Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

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

GESTIONNAIRES

Canada

AVANT-PROPOS

L'ITSM.10.089, *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information,* est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité.

Le présent document remplace l'ITSM.10.189, *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information*, et l'ITSB-89 version 3, *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information du gouvernement du Canada*.

DATE D'ENTRÉE EN VIGUEUR

Le présent document entre en vigueur le 24 septembre 2021.

HISTORIQUE DES RÉVISIONS

Révision	Modifications	Date
1	Première diffusion.	Octobre 2018
2	Publication de la version 2.	24 septembre 2021

VUE D'ENSEMBLE

Le présent document dresse la liste des 10 mesures d'atténuation que votre organisation peut prendre pour protéger ses réseaux connectés à Internet et son information sensible contre les cybermenaces à la sécurité.

La présente version du document comprend les facteurs à considérer par les clients des services infonuagiques et des services gérés. Le présent document remplace les versions précédentes de l'ITSM.10.189, *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information*, et de l'ITSB-89 version 3, *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information du gouvernement du Canada*.

TABLE DES MATIÈRES

LISTE DES FIGURES

1 INTRODUCTION

Le présent document dresse la liste des 10 mesures d'atténuation que votre organisation peut prendre pour protéger ses réseaux connectés à Internet et son information sensible contre les cybermenaces à la sécurité. Prendre chacune de ces 10 mesures vous permet d'ajouter des couches additionnelles de défense à votre environnement et de faire en sorte que les auteurs de menace aient plus de difficulté à exploiter les vulnérabilités touchant vos réseaux, vos systèmes et votre information en vue de les compromettre.

Bien qu'il soit recommandé de mettre en place l'ensemble des 10 mesures, on convient que votre organisation pourrait ne pas être en mesure de le faire. Votre organisation devrait procéder à une évaluation des risques afin de déterminer ses exigences et ses priorités en matière de sécurité. Au moment de prendre ces mesures, vous devriez les adapter à l'environnement de votre organisation et appliquer toute mesure additionnelle nécessaire pour protéger vos systèmes et votre information les plus sensibles.

Les ministères et les organismes du gouvernement du Canada (GC) sont invités à consulter les exigences en matière de cybersécurité abordées dans la *Directive sur les services et le numérique* du GC [1][1]. Si votre organisation ne fait pas partie du GC, vous pouvez vous reporter à cette politique au moment de créer votre propre programme de sécurité et vos propres politiques en la matière. Pour de plus amples renseignements sur la mise en œuvre des contrôles de cybersécurité de base, prière de consulter le document *Contrôle de cybersécurité de base pour les petites et moyennes organisations* [2].

[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.

2 LES 10 MESURES DE SÉCURITÉ

Les 10 mesures de sécurité comprennent les mesures prioritaires que votre organisation devrait adopter comme base de référence pour renforcer son infrastructure de TI et protéger ses réseaux. Bien qu'il soit recommandé de suivre l'ordre numérique de ces mesures (en commençant par la mesure 1) pour accroître vos efforts de protection contre les cybermenaces, vous pouvez changer la séquence des mesures de manière à répondre aux besoins et aux exigences de votre organisation. À mesure que vous ajoutez des mesures de sécurité dans votre environnement, votre exposition aux menaces (c.-à-d., tous les points d'extrémité disponibles qu'un auteur de menace peut tenter d'exploiter) diminue, alors que votre posture de sécurité augmente.

Il convient de se rappeler que ces mesures ne sont qu'un point de départ et qu'aucune stratégie ne peut à elle seule prévenir tous les cyberincidents. Le paysage des cybermenaces est en constante évolution et vous devriez vous assurer de réévaluer vos risques et de revoir les efforts que vous déployez en matière de sécurité de sorte à pouvoir tenir compte de toute lacune ou faiblesse.

Au moment de déterminer vos besoins en matière de sécurité, vous devriez également déterminer si votre organisation fait appel à des services infonuagiques ou gérés. Vous devriez évaluer les menaces, les vulnérabilités, les responsabilités communes et les capacités de la plateforme infonuagique de manière à pouvoir mettre en place les mesures de sécurité appropriées. La mise en œuvre des 10 mesures de sécurité peut varier selon les types de services utilisés. Par exemple, les rôles et les responsabilités de votre organisation et du fournisseur de services infonuagiques (FSI) ou fournisseur de services gérés (FSG) dépendront des services que vous utilisez, ainsi que des modèles de services et de déploiement. Par contre, même si elle fait appel à des services infonuagiques ou gérés, votre organisation est toujours responsable sur le plan juridique d'assurer la sécurité de ses données et de rendre des comptes à cet égard. Pour de plus amples renseignements sur la sécurité et les services infonuagiques ou gérés, prière de consulter l'ITSM.50.062, *Gestion des risques liés à la sécurité infonuagique* [3], et l'ITSM.50.030, *Facteurs à considérer par les clients de services gérés en matière de cybersécurité* [4].

