Centre de la sécurité des télécommunications
Communications Security Establishment

Choose a building block

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Conseils en matière de cybersécurité à l'intention des organismes électoraux

GESTIONNAIRES

TLP:WHITE

Canada

AVANT-PROPOS

L'ITSM.10.020, *Conseils en matière de cybersécurité à l'intention des organismes électoraux*, est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité).

DATE D'ENTRÉE EN VIGUEUR

Le présent document entre en vigueur le 26 août 2020.

HISTORIQUE DES RÉVISIONS

Version	Modifications	Date
1	Première version	26 août 2020

VUE D'ENSEMBLE

Le présent document est destiné aux organismes électoraux. Il présente les menaces courantes qui pèsent sur les processus électoraux du Canada et des conseils sur la façon de protéger les personnes et les systèmes associés à ces processus. Les conseils formulés dans le présent document reposent sur des renseignements tirés de diverses sources et visent uniquement à établir une série de recommandations qui pourront être mises en œuvre dans le cadre des politiques et des pratiques actuelles de votre organisme.

Il convient de souligner que le présent document ne vise pas à fournir des conseils exhaustifs sur les mesures à prendre afin de protéger votre organisation contre les cybermenaces. Il revient à votre organisation de définir ses besoins sur le plan des opérations et de la sécurité et de prendre les mesures nécessaires pour assurer la confidentialité, l'intégrité et la disponibilité de ses réseaux, de ses systèmes et de son information.

Le Centre pour la cybersécurité a été créé sous l'égide du Centre de la sécurité des télécommunications le 1er octobre 2018. Le Centre pour la cybersécurité est l'autorité nationale en matière de cybersécurité et sa création a permis de réunir sous un même toit des spécialistes de la sécurité opérationnelle de l'ensemble du gouvernement du Canada (GC). En phase avec la Stratégie nationale de cybersécurité du Canada [1][1], la mise sur pied du Centre pour la cybersécurité marque un tournant vers une approche unifiée à la cybersécurité au Canada. Le Centre pour la cybersécurité fournit des avis et conseils au GC et aux entreprises canadiennes pour veiller à la sécurité, à la stabilité et à la prospérité du pays.

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

TABLE DES MATIÈRES

LISTE DES TABLEAUX

1 INTRODUCTION

À la suite des activités de cybermenace qui ont touché les institutions démocratiques des États-Unis et de l'Europe, des préoccupations ont été soulevées quant aux menaces semblables qui guettent le Canada. Les activités de cybermenace récentes ont également fait ressortir des problèmes liés à l'intégrité des bulletins de vote, des systèmes d'inscription des électeurs et des mesures visant à confirmer l'admissibilité des électeurs.

Les organismes électoraux d'un bout à l'autre du Canada doivent prendre des dispositions afin de protéger les processus et systèmes démocratiques. La compromission éventuelle des données électorales pourrait nuire à la capacité des institutions démocratiques de s'acquitter de leur mandat et risque d'ébranler la confiance du public envers les résultats d'élections et les processus démocratiques.

1.1 CONTEXTE DES RISQUES

Au cours des dernières années, des cyberattaques ont été menées de manière à coïncider avec des élections partout dans le monde. Bien que les auteurs de menace aient employé toute une gamme de techniques dans le cadre de ces attaques, la majorité d'entre elles consistaient en attaques par déni de service distribué (DDoS pour *Distributed Denial of Service*) contre des sites Web de gouvernements et de médias. Lors d'une attaque par déni de service distribué, un auteur de menace tente d'interrompre un site Web ou un système en le submergeant de trafic. Les attaques constatées semblent avoir eu comme objectif de voler des données, de modifier les résultats d'élections et de perturber la publication de ces résultats.

Certaines des activités de menace signalées sont parfois associées à des activités de cybermenace et visent à influencer les électeurs ou à miner la confiance du public envers les résultats d'élections et les processus électoraux. Parmi ces tentatives, on compte les cyberactivités malveillantes constatées par le gouvernement des États-Unis au cours des élections présidentielles de 2016, ainsi que les présumés reportages frauduleux signalés récemment qui visent à influencer l'opinion publique.

