Communications Security Establishment
Centre de la sécurité des télécommunications

CYBER JOURNAL

NUMÉRO 13 – AOÛT 2018

DANS CE NUMERO

MOT D'OUVERTURE

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

MELTDOWN ET SPECTRE

SUJET TENDANCE : L'INFONUAGIQUE

DU NOUVEAU SUR LA COMSEC

ASSEMBLYLINE

LE CST DANS LA COMMUNAUTÉ : HACKERGAL

NOUVELLES DU CFSTI

AU SUJET DU PRÉSENT BULLETIN

ABONNEMENT

COMMUNIQUEZ AVEC NOUS

UN PARTENARIAT POUR DES SYSTÈMES CANADIENS SÉCURISÉS ET RÉSILIENTS

La cybersécurité représente l'un des plus grands défis économiques et sociaux que nous devons relever dans l'ère numérique d'aujourd'hui. Par la création du Centre canadien pour la cybersécurité, annoncée dans le Budget de 2018, le gouvernement fédéral démontre son engagement à assurer la cybersécurité du Canada. En réunissant des unités clés de Sécurité publique Canada, de Services partagés Canada et du CST, le Centre pour la cybersécurité préconise une approche collective fondée sur l'expertise canadienne de calibre mondial que nous possédons déjà en matière de cybersécurité.

Le Centre sera ouvert au public, et des intervenants des secteurs privé et public et du milieu universitaire pourront y travailler côte à côte, dans des espaces de collaboration et d'innovation, afin de confronter les enjeux les plus complexes de la cybersécurité au Canada.

En travaillant en collaboration, nous pourrons rassembler les problèmes qui nous touchent et trouver des solutions communes, tout en développant des techniques et des outils de cyberdéfense plus robustes. Le but ici, c'est de travailler de façon plus intelligente, pas plus fort, afin de contrer les menaces complexes auxquelles nous devons tous faire face.

Le Centre pour la cybersécurité servira de guichet unique où les utilisateurs et les organisations trouveront le soutien qu'il leur faut pour renforcer leur sécurité et leur résilience afin de se prémunir contre les cybermenaces. Le Centre formulera des avis raisonnables, compréhensibles, réalistes et efficaces pour les Canadiens, tant pour les citoyens que les organisations.

La création du Centre démontre clairement que le gouvernement du Canada comprend la nature essentielle de la cybersécurité et endosse un rôle de direction en ce sens. Par cet investissement dans la cybersécurité, le Canada se montre déterminé à renforcer la sécurité et la résilience afin de se protéger contre les cybermenaces.

Original en anglais signé par

Scott Jones
Dirigeant désigné, Centre canadien pour la cybersécurité et chef adjoint, Sécurité des TI

www.cse-cst.gc.ca

Les conseils présentés ne sont ni exhaustifs, ni universels.

LE CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Le milieu canadien de la cybersécurité entre dans une ère nouvelle et excitante. Dans le Budget de 2018, le gouvernement a reconnu l'importance d'investir dans la cybersécurité. En matière d'économie et de sécurité nationale, la cybersécurité représente l'un des plus importants défis auquel doit faire face le Canada, et nous devons miser sur la collaboration si nous voulons le relever. Le gouvernement a réaffirmé son engagement visant à instaurer un système fédéral de gouvernance solide destiné à protéger les Canadiens et leurs renseignements personnels sensibles.

Dans le Budget, des fonds ont été accordés à la Stratégie nationale de cybersécurité, qui propose de nombreuses initiatives auxquelles plusieurs organismes fédéraux seront appelés à participer. Sécurité publique Canada dirige cette stratégie, qui découle des consultations menées dans le cadre de l'examen de la cybersécurité de 2016. L'une des plus importantes initiatives consiste en la création du Centre canadien pour la cybersécurité, lequel sera chapeauté par le CST. Le Budget prévoit une somme de 155,2 M$ sur cinq ans pour la création de ce centre, de même que 44,5 M$ par la suite.

Le Centre pour la cybersécurité préconisera une approche collective en matière de cybersécurité, qui permettra de tabler sur l'expertise de calibre mondial que le Canada a déjà acquise dans le domaine. Au Canada, c'est le Centre pour la cybersécurité qui fera autorité à l'échelle fédérale. Il s'agira de la source d'expertise unifiée du gouvernement du Canada pour les conseils, avis et services en soutien aux activités de cybersécurité.