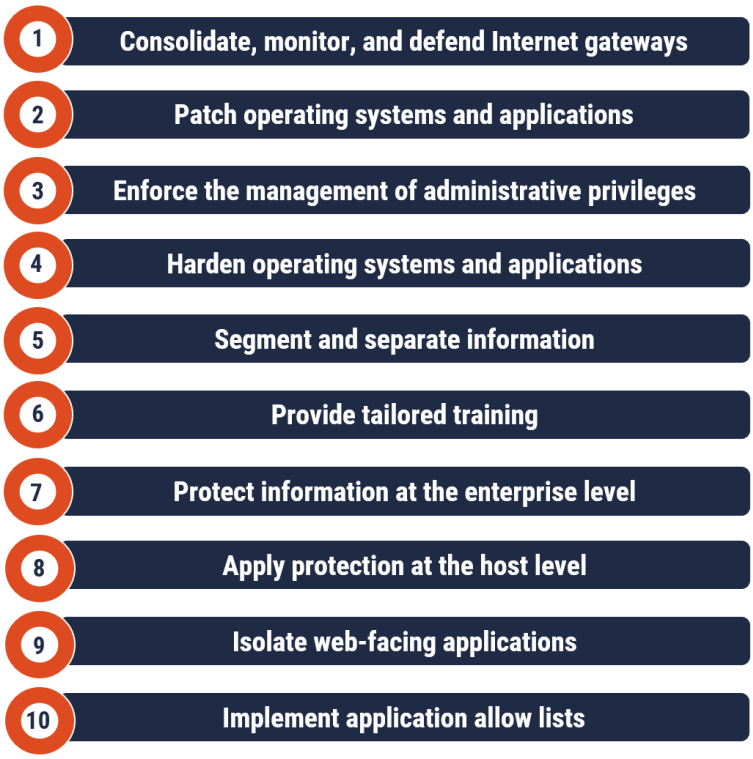

Figure 1 : Les 10 mesures de sécurité des TI

2.1 INTÉGRER, SURVEILLER ET DÉFENDRE LES PASSERELLES INTERNET

La mesure 1 consiste à intégrer, à surveiller et à défendre vos passerelles Internet. Vos passerelles Internet sont des points de vérification installés en périphérie de votre réseau. Elles surveillent le trafic entrant et sortant pour assurer la protection de votre organisation. Les ministères et organismes du GC devraient réduire le nombre de connexions externes discrètes à leurs réseaux ministériels en faisant appel aux passerelles Internet consolidées de Services partagés Canada.

Votre organisation devrait également assurer la surveillance de son serveur de système de noms de domaine (DNS pour *Domain Name System*). L'Autorité canadienne pour les enregistrements Internet (ACEI) offre un service DNS protégé gratuit, le Bouclier canadien, qui empêche les connexions à des sites Web malveillants susceptibles d'infecter les dispositifs et de voler les renseignements personnels.

Il incombe à votre organisation de surveiller l'ensemble du trafic entrant et sortant à ces passerelles, même si vous avez recours à des services infonuagiques. Pour simplifier cette tâche, il convient de réduire le nombre de connexions externes à votre réseau. Vous devriez d'abord établir la base de référence des tendances suivies par le trafic normal afin de pouvoir détecter les écarts et de prendre les mesures nécessaires.

Si vous utilisez des services infonuagiques, vous devez également tenir compte du flux de données que votre organisation transmet à tout système ou service infonuagique. Selon le degré de sensibilité des données transmises à ces services et la version du protocole de sécurité de la couche transport (TLS pour *Transport Layer Security*) utilisée par le fournisseur, il pourrait être préférable de mettre en place un réseau privé virtuel (RPV). Un RPV permet d'établir une connexion sécurisée entre deux points et peut servir à protéger les données sensibles lorsqu'elles transitent entre ces deux points. Selon le degré

de sensibilité de vos données, vous pourriez envisager de mettre en place des modèles de connexion dédiés (c.-à-d., la façon dont votre organisation se connecte aux services infonuagiques). Dans un tel cas, vous devrez négocier avec votre fournisseur et pourriez avoir à configurer et à mettre en place des mesures comme la sécurité du protocole Internet (IPsec pour *Internet Protocol Security*) ou la sécurité du contrôle d'accès au support (MACsec pour *Media Access Control Security*).

