CAN/CIOSC 104:2021
NORME NATIONALE DU CANADA

Contrôles de cybersécurité de base des petites et moyennes organisations

03.100.01; 35.030

Page laissée intentionnellement vierge

Table des matières

Introduction ..... **vii**

1 Portée **1**

2 Références normatives **1**

3 Termes et définitions **1**

4 Contrôles organisationnels **6**

4.1 Direction 6

4.2 Responsabilité 6

4.3 Sensibilisation en matière de cybersécurité 7

4.4 Évaluation des risques de cybersécurité 8

5 Contrôles de base **9**

5.1 Plan d'intervention en cas d'incident 9

5.2 Application automatique de correctifs aux applications et systèmes d'exploitation 10

5.3 Activation des logiciels de sécurité 11

5.4 Configuration des appareils pour assurer la sécurité 11

5.5 Utilisation d'une authentification robuste des utilisateurs 12

5.6 Sauvegarde et chiffrement des données 13

5.7 Établissement de défenses de base sur le périmètre 14

5.8 Contrôle et autorisation de l'accès 15

6 Contrôles de base propres à l'environnement d'exploitation **15**

6.1 Sécurité des services mobiles 15

6.2 Sécurité des services infonuagiques et des services de TI externalisés 17

6.3 Sécurité des sites Web 18

6.4 Sécurité des supports amovibles 18

6.5 Systèmes de points de vente et systèmes financiers 19

6.6 Gestion des journaux de sécurité informatique 19

Annexe A (informative) **21**

A. Modèle de plan d'intervention en cas d'incident 21

Annexe B (normative) **28**

B. Questionnaire d'évaluation des risques de cybersécurité 28

Bibliographie **30**

Page laissée intentionnellement vierge

Avant-propos

Le Conseil stratégique des DPI (CSDPI) est un organisme sans but lucratif offrant une tribune nationale aux membres des secteurs public et privé qui s'emploient à transformer, à façonner et à orienter l'écosystème canadien de l'information et de la technologie.

Ses normes sont élaborées conformément aux *Exigences et lignes directrices – Accréditation des organismes d'élaboration de normes* (13 juin 2019) du Conseil canadien des normes (CCN).

Il est à noter que certains éléments de la présente norme peuvent faire l'objet de droits de brevet. Le CSDPI ne saurait être tenu responsable de ne pas avoir indiqué ces droits. Les droits de propriété intellectuelle identifiés lors de l'élaboration de la présente norme figurent dans l'introduction.

Pour en savoir plus sur le CSDPI :

Conseil stratégique des DPI
1000 Innovation Dr., bureau 500,
Ottawa (Ontario) K2K 3E7
ciostrategycouncil.com

Les Normes nationales du Canada sont élaborées par les organismes titulaires de l'accréditation du CCN, conformément aux exigences et lignes directrices de ce dernier. On trouvera des renseignements supplémentaires sur les Normes nationales du Canada au www.ccn.ca.

Le CCN est une société d'État qui fait partie du portefeuille d'Innovation, Sciences et Développement économique Canada (ISDE). Pour améliorer la compétitivité économique du Canada et le bien-être collectif de la population canadienne, le CCN dirige et facilite l'élaboration et l'utilisation des normes nationales et internationales. Il coordonne aussi la participation du Canada à l'élaboration des normes et définit des stratégies pour promouvoir les efforts de normalisation canadiens.

Le CCN fournit des services d'accréditation à divers clients, dont des organismes de certification de produits, des laboratoires d'essai et des organismes d'élaboration de normes. La liste des programmes du CCN et des organismes accrédités peut être consultée sur le site www.ccn.ca.

Page laissée intentionnellement vierge

Introduction

Voici la première version de la norme CAN/CIOSC 104:2021, *Contrôles de cybersécurité de base des petites et moyennes organisations*.

Cette norme a été élaborée par le Comité technique 5 (TC 5) du Conseil stratégique des DPI sur la cybersécurité, qui se compose de plus de 140 grands penseurs et experts en cybersécurité et en sujets connexes. Elle a été approuvée par un groupe avec droit de vote formé par le Comité technique comprenant 3 producteurs, 3 représentants du secteur public, d'un organisme de réglementation ou d'un organisme responsable des politiques, 3 utilisateurs et 3 représentants de la collectivité.

Toutes les unités de mesure utilisées sont exprimées conformément au Système international d'unités (SI). La norme sera soumise à l'examen du Comité technique au plus tard un an après sa date de publication, à la suite de quoi elle pourra être rééditée, révisée, confirmée ou abandonnée.

Bien que son but premier soit énoncé sous la rubrique « Portée », il est important de retenir qu'il incombe à l'utilisateur de juger si elle convient à une application donnée.

La norme est conçue pour être utilisée dans l'évaluation de la conformité.

Utilisation du présent document

Idéalement, les organisations investissent en cybersécurité de manière à équilibrer leurs risques en la matière et leurs objectifs opérationnels. Cependant, comme les petites organisations ne disposent pas des ressources nécessaires pour concevoir des plans de cybersécurité personnalisés, la présente norme décrit des contrôles de sécurité (à appliquer) dont elles peuvent se servir comme base.

Les exigences présentées sont divisées en deux niveaux : 1 et 2.

Les exigences de niveau 1 s'adressent aux petites organisations pour qui la cybersécurité est un domaine nouveau. Ces organisations n'ont généralement pas assez de ressources pour investir en TI ou utiliser des services de TI externalisés, et ne possèdent qu'une connaissance de base de la cybersécurité.

Les exigences de niveau 2 s'ajoutent à celles de niveau 1 à mesure qu'une organisation gagne en maturité et renforce sa posture de cybersécurité. Pour adopter les exigences de niveau 2, une organisation doit avoir mis en œuvre celles de niveau 1, connaître les fondements de la cybersécurité et les risques connexes qui les concernent, et chercher à s'améliorer dans ce domaine.

ICS 03.100.01; 35.030

THIS NATIONAL STANDARD OF CANADA IS AVAILABLE IN BOTH FRENCH AND ENGLISH.

Page laissée intentionnellement vierge

Contrôles de cybersécurité de base des petites et moyennes organisations

1 Portée

La présente norme établit les contrôles de cybersécurité minimaux à l'intention des petites et moyennes organisations, lesquelles comptent généralement moins de 500 employés.

NOTE 1 : Les organisations comptant plus de 500 employés peuvent aussi se fonder sur la présente norme pour améliorer leur posture de cybersécurité. Elles devront déterminer si leur contexte justifie des investissements supplémentaires en la matière.

NOTE 2 : Les organisations (de toutes tailles) qui traitent des renseignements personnels, confidentiels, sensibles ou financiers, qui ont besoin d'une haute disponibilité de leurs systèmes ou qui servent des secteurs à risque élevé (ex. : infrastructure critique ou défense) peuvent nécessiter des contrôles de cybersécurité supplémentaires ou avoir des exigences dépassant la portée du présent document. Chaque organisation doit évaluer ses propres besoins.

NOTE 3 : Il est recommandé aux organisations de toujours considérer la sécurité physique comme un élément essentiel de leur programme de cybersécurité, mais compte tenu de la complexité de la tâche et des ressources nécessaires, ce travail dépasse la portée de la présente norme.

2 Références normatives

La présente norme renvoie aux documents suivants de telle sorte qu'une partie ou la totalité de leur contenu constitue une exigence normative. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, c'est la dernière édition des documents mentionnés qui s'applique (y compris les éventuelles modifications).

Open Web Application Security Project (OWASP), *Top 10 Vulnerabilities*.

Conseil des normes de sécurité PCI, *Norme de sécurité des données de l'industrie des cartes de paiement* (PCI DSS).

