OPTIMISÉ PAR
L'Institut des services axés sur les citoyens

CITOYENS en tête

Cybersécurité

Un regard sur l'environnement canadien

RAPPORT EXÉCUTIF MENSUEL DU CONSEIL MIXTE

(Produit du Comité de recherche)

Juin 2020

Source de l'image : Pikist

1. Introduction

La cybersécurité doit être une question prioritaire afin de permettre aux gouvernements de lutter efficacement contre la cybercriminalité. Cela dit, la tenue à jour des pratiques exemplaires tout en gérant les vulnérabilités et en appliquant des rustines aux systèmes les plus essentiels destinés au public est tout un tour de force lorsque les administrations travaillent seules. Les administrations et les organisations qui les composent ont de nombreux avantages à collaborer pour cerner et résoudre les problèmes de cybersécurité, et les experts recommandent des règlements de sécurité mutuellement avantageux.

Dans le présent rapport exécutif, nous vous présenterons quelques-unes des principales organisations et initiatives de cybersécurité, nous décrivons les possibilités et les défis prioritaires dans l'espace de cybersécurité, et nous déterminerons où les gouvernements devraient concentrer leurs efforts.

La cybercriminalité mondiale annuelle coûtera au monde plus de 6 000 milliards de dollars par an d'ici 2021, une hausse par rapport aux 3 000 milliards de dollars de 2015. Il s'agit du plus grand transfert de richesse économique de l'histoire, et il est plus rentable que le commerce mondial de toutes les grandes drogues illégales combinées.

2. Principales organisations et initiatives de cybersécurité à l'échelle nationale

Il y a de nombreux organismes et ministères dans l'ensemble des gouvernements qui jouent un rôle en matière de cybersécurité au Canada. Voici quelques points à garder à l'esprit :

Centre canadien pour la cybersécurité

- La source unique et unifiée en matière de conseils, d'orientation, de services et de soutien en cybersécurité pour le gouvernement, les propriétaires et exploitants d'infrastructures essentielles, le secteur privé et le public canadien.

Centre antifraude du Canada

- Recueille des renseignements sur la fraude et le vol d'identité et fournit des renseignements sur les escroqueries passées et actuelles qui touchent les Canadiens.

Secrétariat du Conseil du Trésor du Canada

- Établit et supervise une approche pangouvernementale de la cybersécurité, y compris l'établissement d'une orientation pangouvernementale et l'établissement de priorités pour assurer la sécurité des systèmes et des réseaux de la TI du gouvernement.

Sécurité publique Canada

- Le ministère travaille en étroite collaboration avec des partenaires nationaux et internationaux dans le cadre de l'effort mondial visant à protéger les biens et les renseignements essentiels et à lutter contre la cybercriminalité.

Pour en apprendre davantage sur la cybersécurité au gouvernement fédéral du Canadien, cliquez ici.

Les administrations prendront note des suivants

- Canada
  - Nouveau-Brunswick
  - Colombie-Britannique
- Scène internationale
  - Royaume-Uni (le National Cyber Security Centre)
  - États-Unis (Département de la Sécurité intérieure, National Institute of Standards and Technology)

3. Les thèmes de la cybersécurité qui sont prioritaires pour les gouvernements

Les cyberattaques contre les systèmes gouvernementaux augmentent, les technologies de la fonction publique deviennent un élément clé des services fondés sur la valeur, et les perturbateurs extérieurs prennent des mesures dans la sphère publique. Ce sont là quelques-uns des thèmes sur lesquels les sources du secteur public disent que l'industrie est actuellement concentrée.

Rançongiciels

« Le rançongiciel est un type de logiciel malveillant qui verrouille un système informatique jusqu'à ce que la victime paie l'extorqueur pour le code clé pour déverrouiller l'appareil[1]. »

Cyberassurance

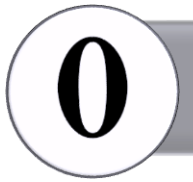
« La cyberassurance est un produit d'assurance conçu pour aider les entreprises à se prémunir contre les effets possiblement dévastateurs de la cybercriminalité[2]. »

Divulgiciels

« Le divulgiciel vise à demander un bien, un service ou un paiement pour prévenir la violence ou la destruction de biens. Certains cybercriminels… demandent de l'argent avant de vous blesser[1]. »

Risques pour la sécurité au travail à domicile

Puisque de nombreuses organisations ont mis en place des procédures de travail à domicile, le risque de cyberattaques et d'atteintes à la sécurité est élevé.