Vous pouvez également externaliser les activités de surveillance à un fournisseur de services de sécurité gérés (FSSG). Si vous travaillez avec un fournisseur de services qui offre des services de passerelles sécurisées, vous devriez clairement déterminer les rôles et les responsabilités de votre organisation et du fournisseur de services en ce qui a trait à la surveillance du trafic et au signalement des anomalies ou des activités malveillantes.

Vous pouvez mettre en place des mécanismes de cyberdéfense additionnels pour surveiller les entrées non autorisées, les exfiltrations de données ou toute autre activité malveillante, et intervenir en conséquence. Si une activité malveillante est détectée, ces solutions de cyberdéfense devraient être en mesure de fermer les points d'accès de façon à stopper les exfiltrations de données et à bloquer les attaques.

Publications connexes :

- ITSM.50.030, *Facteurs à considérer par les clients de services gérés en matière de cybersécurité* [4]
- ITSAP.80.101, *Les réseaux privés virtuels* [5]

2.2 APPLIQUER DES CORRECTIFS AUX APPLICATIONS ET AUX SYSTÈMES D'EXPLOITATION

La mesure 2 consiste à appliquer régulièrement les correctifs aux applications et aux systèmes d'exploitation de votre organisation. Les mises à jour et les correctifs permettent non seulement de corriger les bogues ou d'améliorer l'utilisation ou la performance des appareils, mais aussi de corriger les vulnérabilités de sécurité connues.

Mettez en place une stratégie de gestion des correctifs pour les systèmes d'exploitation et les applications tierces pour réduire l'exposition de votre organisation aux vulnérabilités connues. Dès qu'un correctif de sécurité est publié par un fournisseur, vous devez suivre le processus de gestion des correctifs de votre organisation afin de l'appliquer le plus rapidement possible. Vous pouvez faire appel à un système automatique de gestion des correctifs pour les appliquer de façon opportune.

Il convient d'utiliser des versions des systèmes d'exploitation et des applications qui sont prises en charge, testées et mises à niveau. Le déploiement d'applications ou de systèmes d'exploitation qui ne sont pas pris en charge, et pour lesquels aucune mise à jour n'est disponible, accroît les risques d'exploitation des vulnérabilités, puisqu'aucun mécanisme n'est en place pour les atténuer.

Si vous avez externalisé vos services de TI à un FSI ou à un FSG, vous devriez passer en revue votre contrat de service afin de déterminer les rôles et les responsabilités en ce qui a trait à la gestion des correctifs. Ceux-ci varieront selon votre modèle de service infonuagique. Par exemple, dans le cas d'une infrastructure-service (IaaS pour *Infrastructure as a Service*) ou d'une plateforme-service (PaaS pour *Platform as a Service*), il vous incombe de mettre à jour vos systèmes et vos applications et d'appliquer les correctifs. Dans le cas d'un logiciel-service (SaaS pour *Software as a Service*), le FSI est responsable de l'application des mises à jour et des correctifs. Toutefois, même si vous utilisez un fournisseur de services,

il vous revient d'installer les mises à jour et les correctifs sur les périphériques ou les systèmes et appareils qui ne font pas partie du contrat.

Publications connexes :

- ITSAP.10.096, *Application des mises à jour sur les dispositifs* [6]

2.3 METTRE EN VIGUEUR LA GESTION DES PRIVILÈGES D'ADMINISTRATEUR

La mesure 3 consiste à imposer la gestion des privilèges d'administrateur. Mettez en pratique le principe du droit d'accès minimal pour vous assurer que les utilisateurs ne disposent que des accès et des privilèges dont ils ont besoin dans le cadre de leurs fonctions. Vous devriez limiter le nombre d'administrateurs ou d'utilisateurs privilégiés pour ce qui est des systèmes d'exploitation et des applications.

