Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

CYBERJOURNAL

NUMÉRO 3 – ÉTÉ 2013

DANS CE NUMÉRO

Zones de sécurité de réseau

Sécurisation des réseaux locaux sans fil

Gestion des risques liés aux iPad

Stratégie de gestion des risques

Réduire au minimum le nombre d'utilisateurs possédant des droits d'accès

Formation – Faits saillants

Mesures d'atténuation liées à Java

Correctifs de sécurité et CVE

Responsabilisation en matière de COMSEC

Au sujet du présent bulletin

Abonnez vous

Communiquez avec nous

SÉCURITÉ DES RÉSEAUX : PROTÉGER NOS BIENS D'INFORMATION

Le gouvernement du Canada (GC) compte sur ses réseaux câblés et sans fil pour assurer ses communications et mener à bien ses activités quotidiennes. Malheureusement, les acteurs de menace découvrent toujours de nouvelles vulnérabilités permettant d'exploiter les réseaux du GC.

Toute compromission des réseaux du GC entraîne des coûts et menace la disponibilité, la confidentialité et l'intégrité des biens d'information qui s'y trouvent. L'élaboration d'un plan de sécurité complet et rigoureux passe par la reconnaissance que les risques découlent non seulement d'acteurs malveillants, mais également de la complexité inhérente de la technologie et des erreurs involontaires des utilisateurs.

Comme on retrouve à la fois des novices et des spécialistes en matière de sécurité des TI au sein du GC, il est nécessaire de mettre en œuvre des protections techniques et de sensibiliser l'ensemble des employés. La prise de conscience du danger est une étape intégrante à l'élaboration d'une stratégie de défense axée sur la gestion des risques et d'initiatives pédagogiques.

Dans cette édition du Cyberjournal, le CSTC propose des conseils et de l'encadrement sur les processus, les procédures et les politiques en vue de bien planifier, mettre en œuvre, gérer et soutenir la sécurité et les risques associés aux réseaux informatiques du GC.

Toni Moffa
Chef adjointe, Sécurité des TI

www.cse-cst.gc.ca

Canada

Réservé à des fins officielles du gouvernement. Les conseils présentés ne sont ni exhaustifs, ni universels.

ZONES DE SÉCURITÉ DE RÉSEAU

Le recours à des zones de sécurité de réseau afin de protéger les biens de grande valeur occupe la septième position dans la liste des 35 mesures d'atténuation les plus efficaces du CSTC. Un simple réseau ministériel comportant une zone de sécurité unique crée une situation dans laquelle tous les biens d'information sont protégés par un seul périmètre qui, une fois pénétré, exposera l'ensemble du réseau. Un réseau ministériel fondé sur des zones de sécurité multiples résiste mieux aux cyberintrusions puisqu'il faut alors pénétrer chaque zone successivement pour compromettre l'ensemble du réseau.

Problème : On peut envisager deux scénarios si un réseau sans zone de sécurité contient à la fois de l'information non classifiée et sensible : soit l'information non classifiée sera trop protégée, soit l'information sensible ne sera pas suffisamment protégée.

- La surprotection de l'information non classifiée donne lieu à un accroissement des coûts de l'infrastructure TI et à un resserrement des contrôles d'accès; une telle situation nuit aux utilisateurs légitimes en restreignant l'accès au réseau et en limitant la disponibilité de l'information non classifiée;
- La sous-protection de l'information sensible peut mener à une perte de confidentialité, d'intégrité et de disponibilité, en exposant de l'information sensible à des utilisateurs non autorisés sur le réseau.

Mesures d'atténuation : Une zone de sécurité de réseau est une structure utilisée pour assurer la sécurité au sein d'un environnement réseau interconnecté. Chaque « zone de sécurité » est une zone distincte (sous-réseau) qui comporte une exigence de sécurité spécifique et une frontière bien définie. On utilise les zones de sécurité pour atténuer les menaces visant les biens sur le réseau en mettant en œuvre une structure de « sécurité en profondeur » au moyen de frontières de sécurité multiples ou imbriquées. Pour assurer une sécurité renforcée, il faut :

1. restreindre l'accès à chaque « zone » à des points d'entrée spécifiques;
2. restreindre l'accès à chaque « zone » aux utilisateurs dûment authentifiés;
3. surveiller et filtrer le trafic réseau aux points d'entrée.