Sécurité confiance zéro

« Confiance Zéro affirme que quiconque se connecte à un réseau – qu'il soit externe ou externe – représente une menace possible. Cette approche remplace l'approche "château entouré de douves" en matière de sécurité, où les organisations protègent leurs périmètres et assument que tout à l'intérieur est donc sûr[3]. »

Stratégie de sécurité axée sur le risque

Même si les gouvernements s'orientent vers une approche axée sur les risques en matière de sécurité des renseignements, il faut équilibrer la sécurité et les besoins des utilisateurs.

1. « Cyber Extortion: Ransomware vs. Extortionware » 2018, alpinesecurity.com (en anglais)
2. « What is Cyber Insurance? » 2020. cisco.com (en anglais)
3. « How governments can trust IT security: It's all about identity » 2020, gcn.com (en anglais)

4. Étude de cas : Le Centre canadien pour la cybersécurité (CCC)

Le secteur public s'engage à promouvoir la collaboration bilatérale sur la cybersécurité au Canada. Certaines organisations, comme le Centre canadien pour la cybersécurité (CCC), offrent un soutien interjuridictionnel qui peut faciliter la collaboration dans le domaine de la cybersécurité.

Qu'est-ce que le CCC?

En vertu de la *Loi sur le Centre de la sécurité des télécommunications* (CST), le financement a été approuvé pour le nouveau Centre canadien de la cybersécurité (CCC), qui a regroupé les efforts fédéraux sous un même cadre. Le CST est le chef de file national du Canada en matière de renseignements étrangers sur les transmissions et d'opérations cybernétiques, ainsi que l'autorité technique en matière de cybersécurité[1].

Le CST est né des efforts de décodage de la Seconde Guerre mondiale au Conseil national de recherches du Canada, et son objectif initial était un organisme de cryptologie qui aide à déchiffrer le renseignement d'adversaires étrangers. Le CCC, également connu sous le nom de « Centre pour la cybersécurité », a ouvert ses portes le 1er octobre 2018 pour appuyer le leadership et la collaboration entre les différents ordres de gouvernements ainsi qu'entre les partenaires nationaux et internationaux, tout en fournissant une ressource unique claire et fiable aux citoyens et aux entreprises canadiens. Il s'agit de l'autorité du Canada en matière de cybersécurité et une source unique de conseils, d'orientation, de services et de soutien d'experts du gouvernement du Canada[2].

Pour en apprendre davantage sur le CCC, cliquez ici.

Orientation, outils et services du CCC

Le soutien du CCC peut contribuer à favoriser la collaboration dans l'écosystème canadien de la cybersécurité, par les moyens suivants :