Créez des comptes dotés de niveaux de droits administratifs distincts de manière à limiter les risques d'exposition dans l'éventualité où un compte d'administration serait compromis. Pour prévenir les expositions découlant d'attaques par hameçonnage ou par maliciel, il conviendra d'effectuer les tâches administratives à partir d'un poste de travail réservé à cette fin et 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 d'administration. Les administrateurs devraient disposer d'un compte d'administration distinct et d'un compte utilisateur général. Ils pourront ainsi utiliser leur compte d'administration pour exécuter des tâches administratives et utiliser leur compte utilisateur général pour les autres tâches (p. ex. vérifier les courriels). Utiliser le même hôte pour mener des activités de nature administrative et générale constitue un risque, puisque cet hôte pourrait être compromis lors de la réalisation d'activités générales (p. ex. ouvrir un courriel malveillant ou y répondre, ou cliquer sur des liens malveillants). Advenant la compromission de l'hôte, les justificatifs administratifs de l'utilisateur pourraient également être compromis. En règle générale, il est plus facile de réagir à la compromission d'un compte utilisateur courant qu'à celle d'un compte d'administration.

Votre organisation devrait mettre en œuvre une solution pour protéger les mots de passe des comptes d'administration. Pour accroître l'assurance de l'authenticité des justificatifs d'utilisateur, il est fortement recommandé de faire appel à l'authentification multifacteur (MFA pour *Multi-Factor Authentication*), dans la mesure du possible, pour l'ensemble des utilisateurs et des applications.

Révisez et validez régulièrement la liste d'utilisateurs administratifs de votre organisation pour veiller à ce que les privilèges soient révoqués dès que les utilisateurs n'en ont plus besoin (p. ex. changement de rôle ou de personnel).

Si vous utilisez des services infonuagiques, il vous incombera d'assurer la gestion du contrôle d'accès. Si vous avez externalisé vos services de TI à un FSG, vous devriez savoir à quels utilisateurs il convient d'accorder des accès privilégiés.

Publications connexes :

- ITSAP.10.094, *Gestion et contrôle des privilèges administratifs* [7]
- ITSAP.30.030, *Sécurisez vos comptes et vos appareils avec une authentification multifacteur* [8]

2.4 RENFORCER LES SYSTÈMES D'EXPLOITATION ET LES APPLICATIONS

La mesure 4 consiste à renforcer les systèmes d'exploitation et les applications de votre organisation. Votre organisation devrait être au courant de toutes les applications utilisées. Des configurations par défaut ou des erreurs de configuration pourraient rendre vos réseaux, vos systèmes et vos dispositifs vulnérables. Vous devriez mettre en place des contrôles de sécurité pour renforcer les systèmes d'exploitation. Pour de plus amples renseignements sur la sélection et l'application des contrôles de sécurité, prière de consulter l'ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [9].

Pour prévenir la compromission d'actifs et d'infrastructures connectés à Internet, votre organisation devrait désactiver tous les ports et les services non essentiels et supprimer les comptes inutiles. Évaluez toutes les applications de tierces parties pour déterminer 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). Vous devriez également procéder à une vérification au niveau de l'organisme et mettre en place une solution antivirus dans le cadre de votre configuration sécurisée.

Si vous utilisez des services infonuagiques ou gérés, il pourrait incomber à votre fournisseur de renforcer les systèmes d'exploitation et les applications, selon vos modèles de services et de déploiement. Par exemple, dans un modèle IaaS ou PaaS, votre organisation est tenue de renforcer les systèmes d'exploitation et les applications. Dans un modèle SaaS, cette tâche relève plutôt du fournisseur de services. Votre organisation est responsable de tout l'équipement sur site nécessaire pour intégrer des composants ou des solutions hybrides.

Publications connexes :

- ITSP.70.012, *Conseils sur le renforcement de la sécurité de Microsoft Windows 10 Enterprise* [10]

2.5 SEGMENTER ET SÉPARER L'INFORMATION

La mesure 5 consiste à segmenter et à séparer l'information. Votre organisation devrait faire l'inventaire de ses renseignements organisationnels essentiels et les catégoriser selon leur degré de sensibilité ou leur incidence sur la vie privée.

Il est recommandé de zoner les réseaux en segmentant les services d'infrastructure en groupes logiques qui répondent aux mêmes stratégies de sécurité en matière de 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. Vous devriez également surveiller et appliquer les contrôles visant à maintenir la protection et l'intégrité des différentes zones.

Les principes de zonage continuent de s'appliquer si votre organisation fait appel à des services infonuagiques ou gérés. Si vous faites appel à un modèle de déploiement infonuagique partagé, par exemple, vous devriez vous assurer que vos données sont séparées de celles appartenant aux autres locataires.