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent :

accès non autorisé
Accès à un réseau physique ou logique, à un système ou à des données sans autorisation.

accès protégé Wi-Fi
Protocole de sécurité et programme de certification de la sécurité conçus par la Wi-Fi Alliance pour protéger les réseaux informatiques sans fil.

[SOURCE : ISO 20415:2019]

application de correctifs
Mise à jour d'un logiciel ou d'un micrologiciel.

atteinte à la vie privée
Incident impliquant la perte réelle ou présumée d'information personnelle.

atteinte aux données
Incident de cybersécurité où une personne s'empare d'une information sensible sans l'autorisation du propriétaire.

authentification à facteurs multiples
Méthode d'*authentification* qui exige, pour vérifier l'identité de l'utilisateur, une combinaison de facteurs (deux ou plus) : quelque chose que l'utilisateur connaît (ex. : mot de passe) ou possède (ex. : jeton physique), ou un attribut physique (ex. : biométrie).

chiffrement
Modification de la forme de l'information pour en cacher le contenu et empêcher l'accès non autorisé.

[SOURCE : Centre canadien pour la cybersécurité]

code malveillant
Programme ou code écrit pour recueillir de l'information sur un système ou un utilisateur, détruire des données de système, faciliter une intrusion plus en profondeur dans un système, falsifier des données ou des rapports de système, ou créer des nuisances ralentissant les opérations du système et les activités du personnel de maintenance.

NOTE 1 : Une attaque par code malveillant prend diverses formes : virus, ver, cheval de Troie ou autre exploit automatisé.

NOTE 2 : Les codes malveillants sont aussi souvent appelés « maliciels ».

[SOURCE : IEC/TS 62443-1-1:2009]

confidentialité
Capacité à protéger l'information sensible contre l'accès non autorisé.

confirmation des caractéristiques biologiques ou comportementales
Méthode de vérification de l'identité qui se fonde sur des caractéristiques biologiques (anatomie et physiologie; ex. : visage, empreintes digitales, rétines) ou comportementales (ex. : rythme de la frappe au clavier, démarche) pour prouver que la personne présentant des renseignements sur une identité est bien celle qui possède cette identité.

NOTE : La confirmation des caractéristiques biologiques ou comportementales se fait par un

protocole de sommation et réponse : les caractéristiques consignées dans un dossier ou une base de données sont comparées à celles de la personne qui présente les renseignements sur l'identité.

[SOURCE : CAN/CIOSC 103-1:2020]

défaillance du réseau (généralisée)
Incident portant atteinte à la confidentialité, à l'intégrité ou à la disponibilité d'un réseau.

défaillance du système d'applications
Incident portant atteinte à la confidentialité, à l'intégrité ou à la disponibilité d'une application.

déni de service
Voir « interruption de service ».

devrait/devraient
Indication d'une possibilité de choix avec une préférence marquée; équivalent à « il est fortement recommandé ».

divulgation non autorisée
Incident portant atteinte à la confidentialité, à l'intégrité ou à la disponibilité de données.

DMARC
Protocole d'authentification des courriels, abrégé de l'anglais *domain-based message authentication, reporting & conformance*. Il permet au propriétaire d'un domaine de courriel donné de protéger son domaine contre une utilisation non autorisée, couramment appelée « usurpation par courriel ».

doit/doivent
Indication d'une exigence pour la conception ou l'application d'une méthode d'essai.

droit d'accès minimal
Principe selon lequel on n'accorde à l'utilisateur que les autorisations d'accès dont il a besoin pour accomplir les tâches autorisées. Ce principe limite les dommages pouvant résulter d'une utilisation non autorisée, incorrecte ou accidentelle d'un système d'information.

[SOURCE : Centre canadien pour la cybersécurité]

gestion de la mobilité d'entreprise
Ensemble de systèmes gérant des services ou des dispositifs informatiques mobiles pour une organisation.

gestionnaire de mots de passe
Programme informatique permettant à l'utilisateur de stocker, de produire et de gérer des mots de passe pour des applications locales et des services en ligne. Il aide à produire et à récupérer des mots de passe complexes en les stockant dans une base de données chiffrée ou en les calculant sur demande.

incident de cybersécurité
Tentative non autorisée, réussie ou non, d'accéder à une ressource de système ou à un réseau informatique, de le modifier, de le détruire, de le supprimer ou de le rendre inutilisable.

information sensible
Information devant être protégée contre la divulgation non autorisée.

intégrité
Capacité à protéger l'information contre la modification et la suppression non autorisées.

interruption de service
Incident empêchant l'accès à un service ou perturbant autrement le fonctionnement normal.

maliciel
Logiciel malveillant conçu pour infiltrer ou endommager un système informatique. En voici quelques formes courantes : virus, ver, cheval de Troie, logiciel espion et logiciel publicitaire.

[SOURCE : Centre canadien pour la cybersécurité, *Glossaire*]

OWASP
Open Web Application Security Project.

pare-feu
Barrière de sécurité entre deux périmètres contrôlant le volume et les types de trafic autorisé à passer de l'un à l'autre.

perte d'information
Voir « divulgation non autorisée ».

peut/peuvent
Indication d'une possibilité de choix avec une préférence implicite.

plan d'intervention en cas d'incident
Document établissant les processus, les procédures et les documents portant sur la façon dont l'organisation détecte les incidents, intervient et se rétablit en cas d'incident. Les cybermenaces, les catastrophes naturelles et les pannes imprévues sont des exemples d'incidents qui touchent les réseaux, systèmes et appareils des organisations.

[SOURCE : Centre canadien pour la cybersécurité]

préjudice
Dommage subi par une organisation lorsque ses systèmes et actifs informatiques sont compromis.

rançongiciel
Type de *maliciel* empêchant un utilisateur d'accéder à un système ou à des données jusqu'à ce qu'il ait versé des fonds ou remis un bien matériel ou virtuel.

réseau local sans fil (WLAN)/(Wi-Fi)
Technologie de réseautage local sans fil qui permet la connexion d'appareils électroniques au réseau, principalement au moyen des bandes radio de 2,5 GHz et de 5 GHz.

NOTE 1 : « Wi-Fi » est une marque de commerce de la Wi-Fi Alliance.

NOTE 2 : « Wi-Fi » est couramment utilisé comme synonyme de « WLAN », puisque la plupart des réseaux WLAN modernes reposent sur les normes du Wi-Fi.

[SOURCE : ISO/IEC 27033-6:2016]

réseau privé virtuel (**VPN)**
Réseau informatique logique à utilisation restreinte construit à partir des ressources d'un réseau physique en faisant appel au chiffrement ou en mettant sous tunnel des liaisons du réseau virtuel à travers le réseau réel.

[SOURCE : ISO/IEC 18028-3:2005]

service ayant des répercussions
Service ayant des répercussions humaines, p. ex. finances, soutien (ou assistance), logement, éducation, recrutement et prestations.

service mobile sécurisé
Sécurité d'un appareil mobile (ex. : téléphone cellulaire, tablette).

support amovible sécurisé
Sécurité d'un support amovible (ex. : clé USB).

système de noms de domaine (DNS)
Nomenclature distribuée et hiérarchisée mondiale servant à identifier les entités connectées à Internet.

NOTE : Les domaines de premier niveau sont au sommet de la hiérarchie.

[SOURCE : ISO/TR 14873:2013]

TI
Technologies de l'information.

utilisation non autorisée
Utilisation d'un réseau physique ou logique, d'un système ou de données sans autorisation.