En elle même, la mise en œuvre de zones de sécurité de réseau ne satisfait pas à toutes les exigences de sécurité; cette structure doit être utilisée en conjonction avec la mise en place de contrôles de sécurité au niveau des plateformes, des applications et des systèmes administratifs dans le contexte plus général de l'architecture d'entreprise de sécurité (ASE).

Pour obtenir plus de détails à ce sujet, consultez les guides ITSG-22 : Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada et ITSG-38 : Établissement des zones de sécurité dans un réseau.

Pour la liste complète des 35 mesures d'atténuation les plus efficaces du CSTC, cliquez ici.

NOUVELLES PUBLICATIONS!

ITSG-41 : Exigences en matière de sécurité des réseaux locaux sans fil

ITSB-98 : Atténuation des vulnérabilités de Java

ITSB-65 : Gestion des risques associés aux iPad

ITSB-64 : Solutions de gestion des postes mobiles (MDM)

ITSA-64 : Le magazine Forbes contient un routeur Wi-Fi dissimulé

DE BONS CONSEILS POUR TOUS

Maintenez vos logiciels à jour
De nouvelles versions de vos logiciels sont souvent publiées afin de corriger des problèmes de sécurité.

Utilisez un logiciel antivirus
Utilisez un produit offert par une entreprise de bonne réputation et tenez le à jour.

Surveillez vos comptes de médias sociaux
Évitez de copier des renseignements personnels sensibles sur Internet et vérifiez vos paramètres en matière de protection des renseignements personnels sur chaque réseau social.

N'ouvrez pas les courriels suspects
Si vous recevez un courriel qui vous semble étrange, ne l'ouvrez pas et ne cliquez sur aucun lien qu'il contient.

Faites des copies de sauvegarde de vos fichiers
Planifiez à l'avance et enregistrez vos données sur un support secondaire comme un disque dur externe.

Utilisez des mots de passe robustes
Vos mots de passe doivent contenir à la fois des lettres majuscules et minuscules, des chiffres et des symboles.

Utilisez des mots de passe multiples
Si votre mot de passe unique est compromis, un attaquant pourrait être en mesure d'accéder à vos autres comptes.

Prenez garde au vol
Les dispositifs perdus ou volés constituent un risque pour vos renseignements personnels et professionnels.

Réservé à des fins officielles du gouvernement. Les conseils présentés ne sont ni exhaustifs, ni universels.

SÉCURISATION DES RÉSEAUX LOCAUX SANS FIL

Connaissez vous les menaces les plus courantes pour les réseaux locaux sans fil (WLAN)?

1. Association non autorisée (accidentelle ou malveillante);
2. Création de réseaux ad hoc;
3. Clonage d'identité;
4. Déni de service;
5. Interception sans fil;
6. Vol de dispositif.

Bien que les WLAN offrent de nombreux avantages en comparaison des réseaux locaux câblés, notamment des coûts de câblage plus faibles, un déploiement plus facile dans les immeubles existants et la prise en charge des communications en itinérance, ils s'exposent également à un plus grand nombre de risques pour la sécurité. Les WLAN sont de plus en plus populaires au sein du GC. Ce paradigme technologique soumet les ministères à des vulnérabilités supplémentaires susceptibles de compromettre la confidentialité, l'intégrité ou la disponibilité de leurs systèmes d'information et de leurs biens de TI.

Les frontières physiques de la zone de couverture des WLAN dépassent souvent le périmètre de sécurité physique du ministère; par conséquent, les attaquants ne sont pas obligés de se trouver à l'intérieur des frontières de sécurité physique du ministère pour lancer des attaques dans le réseau.