Avec l'appui de ses partenaires, le Centre pour la cybersécurité sera le mieux placé pour résoudre les difficultés complexes que pose la cybersécurité dans un environnement en constante évolution. Il fera avancer les partenariats et le dialogue avec d'autres administrations, le milieu des affaires, le milieu universitaire et des partenaires internationaux.

En regroupant sous un seul toit l'expertise cybernétique opérationnelle du gouvernement fédéral, le nouveau Centre pour la cybersécurité sera pour les citoyens et les entreprises du Canada une source bien établie et fiable de conseils en la matière.

Le Centre façonnera l'avenir de la cybersécurité du Canada en adoptant une approche de cyberdéfense proactive, novatrice et axée sur la collaboration et en s'appuyant sur les forces qui se sont développées au sein du gouvernement du Canada. Le Centre pour la cybersécurité réunira 750 employés provenant des unités opérationnelles de cybersécurité de Sécurité publique Canada, de Services partagés Canada et du CST. Ces employés auront l'occasion de travailler au sein d'un organisme de pointe unique et axé sur l'avenir. À titre de dirigeant désigné, Scott Jones prendra les rênes du nouveau Centre pour la cybersécurité lorsqu'il ouvrira ses portes en octobre 2018.

Toutes les fonctions du Centre canadien de réponse aux incidents cybernétiques (CCRIC) et de la campagne de sensibilisation « Pensez cybersécurité » de Sécurité publique Canada seront transférées au Centre pour la cybersécurité.

Certaines fonctions du Centre des opérations de sécurité de Services partagés Canada seront transférées au Centre pour la cybersécurité.

Au CST, l'ensemble du secteur d'activités de la Sécurité des TI sera transformé pour faire partie du Centre pour la cybersécurité.

En nous appuyant sur notre expertise collective, nous pourrons établir des partenariats solides, créer de nouvelles techniques de cybersécurité essentielles, et assurer la résilience de l'environnement de cybersécurité. Grâce à cet investissement dans la cybersécurité du Canada, et en continuant de travailler ensemble, nous saurons renforcer la posture du Canada et sa résilience face aux cybermenaces.

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Les conseils présentés ne sont ni exhaustifs, ni universels.

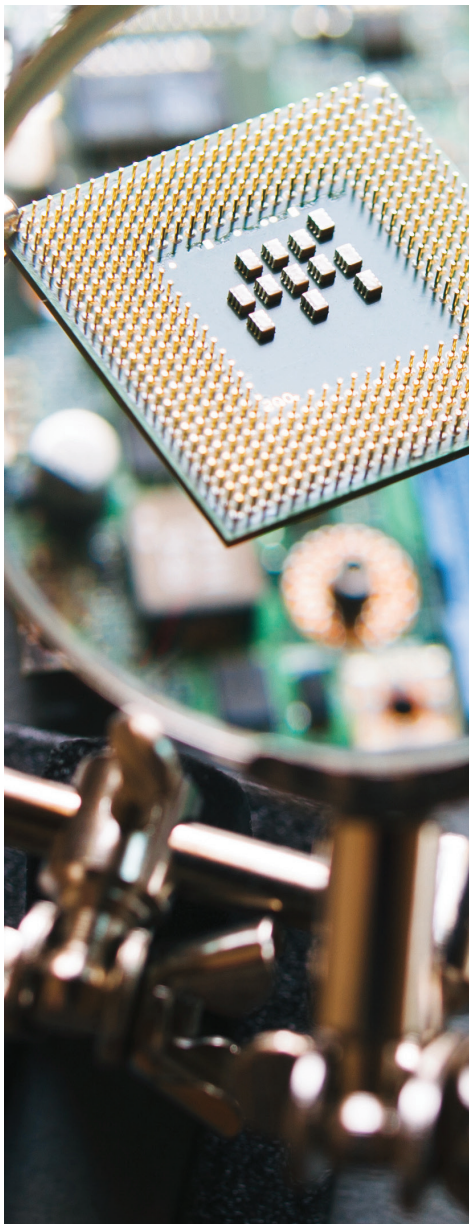
MELTDOWN ET SPECTRE : DEUX VULNÉRABILITÉS QUI CHANGENT LA DONNE POUR LES CYBERMENACES

En janvier dernier, une annonce inquiétante a secoué le monde : presque toutes les puces de processeur d'appareils informatiques comportaient deux vulnérabilités critiques, qu'on a appelées Meltdown et Spectre. En effet, des auteurs de menaces pourraient se servir de ces défauts pour accéder à la mémoire protégée d'ordinateurs, ce qui pose un risque pour les données chiffrées et l'information sensible des utilisateurs. Comme ces défauts touchent pratiquement toutes les puces fabriquées depuis 1995, il s'agit d'un problème d'envergure.