Il est difficile d'identifier avec certitude l'auteur d'une cyberattaque, mais il est probable que les attaques contre d'autres pays aient été menées par des auteurs parrainés par un État. Ces attaques pourraient également être attribuables à des pirates informatiques (qui peuvent avoir vendu leurs services), à des hacktivistes et à des cybercriminels.

1.2 EXEMPLES D'INGÉRENCE ÉLECTORALE

Compte tenu des expériences vécues récemment dans d'autres pays, les organisations appelées à intervenir dans les processus électoraux du Canada devraient se préparer à d'éventuelles attaques et perturbations. Le tableau 1 résume les études de cas récentes sur des perturbations ayant touché d'autres pays :

Tableau 1 : Exemples récents d'ingérence électorale

Année	Sommaire des événements
2015	Au début d'un processus électoral local et d'un référendum sur le vote électronique, les sites Web de la commission électorale, du gouvernement et du service d'inscription d'un pays de l'Union européenne ont été ciblés par une attaque par déni de service (DoS pour *Denial of Service*).
2016	Lors des dernières élections présidentielles aux États-Unis, les deux principaux partis politiques ont été la cible de tentatives de cyberespionage attribuables à la Russie. Des espions russes ont utilisé des cybercapacités pour accéder aux courriels de membres clés du personnel politique travaillant à la campagne du parti démocrate. Ces courriels ont ensuite été divulgués publiquement pour mettre la candidate du parti démocrate dans l'embarras. En 2018, des accusations ont été portées contre des personnes en Russie qui se seraient ingérées dans les élections présidentielles de 2016 aux États-Unis. On observe ainsi un changement vers une approche qui ne consiste plus uniquement à détecter et à contrer les activités malveillantes, mais aussi à confronter et à poursuivre en justice les auteurs de cybermenace qui ciblent le processus démocratique américain.
2017	D'après des reportages publiés dans les médias, le service français du renseignement croit que des réseaux de zombies (botnet) ont été déployés dans les médias sociaux pour influencer les élections présidentielles en France. Certains comptes dans les médias sociaux, les mêmes qui avaient été actifs au cours des élections américaines de l'année précédente, faisaient circuler des renseignements faux et diffamatoires contre l'une des figures majeures des élections. Dans les derniers jours des élections, des milliers de courriels liés à la campagne et appartenant à un parti politique ont été divulgués publiquement.
2019	Selon le service de cyberpolice de l'Ukraine, dans la période précédant les élections présidentielles qui ont eu lieu en Ukraine en mars 2019, des attaquants ont envoyé des courriels d'hameçonnage à des représentants du gouvernement et à des employés de l'État (y compris ceux qui interviennent dans le processus électoral). Ces courriels avaient comme objectif de voler des mots de passe et des renseignements personnels et comportaient des cartes de souhaits infectées par un maliciel. Les auteurs de cybermenace auraient acheté les renseignements personnels de fonctionnaires électoraux sur le Web invisible.

1.3 MENACES LIÉES AUX PROCESSUS ET SYSTÈMES ÉLECTORAUX

Les organismes électoraux canadiens, en collaboration avec leurs pendants internationaux, doivent continuer d'axer leurs efforts sur la protection des processus démocratiques en contrant les menaces émergentes comme celles données en exemple dans le tableau 2. Le tableau ci-dessous présente également des mesures permettant de faire face à ces menaces. Pour en savoir plus, prière de consulter le rapport intitulé *Le point sur les cybermenaces contre le processus démocratique du Canada en 2019* [2].