Compte tenu de l'accroissement des risques potentiels, il faut sélectionner des contrôles de sécurité spécifiques et adapter les éléments de contrôle associés en fonction du type de WLAN déployé. Le guide ITSG-41 : Exigences en matière de sécurité des réseaux locaux sans fil décrit les différents types de WLAN qui correspondent actuellement aux besoins opérationnels du GC :

- Points d'accès du gouvernement;
- Connexion utilisateur sans fil / réseau câblé;
- Interconnexions de réseaux câblés par un pont sans fil.

Les ministères pourront tirer le meilleur parti du guide ITSG-41 au cours des phases d'analyse des besoins et de conception de haut niveau d'un système et ainsi atténuer le plus possible les menaces normalement associées aux WLAN.

GESTION DES RISQUES LIÉS AUX IPAD

La facilité d'utilisation de la tablette iPad, son court délai de démarrage et sa portabilité en font un dispositif bien plus convivial qu'un portable traditionnel. Pour les employés, le iPad est un excellent appareil compagnon, qu'ils utilisent en remplacement du papier pour prendre des notes au cours des réunions et pour lire des documents pendant leurs déplacements. Cette nouvelle tendance incite les employés à obtenir un accès distant au réseau de leur ministère par l'entremise d'un iPad.

Les iPad présentent toutefois de nouveaux risques pour les activités d'une organisation et pour la sécurité de ses données. Les risques pour la sécurité sont nombreux, et il faut les évaluer avec soin, s'assurer de bien les comprendre et mettre en place des contrôles de sécurité et des mesures de protection avant d'autoriser tout accès par des iPad à un réseau ministériel.

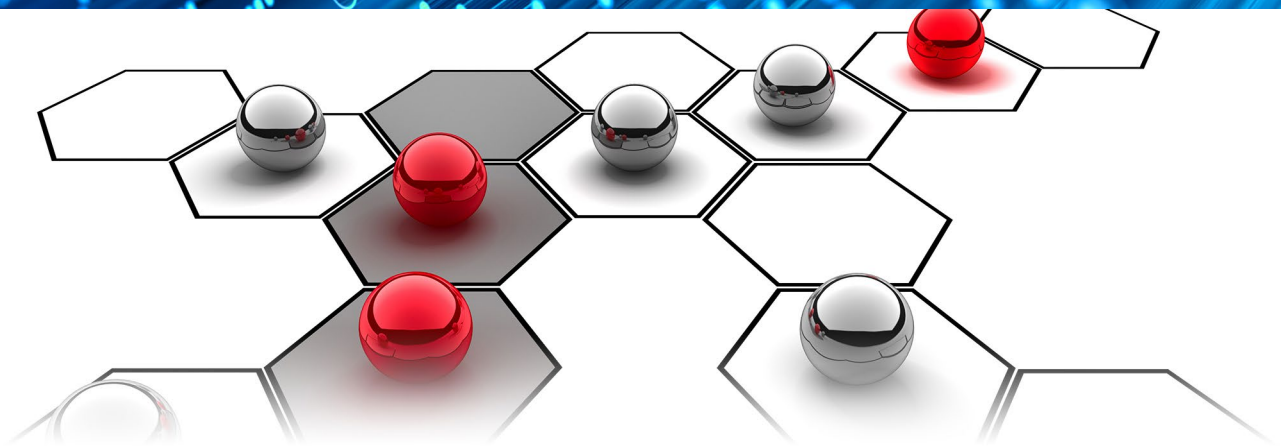
La nature des contrôles de sécurité à mettre en place pour le déploiement des iPad doit être déterminée en fonction du profil de menaces et de risques du ministère. Les contrôles de sécurité doivent être déployés et vérifiés pour l'ensemble du système d'information, et ce, du dispositif iPad individuel jusqu'aux services de réseau du ministère qui gèrent les processus opérationnels et les biens d'information.

Le CSTC a récemment publié le guide ITSB-65 : Gestion des risques associés aux iPad, qui décrit les cinq principales vulnérabilités associées aux iPad et les stratégies d'atténuation et mesures de protection potentielles. Les cinq principales vulnérabilités sont :

1. les données inactives;
2. les maliciels;
3. le débridage;
4. l'accès par le biais d'un réseau sans fil;
5. la configuration et la gestion.