Depuis l'annonce, de nombreux fabricants informatiques et fournisseurs de systèmes d'exploitation ont lancé des correctifs visant à protéger leurs logiciels contre l'exploitation de ces vulnérabilités. Toutefois, un simple correctif ne saurait changer le fait que chacun de nos ordinateurs contient sans doute une puce qui a l'un ou l'autre de ces défauts. Quelles seront donc les conséquences à long terme?

D'abord, il faudrait procéder à la réfection du matériel au plus vite, surtout au sein de certains ministères du gouvernement du Canada. Selon un rapport de Bloomberg, les secteurs réglementés, comme les organismes gouvernementaux et les institutions de santé publique, risquent d'être plus exposés à ces bogues que d'autres organisations. Cela s'explique en partie par le fait que ces organismes utilisent de vieux systèmes désuets et que les correctifs visant à atténuer les risques liés à ces vulnérabilités pourraient ralentir davantage ces systèmes vieillissants.

Pire encore, les auteurs de menaces disposent maintenant de nouvelles vulnérabilités à exploiter : non pas dans les logiciels mais dans le matériel même des ordinateurs. Certes, des défauts ont déjà été décelés dans le matériel informatique, mais jamais de l'ampleur de Meltdown et Spectre. L'exploitation des



vulnérabilités dans le matériel plutôt que les logiciels risque de devenir pratique courante.

Il est avantageux de discuter des problèmes liés au matériel informatique sur la scène publique. On peut maintenant s'attendre à ce que des chercheurs en cybersécurité, des ministères et diverses organisations étudient l'impact de Meltdown et Spectre au cours des prochaines années. Malheureusement, les auteurs de cybermenaces feront de même, et les professionnels de la sécurité devront revoir leur façon de faire afin de pouvoir contrer ces nouvelles menaces.

Même si Meltdown et Spectre sont venus perturber l'environnement de cybersécurité, on peut prendre la situation en main. Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) a diffusé une alerte qui propose des mesures et des liens vers des guides d'atténuation des risques recommandés. Ces sources d'information peuvent aider tant les ministères du gouvernement du Canada que le secteur privé à réduire leur exposition aux menaces et à mieux se préparer à l'évolution des cybermenaces.

Bien que nous ne puissions rien faire dans l'immédiat pour régler les problèmes liés à Meltdown et Spectre, le CST exhorte les organisations à continuer de prendre des mesures proactives et à se tenir au courant des nouvelles vulnérabilités. Assurez-vous de mettre en œuvre des plans robustes pour l'application des correctifs et des processus de renouvellement continu des TI, qui constituent d'importants moyens de défense contre les risques que pose l'infrastructure de TI vieillissante. Si vous suivez les mesures suggérées du CCRIC, les 10 meilleures mesures de sécurité des TI du CST et les pratiques exemplaires en cybersécurité, vous éloignerez le spectre des cybermenaces.

Les conseils présentés ne sont ni exhaustifs, ni universels.

INFONUAGIQUE : LES BONS CÔTÉS DU NUAGE

Vous entendez parler du nuage partout et vous vous demandez pourquoi? C'est que l'infonuagique présente de nombreux avantages qui peuvent transformer votre quotidien en offrant un accès pratique et sur demande à un répertoire partagé de ressources informatiques configurables. Cet outil connaît de plus en plus de succès auprès du gouvernement, des entreprises et des particuliers en raison de ses avantages quant à la productivité et à la sécurité, et des économies qu'il permet de faire. Grâce à l'infonuagique, les utilisateurs peuvent trouver des solutions ciblées et créatives aux problèmes opérationnels de tous les jours, tant sur le plan commercial que personnel.

En passant à l'infonuagique, vous pourriez révolutionner la manière dont vous utilisez les TI.

PERFORMANCE DU SERVICE

L'auto-approvisionnement en ressources informatiques peut réduire considérablement le temps de réponse aux besoins. Les niveaux de service garantis par l'entremise d'un contrat et fondés sur des paramètres aident à assurer des niveaux de rendement uniformes.

