Centre de la sécurité des télécommunications
Communications Security Establishment

CYBER JOURNAL

NUMÉRO 8 | OCTOBRE 2015

DANS CE NUMÉRO

METTRE EN PLACE UN RÉSEAU ROBUSTE

Au cours des derniers mois, les attaques par déni de service distribué (DDoS pour *Distributed Denial of Service*) dont ont fait l'objet les sites du gouvernement du Canada (GC) ont capté l'attention des Canadiens. En dépit de la nature perturbatrice de ces incidents de cybersécurité, les systèmes du GC et l'information canadienne sensible qu'ils contiennent sont demeurés intacts en raison des mesures de sécurité clés qui avaient été mises en place pour les protéger.

Les ministères et organismes du GC offrent des services aux Canadiens et dépendent de la robustesse des systèmes informatiques pour fournir et maintenir des niveaux de service acceptables. Compte tenu des défis qu'il leur faut surmonter sur le plan de la sécurité, il incombe aux ministères de comprendre les mesures de sécurité qui doivent être mises en place pour protéger les données et rétablir rapidement les services après une cyberintrusion.

Des milliers de tentatives d'infiltration des réseaux du gouvernement sont effectuées chaque jour. Avez-vous une idée claire de votre posture de sécurité générale? Avez-vous dressé un plan réaliste pour ce qui est de combler ces lacunes en matière de sécurité?

Comme octobre est le Mois de la sensibilisation à la cybersécurité, je vous encourage à relancer ces discussions importantes au sein de votre ministère. Dans ce numéro du Cyberjournal, nous expliquerons en quoi Les 10 meilleures mesures de sécurité des TI du CST sont importantes pour vous. La protection efficace de nos réseaux et de l'information du Canada passe inévitablement par une bonne compréhension du contexte des menaces en constante évolution et de la façon dont nous pouvons y faire face en tant que collectivité.

Original signé par

Toni Moffa

Chef adjointe, Sécurité des TI

cse-cst.gc.ca

CYBER JOURNAL

NUMÉRO 8 – OCTOBRE 2015

LA RAISON D'ÊTRE DES 10 MESURES DE SÉCURITÉ DES TI

UNE ENTREVUE AVEC SCOTT JONES, MEMBRE DE LA DIRECTION DU CST

Directeur général, Cyberdéfense, CST

La Direction générale de la cyberdéfense assure la protection des principaux systèmes électroniques du GC contre les cyberintrusions.

Pourquoi les 10 mesures les plus efficaces sont-elles si importantes et pour quelles raisons les ministères du GC devraient-ils mettre en œuvre ces mesures de sécurité?

Contrairement aux autres pratiques exemplaires en matière de TI, les 10 mesures sont fondées sur les connaissances pratiques du CST et sur plusieurs années d'expérience consacrées à l'atténuation des milliers de cyberincidents dont ont été la cible les ministères et organismes du GC. Il s'agit d'une liste de mesures concrètes que peuvent prendre les ministères pour renforcer leur sécurité. Ces mesures ont été élaborées spécifiquement pour aider à atténuer les réelles menaces ciblant le GC.

Qu'adviendra-t-il si ces mesures ne sont pas mises en œuvre par la collectivité du GC?

Leur mise en œuvre est capitale. En 2013, toutes les compromissions dont ont fait l'objet les ministères du GC étaient le résultat direct de l'incapacité à mettre en œuvre les 10 mesures de sécurité des TI. Une fois instaurées, ces mesures réduisent considérablement la surface de menace des ministères et accroissent de façon importante les coûts pour les cyberadversaires.

Certaines de ces mesures sont-elles plus essentielles que d'autres?

Les 10 mesures les plus efficaces sont présentées dans un ordre précis. En commençant par la première mesure, utiliser les passerelles Internet de Services partagés Canada (SPC), puis en mettant en œuvre chacune des mesures subséquentes, les ministères protégeront peu à peu leurs systèmes. La mise en œuvre de la première mesure offre aux ministères une certaine protection, mais elle n'est pas suffisante en soi.

Quel conseil donneriez-vous à un ministère qui tente pour une première fois de mettre en œuvre les 10 mesures les plus efficaces et éprouve des difficultés avec une ou plusieurs de ces mesures?

Il est inutile de partir de zéro. Vous n'êtes pas seul. D'autres ministères n'en sont plus à leurs premiers efforts de mise en œuvre. Je vous suggère donc de tirer profit de l'expérience de vos collègues dans d'autres ministères. Cherchez conseils auprès de différentes collectivités par l'entremise de SPC, de la Direction du dirigeant principal de l'information (DDPI) du Secrétariat du Conseil du Trésor du Canada (SCT) et du Conseil des DPI. Certains ministères ont déjà mis en œuvre les 10 mesures de sécurité les plus efficaces.

Croyez-vous que ces mesures de sécurité changeront considérablement au cours des prochaines années?

Il faut s'attendre à des changements puisque le contexte des menaces continuera d'évoluer. Les 10 mesures les plus efficaces visent la vaste majorité des menaces dont font l'objet les systèmes du GC à l'heure actuelle. Ces mesures devront être adaptées en fonction de l'évolution du contexte de menace. Les principes de base invoqués dans la liste des 10 mesures continueront toutefois d'être impératifs.

Pour quelle raison l'utilisation d'une liste blanche des applications est-elle passée de la première à la dixième position?