Tableau 2 : Exemples de menaces liées aux processus et systèmes électoraux

Menace	Mesures visant à atténuer la menace
Manipulation électronique des bulletins de vote.	Élections Canada continue d'employer des processus manuels de vote et de comptage des bulletins de vote.
Atteinte à l'intégrité des données au moyen d'attaques ciblant les services infonuagiques.	Choisir un fournisseur de services infonuagiques qui applique des contrôles de sécurité. Communiquer avec nous pour entreprendre le processus d'évaluation des fournisseurs de services infonuagiques en matière de sécurité des TI afin de déterminer si les contrôles et les processus du fournisseur de services correspondent à vos besoins opérationnels et à vos exigences de sécurité.
Attaques par déni de service distribué ciblant les sites Web d'organismes électoraux, de gouvernements ou de médias dans le but d'empêcher les utilisateurs de les consulter à des moments clés d'une campagne électorale, notamment à la date limite de l'inscription des électeurs ou le jour des élections.	Assurer progressivement la redondance dans l'infrastructure. Continuer de consulter les ressources en constante évolution afin de configurer votre matériel réseau de manière à le protéger contre les attaques.
Attaques par hameçonnage ou piratage psychologique visant à obtenir de l'information sensible.	Veiller à ce que tous les employés suivent de la formation et participent à des exercices pour qu'ils soient en mesure de détecter ces attaques, de se protéger et de protéger votre organisation.

2 PROTÉGER LES SYSTÈMES

La prise de mesures de cybersécurité de base peut contrer les attaques des auteurs de cybermenace. En jumelant ces mesures à des analyses et à des audits périodiques, votre organisation réduira la capacité d'un auteur de cybermenace de causer des dommages d'envergure.

Nous vous recommandons de prendre des mesures de sécurité préventives en mettant en œuvre divers types de contrôles de sécurité en fonction de vos besoins et de vos exigences, selon les catégories ci-dessous :

- **contrôles de sécurité administratifs** : procédures mises en œuvre pour définir les rôles, les responsabilités, les politiques et les fonctions administratives nécessaires pour gérer un environnement (p. ex. les procédures d'embauche, la séparation des tâches);
- **contrôles de sécurité techniques** : solutions matérielles et logicielles mises en œuvre pour contrôler l'accès à l'information et aux réseaux (p. ex. systèmes de détection d'intrusion, pare-feux, logiciels antivirus);
- **contrôles de sécurité physiques** : contrôles visant à protéger les personnes et l'environnement physique (p. ex. serrures, garde-corps).

Pour obtenir de plus amples renseignements, prière de consulter le catalogue des contrôles de sécurité à l'annexe 3A de l'ITSG-33 (*La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*) [3], ainsi que le document intitulé *Contrôles de cybersécurité de base pour les petites et moyennes organisations*, version 1.2 [4].

Pour éviter d'introduire d'autres risques opérationnels, nous vous recommandons de planifier attentivement et de mettre à l'essai tout changement à votre infrastructure ou aux solutions de votre fournisseur de services. Il conviendra de vous pencher tout particulièrement sur les points indiqués dans le tableau 3 ci-dessous.

Pour en savoir plus sur la façon de protéger vos systèmes, prière de consulter l'ITSM.10.021 : *Guide de cybersécurité à l'intention des organismes électoraux* [5]. Nous vous recommandons également de passer en revue l'ITSM.10.189 *: Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information* [6].

