Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Les 10 mesures de sécurité des TI : N° 6, Miser sur une formation sur mesure en matière de cybersécurité

ITSM.10.093

Février 2020

GESTIONNAIRES

Canada

AVANT-PROPOS

La présente est un document NON CLASSIFIÉ qui fait partie d'une série de documents axés sur les 10 mesures de sécurité des TI recommandées dans l'ITSM.10.189, *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information* [1][1].

DATE D'ENTRÉE EN VIGUEUR

La présente publication entre en vigueur le 20 février 2020.

HISTORIQUE DES MODIFICATIONS

Version	Modifications	Date
1	Première version.	20 février 2020

[1] Les numéros entre les crochets renvoient à des éléments de référence figurant à la section Contenu complémentaire du présent document.

APERÇU

L'une des 10 mesures de sécurité des technologies de l'information (TI) consiste à fournir de la formation en cybersécurité à tous les employés, y compris les entrepreneurs, les membres de la haute direction et les cadres. La formation vise à s'assurer que tout le personnel comprend les enjeux liés à la cybersécurité qui sont propres à l'organisation. Votre formation devrait clairement définir les rôles et responsabilités des employés en ce qui a trait à la prévention des menaces et des compromissions, et aux mesures d'intervention à prendre dans de tels cas. Les conseils formulés dans la présente sont fondés sur les contrôles de sécurité mentionnés dans le document intitulé *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33) [2].

Comme les auteurs de menace ciblent les organisations de toutes tailles, ces dernières doivent prendre en considération plusieurs facteurs pour se protéger des attaques. Un de ces facteurs consiste à réduire le niveau de risque de l'organisation en offrant aux employés de la formation sur les enjeux liés à la cybersécurité et en les sensibilisant aux rôles et aux responsabilités qu'ils doivent assumer pour protéger les réseaux, les systèmes et les biens de TI contre les compromissions.

La présente est un document NON CLASSIFIÉ qui fait partie d'une série de documents axés sur les 10 mesures de sécurité des TI recommandées dans l'ITSM.10.189, *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information* [1]. Bien que la mise en œuvre de l'ensemble des 10 mesures de sécurité recommandées puisse rendre votre organisation moins vulnérable aux cybermenaces, vous devriez examiner les activités que vous menez sur le plan de la cybersécurité pour déterminer si la prise de plus amples mesures est nécessaire. Pour de plus amples renseignements sur la mise en œuvre des 10 mesures de sécurité des TI, communiquez par téléphone ou par courriel avec le :

Centre d'appel du Centre canadien pour la cybersécurité (CCC)
contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

TABLE DES MATIÈRES

1 Aperçu de la gestion des risques liés à la sécurité des TI 5
1.1 Les 10 mesures de sécurité des TI 5
1.2 Rapport avec le processus de gestion des risques liés à la sécurité des TI 6
2 Formation en cybersécurité 8
2.1 Formation à l'interne 8
2.2 Formation externe 8
3 Politique et procédures en matière de cybersécurité (AT-1) 9
3.1 Politiques 9
3.2 Procédures 10
4 Sensibilisation de base à la cybersécurité (AT-2) 10
4.1 Sensibilisation à la menace interne 10
4.2 Exercices pratiques 11
5 Formation axée sur les rôles (AT-3) 11
6 Examen des activités de sensibilisation et de formation (AT-4) 12
7 Résumé 13
7.1 Coordonnées 13
8 Contenu complémentaire 14
8.1 Liste des abréviations 14
8.2 Glossaire 14
8.3 Références 15

LISTE DES FIGURES

Figure 1 Les 10 mesures de sécurité des TI – Nº 6, Miser sur une formation et une sensibilisation sur mesure 5
Figure 2 Classes et familles de contrôles de sécurité décrites dans l'ITSG-33 7

LISTE DES ANNEXES

Annexe A ITSG-33, Catalogue des contrôles de sécurité 16
A.1 Contrôles de sécurité opérationnels : Sensibilisation et formation 16

1 APERÇU DE LA GESTION DES RISQUES LIÉS À LA SÉCURITÉ DES TI

1.1 LES 10 MESURES DE SÉCURITÉ DES TI

Le présent document explique comment offrir de la formation en cybersécurité sur mesure au sein de votre organisation. Il est fondé sur les conseils et les contrôles de sécurité formulés respectivement dans l'ITSM.10.189 [1] et l'annexe 3A de l'ITSG-33 [2].

