Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Les 10 mesures de sécurité des TI :

Nº 10, Mettre en place une liste d'applications autorisées

SÉRIE GESTIONNAIRES

ITSM.10.095

Canada

Avant-propos

La présente publication est un document NON CLASSIFIÉ qui fait partie d'une série de documents axés sur les 10 mesures de sécurité des TI recommandées dans l'ITSM.10.189, *Les 10 mesures de sécurité des technologies de l'information visant à protéger les réseaux Internet et l'information* [1][1].

Date d'entrée en vigueur

Le présent document entre en vigueur le 11 août 2022.

Historique des révisions

Révision	Modifications	Date
1	Première diffusion.	11 août 2022

[1] Les numéros entre les crochets renvoient à des références figurant à la section Contenu complémentaire du présent document.

Sommaire

L'une des 10 mesures de sécurité des TI recommandées par le CST, qui sont mentionnées dans le document *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089)* [1] du Centre canadien pour la cybersécurité (Centre pour la cybersécurité), consiste à mettre en place une liste d'applications autorisées. Une liste d'autorisation définit les applications et les fichiers exécutables dont votre organisation autorise l'exécution sur ses systèmes. Ce document traite des nombreuses pratiques exemplaires liées au contrôle des applications autorisées sur vos systèmes. Les conseils formulés dans la présente sont fondés sur les contrôles de sécurité mentionnés dans le document intitulé *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33) [2].

Mettre en place une liste d'applications autorisées vous permet de bloquer l'exécution d'applications non approuvées sur vos systèmes. Vous devez gérer la liste d'autorisation de manière à ce que vos employés puissent accéder aux applications dont ils ont besoin. La gestion d'une telle liste permet également de veiller à ce que les systèmes n'entravent pas le bon déroulement de vos activités en bloquant par erreur du code non malveillant. La mise en place d'une liste d'autorisation est une approche proactive qui permet de bloquer les programmes qui ne figurent pas dans la liste. Il convient de se rappeler qu'il s'agit d'une mesure additionnelle. Pour assurer une meilleure protection de ses réseaux et de ses systèmes, votre organisation devrait également mettre en place des mesures de sécurité supplémentaires.

La présente publication fait partie d'une série de documents axés sur les 10 mesures de sécurité des TI recommandées dans l'ITSM.10.189 [1]. Bien que la mise en œuvre de l'ensemble des 10 mesures de sécurité recommandées puisse rendre votre organisation moins vulnérable aux cybermenaces, vous devriez examiner les activités que vous menez sur le plan de la cybersécurité pour déterminer s'il convient de prendre des mesures supplémentaires. Pour de plus amples renseignements sur la mise en œuvre des 10 mesures de sécurité des TI, veuillez communiquer par téléphone ou par courriel avec le :

Centre d'appel du Centre pour la cybersécurité

contact@cyber.gc.ca

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

D97-4/10-095-2022F-PDF
978-0-660-44899-2

Table des matières

Liste des figures

Liste des tableaux

Liste des annexes

1 Aperçu de la gestion des risques liés à la sécurité des TI

1.1 Les 10 mesures de sécurité des TI

Le présent document fournit des conseils sur la façon de mettre en place une liste d'applications autorisées. Une liste d'autorisation permet de réduire le degré d'exposition de votre organisation aux virus et maliciels susceptibles de compromettre ses réseaux, ses systèmes et ses biens de TI. La présente est fondée sur les conseils et les contrôles de sécurité formulés respectivement dans l'ITSM.10.189 [1] et l'annexe 3A de l'ITSG-33 [2].

Les 10 mesures de sécurité des TI recommandées par le CST qui sont mentionnées à la figure 1 ci-dessous et dans l'ITMS.10.189 [1] sont fondées sur une analyse des tendances inhérentes aux cybermenaces et la répercussion de telles menaces sur les réseaux connectés à Internet. La mise en œuvre de toutes les mesures permettra de corriger la plupart des vulnérabilités liées à la sécurité des TI qui pèsent sur votre organisation.

Les cybermenaces peuvent avoir diverses répercussions sur l'environnement opérationnel et technique de votre organisation. Vous devriez passer en revue vos activités actuelles de gestion de la sécurité et du risque pour veiller à ce qu'elles répondent à vos exigences en matière de sécurité.

