Centre de la sécurité des télécommunications
Communications Security Establishment

NON CLASSIFIÉ

SÉRIE GESTIONNAIRES

CONSEILS EN MATIÈRE DE SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION

LES 10 MESURES DE SÉCURITÉ DES TI VISANT À PROTÉGER LES RÉSEAUX INTERNET ET L'INFORMATION

ITSM.10.189
Octobre 2017

Canada

INTRODUCTION

Les conseils énoncés dans *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information* (ITSM10.189) se fondent sur une analyse que le Centre de la sécurité des télécommunications (CST) a faite sur les tendances suivies par les cybermenaces et sur leurs répercussions sur les réseaux accessibles par Internet. Les organisations qui mettent ces 10 mesures réduiront un nombre considérable de vulnérabilités et seront en mesure de contrer la majorité des cybermenaces actuelles.

SUGGESTION SUR LE PLAN DES POLITIQUES

Le gouvernement du Canada (GC) a produit un certain nombre de politiques visant à favoriser les cyberpratiques sécuritaires. En l'occurrence, les politiques énumérées ci-dessous sont des documents de références sur lesquels les organisations peuvent compter pour leur procurer les éléments essentiels à la création de politiques et à l'établissement des principes qui orienteront les pratiques et les programmes de cybersécurité.

- *Politique sur la gestion des technologies de l'information* [1];[1]
- *Politique sur la sécurité du gouvernement* (PSG) [2];
- *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information* (GSTI) [3].

ENVIRONNEMENTS CONCERNÉS

L'information contenue dans l'ITSM.10.189 indique les pratiques à adopter et offre des conseils en matière de sécurité des TI. Toutefois, un organisme pourrait très bien décider de renforcer la sécurité en ajoutant de nouvelles mesures dans le but d'assurer une protection accrue de ses informations opérationnelles les plus sensibles. En outre, il est essentiel que les organisations aient une connaissance approfondie de leurs environnements respectifs pour être en mesure de protéger adéquatement leur actif informationnel.

[1] Les numéros entre les crochets renvoient à des documents de référence. La liste de ces documents de référence apparaît à la section intitulée *Information complémentaire*.

LES 10 MESURES LES PLUS EFFICACES

Tableau 1 Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information

Rang	Mesure	Description de la mise en œuvre
1	Intégrer, surveiller et défendre les passerelles Internet	Les organismes devraient surveiller le trafic qui circule par leur passerelle Internet. Pour simplifier cette tâche de surveillance, le nombre des connexions externes visant le réseau organisationnel devrait être réduit. Il conviendra d'abord de bien comprendre les tendances suivies par le trafic, puis de réagir à tout changement de tendance. Les organismes bénéficieront de la protection assurée par les mesures de cyberdéfense qui détectent et empêchent les accès non autorisés, l'exfiltration de données et d'autres activités malveillantes. Ces mesures de cyberdéfense pourraient notamment consister en la fermeture de certains points d'accès de façon à stopper les exfiltrations de données et à bloquer les attaques.
2	Appliquer les correctifs aux systèmes d'exploitation (SE) et aux applications	Les organismes devraient mettre en œuvre une politique d'application de correctifs aux systèmes d'exploitation (SE) et aux applications de tierces parties en temps opportun, afin de réduire le degré d'exposition des organismes aux menaces qui pourraient exploiter des vulnérabilités connues du public. Ils devraient utiliser des versions d'application et de SE prises en charge, testées et mises à jour. Le déploiement d'une application ou d'un système d'exploitation qui n'est plus pris en charge accroît les risques d'exploitation des vulnérabilités, puisqu'aucun mécanisme n'est en place pour atténuer les vulnérabilités. En effet, les correctifs doivent être appliqués uniformément, en temps opportun et, si possible, au moyen d'un système automatisé de gestion des correctifs. Il est également logique de disposer d'un mécanisme permettant de recenser les correctifs qui ont été installés, de façon à réduire le temps de réaction aux menaces et à comprendre les risques que comportent d'éventuelles expositions. Le document du CST *ITSB-96 Correction des systèmes d'exploitation et des applications* [4] fournit de plus amples détails sur l'importance des correctifs.
3	Mettre en vigueur la gestion des privilèges d'administrateurs	Les organismes devraient réduire autant que possible le nombre d'utilisateurs possédant des droits d'accès administratifs. De fait, la liste de ces utilisateurs devrait être fréquemment révisée et validée. La création de comptes dotés de niveaux de droits administratifs distincts constitue une pratique exemplaire visant à limiter les risques d'exposition lorsqu'un compte d'administrateurs a été la cible d'une compromission. Les organismes devraient adopter l'une des deux mesures suivantes : adopter une procédure de changement du mot de passe des comptes administratifs selon des échéances préétablies, ou mettre en œuvre une solution pour protéger les mots de passe administratifs. Dans le cas des accès à des applications sensibles ou à des réseaux distants, une authentification à deux facteurs (2FA) devrait être imposée aux fins d'assurance de l'authenticité des justificatifs d'utilisateur. Pour prévenir les expositions découlant d'attaques par hameçonnage ou par tout autre maliciel, il conviendra d'effectuer les tâches administratives à partir d'un poste de travail réservé qui n'est ni connecté à Internet ni doté d'un compte de courrier électronique à accès libre, ou encore dont les fonctions d'accès Internet ou de courrier électronique sont désactivées pour les comptes administratifs. Les comptes d'administrateurs devraient être séparés des comptes organisationnels courants, et les administrateurs devraient toujours agir en fonction du type de compte qu'ils utilisent. Il est plus facile de réagir à la compromission d'un compte utilisateur courant qu'à celle d'un compte d'administrateur.