Le CST a publié en 2014 la liste des 10 mesures de sécurité des TI les plus efficaces. L'utilisation d'une liste blanche des applications est passée de la première à la dixième position, car en dépit de son efficacité technique, sa mise en œuvre constitue l'une des tâches les plus complexes pour un DPI. En outre, comme elle se trouvait en tête de liste, les ministères y concentraient tous leurs efforts et nous ne voulions pas que ces derniers, dans leur volonté de mener à bien cette tâche, en viennent à ne jamais mettre en œuvre d'autres mesures de sécurité plus essentielles. L'utilisation d'une liste blanche des applications demeure une mesure très efficace et une mise en œuvre en plusieurs phases (en commençant, par exemple, par une utilisation sur les serveurs) s'avérera sans doute plus facile, plus rentable et plus efficace contre les auteurs de menaces qui ciblent actuellement le GC.

90 %
Une solution de gestion des correctifs automatisée permet de prévenir 90 % des attaques logicielles.
(SCMagazine, 2012)

37 %
des employés des ministères du GC ont cliqué sur un courriel de harponnage lors d'un récent exercice pratique.
(CBC, 2014)

75 %
Un antivirus traditionnel n'arrive pas à détecter 75 % des logiciels malveillants les plus courants.
(Computer World, 2012)

LES 10 MEILLEURES MESURES

1 Veillez à ce que votre connexion Internet serve vos intérêts plutôt que ceux des auteurs de menaces. Renforcez vos passerelles Internet par celles fournies par SPC et tirez parti de solutions de cyberdéfense personnalisées.

2 Ne laissez pas votre réseau sans défense. Assurez la mise à jour de vos systèmes en mettant en place un cadre de gestion des correctifs.

3 Gardez farouchement les clés de votre réseau. Réduisez le nombre d'utilisateurs ayant des privilèges d'administrateur et faites en sorte qu'ils changent régulièrement leur mot de passe.

4 Personnalisez et configurez votre système d'exploitation de manière à assurer une meilleure protection. Adoptez une approche intégrée en désactivant tous les ports et les services non essentiels, et en supprimant les comptes inutiles.

5 Triez et stockez votre information en fonction de sa valeur. Segmentez vos réseaux informatiques et définissez des exigences distinctes pour ce qui est de la protection de l'information, de même que des politiques et des contrôles de sécurité différents.

6 Fortifiez votre première ligne de défense en favorisant une culture de sensibilisation dans l'ensemble de votre organisme.

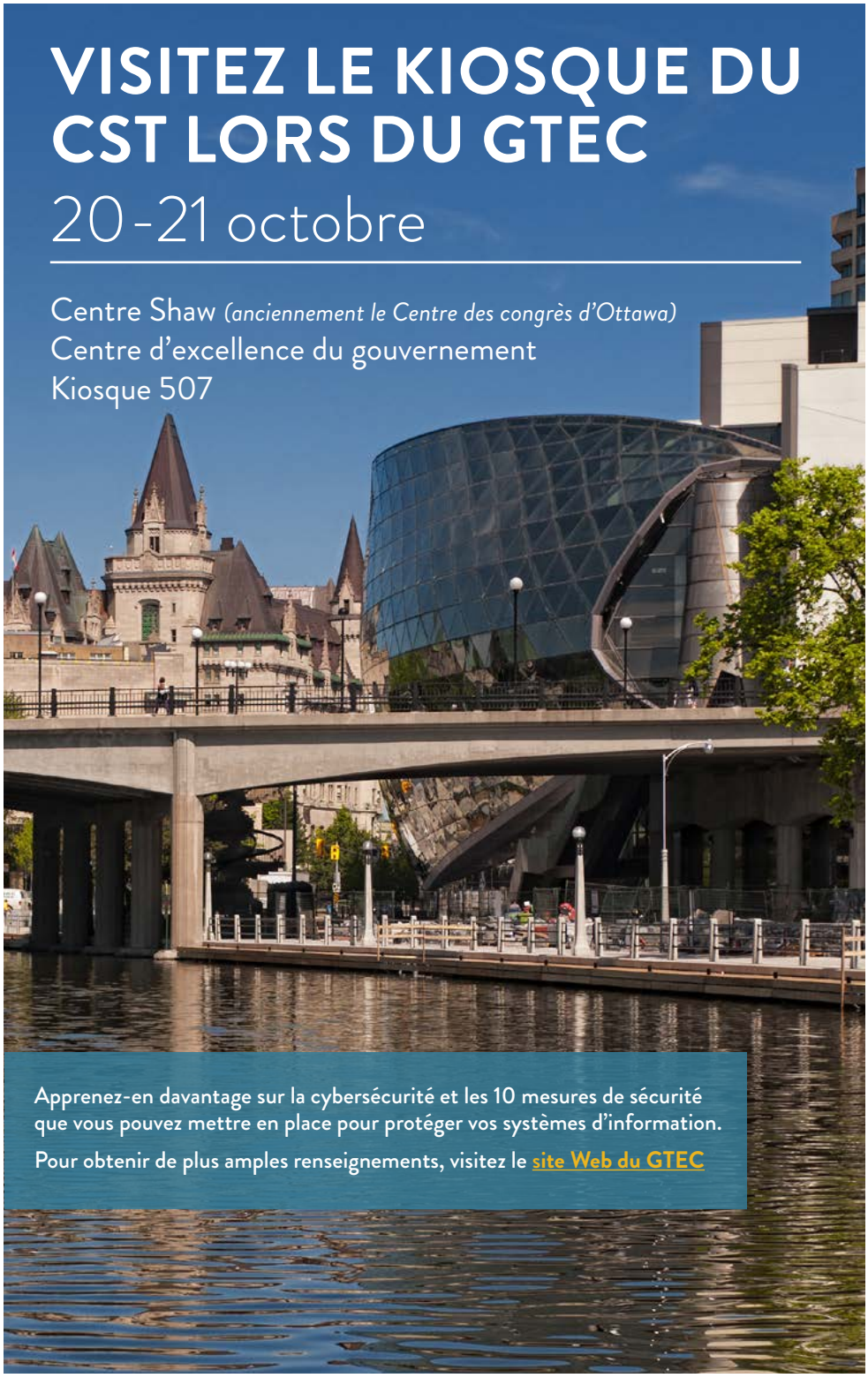
7 Protégez votre information et vos réseaux au moyen d'équipement digne de confiance. Mettez en place un cadre de gestion des appareils et utilisez de l'équipement fourni par le GC.