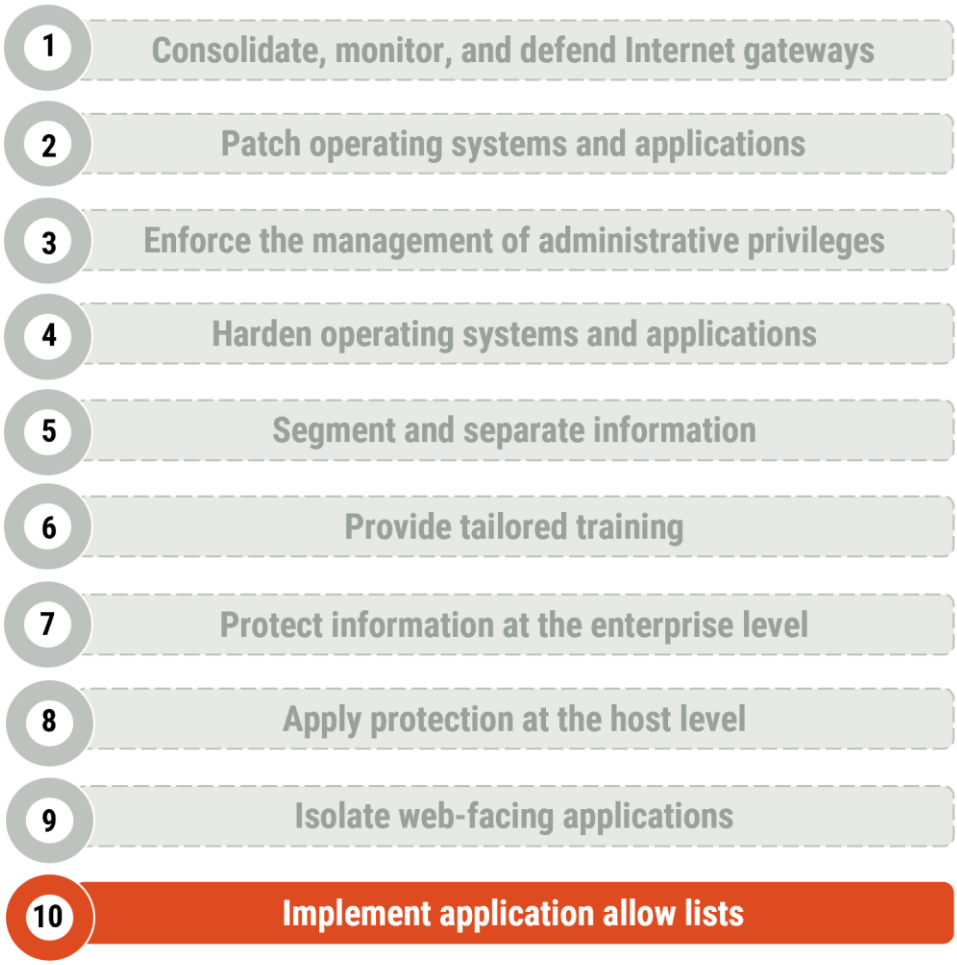

Figure 1 : Les 10 mesures de sécurité des TI : Nº 10, Mettre en place une liste d'applications autorisées

1.2 Rapport avec le processus de gestion des risques liés à la sécurité des TI

Les 10 mesures de sécurité des TI du CST découlent des contrôles de sécurité mentionnés à l'annexe 3A de l'ITSG-33 [2]. L'ITSG-33 [2] décrit les rôles, les responsabilités et les activités qui permettent à une organisation de gérer les risques relevant de la sécurité des TI, et comprend un catalogue de contrôles de sécurité (c.-à-d., un ensemble standardisé d'exigences de sécurité visant à protéger la confidentialité, l'intégrité et la disponibilité des biens de TI). Ces contrôles de sécurité sont regroupés en trois classes, puis subdivisés en plusieurs familles (ou regroupements) de contrôles de sécurité connexes :

- **Contrôles de sécurité techniques :** Contrôles de sécurité qui sont mis en œuvre et exécutés par les systèmes d'information, principalement par l'intermédiaire de mécanismes de sécurité que l'on retrouve dans les composants matériels, logiciels et micrologiciels;
- **Contrôles de sécurité opérationnels :** Contrôles de sécurité de système d'information qui sont mis en œuvre et exécutés principalement par des personnes et qui s'appuient normalement sur des technologies comme les logiciels de soutien;
- **Contrôles de sécurité de gestion :** Contrôles de sécurité qui portent principalement sur la gestion de la sécurité des TI et les risques liés à la sécurité des TI.

Tel qu'il est illustré dans la figure 2, le présent document fait mention de mesures qui relèvent de la famille de contrôles Gestion des configurations (CM pour *Configuration Management*). Il décrit les contrôles suivants :

- **CM-7 Fonctionnalité minimale**

De plus amples renseignements sur le contrôle CM-7 sont fournis à l'annexe A du présent document.

Figure 2 : Classes et familles de contrôles de sécurité applicables décrites dans l'ITSG-33

Vous pouvez utiliser les contrôles de sécurité mentionnés dans le présent document et à l'annexe 3A de l'ITSG-33 [2] pour déterminer la meilleure façon de gérer les risques liés à la cybersécurité de votre organisation et protéger ses réseaux, ses systèmes et ses biens de TI. Il convient toutefois de garder à l'esprit que la mise en œuvre de ces contrôles ne constitue qu'une partie du processus de gestion des risques liés à la sécurité des TI.