4	Renforcer les systèmes d'exploitation (SE) et les applications	Pour prévenir les compromissions d'actifs et d'infrastructures connectés à Internet, les organismes devraient désactiver tous les ports et les services non essentiels et supprimer les comptes inutiles. La vérification au niveau de l'organisme et les solutions antivirus sont des éléments clés de toute configuration sûre. Des contrôles de sécurité supplémentaires devraient être appliqués au SE à l'occasion des mesures de renforcement. À cet effet, les organismes peuvent consulter le document du CST *ITSG-33 – La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [5] pour obtenir de plus amples renseignements sur la sélection et la mise en œuvre de contrôles de sécurité. Les applications de tierces parties devraient être évaluées de façon à établir si elles comportent des fonctions ou composants qui devraient être désactivés en raison de leur inutilité ou qui nécessiteraient une intervention humaine avant d'être activés (p. ex. les macros).
5	Segmenter et séparer les informations	Les organismes devraient disposer d'un registre faisant état de leur information opérationnelle essentielle. Les fonds d'informations doivent être catégorisés en tenant compte des exigences en matière de protection qu'il convient d'appliquer aux informations sensibles ou aux renseignements personnels. Il est recommandé de zoner les réseaux par la segmentation des services d'infrastructure en groupes logiques répondant aux mêmes politiques en matière de sécurité des communications et aux mêmes exigences sur le plan de la protection de l'information. Ce type de conception logique permet de contrôler et de limiter l'accès de même que les flux de communication de données. Il conviendra également que les organismes s'assurent du déroulement normal des activités de surveillance et mettent en place des contrôles visant à maintenir la protection et l'intégrité des différentes zones. Pour obtenir de plus amples conseils, prière de consulter les documents que le CST a préparés à cet effet : *Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada* (ITSG-22) [6] et *Zones de sécurité des réseaux – Considérations en matière de conception liées au placement de services dans des zones* (ITSG-38) [7].
6	Offrir de la formation et de la sensibilisation sur mesure	Les organismes devraient entreprendre régulièrement des activités de sensibilisation aux vulnérabilités actuelles liées aux utilisateurs et aux comportements acceptables des utilisateurs. Les programmes et les activités de sensibilisation à la sécurité des TI doivent être fréquemment révisés, mis à jour et mis à la disposition de tous les utilisateurs ayant accès aux systèmes organisationnels. Certes, les mesures de protection des systèmes endigueront l'effet des activités malveillantes sur les réseaux, mais il n'en demeure pas moins que l'élément humain continuera de poser un risque. Certains cas avérés d'hameçonnage et de traitement inadéquat des supports amovibles démontrent clairement que la sensibilisation est toujours de mise. Qui plus est, il conviendra de signaler toute tentative de compromission à la gestion, ce qui devrait favoriser l'adoption de comportements exemplaires au sein de l'organisme. Quand il est question de protection de l'information, le rôle de la direction dans les processus décisionnels est essentiel, notamment lorsqu'il s'agit de choisir des contrôles de sécurité appropriés. Le CST a publié nombre de documents pouvant aider les employés à se sensibiliser davantage aux effets des cybermenaces et aux mesures d'atténuation qu'il convient d'appliquer. Visiter le site Web du CST pour lire ces documents.
7	Protéger l'information au niveau organisationnel	Les organismes pourraient autoriser les utilisateurs à utiliser leurs dispositifs personnels à des fins professionnelles. Dans certains cas, il peut s'avérer pratique de fournir de l'équipement (p. ex. des serveurs, des postes de travail, des ordinateurs portables et des dispositifs mobiles) aux employés, pour peu que l'on se soit doté d'un cadre de gestion des dispositifs et que l'on applique certains mécanismes de contrôle au moyen,