4 Contrôles organisationnels

4.1 Direction

4.1.1 Contexte

4.1.1.1 La haute direction de l'organisation est ultimement responsable du programme de cybersécurité.

4.1.2 Exigences de niveau 1

4.1.2.1 La haute direction doit montrer l'importance qu'elle accorde au programme de cybersécurité :

a) en veillant à l'établissement d'une politique et d'objectifs de cybersécurité harmonisés à l'orientation stratégique de l'organisation;

b) en veillant à la disponibilité des ressources nécessaires au programme de cybersécurité et à leur harmonisation avec les politiques et les objectifs de cybersécurité;

c) en communiquant l'importance d'une cybersécurité efficace et du respect des exigences du programme de cybersécurité;

d) en établissant des indicateurs pour évaluer le programme de cybersécurité et en surveillant les progrès;

e) en aidant les autres gestionnaires concernés à faire preuve de leadership dans leurs domaines de responsabilité.

4.1.3 Exigences de niveau 2

4.1.3.1 Toutes les exigences de cet article sont considérées comme étant de niveau 1.

4.2 Responsabilité

4.2.1 Contexte

4.2.1.1 Il incombe à la haute direction de l'organisation de définir clairement les rôles et les responsabilités essentiels à la mise en place des contrôles de cybersécurité de base.

4.2.2 Exigences de niveau 1

4.2.2.1 Toutes les exigences de cet article sont considérées comme étant de niveau 2.

4.2.3 Exigences de niveau 2

4.2.3.1 La haute direction doit nommer un membre de l'équipe de direction pour surveiller la sécurité des TI de l'organisation et en rendre compte. Celui-ci doit avoir au moins les responsabilités

suivantes :

a) Élaborer et mettre en place un programme de cybersécurité qui couvre les contrôles de base et s'applique à toute l'organisation.

b) Rédiger et diffuser les politiques et procédures concernant la sécurité de l'information.

c) Coordonner la création et la mise en place d'un programme de sensibilisation et de formation sur la sécurité de l'information qui s'applique à toute l'organisation.

d) Coordonner l'intervention en cas d'atteinte réelle ou présumée à la confidentialité, à l'intégrité ou à la disponibilité des données de l'organisation.

e) Recenser les risques organisationnels et en prioriser la prise en compte selon leur probabilité et leurs répercussions potentielles.

4.3 Sensibilisation en matière de cybersécurité

4.3.1 Contexte

4.3.1.1 Bon nombre d'incidents de cybersécurité impliquent encore une erreur humaine commise durant l'utilisation de systèmes d'information.

4.3.2 Exigences de niveau 1

4.3.2.1 L'organisation doit former ses employés sur les pratiques de sécurité de base en se concentrant notamment sur les mesures suivantes, concrètes et faciles à appliquer :

a) Utilisation de politiques de mot de passe efficaces (voir l'article 5.5)

b) Repérage des courriels et liens malveillants

c) Utilisation de logiciels approuvés

d) Utilisation appropriée d'Internet

e) Utilisation sécuritaire des médias sociaux

4.3.3 Exigences de niveau 2

4.3.3.1 L'organisation doit investir dans la sensibilisation et la formation régulières et continues de ses employés sur la cybersécurité.

4.4 Évaluation des risques de cybersécurité

4.4.1 Contexte

4.4.1.1 L'évaluation des risques de cybersécurité fait partie du cadre dont se sert l'organisation pour recenser, comprendre, prioriser et gérer les risques de cybersécurité qui menacent ses systèmes et actifs de données. Elle facilite la détermination du préjudice potentiel lié à la confidentialité, à l'intégrité et à la disponibilité des systèmes et actifs de données.

4.4.1.2 L'évaluation des risques de cybersécurité aide l'organisation à cerner les menaces et les vulnérabilités préoccupantes et à établir des contrôles de sécurité appropriés pour veiller à la continuité de la prestation des services.

NOTE : L'organisation peut effectuer l'évaluation des risques de cybersécurité elle-même ou faire appel à un tiers.

4.4.2 Exigences de niveau 1

4.4.2.1 L'organisation doit remplir le questionnaire d'évaluation des risques de cybersécurité figurant à l'annexe B.

4.4.3 Exigences de niveau 2

4.4.3.1 Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation doit mener une évaluation des risques de cybersécurité et coordonner la mise en place de contrôles protégeant contre les risques potentiels.

NOTE 1 : Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation devrait demander à des experts d'examiner et de commenter son évaluation des risques de cybersécurité et le choix des contrôles visant à protéger l'organisation contre les risques cernés et évalués.

NOTE 2 : L'organisation peut envisager d'installer des contrôles physiques, mesure qu'elle ajouterait à son cadre pour atténuer les risques de cybersécurité.

4.4.3.2 L'organisation doit dresser et tenir à jour la liste de ses actifs et systèmes d'information. Pour tout actif et système exclus de sa mise en place des contrôles de cybersécurité de base, elle doit consigner cette décision.

4.4.3.3 Les risques de cybersécurité acceptés par l'organisation doivent être consignés et approuvés par un cadre supérieur de l'organisation.

4.4.3.4 L'organisation doit évaluer ses dépenses en TI et ses investissements en sécurité des TI (chiffres bruts et pourcentage des dépenses totales).

4.4.3.5 L'organisation doit évaluer la part de son effectif qui travaille en TI et en sécurité des TI (chiffres bruts et pourcentage de l'effectif total).

4.4.3.6 L'organisation doit s'engager à améliorer progressivement sa cybersécurité.

4.4.3.7 L'organisation doit déterminer les déclencheurs et les seuils de réalisation d'une nouvelle évaluation des risques de cybersécurité ou de révision d'une évaluation existante.

4.4.3.8 Quels que soient les résultats de l'évaluation des risques de cybersécurité, l'organisation doit mettre en place les contrôles fondamentaux ou de base décrits à l'article 5 ainsi que ceux décrits à l'article 6 qui s'appliquent à son environnement opérationnel.

4.4.3.9 L'organisation doit périodiquement revoir et/ou tester les contrôles fondamentaux de cybersecurité afin d'en assurer l'efficacité. Les tests et/ou les revues doivent être effectués au minimum une fois par année, ou lorsque des modifications majeures aux systèmes ont lieu.

5 Contrôles de base

5.1 Plan d'intervention en cas d'incident

5.1.1 Contexte

5.1.1.1 L'organisation doit avoir un plan d'intervention en cas d'incident pour être prête à gérer efficacement les incidents de sécurité. Le présent article décrit un plan modèle; il définit la structure du plan, les rôles et les responsabilités, les types d'incidents communs et les démarches de préparation, d'identification, d'endiguement, d'éradication, de reprise et d'examen des bilans visant à réduire les conséquences des incidents.

L'organisation peut engager un fournisseur de services gérés ou un autre tiers compétent pour soutenir l'exécution du plan d'intervention en cas d'incident.

5.1.2 Exigences de niveau 1

5.1.2.1 L'organisation doit avoir un plan d'intervention en cas d'incident visant des incidents de gravités diverses. Elle devrait aussi avoir un plan pour les types d'incidents qu'elle est incapable de gérer elle-même.

5.1.2.2 Le plan d'intervention en cas d'incident doit établir les personnes responsables de la gestion des incidents et comprendre les coordonnées des parties externes, intervenants et organismes de réglementation pertinents. L'organisation doit rendre accessible une version papier à jour de ce plan au cas où il deviendrait impossible d'accéder à la version numérique.

NOTE : L'organisation devrait établir la méthode de communication avec les parties concernées (internes et externes) en cas d'incident.

5.1.2.3 L'organisation devrait envisager de souscrire à une police d'assurance en matière de cybersécurité qui couvre les activités d'intervention et de reprise en cas d'incident, et justifier

sa décision de ne pas souscrire à une telle police, le cas échéant.

5.1.2.4 L'organisation peut utiliser le modèle de plan d'intervention en cas d'incident (annexe A) pour se conformer aux exigences de l'article 5.1.2.