SÉCURITÉ

Les fournisseurs de services infonuagiques détiennent des certifications de sécurité internationalement acceptées et évaluées par les professionnels de sécurité de tierces parties. Ces certifications comportent des fonctions de sécurité solides qu'un consommateur aurait de la difficulté à financer à lui seul.

INNOVATION

De nouvelles fonctions sont constamment déployées, et le coût est amorti sur l'ensemble de la clientèle. On peut simplement s'abonner à de nouvelles technologies, comme les médias sociaux, les plateformes mobiles et les outils analytiques, ce qui évite de faire d'importants investissements en capital.

AGILITÉ

On peut accéder rapidement à des ressources informatiques à fonctions multiples, selon la capacité requise pour mener des projets de l'étape de la planification à la pleine exploitation.

EXTENSIBILITÉ

Les niveaux de services peuvent être accrus ou réduits en fonction de la demande. Les clients ne payent que les services qu'il leur faut pendant le temps qu'il leur faut.

Les conseils présentés ne sont ni exhaustifs, ni universels.

À CHACUN SON NUAGE. LEQUEL EST POUR VOUS?

Vous avez décidé que l'infonuagique vous convient. Et maintenant? Il s'agit de vous renseigner sur les divers services et modèles de déploiement, puis de choisir ceux qui répondent le mieux aux besoins de votre organisation. Il faut bien y réfléchir, car le choix d'un modèle de service infonuagique aura un effet à long terme sur votre organisation. La même solution ne saurait convenir à tous. C'est important de choisir le modèle approprié de service infonuagique et de déploiement en nuage. La liste ci-dessous n'est pas exhaustive, mais elle fait état des modèles les plus courants.

MODÈLES DE SERVICE

LOGICIEL EN TANT QUE SERVICE (MODÈLE SaaS)	PLATEFORME EN TANT QUE SERVICE (MODÈLE PaaS)	INFRASTRUCTURE EN TANT QUE SERVICE (MODÈLE IaaS)
Le SaaS est un modèle de distribution de logiciels selon lequel des applications sont achetées ou hébergées par un fournisseur de services infonuagiques, puis mises à la disposition des clients, qui peuvent les utiliser sur Internet. On élimine ainsi la nécessité d'installer et de tenir à jour des logiciels sur des ordinateurs locaux. De nombreux ministères du gouvernement du Canada utilisent des services semblables, mais sur un réseau plutôt que sur Internet.	Le PaaS consiste en une plateforme qui fournit un environnement sûr pour développer, tester et déployer des applications. C'est un modèle de service très souple qui permet de procéder rapidement aux déploiements. Il prévoit aussi l'ajout de fonctions additionnelles visant à faciliter le développement et le déploiement d'applications.	Dans un modèle IaaS, les utilisateurs achètent de l'espace de stockage dans le nuage en fonction de leur consommation. Il revient aux utilisateurs d'accéder à leurs propres données, de les surveiller et de les gérer, même si elles sont stockées dans une infrastructure à distance. Les fournisseurs de services infonuagiques de type IaaS assurent habituellement la gestion du matériel, le stockage et le réseautage, de même que d'autres services qui peuvent être assortis à des frais supplémentaires.

MODÈLES DE DÉPLOIEMENT

NUAGE PUBLIC	NUAGE PRIVÉ	NUAGE COMMUNAUTAIRE
Un nuage public permet d'accéder à des ressources partagées de manière économique et efficiente. Ce type de nuage se trouve à l'extérieur de l'organisation, et on a accès à distance aux applications et au stockage de données. Souvent, vous partagez la même infrastructure que plusieurs autres organisations, c'est-à-dire que vos données sont stockées sur le même serveur qu'elles.	Le nuage privé offre au client un meilleur contrôle de son infrastructure et de ses ressources informatiques. Dans ce modèle, les services et l'infrastructure se trouvent sur des réseaux privés et sont déployés à l'intention d'une seule organisation.	Le nuage communautaire consiste en une infrastructure unique partagée par plusieurs organisations et dont l'utilisation est réservée aux utilisateurs approuvés par la communauté en question. Généralement, il est monté par un groupe d'organisations qui ont des objectifs communs. Il peut être géré par l'organisation ou un tiers, et il peut se situer sur place ou à distance.