		notamment, d'un processus de gestion des changements. Dès lors que l'on choisit d'adopter une mesure du type « prenez votre appareil personnel » (PAP), il convient de se doter d'une politique de contrôle qui soit rigoureusement appliquée. Les organismes devraient effectuer quelques recherches sur les technologies utilisateurs et sur les exigences prévues par la loi concernant le recours aux dispositifs personnels au travail. Au demeurant, il conviendra de séparer les informations et les transactions relevant de la sphère personnelle de celles qui appartiennent plutôt à la sphère professionnelle, ce qui évitera d'éventuelles contaminations fortuites. L'une de ces technologies consiste en un système gestion des postes mobiles (MDM pour *Mobile Device Management*) qui assure la protection des dispositifs mobiles et des réseaux auxquels ces dispositifs se connectent.
8	Assurer la protection au niveau de l'hôte	Les organismes devraient déployer une solution de système de prévention des intrusions sur l'hôte (HIPS pour *Host-Based Intrusion Prevention System*) afin de protéger leurs systèmes contre les activités malveillantes connues ou inconnus, comme les virus et les maliciels. Le système HIPS prend des mesures actives pour protéger les systèmes informatiques contre les tentatives d'intrusion en faisant appel à des ensembles prédéfinis de règles visant à reconnaître les comportements inhabituels. Lorsque de tels comportements sont détectés, le mécanisme HIPS bloque le programme ou le processus en cause et l'empêche de mener des activités potentiellement nuisibles. En outre, il importe de surveiller les alertes et l'information de journalisation du système HIPS pour y découvrir les signes avant-coureurs d'une intrusion. Plusieurs fournisseurs proposent des services HIPS commerciaux.
9	Isoler les applications Web	Les organismes devraient utiliser la virtualisation pour créer un environnement dans lequel les applications Web peuvent être exécutées indépendamment. Les navigateurs Internet et les clients de courrier électronique sont des exemples d'applications vulnérables aux exploits qui exécutent des maliciels. Les exploits de sécurité adaptés à de telles applications peuvent être confinés à un « bac à sable ». Les maliciels qui infectent un environnement virtualisé n'ont aucune répercussion en dehors des limites dudit bac à sable. Par conséquent, ils ne peuvent infecter ni l'hôte ni les systèmes de l'organisme.
10	Mettre en œuvre une liste blanche des applications	Les organismes devraient déterminer précisément les applications et les composants d'application qui seront autorisés. Il conviendra donc de bloquer systématiquement tous les éléments ne figurant pas dans la liste, de façon à réduire le risque d'exécution de maliciels du jour zéro. Les technologies investies dans les listes blanches d'applications peuvent indiquer quelles applications seront installées ou exécutées sur un hôte. Il est possible de définir la liste blanche en sélectionnant de nombreux attributs de fichier et de dossier (p. ex. les chemins d'accès, les noms de fichiers, la taille des fichiers, la signature numérique ou l'éditeur, ou encore l'empreinte numérique). Les politiques prônant le recours aux listes blanches d'applications doivent être définies et déployées à l'échelle de l'organisme. Document de référence décrivant le concept de liste blanche : • *ITSB-95 – Utilisation d'une liste blanche des applications*, du CST [8].

RÉSUMÉ

Le document *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.189)* est une liste de mesures de sécurité des TI que les organismes peuvent appliquer dans le but de réduire les risques d'exposition aux activités des auteurs de menace. La mise en œuvre de ces mesures contribue à réduire effectivement les risques. Toutefois, les activités de sécurité des TI doivent être continuellement examinées et, s'il y a lieu, améliorées de façon à réagir adéquatement à l'évolution de l'environnement des cybermenaces.

AIDE ET RENSEIGNEMENTS

Pour obtenir de plus amples renseignements sur les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information du gouvernement du Canada, prière de communiquer avec le Service à la clientèle en matière de STI aux coordonnées suivantes :

Téléphone : 613-991-7654
Courriel : itsclientservices@cse-cst.gc.ca

CONTENU COMPLÉMENTAIRE

LISTE D'ABRÉVIATIONS, D'ACRONYMES ET DE SIGLES

Forme abrégée	Terme
2FA	Authentification à deux facteurs (*Two-Factor Authentication*)
CST	Centre de la sécurité des télécommunications
HIPS	Système de prévention des intrusions sur l'hôte (*Host-based Intrusion Prevention System*)
MDM	Gestion des postes mobiles (*Mobile Device Management*)
PAP	Prenez votre appareil personnel
SE	Système d'exploitation
STI	Sécurité des technologies de l'information
TI	Technologies de l'information

RÉFÉRENCES

Numéro	Référence
1	Secrétariat du Conseil du Trésor du Canada. *Politique sur la gestion des technologies de l'information*, 1er juillet 2007.
2	Secrétariat du Conseil du Trésor du Canada. *Politique sur la sécurité du gouvernement* (PSG), 1er juillet 2009
3	Secrétariat du Conseil du Trésor du Canada. *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information*, non daté.
4	Centre de la sécurité des télécommunications. ITSB-96 – *Correction des systèmes d'exploitation et des applications,* mars 2015.
5	Centre de la sécurité des télécommunications. *ITSG-33 – La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, décembre 2014.
6	Centre de la sécurité des télécommunications. ITSG-22 – *Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada,* juin 2007.
7	Centre de la sécurité des télécommunications. ITSG-38 – *Zones de sécurité des réseaux – Considérations en matière de conception liées au placement de services dans des zones,* mai 2009.
8	Centre de la sécurité des télécommunications. ITSB-95 – *Utilisation d'une liste blanche des applications,* mars 2015.