8 Déployez une solution de système de prévention des intrusions sur l'hôte (HIPS) pour protéger plusieurs points faibles simultanément.

9 Exécutez les navigateurs et les clients de messagerie dans un environnement virtuel isolé, puisqu'ils sont plus susceptibles d'introduire des logiciels malveillants dans vos systèmes.

10 Déterminez quelles sont les applications dont l'exécution est autorisée et bloquez toutes les autres par défaut.

GTEC 2015



VISITEZ LE KIOSQUE DU CST LORS DU GTEC

20-21 octobre

Centre Shaw *(anciennement le Centre des congrès d'Ottawa)*
Centre d'excellence du gouvernement
Kiosque 507

Apprenez-en davantage sur la cybersécurité et les 10 mesures de sécurité que vous pouvez mettre en place pour protéger vos systèmes d'information.

Pour obtenir de plus amples renseignements, visitez le site Web du GTEC

JOHN TURNBULL

DIRECTEUR GÉNÉRAL DE LA CYBERPROTECTION

15 h à 15 h 30,
le 21 octobre
Salle 212

Développement de solutions de sécurité souples : niveaux d'assurance élevé, moyen et de base pour le gouvernement du Canada

L'innovation en matière de technologies est essentielle pour suivre l'évolution des exigences du gouvernement du Canada en matière de communications et de TI. Le Centre de la sécurité des télécommunications, en collaboration avec le Conseil du Trésor et Services partagés Canada, procède à la redéfinition des solutions d'assurance de la sécurité pour le gouvernement du Canada. Cet effort transformera la façon dont le gouvernement développe et déploie des solutions de communication dont le niveau d'assurance est faible, moyen ou élevé. Cette méthode donne une souplesse au développement d'une solution et permet de tirer profit des technologies qui sont disponibles sur le marché. Pensez un instant au jour où il sera possible d'utiliser le BlackBerry Classic ou Passport du gouvernement pour communiquer avec vos collègues en envoyant des messages vocaux ou en échangeant des messages instantanés ou des courriels de façon sécurisée! Joignez-vous au CST pour en apprendre davantage sur la définition des nouveaux niveaux d'assurance et comment ils se traduiront par de nouvelles occasions pour le gouvernement du Canada.

Pour plus de renseignements sur l'horaire des présentations, consultez le Programme des conférences du GTEC.

CYBER JOURNAL

NUMÉRO 8 – OCTOBRE 2015

LA CARTE DE TRAJET DE CYBERSÉCURITÉ DU CST

On sait que les auteurs de menaces tirent parti des habitudes informatiques des employés pour découvrir des points d'entrée dans des systèmes d'intérêt. Il est donc fortement recommandé que les ministères accroissent la sensibilisation de leur personnel en matière de cybersécurité afin d'améliorer leur capacité de reconnaître les activités suspectes. En favorisant une culture de sensibilisation à la sécurité dans l'ensemble de votre organisme, vous fortifiez votre première ligne de défense.

Pour vous aider, le CST a élaboré une nouvelle application interactive sur la cybersécurité qui aborde une multitude de sujets liés à la sécurité dont votre organisme doit tenir compte. Visitez notre Galerie interactive de la STI et prêtez-vous au jeu.

Cette application interactive a remporté trois prix prestigieux :