NUAGE HYBRIDE

Le nuage hybride est une combinaison de nuages publics et privés. Il permet aux organisations d'utiliser plusieurs fournisseurs de service et d'accéder facilement aux options les plus efficientes pour chacun de ses besoins organisationnels.

Les conseils présentés ne sont ni exhaustifs, ni universels.

COMMENT ASSURER LA CYBERSÉCURITÉ? MAÎTRISEZ LES RUDIMENTS DE LA SÉCURITÉ INFONUAGIQUE

Les fournisseurs de services infonuagiques (FSI) offrent des services sur demande et l'accès à des environnements informatiques adaptables, une option souple et novatrice pour remplacer les centres de données conventionnels gérés sur place par les organisations à qui ils appartiennent. Comme pour toute composante des technologies de l'information (TI), il faut étudier attentivement les options de l'infonuagique pour tenir compte des risques liés à la sécurité des TI. On conseille à toutes les organisations, qu'elles soient du secteur public ou privé, d'appliquer les rudiments de la sécurité infonuagique du CST pour analyser leurs besoins particuliers et pour évaluer, choisir, se procurer et surveiller les services du nuage public qui répondent le mieux à ces besoins.

Ce n'est pas toujours évident de comprendre les risques liés à l'adoption de services infonuagiques. Pour vous aider, le CST a fait ressortir les principes fondamentaux de la sécurité qu'il convient de suivre pour intégrer les services infonuagiques dans votre infrastructure des TI existante.

LES RUDIMENTS DE LA SÉCURITÉ INFONUAGIQUE

- Comprendre les exigences opérationnelles en matière de sécurité
- Assurer la protection et la résilience des actifs
- Anticiper une atteinte à la sécurité et planifier en conséquence

- Appliquer des contrôles d'accès robustes
- Vérifier et surveiller l'accès aux services
- Assurer l'utilisation sécurisée des services

- Faire affaire avec des fournisseurs axés sur la sécurité
- Adopter un cycle de conception et de développement axé sur la sécurité
- Assurer une séparation adéquate avec les autres clients

Le CST s'apprête à publier un document détaillé sur les rudiments qui orientera les organisations dans l'évaluation des risques liés à la sécurité qu'il convient de faire avant de passer au nuage. Ces rudiments permettront aux organisations de déterminer si un service infonuagique particulier répond à leurs exigences en matière de sécurité et s'il est en mesure de gérer leurs données en toute sécurité. Suivez ces neuf principes fondamentaux, et la posture de cybersécurité de votre organisation sera au septième ciel, dans le nuage.

Les conseils présentés ne sont ni exhaustifs, ni universels.

DU NOUVEAU SUR LA COMSEC AU CST

En décembre 2017, le CST s'est doté de deux directives qui changent la manière dont l'équipement et les clés cryptographiques sont gérés. Ces nouvelles directives sur la sécurité des réseaux découlent d'efforts concertés à long terme visant à consolider les avis et conseils du CST en matière de sécurité.

La Directive en matière de sécurité des TI sur la gestion de l'équipement et des clés cryptographiques approuvés par le CST pour sécuriser un réseau de télécommunications (ITSD-04A) porte sur l'établissement des autorisations du gouvernement du Canada (GC) en ce qui a trait aux réseaux cryptographiques.

Quant à elle, la Directive en matière de sécurité des TI sur la commande de clés cryptographiques (ITSD-09) porte sur les procédures à suivre pour commander du matériel de chiffrement. Ensemble, ces directives préconisent une approche de gestion déterminante en matière d'emploi des capacités réseau et s'adaptent mieux à la complexification de la prestation des services de sécurité des communications (COMSEC pour *Communications Security*) au sein du GC.

ITSD-04A	ITSD-09
• Autorise les autorités de contrôle (ConAuth) et les autorités de commandement (CmdAuth) à mener leurs activités dans le cadre de la COMSEC de leur ministère • Établit la nécessité d'inscrire les réseaux cryptographiques auprès des Services à la clientèle en matière de COMSEC (SCC) • Propose le Plan de soutien lié au matériel de chiffrement (PSMC) en tant qu'outil essentiel pour le renforcement de la COMSEC	• Établit le processus de commande de clés qui enclenche la COMSEC et la maintient à long terme • Offre le soutien du Centre d'assistance en matière de matériel cryptographique (CAMC) pour toutes les questions liées à la COMSEC

Les conseils présentés ne sont ni exhaustifs, ni universels.