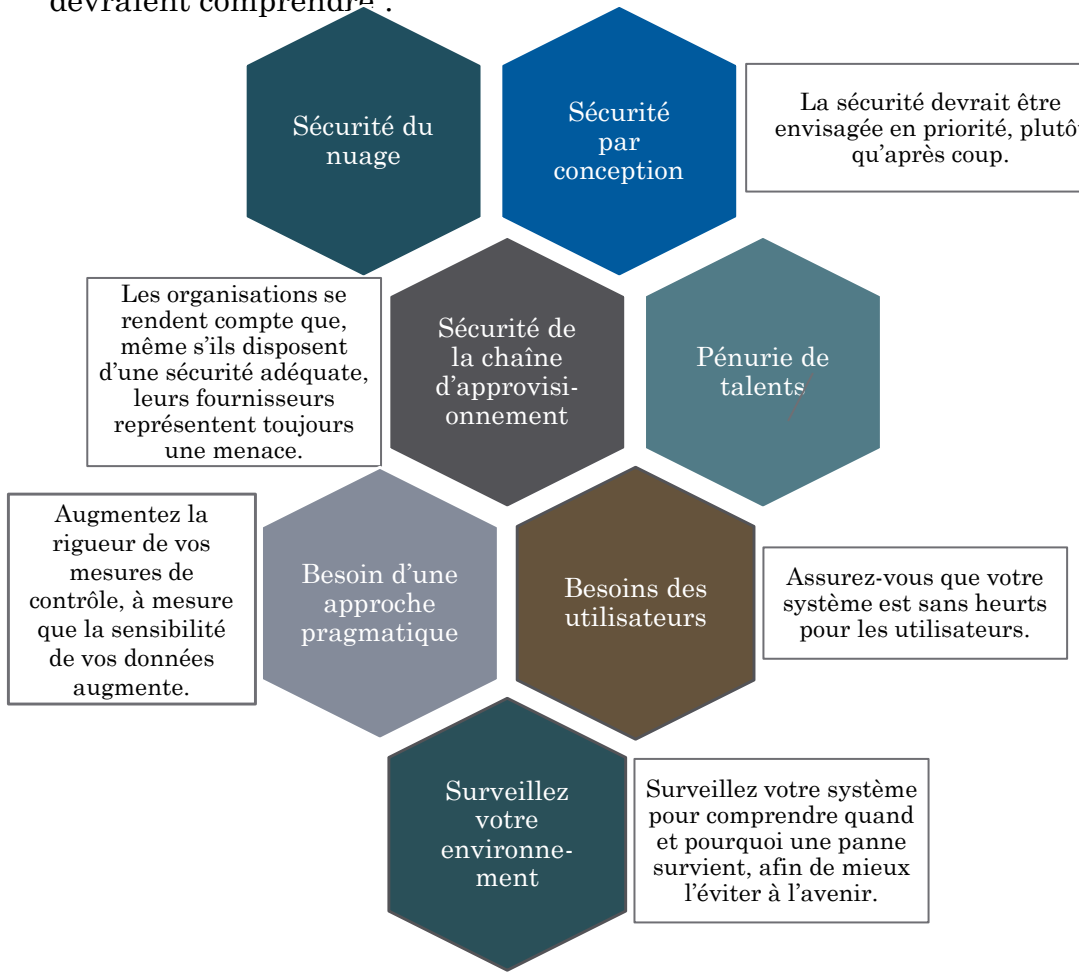
- Communiquer d'incidents de cybersécurité (rapports d'hameçonnage par courriel, entre autres).
- Fournir des conseils et une orientation sur de nombreux sujets, comme l'orientation sur la vidéoconférence, la protection du domaine de courrier, les avantages et risques liés à l'adoption des services fondés sur l'infonuagique par votre organisation et d'autres sujets disponibles à l'adresse suivante : https://cyber.gc.ca.
- Services comme Alerte (courriel sensible au temps lié à un problème informatique à incidence élevée).
- Communiquer des ressources, comme la publication récente « Configurations pour les services Microsoft Office 365 : Modèle de déploiement local dans l'infonuagique publique ». Ce document doit être suivi et on peut donc le fournir sur demande à l'adresse contact@cyber.gc.ca.

Communiquez avec le CCC pour obtenir une liste complète des outils et services disponibles.

1. « Le CST vu de l'intérieur » 2020, cse-cst.gc.ca
2. « À propos du Centre pour la cybersécurité » 2020, cyber.gc.ca

5. Où les gouvernements devraient-ils concentrer leurs efforts sur la cybersécurité?

D'autres mesures doivent être mises en place pour protéger la cybersécurité au Canada. Selon les experts, certains domaines d'intervention clés pour permettre la collaboration du gouvernement en matière de cybersécurité devraient comprendre :



6. COVID-19 entraînant une augmentation des cybermenaces

Dans le contexte de la pandémie de la COVID-19, les Canadiens et les organisations canadiennes ont adopté la technologie pour rester mieux connectés, adopter des ententes de travail de rechange et mettre leurs activités commerciales en ligne. La crise s'est toutefois révélée opportune pour une augmentation de la cybercriminalité.