5.1.3 Exigences de niveau 2

5.1.3.1 Toutes les exigences de cet article sont considérées comme étant de niveau 1.

5.2 Application automatique de correctifs aux applications et systèmes d'exploitation

5.2.1 Contexte

5.2.1.1 Les fournisseurs de TI diffusent régulièrement des mises à jour (correctifs) pour leurs logiciels et micrologiciels afin d'en corriger les défauts et d'en éliminer les vulnérabilités. Le suivi manuel des vulnérabilités associées aux divers éléments d'un réseau demande beaucoup de temps et d'argent. Pour une grande organisation, la gestion des vulnérabilités et des correctifs est un moyen efficace, malgré les coûts, de réduire les risques de cybersécurité.

5.2.1.2 Une petite ou moyenne organisation a la possibilité d'activer la mise à jour automatique de ses logiciels et de son matériel, si une telle option est offerte, ou d'envisager de remplacer ses produits par d'autres offrant cette option. Cette mesure comprend le remplacement des logiciels et du matériel qui ne sont plus visés par des mises à jour parce que le fournisseur ne les prend plus en charge (c.-à-d. des produits ayant terminé leur vie utile). L'organisation s'assure ainsi que ses appareils autonomes, systèmes d'exploitation, applications et logiciels de sécurité sont à jour et exempts de vulnérabilités connues.

5.2.2 Exigences de niveau 1

5.2.2.1 L'organisation doit installer les correctifs de sécurité les plus récents pour l'ensemble de ses logiciels et de son matériel afin de protéger ses actifs contre les vulnérabilités connues.

5.2.2.2 L'organisation doit activer l'application automatique de correctifs pour l'ensemble de ses logiciels et de son matériel, et consigner tous les cas où elle décide de ne pas le faire.

NOTE 1 : Ceci comprend la totalité des serveurs, ordinateurs portables et de bureau, tablettes, téléphones cellulaires et équipement réseau.

NOTE 2 : L'organisation devrait avoir un processus opérationnel assurant la mise à jour manuelle régulière des logiciels et du matériel ne pouvant être mis à jour automatiquement.

NOTE 3 : L'organisation peut établir une procédure d'essai pour assurer que les correctifs ne causent aucune perturbation des activités opérationnelles dans les cas où l'analyse des risques détermine qu'il s'agit d'une mesure judicieuse de réduction des risques.

5.2.2.3 L'organisation doit effectuer une évaluation des risques pour déterminer s'il y a lieu de remplacer les systèmes pour lesquels l'application automatique des correctifs est impossible.

5.2.3 Exigences de niveau 2

5.2.3.1 Toutes les exigences de cet article sont considérées comme étant de niveau 1.

5.3 Activation des logiciels de sécurité

5.3.1 Contexte

5.3.1.1 L'organisation a la possibilité de se protéger contre les menaces posées par les maliciels connus (ex. : virus, vers, chevaux de Troie, rançongiciels, logiciels espions) en configurant et en activant des logiciels antivirus et antimaliciels sur tous les appareils connectés, autant que possible, de manière à assurer la sécurité.

NOTE : L'organisation peut activer tout pare-feu logiciel des appareils de son réseau ou installer et configurer une solution similaire donnant le même résultat.

5.3.2 Exigences de niveau 1

5.3.2.1 L'organisation doit activer des antimaliciels qui se mettent à jour automatiquement et empêchent l'exécution des maliciels sans intervention de l'utilisateur.

5.3.3 Exigences de niveau 2

5.3.3.1 Pour cette section, toutes les exigences sont considérées être de niveau 1.

5.4 Configuration des appareils pour assurer la sécurité

5.4.1 Contexte

5.4.1.1 Les mots de passe administrateur par défaut et les paramètres par défaut qui n'assurent pas la sécurité sont un problème important pour les réseaux d'une organisation. Les fournisseurs et même les revendeurs configurent souvent les appareils avec des mots de passe administrateur établis par défaut, lesquels deviennent souvent publics.

5.4.1.2 L'organisation a la possibilité de modifier tous les mots de passe administrateur des appareils. Cette mesure lui donne aussi l'occasion de vérifier les paramètres par défaut de l'appareil (qui n'assurent peut-être pas la sécurité) pour désactiver les fonctions superflues et activer les fonctions de sécurité nécessaires. Elle peut aussi envisager d'appliquer un profil de configuration sécuritaire comme les Benchmarks du Center for Internet Security, ou d'engager un fournisseur de services de TI ou de services de sécurité gérés qui s'en chargera pour elle.

5.4.2 Exigences de niveau 1

5.4.2.1 L'organisation doit configurer tous ses appareils de sorte à assurer sa sécurité, en :

a) modifiant tous les mots de passe par défaut.

5.4.3 Exigences de niveau 2

5.4.3.1 L'organisation doit configurer tous ses appareils de sorte à assurer sa sécurité, en :

a) désactivant toutes les fonctions superflues (ex. : bloquer les ports inutiles, désactiver les services inutiles, supprimer les logiciels inutiles ou désuets);

b) activant toutes les fonctions de sécurité pertinentes.

NOTE : Il pourrait être impossible d'activer ou de désactiver des fonctions sur certains appareils.

5.5 Utilisation d'une authentification robuste des utilisateurs

5.5.1 Contexte

5.5.1.1 Dans ses politiques d'authentification des utilisateurs, l'organisation est en mesure de veiller à équilibrer la sécurité et la convivialité. Les pratiques d'excellence de l'industrie reposent sur l'authentification à facteurs multiples. Il s'agit d'une combinaison de choses que l'utilisateur connaît (ex. : mot de passe) ou possède (ex. : jeton physique, code généré par une application, appel téléphonique automatisé à un numéro préétabli), ou d'attributs physiques (ex. : biométrie). Les solutions d'authentification à facteurs multiples diffèrent dans leur protection, mais toutes améliorent la posture de cybersécurité globale d'une organisation.

5.5.2 Exigences de niveau 1

5.5.2.1 L'organisation doit mettre en place l'authentification à facteurs multiples, et consigner tous les cas où elle est incapable de le faire ou décide de ne pas le faire.

5.5.2.2 L'organisation doit exiger la modification du mot de passe dans tous les cas présumés ou prouvés de compromission.

5.5.2.3 L'organisation doit avoir des politiques claires sur la longueur et la réutilisation des mots de passe, l'utilisation de gestionnaires de mots de passe et les conditions auxquelles doit satisfaire un utilisateur pour consigner et conserver un mot de passe en toute sécurité.

NOTE : L'organisation peut se baser sur les lignes directrices concernant le choix des mots de passe du *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information* du Centre de la sécurité des télécommunications.

5.5.3 Exigences de niveau 2

5.5.3.1 L'organisation doit se doter d'un gestionnaire de mots de passe ou consigner sa décision de ne pas le faire.

NOTE : Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032) - https://www.cyber.gc.ca/fr/orientation/pratiques-exemplaires-de-creation-de-phrases-de-passe-et-de-mots-de-passeitsap30032

5.6 Sauvegarde et chiffrement des données

5.6.1 Contexte

5.6.1.1 La sauvegarde des données est essentielle pour une reprise rapide après un incident de cybersécurité (ex. : attaque de rançongiciel ou de maliciel), mais aussi en cas de catastrophe naturelle, de défaillance de l'équipement ou de vol.

5.6.1.2 La sauvegarde est aussi utile lorsque l'accès aux systèmes est impossible ou lorsque les données ou renseignements pourraient avoir été falsifiés.

5.6.2 Exigences de niveau 1

5.6.2.1 L'organisation doit déterminer au cas par cas quels logiciels et données opérationnels (y compris l'information sensible) sont essentiels à son fonctionnement ainsi que la fréquence de modification de ces renseignements.

NOTE : Par exemple, les postes de travail et serveurs essentiels pourraient nécessiter une sauvegarde incrémentielle quotidienne, tandis que les ordinateurs de bureau pourraient être restaurés à partir d'une image commune.