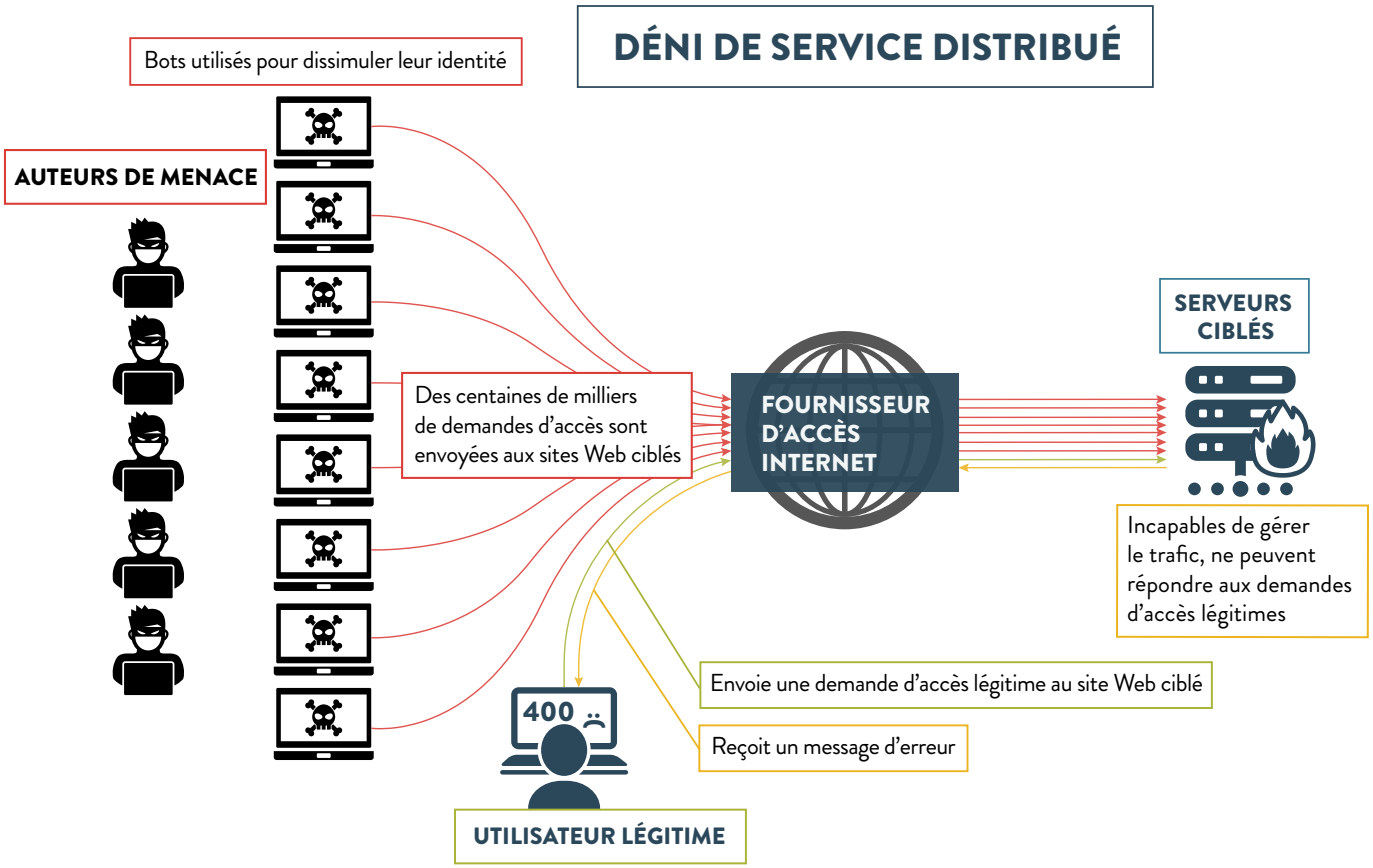
- 2015 Gold Summit International Award for Public Service Multi-Media campaign
- 2015 Merit Award from the International Association of Business Communicators (IABC Ottawa)
- 2015 Federal Information Systems Security Educators' Association (FISSEA) Security Awareness, Training, and Education Contest Peer's Choice Role-Based Training Category

LES DESSOUS DU DÉNI DE SERVICE

On fait souvent référence aux attaques par déni de service (DoS) comme étant des cybermenaces, mais que sont-elles exactement? Les attaques par déni de service sont le résultat de l'envoi massif de données malveillantes par une personne ou un groupe. Elles ont pour but d'empêcher des utilisateurs légitimes d'utiliser des services ou de l'information en ligne, ou de dégrader l'accès à ces services ou à cette information. Les attaques par déni de service visent essentiellement à gêner le fonctionnement des systèmes et sont généralement lancées en vue de protester publiquement contre des mesures prises par des entreprises ou le gouvernement. Dans certains cas, il arrive toutefois que ces attaques soient menées dans le dessein d'acquérir de l'information privilégiée et servent à masquer des compromissions plus sérieuses, comme une exfiltration de données. Outre leur incidence sur la fonctionnalité des systèmes, les attaques par déni de service peuvent avoir les répercussions suivantes :

- Coûts associés au traitement de l'incident;
- Perte ou limitation des fonctionnalités du service touché;
- Perte de productivité;
- Vulnérabilité accrue dans la mesure où les ressources sont affectées à l'atténuation du risque.

Les auteurs de déni de service élaborent ces attaques en vue d'épuiser les ressources d'un réseau, notamment sa bande passante, sa puissance de calcul ou ses systèmes d'exploitation. L'attaque ralentit les fonctions des systèmes et entrave l'accès à celles-ci en paralysant les performances du réseau, en coupant l'accès à un site Web en particulier ou, dans certains cas, en empêchant tout accès à des services Internet. Ces interruptions sont une source de préoccupation pour l'industrie et le gouvernement.