Consultez dans un premier temps les guides ITSB-65 et CSG-30 : Fonctions de sécurité et pratiques exemplaires pour l'iPad d'Apple si vous envisagez d'utiliser ces dispositifs au sein de votre environnement informatique.

Réservé à des fins officielles du gouvernement. Les conseils présentés ne sont ni exhaustifs, ni universels.



DÉFIS COURAMMENT POSÉS PAR L'ADOPTION D'UNE STRATÉGIE DE GESTION DES RISQUES

L'objectif de la gestion des risques liés à la sécurité des TI consiste à s'assurer que les systèmes d'information peuvent appuyer les missions et les objectifs des ministères du GC d'une manière fiable. Si les risques liés à la sécurité des TI ne sont pas gérés correctement, ou s'ils ne sont tout simplement pas gérés, les systèmes d'information peuvent être insuffisamment sécurisés, être trop sécurisés, tenter d'atténuer les mauvaises menaces, ou ne pas être en mesure de protéger la confidentialité, l'intégrité et la disponibilité des activités opérationnelles du ministère. Le guide ITSG-33 présente un processus moderne qui aide les ministères à mettre en place des activités de gestion du risque. Les praticiens de la sécurité peuvent néanmoins être confrontés à plusieurs défis :

1. **Gouvernance**
   Une structure de gouvernance robuste et efficace contribue à assurer que les objectifs conflictuels de parties intéressées multiples puissent être résolus d'une manière adéquate; une structure de gouvernance appropriée doit être en place avant que les projets de TI ne soient entrepris;

2. **Culture organisationnelle**
   Le maintien de voies de communication claires et continues avec l'organisme de gouvernance responsable de la sécurité des TI, la recherche d'occasions d'éduquer les intervenants ainsi que la planification préalable permettront à la culture organisationnelle de surmonter les obstacles posés par les nouveaux défis en matière de sécurité des TI;

3. **Harmonisation entre différentes équipes de l'organisation**
   Il importe que toutes les équipes qui appuient les praticiens de la sécurité des TI (notamment les responsables opérationnels, la fonction de sécurité des TI, les projets de TI et les opérations de TI) harmonisent correctement leurs activités par le biais d'une structure de gouvernance claire, et qu'elles aient des représentants responsables qui collaborent à l'occasion des initiatives de sécurité des TI d'envergure;

4. **Ressources dédiées à la sécurité des TI**
   Les ressources limitées affectées aux activités de sécurité des TI peuvent représenter un défi majeur. Le manque de personnel qualifié, de budget, de temps et de possibilités de formation peut forcer les praticiens de la sécurité à faire des choix difficiles quant à la mise en œuvre des mesures de sécurité des TI au sein de leur organisation. Les praticiens doivent faire savoir à l'organisme de gouvernance responsable de la sécurité des TI de leur organisation quelles seront les conséquences éventuelles du manque de ressources disponibles;

5. **Processus arrivés à maturité**
   Un autre défi réside dans le degré de maturité atteint par les processus utilisés lors de la conception, du développement et de l'exploitation des systèmes d'information. Pour une organisation qui dispose de processus arrivés à maturité en matière de supervision de la sécurité des TI, de gestion de projets, d'ingénierie de systèmes, d'ingénierie de sécurité des systèmes et d'opérations de TI, l'adoption des lignes directrices de l'ITSG-33 nécessitera relativement peu de ressources et de temps. Dans le cas d'une organisation qui ne dispose pas de processus établis, il est recommandé de mettre lentement en application les lignes directrices de l'ITSG-33 par le biais d'initiatives multiples réalisées sur une certaine période de temps;

Pour en apprendre davantage à ce sujet, visitez le répertoire de nos publications sur les TI et téléchargez le guide ITSG-33 : La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie ou les éditions précédentes du Cyberjournal.