5.6.2.2 L'organisation doit décider pour chaque système la nécessité de la sauvegarde et la fréquence de celle-ci, le cas échéant, puisque les exigences de sauvegarde et de reprise diffèrent.

5.6.2.3 L'organisation doit sauvegarder ses systèmes contenant des données opérationnelles essentielles et vérifier le fonctionnement adéquat et efficace de ses mécanismes de reprise.

5.6.2.4 L'organisation doit remplacer régulièrement les sauvegardes et les conserver dans un emplacement externe sécurisé (lieu physique ou service infonuagique) pour être en mesure de les récupérer en cas de catastrophe (incendie, inondation, tremblement de terre ou incident de cybersécurité localisé).

5.6.2.5 L'organisation devrait envisager de chiffrer ses sauvegardes en veillant à ce que la clé soit récupérable et conservée en sécurité. La clé et les sauvegardes non chiffrées, le cas échéant, devraient être conservées en sécurité et n'être accessibles qu'aux employés ou agents autorisés.

5.6.3 Exigences de niveau 2

5.6.3.1 L'organisation doit tester régulièrement ses procédures de reprise sur un échantillon des données sauvegardées pour vérifier l'intégrité de l'ensemble du processus de sauvegarde et de restauration.

5.7 Établissement de défenses de base sur le périmètre

5.7.1 Contexte

5.7.1.1 Il faut protéger tout réseau connecté à Internet des menaces numériques au moyen d'un pare-feu, soit un logiciel ou un appareil qui surveille le trafic et est capable de défendre le réseau contre les intrusions. Un pare-feu DNS (système de noms de domaine) empêche la connexion aux domaines malveillants connus. Il existe des solutions pour tous les appareils connectés au réseau d'une organisation.

5.7.2 Exigences de niveau 1

5.7.2.1 Toutes les exigences de cet article sont considérées comme étant de niveau 2.

5.7.3 Exigences de niveau 2

5.7.3.1 L'organisation doit avoir un pare-feu entre deux périmètres pour contrôler le volume et les types de trafic qui peut circuler entre ces périmètres.

5.7.3.2 L'organisation devrait envisager de mettre en place un pare-feu DNS pour les requêtes DNS dirigées vers Internet.

5.7.3.3 L'organisation doit activer tout pare-feu logiciel des appareils de son réseau ou consigner toute mesure mise en place au lieu de ces pare-feu.

5.7.3.4 L'organisation doit exiger une connexion chiffrée à toutes ses ressources de TI et une connexion VPN avec authentification à facteurs multiples pour tout accès à distance à ses réseaux.

5.7.3.5 L'organisation doit utiliser un réseau Wi-Fi sécurisé, minimalement de type WPA2-AES et préférablement de type WPA2-Enterprise ou WPA3-Enterprise, qui respecte les exigences de l'article 5.5 sur les mots de passe.

5.7.3.6 L'organisation devrait segmenter ses réseaux de sorte que les réseaux accessibles à la clientèle ou au public soient séparés (ou isolés) des réseaux opérationnels.

5.7.3.7 L'organisation doit veiller à l'application du protocole DMARC dans ses services de courriel.

5.7.3.8 L'organisation doit veiller à la mise en place du filtrage des courriels.

5.8 Contrôle et autorisation de l'accès

5.8.1 Contexte

5.8.1.1 Le respect du principe du droit d'accès minimal, c'est-à-dire une utilisation limitée aux fonctions nécessaires, améliore la posture de cybersécurité de l'organisation.

5.8.2 Exigences de niveau 1

5.8.2.1 Toutes les exigences de cet article sont considérées comme étant de niveau 2.

5.8.3 Exigences de niveau 2

5.8.3.1 L'organisation ne doit accorder aux comptes que l'accès aux fonctions nécessaires à l'accomplissement des tâches et restreindre les privilèges d'administrateur à ceux qui en ont besoin.

5.8.3.2 L'organisation doit révoquer l'accès aux comptes et aux fonctions lorsque celui-ci n'est plus nécessaire à l'accomplissement des tâches.

5.8.3.3 L'organisation doit réserver l'utilisation des comptes administrateur aux activités administratives (et interdire les activités typiques d'utilisateur comme l'accès aux courriels et la navigation sur le Web).

5.8.3.4 L'organisation devrait envisager de mettre en place un système centralisé de contrôle des autorisations.

6 Contrôles de base propres à l'environnement d'exploitation

6.1 Sécurité des services mobiles

6.1.1 6.1.1 Contexte

6.1.1.1 Les appareils mobiles comme les téléphones cellulaires sont essentiels pour la plupart des organisations. Il revient à chacune d'elles de choisir le modèle de propriété qu'elle adoptera pour ces appareils. Habituellement, soit elle fournit aux employés un appareil, soit elle les autorise à utiliser leur propre appareil. Dans les deux cas, l'organisation doit prendre des mesures pour sécuriser l'accès à son information sensible et à son infrastructure de TI à partir de ces appareils.

6.1.1.2 Il existe de nombreuses solutions pour séparer les données professionnelles des données personnelles (applications, comptes de courriel, contacts, etc.) sur les appareils mobiles, que ceux-ci appartiennent à l'organisation ou aux employés. Ces solutions vont de l'utilisation d'applications différentes pour le travail et la vie privée à l'emploi de dossiers sécurisés natifs ou de fonctions de verrouillage pour l'information sensible de l'organisation. Il importe que l'organisation détermine comment créer cette séparation d'une manière qui équilibre ses besoins opérationnels et en matière de sécurité.

6.1.1.3 Les applications améliorent parfois grandement les capacités et la productivité des appareils mobiles, mais sont aussi susceptibles de créer un risque. Une organisation ayant une infrastructure et des processus opérationnels de TI matures peut choisir d'utiliser une solution de gestion de la mobilité d'entreprise lui permettant d'améliorer ses activités et sa gestion des appareils mobiles. Les solutions de ce type ont diverses capacités, mais offrent en général des fonctions de gestion, de vérification et de prise en charge des appareils mobiles utilisés au travail. Certaines peuvent aussi effacer à distance les données sur les appareils.

6.1.2 Exigences de niveau 1

6.1.2.1 Toutes les exigences de cet article sont considérées comme étant de niveau 2.

6.1.3 Exigences de niveau 2

6.1.3.1 L'organisation qui utilise des services mobiles (ex. : téléphones cellulaires) doit choisir un modèle de propriété pour les appareils mobiles et consigner ses raisons et les risques connexes.

6.1.3.2 L'organisation qui utilise des services mobiles (ex. : téléphones cellulaires) doit :

a) exiger la séparation entre les données professionnelles et personnelles sur les appareils mobiles ayant accès à ses ressources de TI et consigner les détails de cette séparation;

b) veiller à ce que les employés ne téléchargent des applications qu'à partir de la liste de sources de confiance qu'elle aura établie;

c) exiger que les appareils mobiles stockent l'information sensible sous une forme chiffrée sécurisée;

d) envisager de mettre en œuvre une solution de gestion de la mobilité d'entreprise sur les appareils mobiles et, si elle choisit de ne pas le faire, consigner les risques qu'elle assume en ce qui concerne la vérification, la gestion et les fonctions de sécurité des appareils;

e) encourager ou contraindre les utilisateurs à :

- désactiver la connexion automatique aux réseaux ouverts;
- éviter la connexion aux réseaux Wi-Fi inconnus;
- limiter l'utilisation de la technologie Bluetooth et de la communication en champ proche pour la transmission d'information sensible;
- utiliser le réseau Wi-Fi de l'organisation ou le réseau cellulaire plutôt qu'un réseau Wi-Fi public;

f) envisager d'utiliser un mode sécurisé (ex. : VPN, bureau virtuel) pour la connexion aux réseaux Wi-Fi publics et, si elle choisit de ne pas le faire, donner ses raisons.