Tableau 3 : Mesures de cybersécurité de base visant à protéger les systèmes

Mesures de sécurité	Exemples
Protection des renseignements personnels	Gérer l'information nominative (PII pour *Personally Identifiable Information*) et les systèmes qui contiennent des jeux de données comportant une telle information (p. ex. les systèmes de gestion électorale [SGE]), conformément à la *Loi sur la protection des renseignements personnels* et à la *Loi sur la protection des renseignements personnels et les documents électroniques*.
Mesures réglementaires	Stocker les données sensibles de manière à respecter les exigences législatives et réglementaires. Par exemple, selon l'*Avis de mise en œuvre de la Politique sur la technologie de l'information* (AMPTI) portant sur l'*Orientation relative à la résidence des données électroniques* du Secrétariat du Conseil du Trésor (SCT) [7], tous les organismes du GC doivent stocker les données sensibles, y compris l'information nominative, dans des centres de données situés dans les frontières géographiques du Canada pour veiller à ce que cette information soit assujettie aux lois canadiennes sur la protection des renseignements personnels.
Sauvegardes	Effectuer régulièrement la sauvegarde de tout SGE (tout particulièrement la liste électorale). Il convient de stocker les sauvegardes hors ligne, dans un emplacement sécurisé distinct, et de mettre à l'essai les procédures de sauvegarde et de restauration des systèmes et de l'information. Conserver les coordonnées des principaux fournisseurs (p. ex. pour les logiciels et les fournisseurs de SGE) à portée de la main. Il convient de rappeler que, lors d'un incident, les mécanismes habituels permettant de trouver les coordonnées pourraient ne pas être accessibles.
Mises à jour et correctifs	Mettre à jour les logiciels et le matériel de votre infrastructure et appliquer les correctifs connexes.
Appareils des utilisateurs finaux	Veiller à ce que le personnel utilise des appareils gérés par l'organisation pour mener ses activités professionnelles, notamment la gestion de la liste électorale.
Comptes d'administrateur	Surveiller et restreindre les activités liées aux comptes d'administrateur en appliquant le principe du droit d'accès minimal (c'est-à-dire accorder l'accès administratif uniquement aux personnes qui en ont besoin pour exercer leurs fonctions). Tout dépendant du niveau d'accès aux systèmes électoraux dont bénéficient les membres de votre personnel opérationnel, ces derniers pourraient être en mesure d'effectuer des actions exigeant un accès privilégié sur les données contenues dans les SGE. Si c'est le cas, vous devrez peut-être considérer ces membres comme des administrateurs de systèmes.

	Passer régulièrement en revue les droits d'accès de chaque employé pour vous assurer que chacun bénéficie d'un niveau d'accès correspondant à son rôle.

3 PROTÉGER LES PERSONNES

Des auteurs de menace pourraient tenter d'exploiter votre personnel et toute autre personne liée au processus électoral, surtout aux moments où la pression s'intensifie (comme le jour des élections). Ils pourraient avoir recours à divers modes d'attaque, notamment l'hameçonnage et le piratage psychologique, afin d'accéder à de l'information sensible. Les titulaires de postes de direction ou les représentants officiels, ou encore les employés qui soutiennent directement ceux-ci, sont plus susceptibles d'être ciblés par ces attaques, car les renseignements à leur sujet sont publics. Certaines personnes pourraient dévoiler par mégarde de l'information qui permettrait à des auteurs de menace de manipuler ou de compromettre les processus électoraux. Il convient de s'assurer que tous les membres du personnel, et surtout les fonctionnaires électoraux, comprennent qu'ils doivent être prudents lorsqu'ils donnent des précisions sur les fonctions qu'ils exercent dans le cadre des élections.

3.1 FORMATION EN CYBERSÉCURITÉ

Dans le cadre de vos processus de gestion des risques, vous devriez fournir de la formation obligatoire sur la cybersécurité aux personnes appelées à contribuer aux processus électoraux. La formation devrait porter notamment sur la détection des attaques par hameçonnage et le piratage psychologique. Vous devriez également mettre en place des processus qui aideront votre personnel à éviter de tomber dans le piège lors de telles attaques.

> Par exemple, un employé pourrait recevoir un courriel qui semble provenir d'un fournisseur et dans lequel ce dernier indique qu'il faut mettre à jour de façon urgente son logiciel. Il pourrait s'agir d'un message tout à fait légitime, mais vous devriez avoir établi clairement les procédures à suivre pour valider ce type de courriel. Le destinataire devrait confirmer auprès d'autres sources que le contenu du message est valable (p. ex. en consultant le site Web du fournisseur pour déterminer si la mise à jour y est annoncée). Il importe de vous assurer que les membres de votre personnel savent comment obtenir de l'aide s'ils reçoivent des messages suspects ou inhabituels (p. ex. par courriel, par texto ou par téléphone).