Les 10 mesures de sécurité des TI recommandées par le CST qui sont mentionnées à la figure 1 ci-dessous et dans l'ITMS.10.189 [1] sont fondées sur une analyse des tendances inhérentes aux cybermenaces et la répercussion de telles menaces sur les réseaux connectés à Internet. La mise en œuvre de toutes les mesures permettra de corriger la plupart des vulnérabilités liées à la sécurité des TI qui pèsent sur votre organisation.

L'incidence des menaces à la cybersécurité les plus courantes pourrait varier d'une organisation à l'autre. Pour satisfaire vos besoins en matière de sécurité, vous devez examiner les activités actuellement menées par votre organisation sur le plan de la sécurité et de la gestion des risques.

Figure 1 Les 10 mesures de sécurité des TI – Nº 6, Miser sur une formation et une sensibilisation sur mesure

1.2 RAPPORT AVEC LE PROCESSUS DE GESTION DES RISQUES LIÉS À LA SÉCURITÉ DES TI

Les 10 mesures de sécurité des TI du CST découlent des contrôles de sécurité mentionnés à l'annexe 3A de l'ITSG-33 [2]. L'ITSG-33 [2] décrit les rôles, les responsabilités et les activités qui permettent à une organisation de gérer les risques relevant de la sécurité des TI, et comprend un catalogue de contrôles de sécurité (c.-à-d., un ensemble standardisé d'exigences de sécurité visant à protéger la confidentialité, l'intégrité et la disponibilité des biens de TI). Ces contrôles de sécurité sont regroupés en trois classes, puis subdivisés en plusieurs familles (ou regroupements) de contrôles de sécurité connexes :

- **Contrôles de sécurité techniques** : Contrôles de sécurité qui sont mis en œuvre et exécutés par les systèmes d'information, principalement par l'intermédiaire de mécanismes de sécurité que l'on retrouve dans les composants matériels, logiciels et micrologiciels;
- **Contrôles de sécurité opérationnels** : Contrôles de sécurité de système d'information qui sont mis en œuvre et exécutés principalement par des personnes et qui s'appuient normalement sur des technologies tels les logiciels de soutien;
- **Contrôles de sécurité de gestion** : Contrôles de sécurité qui portent principalement sur la gestion de la sécurité des TI et les risques liés à la sécurité des TI.

Tel qu'il est indiqué à la figure 2, les conseils formulés dans la présente concernent les contrôles de sécurité opérationnels associés à la famille Sensibilisation et formation (AT). Ce document fait mention de mesures qui permettent de satisfaire les contrôles de sécurité suivants :

- **AT-1 Politique et procédures de formation et de sensibilisation à la sécurité;**
- **AT-2 Sensibilisation à la sécurité;**
- **AT-3 Formation à la sécurité axée sur les rôles;**
- **AT-4 Dossiers de formation à la sécurité.**

De plus amples renseignements sur les contrôles AT-1, AT-2, AT-3 et AT-4 sont fournis à l'annexe A du présent document.