6.2 Sécurité des services infonuagiques et des services de TI externalisés

6.2.1 Contexte

6.2.1.1 Une organisation a généralement recours à un fournisseur tiers de services de TI ou de services gérés pour ses besoins de stockage et de traitement infonuagiques, la gestion ou l'hébergement de son site Web et la gestion de ses systèmes de paiement en ligne. Il est important qu'elle tienne compte de son seuil de tolérance aux risques quant à la réglementation en vigueur aux endroits où ses fournisseurs stockent ou utilisent son information sensible.

6.2.2 Exigences de niveau 1

6.2.2.1 L'organisation qui utilise des services infonuagiques ou des services de TI externalisés doit évaluer son seuil de tolérance au risque quant aux méthodes utilisées par ses fournisseurs pour accéder à son information sensible et traiter celle-ci.

6.2.3 Exigences de niveau 2

6.2.3.1 L'organisation qui utilise des services infonuagiques ou des services de TI externalisés doit :

a) exiger de ses fournisseurs de services infonuagiques qu'ils présentent un rapport SSAE 18 de l'Association of International Certified Professional Accountants (AICPA) ou un document équivalent indiquant qu'ils se conforment aux principes des services Trust, ou une analyse documentée expliquant pourquoi ils ne le font pas;

   NOTE : C'est l'organisation qui détermine l'équivalence avec la norme SSAE 18 de l'AICPA.

b) évaluer son seuil de tolérance aux risques quant aux régimes juridiques applicables au stockage et à l'utilisation de son information sensible par ses fournisseurs;

c) veiller à ce que son infrastructure de TI et ses utilisateurs communiquent de façon sécurisée avec les applications et services infonuagiques;

d) veiller à ce que les comptes administrateur des services infonuagiques utilisent une méthode d'authentification à facteurs multiples et soient différents des comptes administrateur internes.

6.3 Sécurité des sites Web

6.3.1 Contexte

6.3.1.1 Il est possible de veiller à la sécurité de ses sites Web en tenant compte des 10 principales vulnérabilités relevées par l'Open Web Application Security Project (OWASP) : injection, violation d'authentification, exposition de données sensibles, entités XML externes, violation du contrôle de l'accès, mauvaise configuration de la sécurité, vulnérabilité aux scripts intersites, désérialisation non sécurisée, utilisation d'éléments ayant des vulnérabilités connues, et journalisation et surveillance insuffisantes.

6.3.1.2 Il peut être utile pour l'organisation de comprendre dans quelle mesure appliquer la norme de vérification de sécurité des applications (Application Security Verification Standard, ASVS) de l'OWASP pour chacun de ses sites Web; il peut aussi s'agir d'une exigence de clients.

6.3.1.3 La conformité à l'ASVS peut faire partie des exigences contractuelles relatives aux sites Web externalisés. L'organisation peut aussi se préparer à investir dans la conformité à ces exigences pour ses sites Web conçus et exploités à l'interne.

6.3.2 Exigences de niveau 1

6.3.2.1 Toutes les exigences de cet article sont considérées comme étant de niveau 2.

6.3.3 Exigences de niveau 2

6.3.3.1 L'organisation qui déploie des sites Web doit veiller à ce que ses sites tiennent compte des 10 principales vulnérabilités relevées par l'OWASP.

NOTE : Pour une liste complète des outils de détection des vulnérabilités, consulter la page « Vulnerability Scanning Tools » du site Web de l'OWASP.

6.3.3.2 L'organisation doit s'assurer de comprendre dans quelle mesure appliquer l'ASVS de l'OWASP pour chacun de ses sites Web.

6.4 Sécurité des supports amovibles

6.4.1 Contexte

6.4.1.1 Les supports amovibles, comme les disques durs portatifs, les clés USB et les cartes mémoire flash sont pratiques pour transférer des fichiers entre les appareils. Cependant, comme ils sont petits et portatifs, ils sont susceptibles d'être perdus ou volés, ce qui pourrait entraîner une atteinte aux données et l'infiltration de fichiers malveillants dans le réseau de l'organisation. Comme il peut être difficile d'en empêcher toute utilisation, l'organisation peut n'autoriser que celle de lecteurs chiffrés commerciaux qu'elle fournit. Elle devrait envisager d'employer des outils lui permettant de contrôler les accès et de surveiller les fichiers transférés.

6.4.1.2 Il importe que l'organisation assure un contrôle strict des dispositifs de stockage, y compris les supports amovibles. Ce contrôle comprend l'élimination adéquate de ces supports.

6.4.2 Exigences de niveau 1

6.4.2.1 L'organisation qui utilise des supports amovibles doit n'autoriser que l'utilisation des supports amovibles sécurisés lui appartenant.

6.4.3 Exigences de niveau 2

6.4.3.1 L'organisation qui utilise des supports amovibles doit :

a) en assurer un contrôle strict;

b) exiger l'utilisation du chiffrement sur tous les supports;

c) prévoir des processus pour le nettoyage ou la destruction des supports avant leur élimination.

6.5 Systèmes de points de vente et systèmes financiers

6.5.1 Contexte

6.5.1.1 Il importe que l'organisation isole ses systèmes de points de vente et ses systèmes financiers de l'Internet et des autres parties de son réseau au moyen d'un pare-feu pour protéger ses actifs de données.

6.5.2 Exigences de niveau 1

6.5.2.1 L'organisation qui utilise des systèmes de points de vente et des systèmes financiers doit se conformer à la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) et isoler ces systèmes d'Internet.

6.6 Gestion des journaux de sécurité informatique

6.6.1 Contexte

6.6.1.1 La collecte, l'analyse et la gestion de journaux font partie intégrante des bonnes pratiques de TI et sont fondamentales pour la vérification des contrôles de sécurité des TI et la gestion des incidents. Quelle que soit sa taille, l'organisation devrait avoir une politique de gestion des journaux répondant à ses besoins. Plusieurs types de journaux sont possibles : registre des connexions des utilisateurs, des accès aux fichiers ou aux données, ou de l'état de la configuration des appareils ou des comptes utilisateur, indiquant par exemple les logiciels installés et leur version; registre du pare-feu ou du système de détection d'intrusion; etc.

6.6.2 Exigences de niveau 1

6.6.2.1 Toutes les exigences de cet article sont considérées comme étant de niveau 2.

6.6.3 Exigences de niveau 2

6.6.3.1 L'organisation doit avoir une bonne compréhension de ses capacités et de ses besoins en matière de journalisation de sécurité, et avoir une politique de gestion connexe adéquate.

NOTE : La publication *NIST SP 800-92, Guide to Computer Security Log Management* présente des éléments à prendre en compte dans la gestion des journaux de sécurité, accompagnés d'exemples. L'une des étapes cruciales pour élaborer l'approche de gestion des journaux et des incidents est de connaître les données accessibles et les lacunes.

Annexe A
(informative)

A. Modèle de plan d'intervention en cas d'incident

A.1 Portée

A.1.1 Le présent plan d'intervention en cas d'incident s'applique à l'ensemble des réseaux, systèmes, données et membres de l'organisation, y compris tout employé, entrepreneur et fournisseur qui accède à ces réseaux, systèmes et données. Les membres de l'organisation qui peuvent avoir à diriger l'équipe d'intervention en cas d'incident ou à en faire partie doivent prendre connaissance de ce plan et se préparer à collaborer en vue de réduire au minimum les conséquences des incidents sur l'organisation.

A.1.2 Le présent plan constitue pour l'organisation un moyen d'établir ses capacités de traitement des incidents et d'intervention, ainsi que les mesures à prendre en réponse aux incidents de sécurité courants.