L'ITSG-33 [2] décrit un processus fondé sur deux niveaux d'activités de gestion des risques liés à la sécurité, à savoir les activités menées au niveau organisationnel (ou ministériel) et celles menées au niveau du système d'information. Mener à bien ces deux niveaux d'activités de gestion des risques vous aidera à déterminer les besoins en matière de sécurité pour l'ensemble de votre organisation et pour ses systèmes d'information. Après avoir compris vos besoins pour chaque niveau, vous serez en mesure d'établir les contrôles de sécurité que votre organisation doit mettre en place et maintenir pour satisfaire un niveau de risque acceptable. Après avoir sélectionné les contrôles de sécurité appropriés, il convient de les adapter de manière à ce qu'ils répondent à vos besoins opérationnels et en matière de sécurité.

2 Présentation des listes d'applications autorisées

La mise en place d'une liste d'applications autorisées est l'une des mesures essentielles qu'il est possible de prendre pour réduire le degré d'exposition de votre organisation aux cybermenaces. Bien que certains systèmes d'exploitation intègrent une technologie permettant l'utilisation de listes d'applications autorisées, votre organisation devrait adopter une stratégie pour créer et mettre en place de telles listes sur ses dispositifs mobiles et locaux.

Pour de plus amples renseignements sur les listes d'autorisation, prière de consulter la publication de la National Institute of Standards and Technology (NIST) intitulée *Special Publication 800-167* [3].

2.1 Listes d'autorisation et d'exclusion

Une liste d'autorisation permet à votre organisation de sélectionner et d'approuver les applications et les composants d'applications (p. ex. programmes exécutables, bibliothèques de logiciels, fichiers de configuration) dont l'exécution est autorisée sur ses systèmes. Elle réduit considérablement les risques que des maliciels s'exécutent sur les systèmes et que les utilisateurs installent des logiciels non autorisés. Malgré l'efficacité d'une telle approche, votre organisation devrait s'assurer de mettre en place une liste d'autorisation qui n'entrave pas l'utilisation attendue des systèmes organisationnels, comme le blocage erroné de code non malveillant.

Votre organisation peut utiliser une liste d'applications autorisées à d'autres fins que le contrôle de l'accès aux applications. Les exemples peuvent comprendre ce qui suit :

- **Inventaire des logiciels** : Pour conserver un inventaire des applications et des versions d'applications installées sur chaque hôte de sorte que votre organisation puisse identifier les applications non autorisées;
- **Surveillance de l'intégrité des fichiers :** Pour surveiller les tentatives de changements liées aux fichiers d'application et les signaler;
- **Intervention en cas d'incident :** Pour utiliser la liste d'applications autorisées de manière à vérifier la présence de fichiers malveillants sur d'autres hôtes.

La liste d'exclusion permet aux administrateurs de maintenir une liste des applications dont l'accès au système est interdit et d'empêcher leur installation ou leur exécution. Les applications sont exclues si on les sait malveillantes ou si leur utilisation est considérée comme inappropriée au sein de votre organisation. Pour maintenir une telle liste, votre administrateur de système doit vérifier tous les nouveaux fichiers sur un système, confirmer qu'ils ne sont pas malveillants et les bloquer si c'est le cas. Les cybermenaces changent et s'accroissent sans cesse, ce qui complique le recours aux listes d'exclusion et les rend moins efficaces que les listes d'autorisation. Les solutions faisant appel aux listes d'exclusion ont également une incidence importante sur les performances des programmes au moment de leur démarrage ou de leur exécution.

2.2 Méthodes de création d'une liste d'autorisation

Pour créer une liste d'autorisation, vous pouvez combiner l'information obtenue du fournisseur relativement aux bonnes applications connues et celle que votre organisation a recueillie concernant les caractéristiques de ses applications

personnalisées ou exclusives. Une autre méthode consiste à créer une base de référence valide connue en analysant les fichiers sur un hôte propre.

Vous devez mettre à jour votre liste d'autorisation après avoir appliqué des mises à jour ou des correctifs aux applications autorisées ou avoir autorisé et installé de nouvelles applications sur des hôtes.

2.2.1 Attributs de fichiers et de dossiers

Votre liste d'autorisation peut être basée sur les différents attributs des fichiers et dossiers des applications (voir le tableau 1). Bien qu'il ne s'agisse pas d'une liste complète, certains exemples comprennent des attributs comme le chemin d'accès des fichiers, leur nom, leur taille, leur signature numérique ou leur éditeur, et leur code de hachage cryptographique. Il est recommandé d'utiliser plusieurs attributs pour définir votre liste d'autorisation, particulièrement si vous employez des attributs plus simples comme le chemin d'accès des fichiers, leur nom ou leur taille.