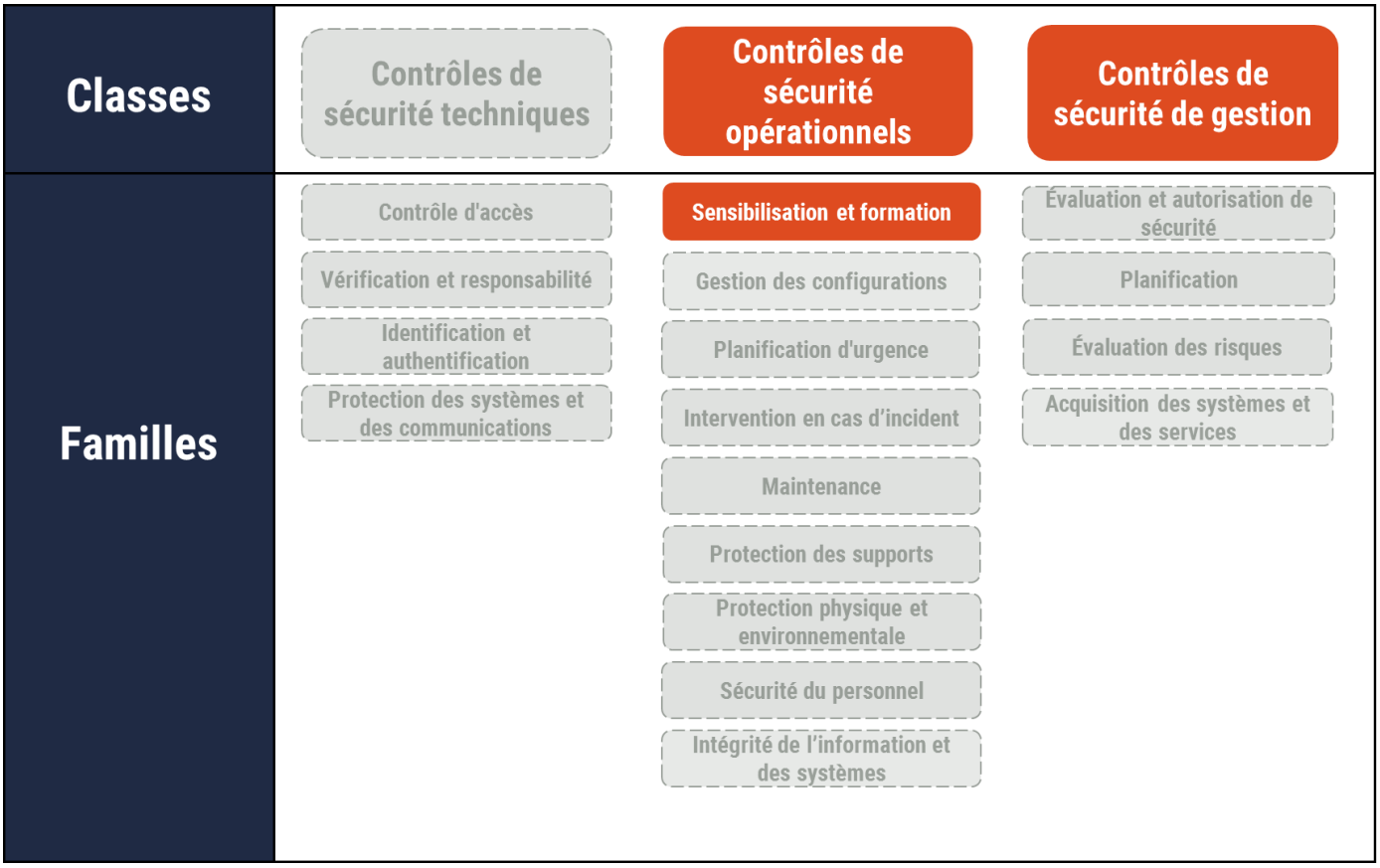

Figure 2 Classes et familles de contrôles de sécurité décrites dans l'ITSG-33

Vous pouvez utiliser les contrôles de sécurité mentionnés dans le présent document et à l'annexe 3A de l'ITSG-33 [2] pour déterminer la meilleure façon de gérer les risques liés à la cybersécurité de votre organisation et protéger ses réseaux, ses systèmes et ses biens de TI. Il convient toutefois de garder à l'esprit que la mise en œuvre de ces contrôles ne constitue qu'une partie du processus de gestion des risques à la sécurité des TI.

L'ITSG-33 [2] décrit un processus fondé sur deux niveaux d'activités de gestion des risques liés à la sécurité des TI, à savoir les activités associées au niveau organisationnel et au niveau des systèmes d'information. Ces deux niveaux d'activités vous aideront à déterminer vos exigences en matière de sécurité pour l'ensemble de l'organisation et ses systèmes d'information. Après avoir compris vos exigences pour chaque niveau, vous serez en mesure d'établir les contrôles de sécurité que votre organisation devra mettre en place et maintenir pour satisfaire un niveau de risque acceptable.

2 FORMATION EN CYBERSÉCURITÉ

Le présent document explique les mesures à prendre pour mettre en place un programme de formation et de sensibilisation à la cybersécurité au sein de votre organisation. Ces mesures sont fondées sur les contrôles de sécurité AT-1, AT-2, AT-3 et AT-4. Elles comprennent ce qui suit :

- élaborer des politiques et des procédures;
- offrir une formation de sensibilisation de base à la cybersécurité;
- faire appel à des exercices pratiques pour sensibiliser davantage les employés.