Réservé à des fins officielles du gouvernement. Les conseils présentés ne sont ni exhaustifs, ni universels.

RÉDUIRE AU MINIMUM LE NOMBRE D'UTILISATEURS POSSÉDANT DES DROITS D'ACCÈS ADMINISTRATIFS

La réduction au minimum du nombre d'utilisateurs qui possèdent des droits d'accès administratifs au niveau du domaine ou au niveau local occupe la quatrième position dans la liste des 35 mesures d'atténuation les plus efficaces du CSTC. Le concept du « droit d'accès minimal » vise à renforcer la sécurité en ramenant les privilèges d'accès d'un utilisateur au minimum nécessaire pour exécuter les tâches associées à ses responsabilités professionnelles. Les problèmes surviennent lorsque des utilisateurs possédant de tels droits accèdent régulièrement au système en utilisant leurs privilèges d'accès, par exemple :

- Alors qu'il a accès à un système à un niveau privilégié, un utilisateur légitime peut faire une erreur et endommager par inadvertance l'environnement réseau;
- Un intrus peut obtenir les justificatifs d'identité d'un utilisateur légitime qui possède des droits d'accès privilégiés, et ainsi être en mesure d'accéder librement à des biens d'information précieux et de modifier délibérément des systèmes placés sous le contrôle de l'utilisateur légitime.

Règle générale, les politiques ne sont ni vérifiées ni appliquées sur une base régulière. 59 % des organisations n'ont ou n'imposent aucune politique de gouvernance des accès, et 61 % ne vérifient pas les demandes d'accès en tenant compte des politiques de sécurité avant d'accorder un accès.

Ponemon Institute, Rapport sur les tendances et la gouvernance des accès pour 2010

La mise en œuvre du principe du « droit d'accès minimal » aide à atténuer le problème en réduisant au minimum l'exposition des sessions à accès privilégié aux cyberintrus. Selon ce principe, les utilisateurs doivent utiliser deux séries de justificatifs d'identité : une comportant des droits d'accès minimaux pour les activités quotidiennes (c. à d. qui se limitent à des changements apportés à l'environnement local uniquement), et une autre comportant des droits d'accès privilégiés, à utiliser seulement lorsque nécessaire pour apporter des modifications à l'environnement réseau.

Pour tirer le maximum du principe du droit d'accès minimal appliqué aux administrateurs :

1. Utilisez idéalement des comptes de groupe de domaines comportant des privilèges administratifs adaptés, plutôt que des comptes d'administrateur locaux. Utilisez des groupes de sécurité de domaine pour contrôler les accès aux biens qui se trouvent sur le réseau;
2. À tout le moins, ne permettez pas la création de comptes d'administrateur locaux dont les justificatifs d'identité sont partagés entre plusieurs hôtes. S'il est possible d'exécuter les fonctions administratives sans avoir à utiliser le compte d'administrateur local, désactivez ce compte;
3. Forcez le changement des mots de passe de niveau administrateur selon un calendrier préétabli ou après un incident de sécurité.

Le principe du droit d'accès minimal appliqué aux administrateurs limite les dommages potentiels pouvant résulter d'un système compromis en réduisant au minimum l'utilisation de justificatifs d'identité partagés au sein de l'environnement du réseau ministériel. Cette approche permet d'assurer une sécurité en profondeur en forçant un intrus potentiel à compromettre plusieurs biens sur le réseau avant d'affaiblir la sécurité du réseau. Elle permet par ailleurs d'assurer une gestion efficace des justificatifs d'identité confiés aux utilisateurs qui possèdent des droits d'accès privilégiés.

Pour obtenir plus de détails à ce sujet, consultez le guide ITSB-94 : Restriction du nombre d'utilisateurs possédant des droits d'accès administratifs.

RELIEZ CHAQUE MENACE À SON EFFET

1. VIRUS
2. VER
3. CHEVAL DE TROIE
4. LOGICIEL ESPION
5. CANULAR
6. PORTE DÉROBÉE

A. Se fait passer pour un programme utile, exécute des fonctions clandestines qui excèdent les fonctions officielles du programme, provoque l'altération de données.