Il existe plusieurs types d'attaques par déni de service. Certains ciblent une infrastructure particulière, d'autres les applications et les bases de données internes d'un réseau. Le type le plus courant utilise l'envoi massif de données pour inonder un réseau d'information, ce qui provoque une surconsommation de la bande passante et une détérioration des performances du serveur réseau. Lors d'une telle attaque, plusieurs ordinateurs

sont contrôlés à distance par plus d'un auteur de menace. Cette menace de grande ampleur constitue un déni de service distribué (DDoS) dans le cadre duquel un groupe d'ordinateurs, composé de centaines ou de milliers d'hôtes compromis (c.-à-d. un réseau de zombies), envoie automatiquement des commandes malveillantes vers une cible unique en vue de dégrader les performances du système ciblé. Il est alors difficile d'établir l'origine de ces incursions par DDoS puisqu'elles impliquent l'hôte ayant été compromis et non l'auteur de menace responsable de l'attaque.

Les activités du GC reposent sur de nombreux services en ligne et ceux-ci sont susceptibles de devenir la cible d'attaques par déni de service. La vaste disponibilité des outils de DDoS sur le Web est un autre facteur qui amplifie ce risque. Pour réduire la probabilité que survienne une attaque par déni de service, il est essentiel d'utiliser des limitations de connexion aux réseaux, des contrôles d'accès aux routeurs, un système de détection d'intrusion et un coupe-feu adéquatement configuré. Il arrive à certaines occasions que les ministères du GC fassent appel à un fournisseur d'accès Internet (FAI) dont les réseaux offrent une bande passante suffisante pour résister aux attaques par DDoS.

Pour protéger leurs réseaux et assurer une meilleure défense, les ministères du GC devraient notamment :

- ✓ Mettre à jour régulièrement les systèmes et appliquer les correctifs;
- ✓ Limiter le nombre de comptes d'administrateur;
- ✓ Installer les plus récentes versions du logiciel antivirus;
- ✓ Configurer les coupe-feu de manière à limiter le trafic à un niveau approprié;
- ✓ Sensibiliser les utilisateurs aux dangers des courriels de harponnage.

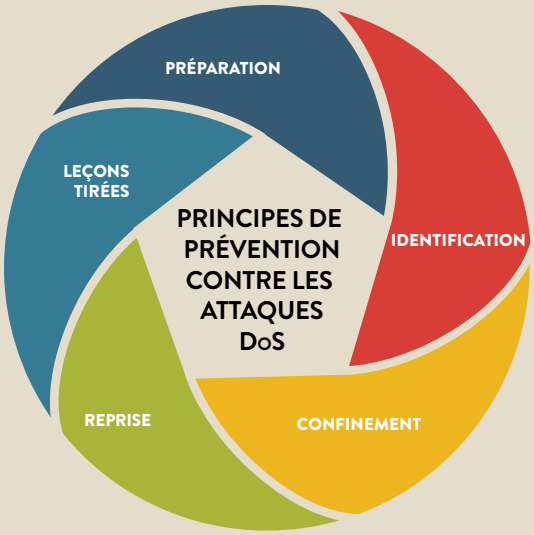
LE CENTRE CANADIEN DE RÉPONSE AUX INCIDENTS CYBERNÉTIQUES (CCRIC) RECOMMANDE LA MISE EN OEUVRE DE CES DIRECTIVES VISANT À ATTÉNUER LES ATTAQUES PAR DÉNI DE SERVICE :

PRÉPARATION

Mettez en place des procédures et des directives claires et exhaustives bien avant que surviennent les attaques.

IDENTIFICATION

Portez attention aux indicateurs d'une attaque par déni de service comme une piètre performance du réseau, l'inaccessibilité de certains services ou une panne de système.



LEÇONS TIRÉES

Dès que possible, passez en revue l'ensemble des décisions prises et des étapes effectuées tout au long du cycle de traitement de l'incident et déterminez les points à l'égard desquels des améliorations devraient être apportées.

CONFINEMENT

Déterminez clairement le périmètre du réseau et les actifs exposés à l'attaque. Installez des systèmes de sécurité de réseau comme des technologies de coupe-feu modernes et envisagez l'utilisation d'un service de protection contre les DDoS offert par un FAI ou par infonuagique.

REPRISE

Les attaques par déni de service peuvent exploiter les limites des ressources d'un serveur. Mettez donc en place un modèle de dimensionnement souple pour ces ressources. Les journaux de connexion peuvent également fournir une liste des adresses IP potentiellement suspectes (si elles ne sont pas falsifiées) au FAI en amont de la cible, à l'équipe d'intervention en cas d'urgence informatique (CERT) nationale et aux organismes chargés de l'application de la loi, et ainsi faciliter la coordination des efforts d'atténuation et d'enquête.

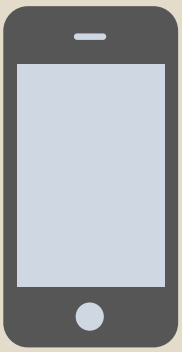
CYBER JOURNAL

NUMÉRO 8 – OCTOBRE 2015

SÉCURITÉ DES DISPOSITIFS MOBILES

Les employés du gouvernement jouent un rôle essentiel dans la protection des biens et de l'information clés du GC. Il est important de se rappeler que les dispositifs mobiles que vous utilisez (en particulier lors de voyages internationaux) peuvent être compromis, ce qui risque d'avoir des répercussions néfastes sur votre ministère, ses renseignements, ses opérations et sa réputation.

POURQUOI VOUS CIBLER?