2.1 FORMATION À L'INTERNE

Les employés doivent comprendre les rôles et les responsabilités qu'ils assument sur le plan de la cybersécurité, puisque leurs activités et leur sensibilisation globale ont une incidence sur la posture de cybersécurité de votre organisation. Sensibiliser vos employés aux enjeux liés à la cybersécurité vous aidera à protéger vos réseaux, vos systèmes et vos biens de TI contre les cyberattaques et les compromissions. Grâce à une formation adéquate, vos employés arriveront entre autres à reconnaître et à gérer correctement les courriels malveillants. Une bonne formation permettra aux employés de contribuer positivement à la culture de cybersécurité de votre organisation.

Il conviendra d'examiner fréquemment votre programme et vos activités de sensibilisation à la cybersécurité pour en assurer l'efficacité et apporter des changements au besoin. Pour obtenir le soutien des équipes de gestion et de haute direction, vous devriez mettre à leur disposition de la documentation qui démontre en quoi les activités de formation accroissent la sensibilisation des employés à la cybersécurité. Vous pouvez, par exemple, demander à l'équipe chargée de la sécurité des TI de leur envoyer des rapports réguliers sur les cyberattaques et les compromissions. Ces rapports peuvent être utilisés pour déterminer s'il est nécessaire d'offrir une formation plus approfondie en cybersécurité, et évaluer l'efficacité de la formation actuelle.

2.2 FORMATION EXTERNE

Bien que le présent document porte sur la façon d'offrir une formation à l'interne, vous devriez également explorer les possibilités de formation offertes à l'extérieur de votre organisation.

Le Carrefour de l'apprentissage du Centre pour la cybersécurité (CACC) propose des programmes de formation en classe et en ligne destinés à divers publics, notamment le personnel n'ayant pas de compétences techniques, les praticiens des TI et les gestionnaires de niveau supérieur. En ce moment, ces programmes sont offerts essentiellement aux employés du gouvernement du Canada (GC) et des partenaires nationaux, mais le personnel des gouvernements provinciaux et municipaux, et des partenaires du secteur privé qui collaborent avec les ministères du GC, peut également s'y inscrire.

Les cours du CACC peuvent être offerts à l'ensemble d'une organisation, à de petits groupes ou à des employés en particulier. Ils portent sur les sujets suivants :

- la gestion des risques liés à la sécurité des TI;
- la cybersécurité pour les développeurs et les praticiens de la sécurité;
- la sécurité des communications;
- la sécurité cryptographique.

L'offre de cours est sujette à changement. Pour de plus amples renseignements à ce sujet, vous pouvez consulter le calendrier des cours sur le site Web du CACC.

Carrefour de l'apprentissage du Centre pour la cybersécurité
education@cyber.gc.ca
https://cyber.gc.ca/fr/carrefour-de-lapprentissage

3 POLITIQUE ET PROCÉDURES EN MATIÈRE DE CYBERSÉCURITÉ (AT-1)

Les conseils formulés dans la présente section sont basés sur le contrôle **AT-1, Politique et procédures de formation et de sensibilisation à la sécurité**. De plus amples renseignements sur le contrôle AT-1 sont fournis à l'annexe A du présent document.

3.1 POLITIQUES

Les politiques en matière de cybersécurité dictent les comportements attendus des employés et l'utilisation acceptable des réseaux, des systèmes, des biens de TI et de l'information de l'organisation. Elles définissent les rôles et responsabilités de tous les employés, y compris les entrepreneurs, les membres de la haute direction et les cadres, pour ce qui est de prévenir les menaces à la cybersécurité et les compromissions, de les reconnaître et de prendre les mesures d'intervention nécessaires. Votre politique devrait également faire mention du rôle et des responsabilités que la direction doit assumer pour soutenir le programme de formation et de sensibilisation à la cybersécurité de son organisation.

Il pourrait être nécessaire de créer d'autres politiques sur l'utilisation acceptable de la messagerie électronique, d'Internet, de supports amovibles (p. ex., les appareils mobiles et les clés USB) et des autres applications et services utilisés par l'organisation. Vous devriez également mettre en place une politique qui tient compte des exigences en matière de sécurisation et de manipulation de l'équipement TI, des biens de TI et de l'information sensible.