A.2 Exigences

A.2.1 Tout employé, entrepreneur, consultant, salarié temporaire ou autre membre de l'organisation et de ses filiales qui se rend compte d'un incident de cybersécurité ou de la possibilité d'un tel incident doit immédiatement en informer son superviseur et le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation.

A.2.2 Les renseignements suivants sont notés lors du signalement d'un incident de sécurité réel ou potentiel (ex. : intrusion) :

a) Déroulement de l'incident

b) Endroit de l'incident (ex. : service de l'organisation)

c) Moment de l'incident

d) Manière et moment de la découverte de l'incident

e) Type d'incident (si connu)

f) Équipement ou partie de l'environnement de TI touché

g) Mesures correctives prises (le cas échéant)

A.2.3 Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation examine les circonstances de l'incident réel ou potentiel, lequel est signalé dès sa découverte, et les renseignements ci-dessus sont consignés.

A.2.4 L'organisation enquête sur tout signalement d'incident de sécurité en suivant les étapes standard (préparation, identification, endiguement, éradication, reprise, bilan) ou un processus équivalent (ci-après, le processus de gestion des incidents de sécurité) :

a) Préparation

i) L'organisation conserve une version papier du plan d'intervention en cas d'incident, en plus de sa version numérique, pour en assurer l'accessibilité quel que soit l'état de l'infrastructure de TI interne.

NOTE : La politique de conservation de l'organisation prévoit des exigences et des obligations concernant la conservation des documents et des dossiers et les contrôles de vérification.

ii) Le plan d'intervention en cas d'incident est révisé chaque année et après chaque incident.

iii) Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation établit à l'avance la composition de l'équipe requise pour mettre en œuvre le processus de gestion des incidents de sécurité (ci-après, « l'équipe d'intervention en cas d'incident de sécurité »).

iv) La composition de l'équipe d'intervention en cas d'incident de sécurité est indiquée dans le plan d'intervention en cas d'incident.

v) Tout employé, entrepreneur, consultant, travailleur temporaire ou autre de l'organisation, y compris les membres de l'équipe d'intervention en cas d'incident de sécurité, est formé convenablement de sorte qu'il comprenne le processus de gestion des incidents de sécurité et le rôle qu'il a à y jouer.

vi) Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation organise des exercices de formation annuels sur les incidents de sécurité en collaboration avec l'équipe d'intervention en cas d'incident de sécurité.

NOTE : Ces exercices permettent à l'équipe d'intervention en cas d'incident de sécurité d'acquérir une connaissance préalable des types d'incidents et d'être prête à répondre aux éléments connus de sorte à pouvoir se concentrer sur les éléments inconnus, et de mettre à l'essai de manière exhaustive le plan, l'équipe et les outils.

vii) Les documents sur l'environnement de TI de l'organisation (renseignements de référence, sur les dépendances et sur les fournisseurs) sont tenus à jour et accessibles en tout temps.

b) Identification

i) Tout employé, entrepreneur, consultant, travailleur temporaire ou autre membre de l'organisation, y compris les membres de l'équipe d'intervention en cas d'incident de sécurité, se renseigne sur les types d'incidents de sécurité suivants :

- Utilisation ou accès non autorisé
- Interruption ou déni de service
- Code malveillant
- Défaillance du réseau (généralisée)
- Défaillance du système d'applications
- Divulgation non autorisée ou perte d'information
- Atteinte à la vie privée
- Atteinte aux données ou à la sécurité de l'information
- Autre (tout autre incident touchant les réseaux, systèmes ou données)

ii) Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation détermine la gravité (voir le tableau 1) de l'incident selon les facteurs suivants : nombre de systèmes touchés, caractère essentiel des systèmes touchés, nombre de personnes et d'équipes touchées (jusqu'à la totalité de l'organisation), nombre de secteurs d'activité touchés et conséquences de l'incident. Il examine le contexte opérationnel pertinent et les autres activités en cours de l'organisation pour bien comprendre les conséquences et l'urgence de la prise de mesures correctives.

iii) Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation examine l'information disponible pour déterminer l'importance connue des conséquences et la comparer à son ampleur estimée en tenant compte de la possibilité et de la rapidité de propagation. Il évalue les conséquences potentielles pour l'organisation sur le plan des finances, de la marque, de la réputation, etc.

NOTE : L'incident de sécurité peut résulter d'une menace simple ou sophistiquée ou d'une attaque automatisée ou manuelle, ou être un acte de nuisance ou de vandalisme.

iv) Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation détermine s'il y a présence d'une vulnérabilité et d'un

exploit, si des signes révèlent quelle vulnérabilité est exploitée et s'il existe un correctif. Il détermine aussi s'il s'agit d'une nouvelle menace (du jour zéro) ou d'une menace connue, et estime le travail d'endiguement requis.

Catégorie	Indicateurs	Portée
1 – Critique	Perte de données, maliciel	Généralisée, serveurs critiques ou fuite de données
2 – Élevé	Menace théorique devenue active	Généralisée, serveurs critiques ou fuite de données
3 – Modéré	Hameçonnage par courriel ou infection active en propagation	Généralisée
4 – Faible	Maliciel ou hameçonnage	Un seul hôte ou une seule personne

Tableau 1 : Gravité des incidents

v) Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation prépare un plan de communication en cas d'incident de sécurité qui demeurera facilement accessible en cas d'un tel incident et contient les coordonnées du personnel de l'organisation, de l'équipe d'intervention en cas d'incident de sécurité et des tierces parties pertinentes, comme la compagnie d'assurance en matière de cybersécurité.

vi) Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation évalue la situation et détermine s'il y a eu atteinte à la vie privée en répondant aux deux questions suivantes :

- **L'incident touche-t-il des renseignements personnels identificatoires?** Pour vérifier s'il y a atteinte à la vie privée, il faut déterminer le type de renseignements touchés par l'incident.

- **Y a-t-il eu divulgation non autorisée?** Qu'elle ait été intentionnelle, involontaire ou de nature criminelle, une divulgation non autorisée constitue une atteinte à la vie privée.

NOTE 1 : Si la réponse aux deux questions est « oui », il y a eu atteinte à la vie privée.

NOTE 2 : S'il y a eu atteinte à la vie privée, l'organisation peut être tenue de le signaler à l'autorité compétente.

vii) Ayant déterminé le type et la gravité de l'incident et s'il y a eu atteinte à la vie privée, le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation est en mesure de confirmer si un incident de sécurité s'est produit. Le cas échéant, les étapes suivantes du plan d'intervention en cas d'incident sont effectuées.

viii) Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation réunit immédiatement l'équipe d'intervention en cas d'incident de sécurité pour préciser la nature de l'incident et recueillir des données à son sujet.

ix) L'équipe d'intervention en cas d'incident de sécurité établit la priorité de l'incident et consigne l'information recueillie et les décisions, notamment :

- le signalement initial, le type et la gravité de l'incident, la détermination concernant l'atteinte à la vie privée, et les mesures prises;
- l'analyse des précurseurs et des indicateurs;
- les incidents de sécurité connus apparemment semblables;
- tout acteur, mécanisme, application, vecteur d'attaque possible et tout autre renseignement facilitant l'endiguement et l'éradication de la cause profonde de l'incident.

c) Endiguement

i) L'équipe d'intervention en cas d'incident de sécurité consigne tout renseignement obtenu et toute mesure prise durant l'endiguement de l'incident, qui comprend les interventions suivantes :

- Circonscrire immédiatement l'incident, dans la mesure du possible, en isolant l'infrastructure touchée.
- Déterminer la source de l'incident, notamment la vulnérabilité exploitée.
- Corriger immédiatement toute vulnérabilité cernée ou mettre en place des solutions de contournement pour pallier les systèmes touchés.
- Évaluer en continu les conséquences et les préjudices, et confirmer la portée de l'incident.
- Déterminer les changements de l'environnement (fichiers, connexions, processus, comptes, accès, etc.).
- Obtenir, conserver, mettre en sécurité et consigner les preuves, et préserver la chaîne de possession.