CHAÎNE DE MONTAGE

ASSEMBLYLINE – AUTOMATISER L'ANALYSE DES MALICIELS POUR VOUS FACILITER LA TÂCHE

Assemblyline est un outil d'analyse et de détection de maliciels développé par le CST, qui a été mis à la disposition de la collectivité de la cybersécurité en octobre 2017. La diffusion d'Assemblyline sert les intérêts du Canada et le travail qu'effectue le CST pour protéger les systèmes canadiens et permet à la collectivité de la cybersécurité d'assurer l'évolution de ce logiciel de source ouverte fort utile.

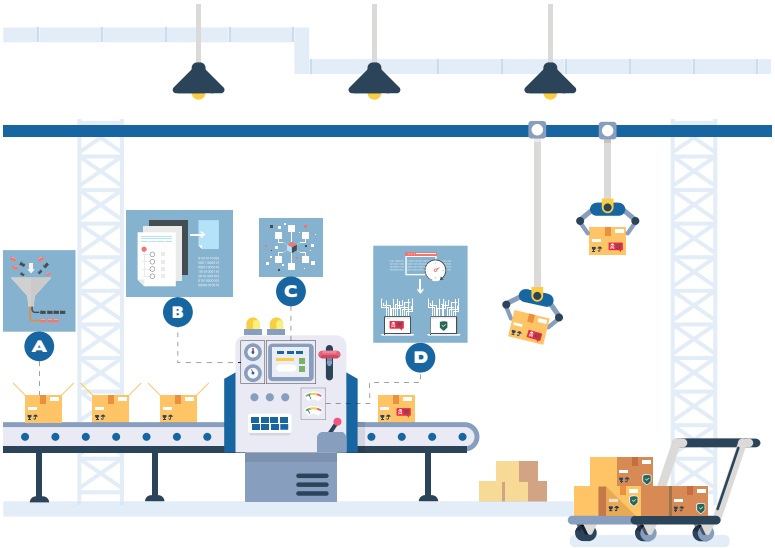
Le CST, qui a déjà eu la réputation d'être un « organisme d'espionnage ultra-secret », a franchi une grande étape en rendant public l'un de ses outils pour la toute première fois. Plus important encore, cet outil facilite grandement la tâche aux professionnels de la cybersécurité.

Assemblyline a été conçu pour accroître la transparence dans la manière dont les données liées aux maliciels sont recueillies et utilisées. Le Canada continue d'adopter de nouvelles technologies numériques, ce qui augmente de façon considérable la quantité de données que les organisations doivent traiter chaque jour. Or, compte tenu des 377 000 utilisateurs qui accèdent aux réseaux internes du gouvernement, il est devenu pratiquement impossible de gérer les maliciels au cas par cas.

Grâce aux fonctions du logiciel qui permettent de détecter et de trier automatiquement les maliciels, les professionnels de la cybersécurité pourront plutôt se concentrer sur l'analyse des anomalies puisque leur temps ne sera plus accaparé par les problèmes courants. En créant une plateforme de source ouverte qui permet à d'autres parties de collaborer et d'automatiser la détection des maliciels, les développeurs ont réussi à faciliter la tâche de bien des gens, y compris la leur.

Comme de nombreuses organisations utilisent maintenant Assemblyline, l'environnement global de cybersécurité s'apprête à être plus fort que jamais. Malgré ces progrès, pour que l'outil continue de s'améliorer, tous les utilisateurs doivent continuer de travailler en collaboration. La rétroaction qu'ils donneront au CST lui permettra d'améliorer non seulement Assemblyline mais aussi de futurs outils, ce qui renforcera la résilience du Canada face aux cybermenaces.

On peut se procurer Assemblyline sur BitBucket. Il convient de noter qu'Assemblyline n'est pas conçu pour remplacer les antivirus commerciaux. Si la cybersécurité vous intéresse, joignez-vous au groupe Google d'Assemblyline : https://groups.google.com/d/forum/cse-cst-assemblyline.



Les conseils présentés ne sont ni exhaustifs, ni universels.

LE CST DANS LA COMMUNAUTÉ : LE CST RETOURNE SUR LES BANCS D'ÉCOLE AVEC HACKERGAL

Dans le dernier numéro, nous avons fait état des efforts qu'a déployés récemment le CST pour remédier à la pénurie croissante de compétences ans le domaine de la cybersécurité. Dans le cadre de programmes d'approche communautaire visant toute une gamme d'écoles et de centres communautaires, le CST a présenté à des étudiants et à des adultes les possibilités de carrière dans les domaines de la science, des technologies, de l'ingénierie et des mathématiques (STIM).