Toutes les politiques devraient être rédigées dans un langage clair et simple et employer la terminologie du domaine. Une politique efficace pourra être mise en application et comportera un plan de surveillance de la conformité. Il conviendra de s'assurer que tous les nouveaux employés, qu'il s'agisse d'entrepreneurs, de membres de la haute direction et de cadres, savent qu'il leur faut lire les politiques de l'organisation et s'engager à les respecter. Les séances d'orientation et de formation offertes aux nouveaux employés devraient fournir un aperçu de l'ensemble des politiques.

3.2 PROCÉDURES

Les procédures régissent la façon dont les employés satisfont aux exigences des politiques et mènent à bien les processus opérationnels. Vous devriez mettre en place des procédures qui aideront les employés à assumer leurs responsabilités en matière de cybersécurité, comme signaler les incidents de sécurité et suivre le plan de gestion des incidents de l'organisation. Voici des exemples de procédures mises en œuvre couramment :

- entreposer et sécuriser l'équipement et les biens de TI;
- effectuer des sauvegardes;
- mener des évaluations de sécurité;
- détecter et signaler les courriels malveillants;
- signaler les incidents de sécurité.

4 SENSIBILISATION DE BASE À LA CYBERSÉCURITÉ (AT-2)

Les conseils formulés dans la présente section sont basés sur le contrôle **AT-2, Sensibilisation à la sécurité**. Les sous-sections 4.1 et 4.2 décrivent les façons d'accroître la formation et la sensibilisation de base en abordant la menace interne et en faisant appel à des exercices pratiques. Ces améliorations sont fondées sur les améliorations des contrôles AT-2. De plus amples renseignements à ce sujet sont fournis à l'annexe A du présent document.

Il incombe à votre organisation d'élaborer les plans de formation. On recommande d'offrir de la formation en cybersécurité de base à tous les employés actuels ou nouveaux, y compris les entrepreneurs, les membres de la haute direction et les cadres. Les séances de formation de base devraient faire mention des comportements attendus et des exigences de la politique.

Il faudrait également offrir de la formation advenant la mise en place de nouveaux systèmes d'information ou la modification de systèmes existants. Une formation assistée par ordinateur peut alors être offerte aux employés pour les aider à rafraîchir leurs connaissances des politiques et des procédures au besoin.

Bien que l'environnement de votre organisation puisse exiger l'ajout de sujets additionnels, vos programmes de formation devraient traiter de ce qui suit, au minimum :

- détecter et gérer les courriels malveillants;
- gérer et sécuriser les biens de TI et l'information sensible;
- reconnaître les indicateurs potentiels de menace interne;
- signaler les incidents de sécurité et les menaces internes potentielles.

4.1 SENSIBILISATION À LA MENACE INTERNE

Par **menace interne**, on entend une menace envers votre organisation qui émane de l'intérieur, comme des employés ou des entrepreneurs actuels ou anciens. Une menace interne peut accéder à l'information sensible (p. ex., des données financières, des renseignements personnels ou l'information concernant les pratiques de sécurité, les données et les systèmes de l'organisation) ou la modifier pour en tirer des gains personnels ou financiers. Elle peut également agir de

manière à entraver les activités de votre organisation (p. ex., verrouiller les comptes, chiffrer ou supprimer de l'information essentielle, ou détruire des actifs importants).

Vous devriez sensibiliser les employés aux indicateurs potentiels de la menace interne. Parmi ces indicateurs, on retrouve, entre autres, des comportements tels que l'insatisfaction prolongée des employés et des agissements de plus en plus hostiles, des tentatives d'accès non autorisé à de l'information et à des justificatifs d'identité, un accès inexpliqué à des ressources financières ou le non-respect d'autres politiques et procédures de l'organisation. Vous devriez également sensibiliser les employés à la marche à suivre pour signaler des menaces internes potentielles sans crainte de représailles.

4.2 EXERCICES PRATIQUES

L'ajout d'exercices pratiques aux séances de formation permettra de tester la compréhension des employés par rapport aux politiques et aux politiques de cybersécurité, et de réaffirmer les objectifs de formation. Voici des exemples de tels exercices :

- distinguer les courriels de harponnage des courriels réels;
- reconnaître les applications compromises et vérifier la compréhension des employés quant à la façon de signaler les incidents de sécurité;
- analyser les tentatives de piratage psychologique qui ont pour objectif de recueillir de l'information ou d'obtenir un accès non autorisé.

Ces exercices doivent être effectués en concertation avec les secteurs des TI et de la sécurité.