- Vol et transmission de contenu
- Collecte de données sensibles
- Suivi de vos déplacements
- Modification de vos paramètres
- Réduction de la vitesse de traitement
- Pannes généralisées de système

QUELS SONT LES RISQUES?

- Vol
- Interception (voix et données)
- Maliciels et virus
- Détournement du dispositif
- Pollupostage et harponnage
- Déni de service, interférence ou brouillage
- Mystification ou usurpation d'identité
- Compromission des réseaux à domicile ou du GC

CONSEILS

- Réservez les tâches importantes, comme les transactions bancaires en ligne, pour les réseaux sécurisés.
- N'utilisez jamais votre dispositif mobile pour des discussions de nature sensible ou pour envoyer des messages texte ou des SMS de nature sensible.
- N'utilisez pas de réseaux inconnus ou des points d'accès wifi gratuits.
- L'utilisation des médias sociaux peut poser un risque pour l'information relative à votre emploi, votre famille et votre emplacement géographique.

VOUS VOYAGEZ?

- Avant de partir, communiquez avec votre équipe de sécurité des TI pour obtenir les politiques du ministère et des conseils supplémentaires.
- Utilisez l'équipement fourni par le gouvernement (EFG) plutôt que des dispositifs personnels.
- Désactivez les fonctions telles que Bluetooth et le casque d'écoute sans fil pendant le voyage.
- Tenez pour acquis que toutes les communications transmises par des fournisseurs publics risquent d'être interceptées.
- Signalez tout problème suspect dès que possible à la direction des TI de votre ministère ou organisme.

Pour obtenir de l'information et des conseils sur la façon d'assurer la protection de vos technologies mobiles lors de vos voyages à l'étranger, consultez l'ITSB-87, Technologies mobiles pour les voyages internationaux – Conseils pour les employés du gouvernement du Canada en voyage d'affaires et l'ITSB-88, Technologies mobiles pour les voyages internationaux – Conseils pour les gestionnaires en sécurité des TI du gouvernement du Canada.

CYBER JOURNAL

NUMÉRO 8 – OCTOBRE 2015

MOIS DE LA SENSIBILISATION À LA CYBERSÉCURITÉ 2015

Au cours du mois d'octobre, prenez quelques instants pour passer en revue les pratiques en matière de sécurité disponibles en ligne. Sécurité publique Canada a fourni une liste de conseils de sécurité qui vous aideront à assurer la protection de votre ordinateur personnel.

✓ Protégez votre identité

Utilisez différents noms d'utilisateur et mots de passe pour vos différents comptes. Optez pour une combinaison de chiffres, de lettres et d'autres caractères qu'il sera difficile de deviner.

✓ Activez votre coupe-feu

Faciles à activer, les coupe-feu constituent votre première ligne de défense : ils bloquent les connexions vers des sites inconnus ou falsifiés, et empêchent les virus et les pirates informatiques d'accéder à votre ordinateur

✓ Utilisez un logiciel antivirus

Installez un logiciel antivirus pour éviter que des virus n'infectent votre ordinateur. Le logiciel antivirus doit être mis à jour régulièrement.

✓ Bloquez les attaques d'espiogiciels

Installez un anti-espiogiciel pour éviter qu'un tel logiciel ne s'installe sur votre ordinateur.

✓ Installez les plus récentes mises à jour de votre système d'exploitation

Assurez-vous que votre système d'exploitation et vos applications sont pris en charge et à jour.

✓ Demandez l'aide d'un expert

Un expert en informatique ou un fournisseur local pourra vous aider à installer ou à assurer la maintenance de vos applications.

✓ Conservez des copies de sauvegarde

Protégez vos fichiers importants contre les virus et les risques de dégâts matériels, comme une inondation ou un incendie, en faisant des copies de sauvegarde régulières de vos fichiers sur un disque externe.

✓ Protégez votre réseau sans fil

Les réseaux sans fil (Wi-Fi) sont vulnérables aux intrusions s'ils ne sont pas protégés correctement après leur installation. Vous pouvez configurer vous-même votre réseau ou demander à un expert d'installer votre routeur sans fil.

✓ Supprimez les courriels envoyés par des expéditeurs inconnus

N'ouvrez jamais les courriels ou les pièces jointes envoyés par une personne que vous ne connaissez pas, et ne cliquez jamais sur un lien hypertexte figurant dans un tel courriel au risque d'infecter votre ordinateur avec un virus ou un espiogiciel. Supprimez plutôt ces courriels immédiatement.

✓ Faites preuve de prudence lorsque vous naviguez sur Internet

Soyez vigilant avant de communiquer en ligne votre nom, votre adresse, votre numéro de téléphone et vos données financières. Assurez-vous que le site Web est sécurisé et que les paramètres de confidentialité sont activés.

COMPRENDRE L'EXPLOIT DU JOUR ZÉRO

En avril 2014, une faille logicielle dans Open SSL communément appelée « bogue Heartbleed » s'est immiscée dans près des deux tiers des serveurs Web de la planète. L'exploit du jour zéro a ouvert la porte à d'éventuelles divulgations d'informations confidentielles (notamment des mots de passe ou des renseignements personnels et organisationnels) qui sont enregistrées en mémoire; il est d'ailleurs à l'origine d'une atteinte à la protection des renseignements personnels survenue à l'Agence du revenu du Canada (ARC).