B. Faux courriel qui incite le lecteur à supprimer des fichiers exécutables valides.

C. Méthode visant à contourner les procédures normales d'authentification de manière à permettre à un attaquant d'accéder à distance à un ordinateur.

D. Capable de faire une copie de son propre code, n'a pas besoin d'un fichier hôte pour se répliquer, peut endommager un ordinateur ou compromettre sa sécurité.

E. Se copie sur un nouvel hôte, se propage automatiquement, peut endommager des données ou faire planter l'ordinateur.

F. Petite portion de code intégrée dans un fichier, capable de suivre activement toutes les activités du navigateur et de faire rapport au serveur d'une entreprise de marketing.

Réponses à la page 8.

Réservé à des fins officielles du gouvernement. Les conseils présentés ne sont ni exhaustifs, ni universels.

Salon des Gouvernements Innovateurs du Canada

GTEC2013

www.gtec.ca

Un gouvernement agile : ouvert, collaboratif, mobile

7 au 10 octobre 2013 | Centre des congrès d'Ottawa

Visitez le Centre de la sécurité des télécommunications au GTEC 2013 pour en apprendre davantage sur la cybersécurité et sur la sécurité des dispositifs mobiles

POINTS D'ACCÈS WI-FI INTÉGRÉS

De nouveaux systèmes électroniques sont continuellement offerts à des coûts plus faibles et dans des formats de plus en plus compacts; il est donc de plus en plus facile de les incorporer à des produits qui n'étaient pas associés aux systèmes électroniques par le passé.

Par exemple, l'édition d'avril du magazine Forbes a contenu une campagne publicitaire de Microsoft qui vise à promouvoir son nouveau progiciel infonuagique Office 365. La page de couverture du magazine a comporté une grande image orange portant la mention « Free Wi-Fi » (Wi-Fi gratuit). Dans le magazine, un encart publicitaire en carton a masque un routeur sans fil pleinement fonctionnel qui, une fois activé, a offert un service gratuit de point d'accès Wi-Fi pendant 15 jours pour cinq utilisateurs simultanés.

Nota : Les points d'accès Wi Fi sont traités en tant qu'articles réglementés et leur utilisation doit être interdite dans les installations sécurisées, puisqu'ils constituent une menace technique potentielle pour les données et systèmes du GC.

Pour de plus amples renseignements à ce sujet, télécharger : ITSA-64 : Le magazine Forbes contient un routeur Wi-Fi dissimulé.

FORMATION EN SÉCURITÉ DES TI – FAITS SAILLANTS

Le Centre de formation en sécurité des TI (CFSTI) a publié son nouveau catalogue et le calendrier des cours pour 2013 2014. Dans ce catalogue, vous trouverez différentes possibilités de formation qui vous aideront à tenir à jour vos connaissances en matière de cybersécurité, à l'appui de votre rôle au sein de votre ministère ou organisme. Vous y trouverez aussi différents conseils sur la sécurité des TI ainsi que les coordonnées des personnes-ressources du CSTC.

NOUVEAU!

Catalogue du Centre de formation en sécurité des TI

Calendrier des cours du Centre de formation en sécurité des TI

CHANGEMENTS APPORTÉS AUX COURS ET AUX PROGRAMMES D'ÉTUDES

L'environnement TI dans lequel nous travaillons évolue rapidement alors que de nouvelles menaces émergent; par conséquent, les exigences et les pratiques exemplaires en matière de sécurité des TI évoluent continuellement. Le CFSTI réexamine régulièrement ses cours et ses programmes d'études pour vérifier leur pertinence, leur conformité et leur efficience, et peut les modifier s'il le juge nécessaire.