Publications connexes :

- ITSP.80.022, *Exigences de base en matière de sécurité pour les zones de sécurité de réseau* [11]

- ITSG-38, *Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones* [12]

2.6 MISER SUR UNE FORMATION ET UNE SENSIBILISATION SUR MESURE

La mesure 6 consiste à fournir à vos employés une formation en matière de cybersécurité sur mesure. Bien qu'on puisse s'attendre à ce que les mesures de sécurité des systèmes arrivent à prévenir les activités malveillantes sur les réseaux, il convient de considérer plusieurs facteurs pour assurer la gestion des risques. Il est possible de réduire le niveau de risque de votre organisation en offrant aux employés de la formation sur les enjeux liés à la cybersécurité et en les sensibilisant aux rôles et aux responsabilités qu'ils doivent assumer pour protéger les réseaux, les systèmes et les biens de TI.

Votre organisation devrait miser sur la formation et la sensibilisation pour atténuer les cybermenaces et les vulnérabilités, ainsi que gérer les exigences sur le plan des stratégies (p. ex. comportements attendus des utilisateurs). Vous devriez passer en revue vos programmes et vos activités en matière de sensibilisation à la sécurité des TI sur une base régulière et vous assurer qu'ils sont accessibles à tous les utilisateurs ayant accès aux systèmes de votre organisation.

Notre site Web (**cyber.gc.ca**) présente un catalogue de publications sur divers sujets liés à la cybersécurité. Ces publications peuvent aider les employés à se sensibiliser davantage aux cybermenaces et aux pratiques exemplaires qu'il convient d'adopter. Vous pouvez également consulter le site de Pensez cybersécurité, une campagne nationale de sensibilisation du public visant à informer les Canadiens des questions de cybersécurité.

Publications connexes :

- *ITSM.10.093, Les 10 mesures de sécurité des TI : Nº 6, Miser sur une formation sur mesure en matière de cybersécurité* [13]
- ITSAP.10.093, *Offrir aux employés une formation sur mesure en cybersécurité* [14]

2.7 PROTÉGER L'INFORMATION AU NIVEAU DE L'ORGANISATION

La mesure 7 consiste à protéger l'information au niveau de l'organisation. L'information de votre organisation est essentielle au bon déroulement de vos activités et une cible de choix pour les auteurs de menace. Vous devriez vous assurer que votre information est gérée de façon appropriée tout au long de son cycle de vie (p. ex. étiquetage, traitement, conservation et destruction des données).

Au moment de déployer des appareils mobiles dans votre organisation, vous devriez tenir compte des risques et des avantages liés aux différents modèles de déploiement. 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, à condition de s'être doté d'un cadre de gestion des dispositifs et d'avoir instauré un processus de gestion de changement des configurations. Si votre organisation décide d'autoriser les employés à utiliser leurs propres dispositifs à des fins professionnelles, il conviendra de mettre en place une stratégie de contrôle rigoureuse et de passer en revue les technologies et les exigences juridiques en matière de ségrégation des renseignements personnels et organisationnels. Votre organisme peut utiliser la gestion unifiée des dispositifs d'extrémité (UEM pour *Unified Endpoint Management*) pour assurer la sécurité des dispositifs mobiles. L'UEM combine les fonctionnalités de la gestion des postes mobiles et des processus de gestion de la mobilité d'entreprise.

Vous pouvez utiliser les systèmes et les services fournis par des FSI, des FSG ou des FSSG. Dans tous les cas, votre organisation demeure légalement responsable de la protection de ses données et doit rendre des comptes à cet égard. Lorsque des données sont stockées à l'extérieur de l'infrastructure de votre organisation, vous devez savoir où le stockage est effectué (c.-à-d. l'emplacement géographique). Les données stockées à l'extérieur du Canada sont assujetties à des lois et à des règlements différents en matière de protection des renseignements personnels, de sécurité et de propriété des données. Si vous utilisez des services infonuagiques ou gérés qui stockent des données à l'extérieur du Canada, passez en revue les lois applicables dans l'emplacement géographique où résident les données et évaluez les répercussions possibles sur la protection des renseignements personnels.