Un exploit du jour zéro tire parti d'une vulnérabilité d'une application informatique ou d'un système d'exploitation qui est inconnue des développeurs de logiciels et pour laquelle il n'existe toujours pas de correctif. Par respect d'une certaine éthique, les spécialistes qui découvrent des vulnérabilités logicielles sont tenus de les signaler gratuitement et en toute confidentialité aux développeurs concernés. Les développeurs peuvent alors concevoir et diffuser un correctif visant à stopper l'exploitation de ladite vulnérabilité.

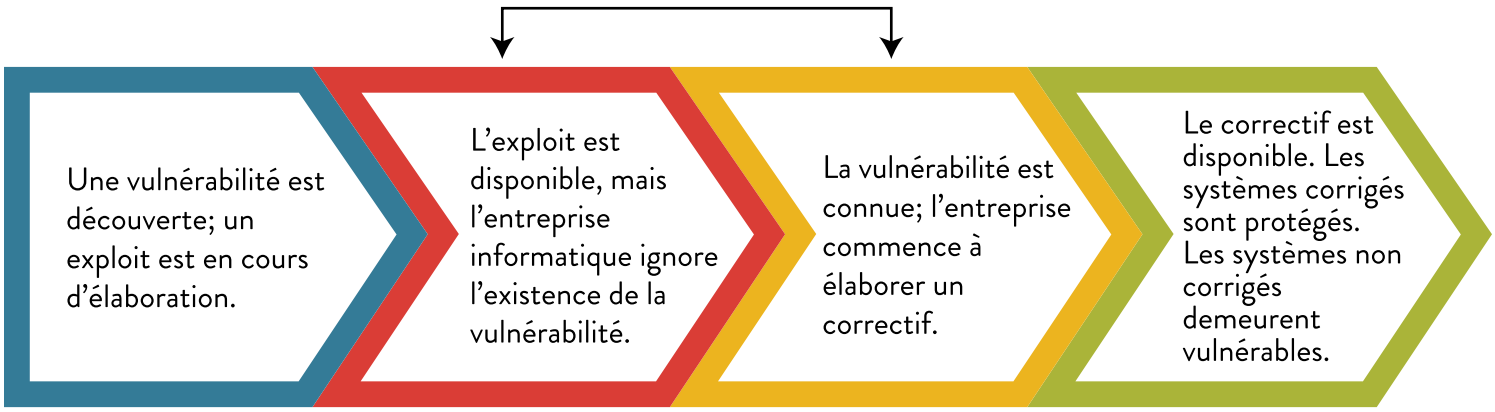
Dans certains cas, toutefois, ceux qui dépistent les vulnérabilités annoncent leur découverte sur le Web sans avoir préalablement avisé l'entreprise concernée.

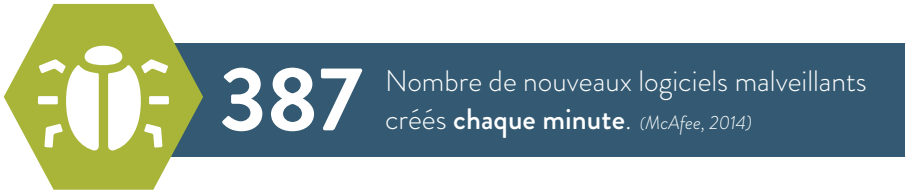
Dans ce cas de figure, les auteurs de cybermenaces ont souvent le temps d'élaborer des exploits avant que les correctifs ne soient prêts, donnant ainsi zéro jour pour développer un correctif. Au reste, un auteur de cybermenaces pourrait développer une trousse d'exploit pour une vulnérabilité particulière et vendre cette trousse à d'autres auteurs de cybermenaces. Il arrive souvent que les développeurs ne soient avertis des vulnérabilités qu'après que ces dernières aient été détectées et exploitées.

Ainsi, l'exploit du jour zéro continue de représenter une menace. Le CST incite fortement les ministères à mettre en place une liste blanche des applications en vue d'autoriser les applications et composantes d'applications autorisées et de refuser automatiquement l'accès à toute autre application non autorisée. Pour de plus amples renseignements, consultez Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information.

PHASES DE L'EXPLOIT DU JOUR ZÉRO

RISQUES LES PLUS ÉLEVÉS





WINDOWS XP N'EST PLUS PRIS EN CHARGE

Le CST encourage fortement les ministères et organismes du GC à remplacer le système d'exploitation Windows XP sur leurs postes de travail et leurs dispositifs.

Selon l'AMPTI 2015-01 du Secrétariat du Conseil du Trésor (SCT), les ministères et organismes du GC sont tenus de se conformer aux directives suivantes :

- Il est interdit de connecter des dispositifs tournant sur XP aux réseaux du GC ou à Internet après le 31 mars 2015.
- Les dispositifs tournant sur XP qui sont requis à des fins opérationnelles doivent obligatoirement être isolés et contenus dans un environnement réseau étroitement contrôlé.
- Les dispositifs tournant sur XP qui sont exploités dans des zones d'isolement ne serviront qu'à titre de mesure temporaire. La stratégie opérationnelle et les motifs doivent être soumis chaque année à la Direction du dirigeant principal de l'information (DDPI) du SCT à titre d'élément constitutif du plan ministériel en matière de TI.
- Les dirigeants principaux de l'information (DPI) ou leur équivalent doivent établir des mesures actives visant à assurer la conformité à la présente directive.
- Les ministères du GC ne sont pas autorisés à conclure, avec Microsoft, des ententes de soutien personnalisées pour Windows XP.