Le cours 102 a été remplacé pour tenir compte de la nouvelle approche décrite dans le guide ITSG-33. Les nouveaux concepts de l'ITSG-33 et l'information connexe sont abordés dans un nouveau cours intitulé « Processus d'application de la sécurité dans les systèmes d'information (PASSI) » (105). Ce cours explique l'intégration des principes de gestion des risques liés à la sécurité des TI dans le Cycle de développement des systèmes, comme le décrit le guide ITSG-33 : La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie. À la fin du cours, les participants seront en mesure d'appliquer le Processus d'application de la sécurité dans les systèmes d'information à un projet de TI classique dont l'objectif consiste à mettre en œuvre un nouveau système d'information ou une nouvelle capacité pour un système d'information existant.

Réservé à des fins officielles du gouvernement. Les conseils présentés ne sont ni exhaustifs, ni universels.

MESURES D'ATTÉNUATION LIÉES À JAVA

Java est un langage de programmation et une plateforme informatique servant à de nombreux processus opérationnels et systèmes autorisés. Sa clientèle établie s'élève à près d'un milliard d'utilisateurs. Au cours de la dernière année, des cyberintrus ont découvert et exploité bon nombre des vulnérabilités de Java. Certains exploits pourraient compromettre, sans avertissement, la sécurité de l'information sur le réseau du ministère.

Le délai entre la découverte d'une vulnérabilité et la conception et mise en œuvre d'un correctif facilite l'exploitation de la vulnérabilité en question par les cyberintrus. Or, le réseau d'un ministère demeure vulnérable aux attaques pendant une période prolongée.

Seulement 5,5 % des navigateurs comportant un plugiciel Java utilisent la version la plus récente du plugiciel.

Websense, Rapport sur les menaces pour 2013

La plateforme Java est installée sur des milliers de systèmes du GC. Des ministères dépendent des applications Java, qu'elles soient en lignes ou au niveau du système central, pour exécuter des processus opérationnels valides. Dans la majorité des cas, les systèmes qui utilisent les applications Java font partie de réseaux avec accès à Internet. Cette situation pose un problème si Java est connecté au navigateur par défaut et que l'utilisateur visite un site Web malveillant. L'ordinateur peut alors être exploité grâce aux vulnérabilités du module Java et exposer le contenu du réseau du ministère à des accès non autorisés.

Les stratégies d'atténuation normales (p. ex. la gestion des correctifs de sécurité) ne sont pas suffisantes pour renforcer la sécurité sous Java en raison du déclin perçu de son niveau d'assurance de sécurité. Chaque ministère doit réviser son Évaluation des menaces et des risques (EMR) de manière à y inclure les vulnérabilités Java existantes. Les options d'atténuation suivantes sont recommandées :

- S'assurer d'installer les correctifs de sécurité les plus récents;
- Dans la mesure du possible, désinstaller Java; si ce n'est pas possible :
  - désactiver le plugiciel Java dans le navigateur;
  - désactiver le plugiciel Java dans tous les navigateurs sauf le navigateur par défaut;
  - restreindre l'accès à Java au niveau du coupe feu.

Lire en ligne : Atténuation des vulnérabilités de Java (ITSB-98)

CORRECTIFS DE SÉCURITÉ ET CVE

Lorsque des chercheurs ou des fournisseurs de produits de sécurité découvrent de nouvelles vulnérabilités dans des applications logicielles ou des systèmes d'exploitation, ils publient des correctifs de sécurité. En annonçant ces correctifs, ils rendent publics des vulnérabilités ou risques d'exposition auparavant inconnus : les vulnérabilités et expositions communes (CVE pour Common Vulnerabilities and Exposures).

Les agents de menace surveillent ces annonces et entreprennent immédiatement d'écrire des programmes pour exploiter les lacunes nouvellement révélées avant que les utilisateurs n'installent les correctifs. Plus long est le délai entre la diffusion d'un correctif et son application par les utilisateurs, plus grand est le risque que les CVE soient utilisées pour exploiter des réseaux et systèmes informatiques.

La National Vulnerability Database (Base de données des vulnérabilités nationales) tenue à jour par la NIST aux États Unis recense actuellement plus de 55 000 CVE.