Tableau 1 : Exemples d'attributs de fichiers et de dossiers pour les listes d'autorisation

Caractéristique	Détails
Chemin d'accès du fichier	Autorise les applications qui sont stockées dans un ou plusieurs chemins d'accès en particulier (répertoire ou dossier). L'utilisation de cet attribut évite aux administrateurs de système d'avoir à saisir tous les fichiers dans la liste d'autorisation. **Remarque :** Cet attribut devrait être combiné à d'autres attributs afin de prévenir l'exécution de maliciels qui sont enregistrés dans un répertoire ou dossier approuvé. Vous pouvez faire appel à des contrôles d'accès rigoureux pour veiller à ce que seuls les administrateurs autorisés puissent ajouter ou modifier des fichiers dans le répertoire ou dossier. Pour renforcer votre liste d'autorisation, il convient d'associer plusieurs attributs.
Nom de fichier	Autorise les applications qui portent une nom de fichier en particulier. **Remarque :** Si un fichier est infecté ou remplacé par un fichier malveillant, la liste d'autorisation continuera d'autoriser son exécution, puisque le nom du ficher demeure le même. Pour renforcer votre liste d'autorisation, il convient d'associer plusieurs attributs.
Taille de fichier	Surveille la taille d'une application. **Remarque :** Cet attribut suppose que les fichiers malveillants sont d'une certaine taille. Les auteurs de menace peuvent créer des fichiers malveillants de manière à ce que leur taille corresponde à celle de fichiers inoffensifs. Pour renforcer votre liste d'autorisation, il convient d'associer plusieurs attributs.
Signature numérique	Vérifie les signatures numériques individuelles et les certificats de signature d'une application.
Éditeur	Autorise les applications associées à un éditeur approuvé en particulier. **Remarque :** Si l'identité de l'éditeur est utilisée, on suppose que toutes les applications de l'éditeur approuvé sont également autorisées, ce qui pourrait ne pas être nécessairement le cas.

Caractéristique	Détails
Valeur de hachage	Identifie les fichiers correspondant aux applications autorisées. Une valeur de hachage (ou condensé) est une chaîne courte produite par un algorithme de chiffrement à partir d'un fichier d'entrée, pour laquelle la même entrée génère toujours le même condensé, alors qu'aucune autre entrée ne peut générer un condensé identique ou similaire. **Remarque :** La valeur de hachage sera différente après l'application d'une mise à jour ou d'un correctif. Les administrateurs de système doivent ajouter cette nouvelle valeur de hachage à la liste d'autorisation pour s'assurer que le logiciel puisse continuer de fonctionner. Ils doivent également supprimer les valeurs de hachage existantes des anciennes versions des logiciels qui comportent des vulnérabilités connues.

En plus des attributs de fichiers, la liste d'autorisation de votre organisation peut également autoriser certaines séquences de comportements des utilisateurs et des systèmes (p. ex. une application qui écrit sur un disque dur de façon routinière et légitime).

2.2.2 Fichiers liés aux applications

Les liste d'applications autorisées peuvent surveiller d'autres fichiers liés aux applications, dont les suivants :

- les bibliothèques;
- les scripts;
- les macros;
- les modules d'extension de navigateurs;
- les modules complémentaires de navigateurs;
- les extensions de navigateurs;
- les fichiers de configuration;
- les entrées de registre.

3 Pratiques exemplaires pour la mise en place des listes d'autorisation (CM-7)

Cette section décrit les mesures qu'il convient de prendre pour mettre en place une liste d'applications autorisées sur les systèmes de votre organisation. Les mesures comprises dans le présent document sont basées sur le contrôle de sécurité **CM-7, Fonctionnalité minimale**. Pour de plus amples renseignements sur ce contrôle, consultez l'annexe A1 du présent document et l'annexe 3A de l'ITSG-33 [2].

Il importe de souligner que les pratiques exemplaires mentionnées dans la présente ne sont pas décrites en détail. Comme pour toute solution informatique, votre organisation doit passer en revue ses exigences opérationnelles et en matière de sécurité.

3.1 Évaluer les solutions de listes d'applications autorisées

Avant de procéder à la création et à la mise en place d'une liste d'autorisation, votre organisation devrait déterminer ses besoins opérationnels et ses exigences en matière de sécurité. Elle devrait faire l'examen de ses réseaux et de ses systèmes pour s'assurer de mettre en œuvre une solution compatible. Les systèmes de votre organisation pourraient être sujets à des exigences différentes en matière de sécurité. La stratégie de votre liste d'autorisation devrait en tenir compte.

Vous devriez déterminer quelles ressources sont nécessaires pour bien mettre en œuvre et gérer la liste d'autorisation. Ces ressources peuvent comprendre un administrateur de système chargé de tenir à jour la liste d'autorisation, ainsi que le personnel de soutien nécessaire pour résoudre les problèmes qui surviennent après sa mise en place.