Pour combler ce manque de compétences, le CST se penche également sur la réduction de l'écart grandissant entre les sexes. Comme les organisations vouées à la cybersécurité ont de plus en plus de difficulté à doter leurs postes, il est plus important que jamais de combler cet écart dans le domaine des STIM au Canada.

Et l'écart est grand. Selon les données de Statistique Canada, les femmes représentaient 47 % de la main-d'œuvre canadienne en 2016[1]. Or, cette même année, seulement 23 % d'entre elles occupaient un poste dans le domaine de l'informatique et des systèmes informatiques [2]. Malgré une augmentation de 24 % du nombre de femmes inscrites à des programmes d'études dans les STIM entre 2010 et 2016[3] , les hommes dépassent toujours largement les femmes dans ces domaines.

Pour aider à réduire cet écart entre les sexes, le CST a joué un rôle important dans le « hack-o-thon » organisé par Hackergal en décembre dernier. Hackergal est une organisation canadienne qui a pour mission d'initier les filles d'âge scolaire au codage. Lors de cet événement, les filles ont travaillé en groupe pour apprendre les fondements du codage, puis créer des animations en utilisant un bloc de codage simple.

Les étudiantes partaient de divers niveaux d'expérience – certaines avaient déjà fait du codage alors que d'autres ne s'y connaissaient pas du tout. À la fin de la journée, les équipes ont parlé de leur expérience du codage avec les autres participantes et ont reçu de la rétroaction sur leur scénario, la logique, la créativité et la qualité de leur codage. On leur a également remis des certificats et des insignes en reconnaissance de leur excellent travail. Mais la grande récompense, ce fut la confiance qu'ont gagnée les étudiantes et le plaisir qu'elles ont éprouvé à faire du codage.

Des écoles d'un bout à l'autre du pays ont participé à cet événement d'une journée, et des employées du CST se sont rendues sur place à divers endroits à Ottawa pour donner des ateliers et inspirer les étudiantes en leur racontant leur parcours de carrière. Environ 2 900 filles ont participé à l'événement, ce qui en fait le plus grand hack-o-thon jamais organisé par Hackergal.

Bien que l'événement soit conçu pour capter l'attention des participantes et leur permettre d'avoir du plaisir, l'objectif principal de Hackergal est de stimuler l'intérêt des jeunes filles canadiennes pour la technologie. En déployant des efforts dès maintenant pour combler l'écart entre les sexes dans les domaines des STIM et en bâtissant des milieux de travail inclusifs, nous renforcerons l'économie future du Canada tout en favorisant l'établissement d'une main-d'œuvre qui reflète la diversité de la population canadienne.

En prime, grâce à cet événement, des employées talentueuses du CST ont eu l'honneur de servir de mentores auprès d'étudiantes d'écoles locales d'Ottawa. Pour les bénévoles du CST, ce fut l'occasion de retourner sur les bancs d'école. D'ailleurs, l'une de nos bénévoles a pu remettre les pieds dans l'école secondaire qu'elle a fréquentée, où elle a passé la journée à encourager les étudiantes à faire carrière dans les STIM et à leur montrer toutes les possibilités qui s'offrent ici au Canada. D'autres bénévoles ont été fort impressionnées par la soif d'apprendre des participantes. L'événement s'est déroulé dans une ambiance positive, permettant ainsi aux étudiantes de relever les défis et de poser des questions en sachant que leurs camarades leur accorderaient soutien et encouragement.

[1] Statistique Canada, La Journée internationale de la femme... en chiffres, 2017
[2] Statistique Canada, Tableaux de données - profession, Recensement 2016
[3] Statistique Canada, Effectifs et diplômés postsecondaires au Canada, 2015-2016

Les conseils présentés ne sont ni exhaustifs, ni universels.