5 FORMATION AXÉE SUR LES RÔLES (AT-3)

Cette section est fondée sur le contrôle **AT-3, Formation à la sécurité axée sur les rôles**, et les améliorations apportées à ces contrôles. De plus amples renseignements à ce sujet sont fournis à l'annexe A du présent document.

Le programme et les activités de formation de l'organisation devraient être adaptés de manière à tenir compte des rôles et responsabilités du public visé (c.-à-d., prendre la forme d'une formation axée sur les rôles). Certains rôles, comme les concepteurs, les administrateurs système, les vérificateurs, les architectes d'entreprise ou les responsables de la sécurité des systèmes d'information, peuvent nécessiter un accès à des systèmes d'information qui contiennent ou traitent de l'information sensible, et à des logiciels de niveau système. Il conviendra donc d'offrir de la formation aux employés avant qu'ils n'aient accès à de tels systèmes et logiciels.

Les activités de formation axées sur les rôles devraient comporter des exercices pratiques. Dans le cas des gestionnaires, par exemple, cette activité pourrait comprendre des exercices de simulation basés sur un scénario de compromission et utiliser ce scénario pour passer en revue les rôles et responsabilités clés, de même que le processus d'intervention en cas de compromission ou d'incident. Dans le cas des employés, les activités de formation axées sur les rôles pourraient comprendre des exercices destinés à les aider à reconnaître les communications suspectes et les comportements inhabituels du système, comme du code malveillant.

Vous devriez aborder les différents rôles et responsabilités de nature opérationnelle, technique et gestionnelle qui appuient la sécurité des réseaux, des systèmes et des biens de TI de votre organisation. Vous devriez également discuter de l'utilisation et du fonctionnement des contrôles environnementaux (p. ex., les systèmes de détection et d'extinction

d'incendie, les détecteurs de fumée, les systèmes de gicleurs, l'alimentation électrique, la température et l'humidité) ou des contrôles physiques (p. ex., les alarmes de détection d'intrusion, l'équipement de surveillance, les dispositifs de contrôle d'accès, les gardiens de sécurité) qui servent à protéger les biens de TI, puisque certains de ces contrôles pourraient exiger une formation spécialisée.

6 EXAMEN DES ACTIVITÉS DE SENSIBILISATION ET DE FORMATION (AT-4)

La présente section est basée sur le contrôle **AT-4, Dossiers de formation à la sécurité**. De plus amples renseignements sur le contrôle AT-4 sont fournis à l'annexe A du présent document.

Comme plusieurs autres aspects de votre organisation, vos besoins et exigences en cybersécurité évolueront au fil du temps. Vous devriez passer en revue annuellement l'ensemble de vos activités de formation pour veiller à ce qu'elles tiennent compte de vos stratégies de cybersécurité actuelles. Les modules de formation devraient comprendre tout changement apporté aux politiques relatives à la cybersécurité de votre organisation.

Assurez-vous de documenter et de surveiller toutes les activités de formation pour en déterminer l'efficacité. Vous devriez tenir à jour les dossiers de formation des employés afin de confirmer qu'ils ont bien suivi et réussi les activités de formation.

7 RÉSUMÉ

L'une des 10 mesures de sécurité des TI consiste à fournir de la formation en cybersécurité sur mesure à tous les employés. Il est possible de réduire le niveau de risque de l'organisation en offrant aux employés de la formation sur les enjeux liés à la cybersécurité et en les sensibilisant aux rôles et aux responsabilités qu'ils doivent assumer pour protéger les réseaux, les systèmes et les biens de TI contre les compromissions.

Votre organisation met en place et perpétue une culture rigoureusement axée sur la cybersécurité en veillant à mettre en place des politiques et des procédures en matière de cybersécurité et à offrir de la formation en cybersécurité à ses employés. La formation n'est toutefois qu'un aspect du renforcement de votre posture de cybersécurité. Pour mieux protéger votre organisation contre les cybermenaces, vous devriez passer en revue et mettre en place l'ensemble des mesures recommandées dans l'ITSM.10.189 [1].