Vous devez déterminer si les systèmes d'exploitation de vos hôtes (comme des ordinateurs de bureau, des ordinateurs portables ou des serveurs) sont dotés de technologies de listes d'autorisation intégrées qui conviennent à votre environnement. Ces considérations visent à réduire le niveau d'effort à consacrer à la mise en œuvre d'une solution et à limiter les coûts.

Si votre organisation a recours à des applications en nuage, il convient d'envisager la mise en place d'une technologie hybride pour les applications locales et en nuage, plutôt que des solutions distinctes.

3.2 Déterminer les applications à autoriser

Pour veiller à ce que la liste d'autorisation n'entrave pas le bon déroulement des activités, vous devez dresser une liste des ressources dont votre organisation a besoin pour fonctionner efficacement. Votre organisation devrait ensuite relever toutes les applications et tous les composants d'applications qui peuvent être exécutés sur ses systèmes organisationnels. Pour définir la liste d'autorisation, il est possible de sélectionner de nombreux attributs de fichier et de dossier (comme les chemins d'accès des fichiers, leur nom, leur taille, leur signature numérique ou éditeur, ou leur hachage cryptographique) ou d'autres critères.

Une approche moins exigeante à la mise en place d'une liste d'autorisation consiste à préciser les répertoires (comme C:\Windows ou C:\Program Files) à partir desquels les utilisateurs pourront exécuter des programmes. Cette approche

empêche les applications de s'exécuter à l'extérieur des répertoires déterminés par l'organisation. Il est toutefois recommandé d'envisager une approche plus exhaustive, comme mettre à jour l'environnement d'exploitation standard (SOE pour *Standard Operating Environment*), dans la mesure du possible. Par SOE, on entend l'image et la liste d'applications que votre organisation veut utiliser et mettre à jour. Le recours à un SOE peut aider votre organisation à assurer le maintien, le soutien et la gestion de ses applications de façon rentable et efficace.

3.3 Créer une stratégie

Il convient de s'assurer que la stratégie de la liste d'autorisation respecte vos exigences opérationnelles. Il est recommandé de baser votre liste d'autorisation sur une stratégie tout interdire, permettre par exception. Ainsi, seules les applications autorisées pourront être exécutées sur les systèmes organisationnels.

La stratégie devrait définir les restrictions et l'utilisation acceptable des programmes informatiques sur les systèmes de votre organisation. Elle devrait également comprendre tous les contrôles définis, comme les exceptions liées aux programmes locaux, à l'administration à distance et au partage de fichiers. Votre stratégie devrait indiquer que les utilisateurs généraux ne peuvent pas installer d'applications non autorisées ou apporter des changements aux applications et aux fichiers qu'il est possible d'exécuter sur les systèmes organisationnels.

3.4 Tester la liste d'autorisation

Avant de mettre en place la liste d'autorisation, vous devez la tester et vous assurer qu'elle a été conçue conformément aux exigences. Vous devriez évaluer les aspects suivants de la liste d'autorisation :

- fonctionnalité de base (p. ex. est-il possible d'exécuter les applications autorisées? Les applications exclues sont-elles bloquées?);
- capacités de gestion des administrateurs (p. ex. les administrateurs peuvent-ils appliquer les mises à jour ou les correctifs?);
- journalisation et alertes (p. ex. les modifications sont-elles journalisées?);
- performances (p. ex. quelles sont les performances durant une utilisation normale et maximale?);
- sécurité (p. ex. la solution comporte-t-elle des vulnérabilités qui pourraient être exploitées?).

3.4.1 Modes des listes d'applications autorisées

La plupart des technologies de listes d'autorisation proposent les modes d'exécution opérationnels suivants :

- **Mode Audit :** Génère les données d'analyse en permettant l'exécution et la journalisation des applications, dont celles qui ne se trouvent pas dans la liste d'autorisation.
- **Mode de mise en conformité** : Autorise automatiquement l'exécution des éléments dans la liste d'autorisation et bloque les éléments interdits. Ce mode permet également de guider les utilisateurs en demandant à ces derniers (ou à l'administrateur) d'accepter ou de refuser une tentative d'exécution d'un fichier s'il n'apparaît pas dans la liste d'autorisation ou dans la liste d'exclusion.

En règle générale, on utilise le mode Audit pour évaluer une liste d'autorisation. Le mode de mise en conformité peut être utilisé une fois que votre administrateur de système a évalué les résultats du mode Audit et a confirmé l'efficacité de la liste d'autorisation. Ces journaux d'événements sont également de précieuses ressources en cas d'incident ou s'il faut procéder à une reprise.