La formation devrait également porter sur d'autres sujets comme les attaques par rançongiciel, les maliciels, les lignes directrices sur les mots de passe, les procédures de sécurité physique, la sensibilisation à la protection de la vie privée et l'utilisation en toute sécurité des appareils mobiles et des réseaux sociaux. Il convient de noter que cette liste de sujets n'est pas exhaustive. Pour en savoir plus sur la formation, prière de consulter *Les 10 mesures de sécurité des TI : N° 6, Miser sur une formation sur mesure en matière de cybersécurité* (ITSM.10.093) [8].

Pour obtenir de plus amples renseignements sur les équipes chargées des campagnes électorales, nous vous invitons à consulter le *Guide de cybersécurité à l'intention des équipes chargées des campagnes électorales* [9].

3.2 MENACES INTERNES

Les personnes appelées à intervenir dans les processus électoraux du Canada doivent faire preuve d'intégrité et de discrétion. Or, il importe d'être conscient des risques que peut poser une menace interne. On entend d'une menace interne toute personne qui connaît l'infrastructure ou l'information de votre organisation, ou qui y a accès, et qui utilise ses connaissances ou son accès d'une façon malveillante ou involontaire pour nuire à l'organisation.

Un employé pourrait exploiter intentionnellement l'accès dont il bénéficie à ses propres fins non autorisées. Une menace interne pourrait chercher à manipuler ou à compromettre l'information ou les processus électoraux pour obtenir des gains financiers, pour des raisons idéologiques ou encore pour se faire connaître. Il est toutefois possible qu'un employé porte atteinte à l'information ou aux processus par mégarde, par exemple dans les cas suivants :

- s'il perd un dispositif mobile ou un support amovible;
- s'il permet à des employés d'accéder à de l'information sensible qu'ils n'ont pas l'autorisation de consulter;
- s'il gère mal l'information sensible en la laissant à découvert ou en oubliant d'appliquer les permissions requises.

Vous pouvez prévenir les risques liés aux menaces internes en vérifiant les antécédents des personnes que vous pensez embaucher et en mettant en œuvre des contrôles d'accès (p. ex. principe des droits d'accès minimaux, séparation des tâches) afin de protéger l'information sensible. Pour en savoir plus, veuillez consulter l'ITSAP.10.003 : *Comment protéger votre organisation contre les menaces internes* [10].

3.3 POLITIQUES SUR LA CYBERSÉCURITÉ

Vous devriez mettre en place des politiques et des procédures qui définissent clairement les comportements attendus, les rôles et les responsabilités de tous les employés. Toutes les personnes appelées à intervenir dans les processus électoraux et démocratiques (qu'il s'agisse de fonctionnaires du gouvernement ou de l'administration en question ou des titulaires de postes temporaires chargés de travailler aux bureaux de vote, de gérer le vote postal ou de compter les votes) ont un rôle essentiel à jouer pour assurer la confidentialité, l'intégrité et la disponibilité de l'information et des systèmes connexes. En établissant ces politiques, vous veillez à ce que chacun soit tenu responsable de respecter les pratiques de sécurité de votre organisation.

Il convient de déterminer la fréquence à laquelle vos politiques seront passées en revue (p. ex. une fois par année) afin de veiller à ce qu'elles soient mises à jour en fonction des nouveaux processus et des nouvelles procédures ou des modifications apportées aux processus existants.

4 COMMUNIQUEZ AVEC NOUS

Pour de plus amples renseignements sur la cybersécurité, communiquez par téléphone ou par courriel avec le centre d'appel. Vous pouvez également consulter notre site Web pour trouver des publications sur toute une gamme de sujets liés à la cybersécurité.