Il conviendra de rappeler aux DPI des ministères que les logiciels qui sont exploités dans les réseaux du GC, mais qui ne sont plus pris en charge, accroissent considérablement les risques auxquels s'expose le GC sur le plan de la sécurité informatique.

POUR OBTENIR DE PLUS AMPLES RENSEIGNEMENTS :

- AMPTI 2015-01, Élimination des dispositifs du GC tournant sur Windows XP
- CST, ITSB-68, Cessation de la prise en charge de Microsoft Windows XP SP3 et de Microsoft Office 2003
- CST, ITSB-89, version 3, 10 mesures de sécurité des TI

Il est également possible d'obtenir de l'information par courriel : Division des TI de la DDPI.

RÔLE DU CST DANS LES SOLUTIONS INTERDOMAINES DU GC

Les solutions interdomaines (SID) approuvées peuvent offrir des mesures de contrôle supplémentaires permettant d'atténuer les risques liés à la connexion de réseaux dont les niveaux respectifs de sécurité sont différents.

Pour ce qui a trait aux SID, le but principal du CST est de sensibiliser les preneurs de décisions et les praticiens des ministères aux SID et de leur prodiguer des conseils pour un déploiement sécurisé au sein d'un cadre rigoureux d'atténuation des risques.

À cette fin, le CST offre les services suivants :

- Informer les clients du GC des vulnérabilités et menaces ayant trait aux SID;
- Prodiguer des conseils aux fins des initiatives de SID des ministères du GC à divers stades du développement.

Pour favoriser la prestation de ces services, le CST a institué un groupe de travail sur les SID en février 2015. Le groupe sert ainsi de carrefour permettant aux partenaires de mettre en commun les pratiques exemplaires, et aux praticiens de la sécurité des ministères du GC de faire appel au CST lorsqu'il s'agit de planifier les déploiements de SID actuels et à venir.

Pour de plus amples renseignements concernant, entre autres, les exigences liées aux SID ou le groupe de travail, prière de communiquer avec les Services à la clientèle de la STI.

NOUVELLES EN MATIÈRE DE FORMATION

PROGRAMME DE CERTIFICATION POUR LES GARDIENS COMSEC

Le Centre de formation en sécurité des technologies de l'information (CFSTI) présente le programme de certification pour les gardiens COMSEC (PCGC). Ce programme permettra aux participants d'acquérir les notions de base, de connaître les fondements de la COMSEC et de la cryptographie, et de développer les compétences requises pour l'accomplissement des tâches qui incombent aux gardiens COMSEC.

Ce programme de certification regroupe divers cours dans trois parcours distincts, lesquels fourniront les connaissances dont les gardiens COMSEC auront besoin. Le PCGC se divise en trois parcours similaires, mais indépendants, conçus pour examiner la composition du compte COMSEC. Pour de plus amples renseignements sur le PCGC, visitez le site Web du CFSTI.

PORTAIL WEB DU CFSTI DU CST INSCRIPTION EN LIGNE POUR LES EMPLOYÉS DU GC

Le CFSTI offre maintenant un nouvel outil d'inscription en ligne qui permet aux employés du GC de se créer un profil d'apprentissage individuel et de s'inscrire à des cours en ligne. Cet outil facilitera l'inscription et permettra aux participants d'accéder aux ressources du centre d'apprentissage.

Grâce au profil d'apprentissage, vous pourrez accéder au catalogue du CFSTI, au calendrier de cours, aux nouvelles et aux faits saillants. Vous aurez, entre autres, la capacité de sélectionner vous-mêmes vos cours directement en ligne, de voir les cours auxquels vous êtes inscrits et suivre l'état de ceux-ci, et d'afficher tous les cours que vous avez suivis jusqu'ici. Ce nouveau processus réduit le délai de confirmation suivant votre inscription à un cours. De plus, le système vous rappellera automatiquement votre prochaine expérience d'apprentissage au CFSTI. Le CFSTI est heureux de vous offrir le soutien dont vous avez besoin pour votre apprentissage en matière de sécurité des TI.

La liste complète des programmes et des cours offerts par le CFSTI est affichée au:
www.cse-cst.gc.ca/fr/group-groupe/its-training

AU SUJET DU PRÉSENT BULLETIN

Le Cyberjournal a été créé pour les intervenants et praticiens des TI du GC et est publié périodiquement. Cette publication concrétise l'engagement de la Sécurité des TI du CST à fournir de l'information, des conseils et des recommandations à la collectivité du GC afin d'aider les ministères et les organismes à mieux se protéger contre les cybermenaces. L'objectif est de reprendre les principales questions de sécurité et d'encourager la discussion au sujet de la sécurité au sein des ministères et organismes. De plus, le bulletin fait le point sur les principaux produits et services offerts par le CST et explique aux lecteurs comment les utiliser pour aider leur organisme du GC à se protéger. Pour améliorer la posture de sécurité du GC, il faut sensibiliser tout le monde à la sécurité. Ainsi, nous vous encourageons à diffuser cette information au sein de votre organisme.

ABONNEMENT

Pour vous abonner aux prochains numéros, communiquez avec les Services à la clientèle de la Sécurité des TI à itsclientservices@cse-cst.gc.ca.

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 :
✉ comsecclientservices@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