d) Éradication

i) L'équipe d'intervention en cas d'incident de sécurité consigne tout renseignement obtenu et toute mesure prise durant l'éradication des conséquences de l'incident, qui comprend les interventions suivantes :

- Éliminer toute trace de l'incident.
- Déterminer et atténuer les vulnérabilités relevées durant l'enquête, qu'elles aient été exploitées ou non lors de l'incident.
- Éliminer le maliciel, le virus, le matériel inapproprié et tout autre élément introduit pendant l'incident. Au besoin, suivre les processus de restauration de la sauvegarde pour assurer l'absence de code malveillant dans l'environnement.
- S'il y a découverte d'autres appareils touchés dans l'environnement, reprendre les étapes d'identification et d'endiguement pour ces appareils.
- Poursuivre les recherches et l'enquête jusqu'à ce que l'ensemble du vecteur d'attaque soit compris.
- Enfin, prendre les mesures nécessaires pour empêcher la récurrence de l'incident.

e) Reprise

i) L'équipe d'intervention en cas d'incident de sécurité consigne tout renseignement obtenu et toute mesure prise durant la reprise après l'incident, qui comprend les interventions suivantes :

- Ramener un à un les systèmes touchés à l'état opérationnel de manière à rétablir le fonctionnement en limitant le risque de récurrence de l'incident.
- Surveiller étroitement chaque système remis en service ainsi que tout appareil en périphérie du réseau pour s'assurer que l'incident ne se reproduit pas ou n'est pas encore en cours.
- Veiller à restaurer les systèmes à partir d'une source de confiance non infectée.
- Vérifier que les systèmes touchés fonctionnent normalement.

- Mettre en place une surveillance supplémentaire pour repérer toute activité future associée à l'incident, au besoin.

f) Bilan

i) Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation est chargé de produire un rapport de suivi sur l'incident de sécurité.

ii) Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation organise une réunion avec l'équipe d'intervention en cas d'incident dans les deux semaines pour faire le bilan de l'incident et passer en revue le rapport produit. Cette réunion devrait donner lieu, entre autres, aux résultats suivants :

- Analyse détaillée du déroulement de l'incident décrit dans le rapport
- Description des circonstances de la découverte de l'incident (comment, quand, par qui)
- Description de la portée et de la gravité de l'incident
- Analyse des méthodes d'endiguement et d'éradication de l'incident
- Liste des améliorations possibles en prévision d'incidents futurs
- Attribution des responsabilités relatives au suivi de ces améliorations

iii) Les résultats de la réunion sont consignés et conservés avec les documents sur l'incident de sécurité.

Annexe B
(normative)

B. Questionnaire d'évaluation des risques de cybersécurité

Le questionnaire d'évaluation des risques de cybersécurité ci-dessous vise à sensibiliser les petites et moyennes organisations. Il ne sert pas à porter un jugement ou à produire une cote de risque globale. Comme le mentionne la note 1 de l'article 4.3.2.1, le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation devrait demander à des experts en cybersécurité d'examiner et de commenter son évaluation des risques et le choix des contrôles visant à protéger l'organisation contre les risques cernés et évalués. Aux fins du présent document, on entend par « politique », les règles et les procédures que doit suivre toute personne utilisant un actif ou une ressource de TI de l'organisation. La réponse « Non » à l'une des questions pourrait indiquer l'existence d'un risque pour l'organisation.

1. Les rôles et responsabilités relatifs aux TI et à la sécurité des TI sont-ils clairement définis dans votre organisation?	OUI / NON
2. Votre organisation a-t-elle un plan d'intervention en cas d'incident?	OUI / NON
3. Votre organisation a-t-elle une assurance en matière de cybersécurité?	OUI / NON
4. Votre organisation a-t-elle évalué le préjudice potentiel lié à la confidentialité, à l'intégrité et à l'accessibilité de ses actifs et systèmes d'information? https://lih-cai.cse-cst.gc.ca/login/index.php	OUI / NON
5. Votre organisation stocke-t-elle ou recueille-t-elle des données confidentielles (numéros de cartes de crédit ou de sécurité sociale, renseignements sur les employés, etc.)?	OUI / NON
6. Votre organisation connaît-elle ses responsabilités en vertu de la *Loi sur la protection des renseignements personnels*? https://laws-lois.justice.gc.ca/fra/lois/P-21/index.html	OUI / NON
7. Votre organisation a-t-elle classifié les données stockées?	OUI / NON
8. Votre organisation forme-t-elle ses employés sur ses politiques et procédures de cybersécurité?	OUI / NON
9. Votre organisation a-t-elle une politique interne établissant les dépenses en cybersécurité en fonction du budget total des TI?	OUI / NON
10. Votre organisation forme-t-elle son personnel des TI sur la cybersécurité?	OUI / NON
11. L'application automatique de correctifs est-elle activée partout où elle peut l'être?	OUI / NON
12. Votre organisation a-t-elle une politique sur la sauvegarde et le chiffrement des données opérationnelles essentielles?	OUI / NON
13. Votre organisation a-t-elle une politique sur l'emploi d'une authentification robuste des utilisateurs?	OUI / NON
14. Votre organisation a-t-elle une politique sur l'autorisation et le contrôle de l'accès?	OUI / NON
15. Votre organisation a-t-elle une politique sur la sécurité des sites Web?	OUI / NON
16. Votre organisation a-t-elle une politique sur la sécurité des services mobiles?	OUI / NON

17. Votre organisation a-t-elle une politique sur l'établissement de défenses de base sur le périmètre?	OUI / NON
18. Votre organisation a-t-elle recours à des services de TI de tiers (ex. : services infonuagiques, logiciels à la demande, sauvegarde à distance)?	OUI / NON
19. Votre organisation a-t-elle une politique sur les services de TI de tie?	OUI / NON
20. Votre organisation vérifie-t-elle les contrôles de sécurité en vigueur au moins une fois par année?	OUI / NON
21. Votre organisation soumet-elle ses systèmes d'information à des essais de pénétration et de vulnérabilité au moins une fois par année?	OUI / NON

Bibliographie

[1] CAN/CIOSC 103-1, *Confiance et identité numérique – Partie 1 : Notions fondamentales*.

[2] Centre canadien pour la cybersécurité. *Contrôles de cybersécurité de base pour les petites et moyennes organisations.*

[3] Conseil des normes de sécurité PCI. *Norme de sécurité des données de l'industrie des cartes de paiement* (PCI DSS).

[4] Cyber Essentials, Royaume-Uni.

[5] CyberNB.

[6] IASME. *Governance Standard for Information and Cyber Security*.

[7] IEC TS 62443-1-1:2009, *Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models*.

[8] ISACA. *Cybersecurity Guidance for Small and Medium-sized Enterprises*, 2015.

[9] ISACA. *Implementing Cybersecurity Guidance for Small and Medium-sized Enterprises*, 2015.

[10] ISO 19731:2017, *Analytique numérique et analyses web pour les besoins d'études de marché, études sociales et d'opinion — Vocabulaire et exigences de service*.

[11] ISO/IEC 27000:2018, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*.

[12] ISO/IEC 27001:2013, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences*.

[13] ISO/IEC 27002:2013, *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information*.

[14] ISO/IEC 27032:2012, *Technologies de l'information — Techniques de sécurité — Lignes directrices pour la cybersécurité*.

[15] ITSAP.30.032, *Pratiques exemplaires de création de phrases de passe et de mots de passe*.

[16] National Institute of Standards and Technology (NIST). *Cyber Security Framework*.

[17] Open Web Application Security Project. *Application Security Verification Standard*.

[18] Open Web Application Security Project. *Top 10 Vulnerabilities*.