7.1 COORDONNÉES

Pour de plus amples renseignements sur la mise en œuvre des 10 mesures de sécurité des TI, communiquez par téléphone ou par courriel avec le :

Centre d'appel du CCC
contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

8 CONTENU COMPLÉMENTAIRE

8.1 LISTE DES ABRÉVIATIONS

Terme	Définition
AT	Code de la famille de contrôles de sécurité Sensibilisation et formation (*Awareness and Training*)
CACC	Carrefour de l'apprentissage du Centre pour la cybersécurité
CCC	Centre canadien pour la cybersécurité
GC	Gouvernement du Canada
TI	Technologies de l'information

8.2 GLOSSAIRE

Terme	Définition
Bien de TI	Composante d'un système d'information, ce qui comprend notamment les applications opérationnelles, les données, le matériel et les logiciels.
Confidentialité	Valeur qui est accordée à une information pour indiquer son niveau de sensibilité et les restrictions d'accès mises en place pour empêcher les utilisateurs non autorisés de les consulter.
Contrôle de sécurité	Exigence technique, opérationnelle ou gestionnelle de haut niveau relative à la sécurité, qu'il convient d'appliquer à un système d'information afin de protéger la confidentialité, l'intégrité et la disponibilité des actifs TI connexes. Ces contrôles peuvent être appliqués au moyen de diverses solutions de sécurité, notamment des produits, des politiques, des pratiques et des procédures de sécurité.
Contrôle de sécurité de gestion	Contrôles de sécurité qui portent principalement sur la gestion de la sécurité des TI et les risques liés à la sécurité des TI.
Contrôle de sécurité opérationnel	Contrôles de sécurité qui sont principalement mis en œuvre et exécutés par des personnes, mais habituellement fondés sur l'utilisation de la technologie, par exemple, un logiciel de soutien.
Contrôle de sécurité technique	Contrôles de sécurité techniques qui sont mis en œuvre et exécutés par les systèmes d'information, principalement par l'intermédiaire de mécanismes de sécurité intégrés aux composants matériels, logiciels et micrologiciels.
Cyberattaque	Recours à des techniques électroniques visant à perturber, à manipuler, à détruire ou à scruter clandestinement un système informatique, un réseau ou un dispositif.
Disponibilité	Valeur qui est accordée aux actifs informationnels, logiciels et matériels (l'infrastructure et ses composantes). Les données ayant la valeur la plus élevée doivent être accessibles en permanence. Il est également entendu que la disponibilité comprend la protection des actifs contre les accès non autorisés ou les compromissions.
Hameçonnage	Tentative visant à solliciter de l'information confidentielle appartenant à un individu, à un groupe ou à une organisation en les mystifiant ou en imitant une marque commerciale connue. En l'occurrence, les malfaiteurs incitent les utilisateurs à partager leurs renseignements personnels (numéros de cartes de crédit, données bancaires ou autres renseignements) afin de s'en servir pour commettre des actes frauduleux.

Terme	Définition
Harponnage	Utilisation d'adresses courriel ou de communications électroniques falsifiées pour inciter les employés d'une organisation à révéler de l'information sensible (p. ex., des noms d'utilisateur ou des mots de passe). Les attaques par harponnage se font à petite échelle et sont bien ciblées.
Intégrité	Valeur qui est accordée à l'information pour indiquer dans quelle mesure elle est sensible à la perte de données. Il est également entendu que l'intégrité comprend l'aptitude à protéger l'information contre les modifications ou les suppressions non intentionnelles ou inopportunes. L'intégrité permet de savoir si l'information est conforme à ce qu'elle est censée être. Le concept d'intégrité s'applique également aux processus opérationnels, à la logique des logiciels d'application, au matériel et au personnel.
Maliciel	Logiciel malveillant conçu pour infiltrer ou endommager un système informatique. Les maliciels les plus courants sont les virus informatiques, les vers, les chevaux de Troie, les logiciels espions et les logiciels publicitaires.
Menace	Événement ou acte délibéré, accidentel ou naturel pouvant éventuellement porter préjudice aux actifs et à l'information de TI.
Risque	Dans le contexte de la cybersécurité, la probabilité qu'un auteur de menace se serve d'une vulnérabilité pour accéder aux biens et l'incidence de la menace.
Vulnérabilité	Défectuosité ou lacune inhérente à la conception ou à la mise en œuvre d'un système d'information ou à son environnement, qui pourrait être exploitée par un auteur de menace en vue de compromettre les biens ou les activités d'une organisation.

