système de détection d'intrusion : logiciel visant à détecter en temps réel les tentatives d'intrusion dans les réseaux internes ou dans les ordinateurs. Par exemple, il analyse les données suspectes, détecte les débits de transmission de données trop importants et évalue le nombre d'utilisateurs connectés.
- Antivirus : logiciel destiné à découvrir et à éradiquer les logiciels malveillants. La mise à jour rapide de l'antivirus est essentielle pour assurer la protection de l'organisation contre les nouvelles techniques des logiciels malveillants.
- Test d'intrusion : test consistant à simuler des attaques pour mettre en lumière les faiblesses des réseaux internes et externes, ainsi que des systèmes et des applications.

Gestion des ressources humaines : Cette mesure concerne notamment l'embauche de personnes compétentes et les enquêtes de bonnes mœurs pour les postes critiques. Elle comprend également l'éducation continue, soit la formation et la sensibilisation à la sécurité de l'information. Elle est d'autant plus importante qu'elle vise l'être humain, qui peut constituer un maillon faible de la chaîne de contrôle, notamment lorsqu'il est ciblé par un acte de piratage psychologique.

Détection

Journalisation des activités : La journalisation permet de garder des traces des événements informatiques générés par les utilisateurs des systèmes. Les différentes activités journalisées sont déterminées par l'organisation. Par exemple, elle peut décider de journaliser les activités des administrateurs des technologies de l'information, les opérations influant les bases de données, ainsi que les activités provenant des systèmes de détection d'intrusion et des coupe-feu.

Système de gestion de l'information et des événements de sécurité

Il s'agit d'un outil spécialisé qui permet de centraliser et de corréler les données provenant de plusieurs sources, notamment des alertes et des journaux provenant des coupe-feu, des serveurs ainsi que des systèmes de prévention et de détection d'intrusion.

Gestion des alertes de sécurité : Les alertes de sécurité servent à signaler les anomalies qui doivent être portées à l'attention de l'organisation sur-le-champ pour qu'elle puisse agir rapidement si nécessaire. Ces alertes sont d'abord enregistrées dans les journaux et doivent être gérées à l'aide d'une autre mesure de cybersécurité, soit la gestion des incidents de sécurité. Par exemple, une alerte peut signaler la création du compte d'un administrateur des technologies de l'information, la destruction de journaux, l'exfiltration de données hors du réseau ou des tentatives échouées d'accès à des données confidentielles.

Réponse et récupération

Gestion des incidents de sécurité : Cette mesure vise à donner l'assurance que l'exploitation normale des services est rétablie le plus rapidement possible pendant ou après un incident de sécurité (ex. : attaque d'un pirate informatique provocant un déni de service), et que les répercussions sur l'organisation touchée sont réduites au minimum. La mise en place d'une procédure de communication à différents paliers d'intervenants (ex. : haute direction, gestionnaires, autres ministères et organismes concernés) pourrait s'avérer nécessaire selon la gravité de l'incident. Par ailleurs, une analyse rétrospective de l'incident permet de réduire les probabilités de récidive et d'améliorer les interventions. Voici quelques exemples d'incidents :

Déni de service

Cyberattaque consistant à submerger de requêtes un système informatique dans le but de le rendre inopérant et d'en bloquer l'accès aux utilisateurs légitimes.

- modification non autorisée des paramètres de configuration ;
- anomalies soulevées par le système de détection d'intrusion ;
- nombreuses tentatives d'accès à une base de données.

Gestion de la continuité des services : Cette mesure permet notamment d'établir un plan de continuité des services essentiels. L'organisation doit élaborer des stratégies afin que le risque que les systèmes soient indisponibles soit réduit à un niveau acceptable. Le plan de continuité comprend un plan de reprise informatique. La reprise informatique a déjà été abordée plus en détail dans le *Rapport du Vérificateur général du Québec à l'Assemblée nationale pour l'année 2018-2019* publié en mai 2018.