NOUVELLES DU CFSTI

Au cours des derniers mois, le Centre de formation en sécurité des TI (CFSTI) et l'Agence du revenu du Canada (ARC) ont uni leurs efforts pour élaborer et donner un cours sur la cybersécurité personnalisé à l'intention des informaticiens du groupe CS de l'ARC. Le CFSTI a donné plus de 20 séances de ce cours d'une journée, qui a été adapté aux besoins actuels de l'ARC en matière d'apprentissage, et quelque 600 employés de l'ARC ont reçu la formation. Le cours a porté sur les cybermenaces propres à l'ARC, les rôles et responsabilités de divers postes qui touchent aux processus de cybersécurité et les mesures d'intervention adaptées aux divers rôles qu'il faut prendre en réponse à des incidents liés à la cybersécurité. Une équipe d'instructeurs du CST, en collaboration avec des spécialistes d'expérience de la Sécurité des TI de l'ARC, ont présenté des pratiques exemplaires ainsi que des activités d'apprentissage pratiques. Les informaticiens de l'ARC ont pu ainsi acquérir les connaissances et les compétences nécessaires afin de mieux comprendre le contexte de la cybersécurité.

C'est avec plaisir que le CFSTI annonce la mise sur pied du Programme de formation en cybersécurité pour les cadres du gouvernement du Canada. Ce programme vise à permettre aux cadres supérieurs des ministères et organismes fédéraux d'acquérir des connaissances et d'accéder à des outils et à des ressources pour mieux encadrer leur prise de décision en matière de sécurité des TI et de cybersécurité. Conçu à l'intention de participants qui ne travaillent pas dans le domaine de la sécurité, le programme comporte deux modules en ligne et une séance d'apprentissage par l'action animée par un instructeur qui vise à mieux faire comprendre les cybermenaces et la gestion des risques liés à la sécurité des TI. Chose intéressante, le programme s'adapte au contexte opérationnel particulier des participants et s'appuie sur les menaces et les risques propres au ministère, qui servent de fondement aux discussions et activités dirigées par l'animateur.

Pour organiser une séance de consultation afin de discuter de la prestation de ce programme pour votre organisme, veuillez communiquer avec le CFSTI au 613-991-7110 ou à l'adresse its-education@cse-cst.gc.ca.

Appel aux praticiens de la sécurité des TI! Le Centre de formation en STI tiendra une séance de formation intensive sur la gestion des risques liés à la sécurité des TI du 20 au 23 août. Quelle belle occasion pour les praticiens de la sécurité des TI de l'extérieur de la région de la capitale nationale de venir passer une semaine dans la belle ville d'Ottawa en plein cœur d'été! Ce cours de quatre jours porte sur les grandes notions de la gestion des risques liés à la sécurité des TI, les directives énoncées dans l'ITSG-33, le processus de mise en œuvre de la gestion des risques, ainsi que l'élaboration et l'application de contrôles de sécurité.

AU SUJET DU PRÉSENT BULLETIN

Le Cyberjournal est un bulletin préparé pour les intervenants du gouvernement du Canada et les organismes canadiens qui se penchent sur les technologies actuelles et émergentes. Publié périodiquement, ce bulletin traite des pratiques exemplaires visant à aider les ministères et les organismes à mieux se protéger dans un environnement de menace dynamique.

Par le moyen du Cyberjournal, le CST offre des conseils et des outils afin d'assurer le rôle de premier plan du Canada en ce qui concerne la lutte mondiale contre les cybermenaces. En tant que leader de la cybersécurité au Canada, le CST s'est fixé comme principale priorité d'assurer la protection des renseignements électroniques du Canada.

COMMUNIQUEZ AVEC NOUS

Pour des conseils d'ordre général et de l'assistance relative aux directives de sécurité, communiquez avec les Services à la clientèle de la Sécurité des TI :

✉ itsclientservices@cse-cst.gc.ca
Demandes de renseignements généraux : 613-991-7654

Pour communiquer avec le Centre d'évaluation des cybermenaces :

✉ ctec@cse-cst.gc.ca

Pour toute question relative à un dispositif COMSEC, communiquez avec les Services à la clientèle en matière de COMSEC :

✉ comseclientservices@cse-cst.gc.ca
Demandes de renseignements généraux : 613-991-8495

Les gardiens COMSEC peuvent communiquer avec le Centre d'assistance en matière de matériel cryptographique :

✉ cmac-camc@cse-cst.gc.ca
Demandes de renseignements généraux : 613-991-8600

Pour les services de formation, communiquez avec le Centre de formation en sécurité des TI :

✉ its-education@cse-cst.gc.ca
Demandes de renseignements généraux : 613-991-7110

Les conseils présentés ne sont ni exhaustifs, ni universels.