8.3 RÉFÉRENCES

Numéro	Référence
1	Centre canadien pour la cybersécurité. *ITSM.10.189, Les 10 mesures de sécurité des technologies de l'information visant à protéger les réseaux Internet et l'information,* octobre 2018.
2	Centre canadien pour la cybersécurité. *ITSG-33, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie,* décembre 2014.

Annexe A ITSG-33, Catalogue des contrôles de sécurité

A.1 Contrôles de sécurité opérationnels : Sensibilisation et formation

Le tableau 1 traite des contrôles de sensibilisation et de formation (AT) mentionnés à l'annexe 3A de l'ITSG-33 [2].

Tableau 1 : ITSG-33, Contrôles de sécurité opérationnels : Sensibilisation et formation

Numéro	Contrôle	Exigence	Améliorations de contrôle	Contrôles de l'ITSG-33 connexes
AT-1	Politique et procédures de formation et de sensibilisation à la sécurité	(A) L'organisation élabore, documente et diffuse à [*liste des employés et des rôles définie par l'organisation*] : i. une politique de sensibilisation et de formation à la sécurité qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et le respect; ii. des procédures pour faciliter la mise en œuvre de la politique de sensibilisation et de formation à la sécurité ainsi que des contrôles connexes.	Aucune	Aucun
		(B) L'organisation examine et met à jour : i. la politique de sensibilisation et de formation à la sécurité; ii. les procédures de sensibilisation et de formation à la sécurité.	Aucune	Aucun
AT-2	Sensibilisation à la sécurité	(A) L'organisation dispense une formation de base sur la sensibilisation à la sécurité aux utilisateurs du système d'information (y compris les gestionnaires, les cadres supérieurs et les entrepreneurs) : i. dans le cadre de la formation initiale à l'intention des nouveaux utilisateurs;	**Exercices pratiques :** L'organisation inclut dans la formation des exercices pratiques de sensibilisation à la sécurité qui simulent des cyberattaques.	CA-2 CA-7 CP-4 IR-3
			Menace interne :	PL-4 PS-3

Numéro	Contrôle	Exigence	Améliorations de contrôle	Contrôles de l'ITSG-33 connexes
		ii. au besoin, lorsque des changements apportés au système l'exigent; iii. [*fréquence définie par l'organisation*] par la suite.	L'organisation inclut dans la formation des exercices pratiques de sensibilisation à la sécurité pour que le personnel sache reconnaître les indicateurs potentiels de menace interne et pour qu'il les signale.	PS-6
AT-3	Formation à la sécurité axée sur les rôles	(A) L'organisation offre de la formation à la sécurité axée sur les rôles aux employés qui assument des rôles et des responsabilités en matière de sécurité : i. avant d'autoriser leur accès au système ou avant qu'ils commencent leurs tâches; ii. au besoin, lorsque des changements apportés au système d'information l'exigent; iii. [*fréquence définie par l'organisation*] par la suite.	**Contrôles environnementaux :** L'organisation offre à [*liste des employés et des rôles définie par l'organisation*] la formation initiale sur l'utilisation et le fonctionnement des contrôles environnementaux [*fréquence définie par l'organisation*].	PE-1 PE-13 PE-14 PE-15
			Contrôles de sécurité physique : L'organisation offre à [*liste des employés et des rôles définie par l'organisation*] la formation initiale sur l'utilisation et le fonctionnement des contrôles physiques [*fréquence définie par l'organisation*].	PE-2 PE-3 PE-4 PE-5
			Exercices pratiques : L'organisation inclut dans la formation à la sécurité des exercices pratiques qui renforcent les objectifs de formation.	Aucun
			Communications suspectes et	Aucun

Numéro	Contrôle	Exigence	Améliorations de contrôle	Contrôles de l'ITSG-33 connexes
			comportements anormaux de systèmes : L'organisation offre à son personnel une formation sur [*indicateurs de programmes malveillants définis par l'organisation*] pour qu'il sache reconnaître les communications suspectes et les comportements anormaux dans les systèmes d'information de l'organisation.	
AT-4	Dossiers de formation à la sécurité	(A) L'organisation consigne et surveille les activités de formation individuelles sur la sécurité des systèmes d'information, y compris la formation de base sur la sensibilisation à la sécurité et la formation sur la sécurité propre aux systèmes d'information.	Aucune	AT-2 AT-3
		(B) L'organisation conserve les dossiers de formation individuels pendant [*durée définie par l'organisation*].	Aucune	AT-2 AT-3