3.5 Mettre en place la liste d'autorisation

Il peut être difficile de mettre en place une liste d'applications autorisées dans l'ensemble d'une organisation. On recommande d'adopter une approche progressive et de déployer la liste d'autorisation au sein d'un groupe pilote. L'adoption d'une approche progressive permettra d'évaluer l'incidence d'un tel déploiement et de corriger les problèmes potentiels avant la mise en place de la liste d'autorisation dans l'ensemble de votre organisation. Votre groupe pilote peut comprendre des hôtes utilisés par les employés suivants :

- les cadres supérieurs, leurs adjoints et leurs agents administratifs;
- le personnel des services de soutien, les administrateurs de système et les utilisateurs à qui des privilèges d'administrateur ou des accès privilégiés ont été accordés;
- les utilisateurs ayant accès à de l'information sensible;
- les utilisateurs ayant des accès à distance.

Vous pourriez également envisager d'inclure des services d'entreprise de grande valeur, comme des serveurs d'applications de base (p. ex. les contrôleurs de domaine, les principaux serveurs Active Directory et les serveurs de bases de données) lors du déploiement initial d'une liste d'autorisation.

3.6 Gérer la liste d'autorisation

L'efficacité d'une liste d'autorisation repose sur votre capacité à la tenir à jour. Par exemple, vous devez mettre à jour la liste d'autorisation après avoir apporté des changements aux stratégies, avoir appliqué des mises à jour ou des correctifs aux applications, ou avoir autorisé et installé de nouvelles applications sur des hôtes.

Avec l'adoption croissante des services infonuagiques et de l'hébergement en nuage, les administrateurs de système peuvent ajouter des applications approuvées aux boutiques d'applications et aux catalogues en ligne, ce qui peut mener à une gestion et à une installation plus faciles de celles-ci.

En plus de mettre à jour la liste, vos administrateurs de système devraient continuer d'évaluer les systèmes organisationnels, les surveiller de manière à relever tout problème opérationnel ou lié à la sécurité et procéder à l'évaluation régulière des vulnérabilités.

3.7 Mettre en application la liste d'autorisation

Tel qu'il est indiqué à la section 3.4.1, vous pouvez envisager d'activer le mode de mise en conformité offert par la plupart des technologies de listes d'autorisation. Cela permettra automatiquement d'exécuter les éléments compris dans votre liste d'autorisation et de bloquer ceux qui se trouvent dans votre liste d'exclusion. La publication de la NIST intitulée *Special*

Publication 800-167 décrit les différentes formes du mode de mise en conformité, lesquelles se distinguent par la façon dont le mode gère les éléments qui ne sont pas compris dans vos listes d'autorisation ou d'exclusion [3] :

1. L'**application de la liste d'autorisation** ne permet d'exécuter que les éléments se trouvant dans la liste d'autorisation et bloque les tentatives d'exécution de tous les autres éléments;
2. Les **invites utilisateur** exigent que l'utilisateur (ou dans certains cas, l'administrateur) accepte ou refuse chaque tentative d'exécution d'un fichier qui ne se trouve pas sur la liste d'autorisation ou d'exclusion;
3. L'**application de la liste d'exclusion** bloque l'exécution des éléments compris dans votre liste d'exclusion, mais permet l'exécution de tous les autres éléments.

3.8 Mettre en place des listes d'autorisation sur des dispositifs mobiles

Il peut être difficile de mettre en place une liste d'applications autorisées sur des dispositifs mobiles selon le modèle de déploiement mobile adopté par votre organisation. Les modèles « propriété de l'entreprise, usage professionnel uniquement » (COBO pour *Corporate Owned/Business Only*) et « propriété de l'entreprise avec accès privé » (COPE pour *Corporate Owned/Personally Operated*) permettent à votre organisation d'exercer une plus grande supervision et de réduire les problèmes liés à la mise en place d'une liste d'applications autorisées. Le modèle « prenez vos appareils personnels » (PAP) peut poser certains défis pour votre organisation au moment de mettre en place des listes d'applications autorisées sur des dispositifs mobiles, puisque ces dispositifs n'appartiennent pas à l'organisation, mais bien à leurs utilisateurs.

Plusieurs fournisseurs tiers proposent des services d'évaluation de la sécurité des applications pour les dispositifs mobiles. Ces évaluations peuvent comprendre la vérification de l'information de source ouverte du fournisseur de l'application, l'analyse préliminaire du fichier binaire de l'application en vue de déterminer les risques connus, les évaluations en profondeur des applications, la rétro-ingénierie du code et l'identification des serveurs et des services auxquels l'application se connecte sur Internet.

Ces fournisseurs peuvent associer leurs services aux plateformes de gestion des applications mobiles (MAP pour *Mobile Application Management*) de votre organisation, qui s'intégreront ensuite aux plateformes de gestion des appareils mobiles (MDM pour *Mobile Device Management*) et de gestion unifiée des terminaux (UEM pour *Unified Enterprise Management*) de votre organisation pour lui fournir un moyen de gérer ses boutiques d'applications, ses licences, ses correctifs et ses mises à jour. Il importe de souligner que les installations de listes d'applications autorisées selon le modèle COPE ne sont pas homogènes, puisque la MDM ne permet généralement pas d'installer une liste d'applications autorisées sur le côté personnel de l'appareil. Certaines plateformes et certains fournisseurs peuvent mettre en place une liste d'exclusion du côté personnel de l'appareil pour bloquer l'accès aux applications indésirables ou potentiellement dangereuses.