Par exemple, le CCC a constaté une augmentation du nombre d'escroqueries liées à l'hameçonnage et aux logiciels malveillants dans le domaine de la santé. Les menaces ne concernent pas seulement la santé, car il y a aussi une augmentation de l'activité criminelle en ligne.

Bulletin sur les activités de cybermenaces liées à la COVID-19 :

Le présent bulletin met en garde contre le fait que les auteurs de menace cibleront probablement les organisations menant des recherches liées à la COVID-19 afin de voler la propriété intellectuelle liée à la pandémie. Les intérêts étrangers sont également susceptibles de chercher d'autres renseignements, comme l'avertissement précoce des interventions en santé publique (p. ex., les restrictions de voyage).

Bulletin quotidien : Tendances du mois
Juin 2020

Transformation numérique

La crise de la COVID-19 a signifié un bond en avant dans le passage à la transformation numérique. Vous pouvez en lire davantage ici.

Alors que la pandémie fait des ravages, il est important de maintenir l'élan. Vous pouvez en lire davantage ici.

Services publics axés sur les utilisateurs

Au cours des dernières semaines, certains ministères ont accéléré le changement et lancé de nouveaux services à une vitesse record, mettant sur pied des services publics en quelques jours plutôt qu'en quelques mois. Vous pouvez en lire davantage ici.

Technologie de reconnaissance faciale

Amazon arrête l'utilisation par la police de sa technologie controversée de reconnaissance faciale pendant un an, alors qu'elle attend la législation fédérale pour la réglementer. Vous pouvez en lire davantage ici.

IBM sort du marché de la reconnaissance faciale. Vous pouvez en lire davantage ici.

Autres articles qui méritent d'être soulignés ce mois-ci :

COVID-19 Proves the Essential Nature of Government (en anglais)

IT modernization in the time of COVID-19: How government investment in critical IT systems can enhance citizen services (en anglais)

Foreign cyberthreats to Canada persist: spy agency (en anglais)

Designing public services in a user-centred way in a time of crisis (en anglais)

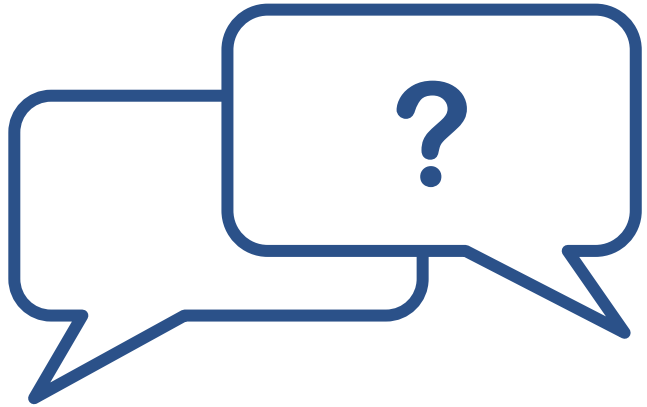
Is a 'Cyber Pandemic' Coming? (en anglais)

Référentiel de recherche

Accédez au référentiel de recherche des Citoyens d'abord ici.

Lectures complémentaires

- Cyber Security Today – A look at the future of work (en anglais)
- Five post-pandemic pivots in Canadian security and intelligence (en anglais)
- Taking a people-centric approach to federal cybersecurity (en anglais)
- Cyber Security Today- Take the time to find ransomware, how a ransomware gang recruits partners and a Norwegian fund victimized for $10 million (en anglais)
- How Security Leaders Can Manage Cyber-Risk During COVID-19 (en anglais)
- Reconnaissance faciale: « Un risque grave de surveillance de masse »



Nous serons ravis d'entendre votre avis!

Connaissez-vous quelqu'un qui souhaite consulter le rapport exécutif des conseils mixtes? Veuillez partager une copie de ce rapport.

Si vous n'êtes pas déjà abonné, vous pouvez maintenant vous abonner pour recevoir le rapport exécutif en vous inscrivant ici. Veuillez faire parvenir vos questions ou suggestions à info@iccs-isac.org.