Remarque : Il incombe aux ministères et aux organismes du GC de s'assurer que leurs installations informatiques situées dans les limites géographiques du Canada ou dans l'édifice d'un ministère du GC à l'étranger (p. ex. un consulat canadien) sont identifiées et évaluées en tant que principale option de transmission pour l'ensemble de l'information numérique et des données sensibles (c.-à-d., PROTÉGÉ B, PROTÉGÉ C et CLASSIFIÉ) contrôlées par le GC. De préférence, les ministères et organismes du GC devraient conserver l'information sensible au Canada. Par ailleurs, ils sont tenus de procéder aux évaluations des risques en fonction de la nature des données et de leur sensibilité, et d'établir leurs exigences en matière de disponibilité. Prière de consulter la *Directive sur les services et le numérique* [1] pour de plus amples renseignements.

Publications connexes :

- ITSAP.10.016, *Conseils de sécurité pour les organisations dont les employés travaillent à distance* [15]
- ITSAP.70.002, *Considérations de sécurité pour les modèles de déploiement de dispositifs mobiles* [16]
- ITSAP.50.112, *Étapes pour gérer les fuites de données dans le nuage* [17]

2.8 ASSURER LA PROTECTION AU NIVEAU DE L'HÔTE

La mesure 8 consiste à protéger l'information au niveau de l'hôte. Vous devriez déployer une solution de système de prévention des intrusions sur l'hôte (HIPS pour *Host-Based Intrusion Prevention System*) afin de protéger vos systèmes contre les activités malveillantes connues ou inconnues, comme les virus et les maliciels. Plusieurs fournisseurs proposent des services HIPS commerciaux.

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. Vous devriez continuer de surveiller les alertes et l'information de journalisation du système HIPS pour y découvrir les signes d'intrusion.

Si vous utilisez des services infonuagiques, vous devez tout de même assurer la protection au niveau de l'hôte et devriez tenir compte des points d'extrémité du nuage, de la transmission des données et de votre architecture (p. ex. bordure et périmètre). Il est recommandé d'utiliser les jeux d'outils fournis par votre FSI et tous les outils de tierces parties qui pourraient possiblement s'appliquer.

2.9 ISOLER LES APPLICATIONS WEB

La mesure 9 consiste à isoler toutes les applications Web. Votre organisation devrait utiliser la virtualisation pour créer un environnement dans lequel les applications Web peuvent être exécutées isolément (p. ex. en bac à sable). Isoler ces applications permet, par exemple, de confiner les maliciels dans votre environnement virtualisé et d'éviter qu'ils se propagent et infectent l'hôte ou l'entreprise.

Publications connexes :

- ITSAP.70.011, *La virtualisation de votre infrastructure* [18]

2.10 METTRE EN PLACE UNE LISTE D'APPLICATIONS AUTORISÉES

La mesure 10 consiste à mettre en place une liste des applications autorisées. La liste d'applications autorisées permet d'établir quels sont les applications et les composants d'applications (p. ex. programmes exécutables, bibliothèques de logiciels, fichiers de configuration) autorisés à s'exécuter sur des systèmes organisationnels. En mettant en place des listes d'applications autorisées, vous pouvez éviter que des applications malveillantes ne soient téléchargées et infectent vos serveurs et vos systèmes.

Votre organisation devrait créer une liste des applications dont l'utilisation est autorisée dans les lieux de travail et qui proviennent de fournisseurs dignes de confiance. Il convient donc de bloquer systématiquement tous les éléments ne figurant pas dans la liste. Vous pouvez définir la liste d'applications autorisées 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). Vous devriez définir et déployer des stratégies liées aux listes d'applications autorisées à l'échelle de l'organisation. N'oubliez pas de mettre à jour votre liste d'applications autorisées au moment d'installer des correctifs ou de procéder à la mise à jour d'une application, ou lorsque vous commencez à utiliser des logiciels ou cessez de les utiliser.

Si vous faites appel aux services d'un FSI ou d'un FSG pour configurer vos listes d'applications autorisées, vous devriez tenir compte de la sensibilité de vos données, ainsi que définir et contrôler les stratégies d'accès à vos données. Mettez en place des contrôles de sécurité des données additionnels pour limiter l'accès à vos données conformément à vos politiques en matière de sensibilité des données.