Centre d'appel
www.cyber.gc.ca
contact@cyber.gc.ca
613-991-8700 ou 1-833-CYBER-88

5 CONTENU COMPLÉMENTAIRE

5.1 LISTE DES ABRÉVIATIONS

Terme	Définition
CST	Centre de la sécurité des télécommunications
DDoS	Déni de service distribué (*Distributed Denial of Service*)
DoS	Déni de service (*Denial of Service*)
GC	Gouvernement du Canada
PII	Information nominative (*Personally Identifiable Information*)
SGE	Système de gestion électorale
TI	Technologies de l'information

5.2 GLOSSAIRE

Terme	Définition
Attaque par déni de service	Toute activité visant à rendre un service inutilisable ou à ralentir l'exploitation et les fonctions d'un système donné.
Confidentialité	Caractéristique de l'information sensible protégée contre tout accès non autorisé.
Contrôles de sécurité administratifs	Procédures mises en œuvre pour définir les rôles, les responsabilités, les politiques et les fonctions administratives nécessaires pour gérer un environnement (p. ex. les procédures d'embauche, la séparation des tâches).
Contrôles de sécurité physiques	Contrôles visant à protéger les personnes et l'environnement physique (p. ex. serrures, garde-corps).
Contrôles de sécurité techniques	Solutions matérielles et logicielles mises en œuvre pour contrôler l'accès à l'information et aux réseaux (p. ex. systèmes de détection d'intrusion, pare-feux, logiciels antivirus).
Disponibilité	Caractéristique de l'information ou des systèmes qui sont accessibles aux personnes autorisées au moment où celles-ci en ont besoin. La disponibilité est un attribut des actifs informationnels, logiciels et matériels (l'infrastructure et ses composantes). Il est également entendu que la disponibilité comprend la protection des actifs contre les accès non autorisés ou les compromissions.
Hameçonnage	Procédé par lequel une tierce partie tente de 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, souvent dans le but de réaliser des gains financiers. Les hameçonneurs incitent les utilisateurs à partager leurs renseignements personnels (numéros de cartes de crédit, données bancaires ou autres renseignements sensibles) afin de s'en servir pour commettre des actes frauduleux.

Terme	Définition
Intégrité	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. L'intégrité s'applique également aux processus opérationnels, aux logiciels, à la logique d'application, au matériel ainsi qu'au personnel.
Liste électorale	Liste des personnes inscrites comme étant admissibles à voter.
Menace interne	Toute personne qui connaît l'infrastructure ou l'information d'une organisation, ou qui y a accès, et qui utilise ses connaissances ou son accès d'une façon malveillante ou involontaire pour nuire à cette organisation.
Piratage psychologique	Attaque dans le cadre de laquelle un auteur de menace tente de manipuler sa cible pour l'amener à effectuer des opérations ou à divulguer de l'information sensible.

5.3 RÉFÉRENCES

Numéro	Référence
1	Sécurité publique Canada. *Stratégie nationale de cybersécurité : La vision du Canada pour la sécurité et la prospérité à l'ère numérique*, 2018.
2	Centre canadien pour la cybersécurité. *Le point sur les cybermenaces contre le processus démocratique du Canada en 2019*.
3	Centre canadien pour la cybersécurité. *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33), novembre 2012.
4	Centre canadien pour la cybersécurité. *Contrôles de cybersécurité de base pour les petites et moyennes organisations*, version 1.2, février 2020.
5	Centre canadien pour la cybersécurité. *Guide de cybersécurité à l'intention des organismes électoraux* (ITSM.10.021), mai 2020.
6	Centre canadien pour la cybersécurité. *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information* (ITSM.10.189), octobre 2018.
7	Secrétariat du Conseil du Trésor du Canada. *Avis de mise en œuvre de la Politique sur la technologie de l'information (AMPTI), Orientation relative à la résidence des données électroniques,* novembre 2017.
8	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), janvier 2020.
9	Centre canadien pour la cybersécurité. *Guide de cybersécurité à l'intention des équipes chargées des campagnes électorales.*
10	Centre canadien pour la cybersécurité. *Comment protéger votre organisation contre les menaces internes* (ITSAP.10.003), février 2020.