4 Résumé

Mettre en place une liste d'applications autorisées est l'une des 10 meilleures mesures de sécurité des TI que nous vous suggérons de mettre en œuvre. Les pratiques exemplaires décrites dans la présente sont basées sur le contrôle de sécurité CM-7 mentionné à l'annexe A. De plus amples renseignements sur les listes d'applications autorisées sont disponibles dans la publication de la NIST intitulée *Special Publication 800-167* [3].

Mettre en place une liste d'applications autorisées permettra de réduire les risques que des applications non autorisées et malveillantes s'exécutent sur vos systèmes. Vous pouvez utiliser une liste d'autorisation comme moyen de bloquer de façon proactive et efficace les maliciels et de les empêcher d'atteindre vos réseaux et vos systèmes et de s'y exécuter.

Cela dit, la mise en œuvre d'une telle liste n'est qu'un des nombreux éléments nécessaires pour améliorer la cybersécurité de votre organisation. Pour mieux protéger votre organisation contre les cybermenaces, vous devriez passer en revue et mettre en place l'ensemble des mesures recommandées dans l'ITSM.10.189 [1].

4.1 Coordonnées

Pour de plus amples renseignements sur la mise en œuvre des conseils formulés dans la présente ou d'une autre des 10 mesures de sécurité des TI, veuillez communiquer par téléphone ou par courriel avec le :

Centre d'appel du Centre pour la cybersécurité

contact@cyber.gc.ca

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

5 Contenu complémentaire

5.1 Liste d'abréviations, d'acronymes et de sigles

Acronyme ou sigle	Définition
CM	Gestion des configurations (code de la famille de contrôles de sécurité) (*Configuration Management*)
CVE	Vulnérabilités et expositions courantes (*Common Vulnerabilities and Exposures*)
CVSS	Système de notation des vulnérabilités courantes (*Common Vulnerability Scoring System*)
CWE	*Common Weakness Enumeration*
NIST	*National Institute of Standards and Technology*
SA	Acquisition des systèmes et des services (code de la famille de contrôles de sécurité) (*System and Services Acquisition*)
SI	Intégrité de l'information et des systèmes (code de la famille de contrôles de sécurité) (*System and Information Integrity*)
SOE	Environnement d'exploitation standard (*Standard Operating Environment*)
TI	Technologies de l'information

5.2 Glossaire

Acronyme ou sigle	Définition
Bien de TI	Composants d'un système d'information, ce qui comprend les applications opérationnelles, les données, le matériel et les logiciels.
Confidentialité	Caractéristique de l'information sensible protégée contre tout accès non autorisé.
Contrôle de sécurité	Exigence technique, opérationnelle ou gestionnelle de haut niveau relative à la sécurité, qu'il convient d'appliquer à un système d'information afin de protéger la confidentialité, l'intégrité et la disponibilité des biens de TI connexes. Ces contrôles peuvent être appliqués au moyen de diverses solutions de sécurité, notamment des produits, des stratégies, des pratiques et des procédures de sécurité.
Contrôle de sécurité de gestion	Classe de contrôles de sécurité qui porte principalement sur la gestion de la sécurité des TI et les risques liés à la sécurité des TI.
Contrôle de sécurité opérationnel	Classe de contrôles de sécurité qui est principalement mise en œuvre et exécutée par des personnes, mais habituellement fondée sur l'utilisation de la technologie, par exemple, un logiciel de soutien.
Contrôle de sécurité technique	Classe de contrôles de sécurité qui est mise en œuvre et exécutée par les systèmes d'information, principalement par l'intermédiaire de mécanismes de sécurité intégrés aux composants matériels, logiciels et micrologiciels.