Publications connexes :

- ITSB-95, *Utilisation d'une liste d'applications autorisées* [19]

3 RÉSUMÉ

Le présent document fait mention des 10 mesures de sécurité des TI que votre organisation peut mettre en place comme mesures de sécurité de référence. En prenant toutes ces mesures, vous pouvez réduire l'exposition aux menaces de votre organisation et renforcer votre posture de sécurité. Par contre, celles-ci ne sont que le point de départ. Votre organisation devrait continuer d'évaluer les menaces et les risques de manière à s'assurer qu'elle met en œuvre des contrôles de sécurité qui répondent à ses besoins en matière de sécurité. Si vous utilisez des services infonuagiques ou gérés, vous devriez tenir compte des menaces et des risques additionnels, et déterminer les rôles et les responsabilités associés à ces mesures de sécurité.

3.1 COORDONNÉES

Pour obtenir de plus amples renseignements sur la façon de mettre en œuvre les 10 mesures de sécurité des TI, prière de visiter le site Web cyber.gc.ca ou de communiquer avec le Centre d'appel.

Centre d'appel du Centre pour la cybersécurité

contact@cyber.gc.ca

613-949-7048 ou 1-833-CYBER-88

4 CONTENU COMPLÉMENTAIRE

4.1 LISTE D'ABRÉVIATIONS, D'ACRONYMES ET DE SIGLES

Terme	Définition
FSG	Fournisseur de services gérés
FSI	Fournisseur de services infonuagiques
FSSG	Fournisseur de services de sécurité gérés
GC	Gouvernement du Canada
HIPS	Système de prévention des intrusions sur l'hôte (*Host-based Intrusion Prevention System*)
IaaS	Infrastructure-service (*Infrastructure as a Service*)
IPsec	Protocole IPsec (*Internet Protocol Security*)
MACsec	Sécurité du contrôle d'accès au support (*Media Access Control Security*)
MFA	Authentification multifacteur (*Multi-Factor Authentication*)
PaaS	Plateforme-service (*Platform as a Service*)
RPV	Réseau privé virtuel
SaaS	Logiciel-service (*Software as a Service*)
SCT	Secrétariat du Conseil du Trésor du Canada
TI	Technologies de l'information
TLS	Protocole de sécurité de la couche transport (*Transport Layer Security*)
UEM	Gestion unifiée des terminaux (*Unified Endpoint Management*)

4.2 GLOSSAIRE

Terme	Définition
Authentification multifacteur	Méthode d'authentification qui consiste à utiliser deux facteurs d'authentification ou plus (p. ex. quelque chose que vous connaissez, quelque chose qui vous caractérise, quelque chose que vous avez) pour confirmer l'identité d'un utilisateur.
Données en transit	Données actives qui se déplacent d'un emplacement à l'autre, comme sur Internet ou dans un réseau privé.
Droit d'accès minimal	Principe de sécurité selon lequel il convient de n'accorder aux utilisateurs que les autorisations d'accès dont ils ont besoin pour accomplir les tâches qui leur ont été dûment attribuées.
Fournisseur de services de sécurité gérés	Fournisseur de services qui surveille et gère les dispositifs et les systèmes de sécurité au nom d'un client.
Fournisseur de services gérés	Entreprise qui gère à distance l'infrastructure de TI et les systèmes utilisateur au nom d'un client.
Fournisseur de services infonuagiques	Tout fournisseur commercial qui offre des services infonuagiques afin d'assurer, sur demande, la disponibilité aux ressources des systèmes informatiques.
Gestion unifiée des terminaux	Outil logiciel qui distribue, gère et contrôle les dispositifs de point d'extrémité (p. ex., les dispositifs de bureau et les dispositifs mobiles).
Liste d'applications autorisées	Liste de contrôle qui indique les applications autorisées à s'exécuter sur les systèmes d'une organisation.
Maliciel	Logiciel malveillant conçu pour infiltrer ou endommager un système informatique. Les maliciels les plus courants sont les virus informatiques, les vers, les chevaux de Troie, les logiciels espions, les logiciels publicitaires et les rançongiciels.
Modèle de déploiement infonuagique	Les modèles de déploiement décrivent le rapport entre le fournisseur de services infonuagiques et le client. On retrouve quatre modèles de déploiement infonuagique : le nuage public, le nuage privé, le nuage communautaire et le nuage hybride.
Modèle de services infonuagiques	Modèle de service décrivant le type de services que le fournisseur fournit aux clients. On retrouve trois modèles de services infonuagiques différents : l'infrastructure-service (IaaS), la plateforme-service (PaaS) et le logiciel-service (SaaS).
Protocole de sécurité de la couche transport	Protocole d'authentification et de sécurité utilisé pour assurer la confidentialité et l'intégrité des données entre deux applications de communication [20].
Réseau privé virtuel	Réseau de communication privé généralement utilisé au sein d'une organisation ou entre plusieurs entreprises ou organisations diverses pour communiquer sur un réseau élargi. Les communications sur le RPV sont habituellement chiffrées ou codées pour protéger le trafic provenant des autres utilisateurs, qui est transmis sur le réseau public ayant recours au RPV.
Risque	Degré de probabilité qu'un auteur de menace exploite une vulnérabilité pour accéder à un bien et répercussions connexes. Le risque est exprimé en fonction d'un niveau (faible, moyen ou élevé).
Système de prévention des intrusions sur l'hôte	Logiciel qui permet de surveiller les activités suspectes sur un hôte unique. 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.
Virtualisation	Simulation d'un logiciel ou du matériel utilisé pour exécuter d'autres logiciels [20].