Une grande proportion des tentatives de compromission couronnées de succès tirent parti d'un petit groupe de vulnérabilités connues du public pour lesquelles il existe déjà des correctifs de sécurité. L'analyse des vulnérabilités qui ont été exploitées avec le plus de succès au sein du GC l'année dernière a révélé que la majorité des situations de compromission auraient pu être évitées si un très petit nombre de CVE avaient été corrigées au moyen de correctifs qui existent déjà depuis longtemps.

Afin de réduire au minimum les risques posés par ces vulnérabilités, les administrateurs de réseau peuvent :

- exécuter des outils de dépistage des vulnérabilités;
- déployer des outils de gestion automatique des correctifs;
- s'abonner à des services de notification sur les vulnérabilités afin de se tenir informés des plus récentes CVE;
- appliquer les correctifs sur tous les systèmes, même les systèmes isolés;
- corriger les vulnérabilités connues le plus rapidement possible, dans les 48 heures dans le cas des CVE critiques.

Pour de plus amples renseignements à ce sujet, téléchargez le guide ITSB-96 : Évaluation des vulnérabilités de sécurité et des correctifs.

Réservé à des fins officielles du gouvernement. Les conseils présentés ne sont ni exhaustifs, ni universels.

RESPONSABILISATION EN MATIÈRE DE COMSEC

Les ministères du GC utilisent les dispositifs et le matériel de chiffrement COMSEC pour protéger l'information sensible. La perte du contrôle exercé sur les dispositifs et le matériel de chiffrement COMSEC est non seulement une source d'embarras, mais aussi une situation qui peut compromettre la sécurité nationale et des ententes internationales. Heureusement, le risque de compromission peut être fortement atténué si les incidents COMSEC sont signalés sans attendre au Bureau national des incidents COMSEC (BNIC) du CSTC au 613 991 8175 par l'entremise de l'autorité COMSEC du ministère (ACM).

Voici les cinq principaux types d'incident signalés par le GC l'an dernier :

1. **Matériel COMSEC ou article cryptographique contrôlé (CCI) perdu ou manquant**
   Incapacité de retracer un matériel COMSEC ou CCI ou d'expliquer son absence;
2. **Destruction de matériel COMSEC ou d'un CCI**
   Défaut de détruire un matériel COMSEC ou CCI dans les délais prescrits;
3. **Matériel COMSEC ou CCI trouvé**
   Découverte de matériel COMSEC ne figurant pas dans l'inventaire COMSEC courant ou en possession d'une personne non autorisée (ou aisément accessible par une personne non autorisée);
4. **Accès non autorisé à du matériel COMSEC ou à un CCI**
   Activité de maintenance non autorisée sur du matériel COMSEC ou défaut de maintenir les contrôles Intégrité par deux personnes (TPI) ou Zones jamais seul (NLZ) obligatoires pour une clé de niveau « TRÈS SECRET »;
5. **Prolongation non autorisée de la cryptopériode**
   Usage ininterrompu d'une clé périmée sans approbation, ou défaut de tenir des dossiers de destruction appropriés.

Réponses au questionnaire de la page 5 : 1-E, 2-D, 3-A, 4-F, 5-B, 6-C

AU SUJET DU PRÉSENT BULLETIN

Le Cyberjournal a été créé pour les intervenants et les praticiens des TI du GC et est publié périodiquement. Cette publication concrétise l'engagement de la Sécurité des TI du CSTC 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. Cette initiative vise à reprendre les principales questions de sécurité et à encourager les discussions au sujet de la sécurité au sein des ministères et organismes. De plus, le bulletin fait le point sur les produits et services clés offerts par le CSTC et indique aux lecteurs comment en profiter 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.

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**
ou ✆ **Demandes de renseignements généraux : (613) 991-7654**

Pour signaler un cyberincident, communiquez 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**
ou ✆ **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** ou
✆ **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**

ABONNEMENT

Pour vous abonner aux prochains numéros, veuillez communiquer avec les Services à la clientèle de la Sécurité des TI à l'adresse suivante : itsclientservices@cse-cst.gc.ca.

Réservé à des fins officielles du gouvernement. Les conseils présentés ne sont ni exhaustifs, ni universels.