Acronyme ou sigle	Définition
Cyberattaque	Recours à des techniques électroniques visant à perturber, à manipuler, à détruire ou à scruter clandestinement un système informatique, un réseau ou un appareil.
Disponibilité	Caractéristique de l'information ou des systèmes qui sont accessibles aux personnes autorisées au moment où celles-ci en ont besoin. La disponibilité est un attribut des actifs informationnels, des logiciels et du matériel informatique (l'infrastructure et ses composantes). Il est également entendu que la disponibilité comprend la protection des actifs contre les accès non autorisés et les compromissions.
Environnement d'exploitation standard	Image et liste des applications utilisées au sein de l'organisation. On ne retrouve aucune norme propre à l'ensemble de l'industrie. L'environnement d'exploitation standard est adapté selon l'organisation.
Hachage cryptographique	Le hachage cryptographique consiste à appliquer un algorithme à des données binaires (p. ex. un fichier) pour produire une chaîne courte appelée valeur de hachage ou condensé de manière à ce que la même entrée génère toujours le même condensé, mais qu'il soit impossible de trouver facilement une autre entrée permettant de générer un condensé identique ou similaire.
Intégrité	Aptitude à protéger l'information contre les modifications ou les suppressions non intentionnelles et inopportunes. L'intégrité permet de savoir si l'information est conforme à ce qu'elle est censée être. Elle s'applique également aux processus opérationnels, à la logique des applications logicielles, au matériel et au personnel.
Liste d'applications autorisées	Liste des applications et des composants d'applications (p. ex. programmes exécutables, bibliothèques de logiciels, fichiers de configuration) dont l'installation et l'exécution sont autorisées sur des systèmes organisationnels.
Liste d'applications interdites	Liste des applications et des composants d'applications non autorisés ou indésirables (p. ex. programmes exécutables, bibliothèques de logiciels, fichiers de configuration) dont l'installation et l'exécution sont interdites sur des systèmes organisationnels.
Menace	Événement ou acte délibéré, accidentel ou naturel pouvant éventuellement porter préjudice aux biens et à l'information TI.
Risque	Degré de probabilité qu'un auteur de menace exploite une vulnérabilité pour accéder à des biens de TI ou pour les compromettre, et répercussions connexes.
Valeur de hachage	Une valeur de hachage (ou condensé) est une chaîne courte produite par un algorithme de chiffrement à partir d'un fichier d'entrée, pour laquelle la même entrée génère toujours le même condensé, alors qu'aucune autre entrée ne peut générer un condensé identique ou similaire.
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 par un auteur de menace en vue de compromettre les actifs ou les activités d'une organisation.

5.3 Références

Numéro	Référence
1	Centre canadien pour la cybersécurité, *ITSM.10.189, Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information*, septembre 2021.
2	Centre canadien pour la cybersécurité, *ITSG-33 IT, Gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, décembre 2014.
3	National Institute of Standards and Technology, *NIST Special Publication 800-167 Guide to Application Whitelisting*, octobre 2015.

Annexe A ITSG-33, Catalogue des contrôles de sécurité

A.1 Contrôles de sécurité opérationnels : Gestion des configurations

Le tableau 2 décrit les contrôles de gestion des configurations (CM) mentionnés à l'annexe 3A de l'ITSG-33 [2].

Tableau 2 : Contrôles de sécurité opérationnels de l'ITSG-33 : Gestion des configurations (CM)

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
CM-7	Fonctionnalité minimale	(A) L'organisation configure le système d'information pour qu'il ne fournisse que les capacités essentielles. (B) L'organisation interdit ou restreint l'utilisation des fonctions, des ports, des protocoles ou des services suivants : [*fonctions, ports, protocoles ou services définis par l'organisation*].	**Examen périodique :** L'organisation examine le système d'information [*fréquence définie par l'organisation*] pour identifier les fonctions, ports, protocoles ou services non requis ou non sécurisés. L'organisation désactive [*fonctions, ports, protocoles et services du système d'information jugés inutiles ou non sécurisés définis par l'organisation*]. Voir les contrôles connexes AC-18, CM-7 et IA-2.	AC-6 CM-2 RA-5 SA-5 SC-7
			Prévention de l'exécution des programmes : Le système d'information empêche l'exécution des programmes conformément aux [*politiques sur l'utilisation de programmes logiciels et restrictions connexes définies par l'organisation; règles d'autorisation des modalités d'utilisation d'un programme*]. Voir le contrôle connexe CM-8.	
			Conformité aux exigences d'enregistrement : L'organisation assure le respect des [*exigences d'enregistrement définies par l'organisation concernant les fonctions, ports, protocoles et services*].	

			Logiciels non autorisés et liste d'exclusion : L'organisation : i. détermine les [*programmes logiciels qui ne peuvent pas être exécutés sur le système d'information*]; ii. a recours à une politique tout permettre, interdire par exception pour empêcher l'exécution des programmes logiciels non autorisés sur le système d'information; iii. examine et met à jour la liste des programmes logiciels non autorisés [*fréquence définie par l'organisation*]. Voir les contrôles connexes CM-6 et CM-8.	
			Logiciels autorisés et listes d'autorisation : i. détermine les [*programmes logiciels qui peuvent être exécutés sur le système d'information*]; ii. a recours à une politique tout interdire, autoriser par exception pour permettre l'exécution des programmes logiciels autorisés sur le système d'information; iii. examine et met à jour la liste des programmes logiciels autorisés [*fréquence définie par l'organisation*]. Voir les contrôles connexes CM-2, CM-6, CM-8, SA-10, SC-34 et SI-7.	