Terme	Définition
Vulnérabilité	Défectuosité ou lacune inhérente à la conception ou à la mise en œuvre d'un système d'information ou à son environnement, qui pourrait être exploitée en vue de compromettre les biens ou les activités d'une organisation.
Zone de sécurité de réseau	Environnement de réseau clairement délimité relevant d'une autorité de zone de sécurité de réseau et caractérisé par un niveau standard de vulnérabilité aux menaces. On distingue les types de zones d'après les exigences de sécurité s'appliquant aux interfaces, au contrôle du trafic, à la protection des données, au contrôle de la configuration de l'hôte et au contrôle de la configuration du réseau.

4.3 RÉFÉRENCES

Numéro	Référence
1	Secrétariat du Conseil du Trésor du Canada, *Directive sur les services et le numérique*, 1er avril 2020.
2	Centre canadien pour la cybersécurité, *Contrôles de cybersécurité de base pour les petites et moyennes organisations*, février 2020.
3	Centre canadien pour la cybersécurité, ITSM.50.062, *Gestion des risques liés à la sécurité infonuagique*, mars 2019.
4	Centre canadien pour la cybersécurité, ITSM.50.030, *Facteurs à considérer par les clients de services gérés en matière de cybersécurité*, octobre 2020.
5	Centre canadien pour la cybersécurité, ITSAP.80.101, *Les réseaux privés virtuels*, octobre 2019.
6	Centre canadien pour la cybersécurité, ITSAP.10.096, *Application des mises à jour sur les dispositifs*, février 2020.
7	Centre canadien pour la cybersécurité, ITSAP.10.094, *Gestion et contrôle des privilèges administratifs*, juillet 2020.
8	Centre canadien pour la cybersécurité, ITSAP.30.030, *Sécurisez vos comptes et vos appareils avec une authentification multifacteur*, juin 2020.
9	Centre canadien pour la cybersécurité, ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, décembre 2014.
10	Centre canadien pour la cybersécurité, ITSP.70.012, *Conseils sur le renforcement de la sécurité de Microsoft Windows 10 Enterprise*, mars 2019.
11	Centre canadien pour la cybersécurité, ITSP.80.022, *Exigences de base en matière de sécurité pour les zones de sécurité de réseau*, février 2021.
12	Centre canadien pour la cybersécurité, ITSG-38, *Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones*, mai 2009.
13	Centre canadien pour la cybersécurité, ITSM.10.093, *Les 10 mesures de sécurité des TI : No 6, Miser sur une formation sur mesure en matière de cybersécurité*, février 2020.
14	Centre canadien pour la cybersécurité, ITSAP.10.093, *Offrir aux employés une formation sur mesure en cybersécurité*, octobre 2020.

Numéro	Référence
15	Centre canadien pour la cybersécurité, ITSAP.10.016, *Conseils de sécurité pour les organisations dont les employés travaillent à distance*, mai 2020.
16	Centre canadien pour la cybersécurité, ITSAP.70.002, *Considérations de sécurité pour les modèles de déploiement de dispositifs mobiles*, juin 2020.
17	Centre canadien pour la cybersécurité, ITSAP.50.112, *Étapes pour gérer les fuites de données dans le nuage*, septembre 2019.
18	Centre canadien pour la cybersécurité, ITSAP.70.011, *La virtualisation de votre infrastructure*, septembre 2020.
19	Centre canadien pour la cybersécurité, ITSB-95, *Utilisation d'une liste d'applications autorisées – Bulletin de sécurité des TI à l'intention du gouvernement du Canada*, mars 2015.
20	National Institute for Standards and Technology, *Computer Security Resource Centre Glossary*, non daté.