Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Protection de l'information désignée dans les organisations et les systèmes ne relevant pas du gouvernement du Canada

Praticien·nes

ITSP.10.171

Canada

Avant-propos

La présente est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal, Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir plus d'information ou suggérer des modifications, veuillez communiquer avec le Centre d'appel :

- contact@cyber.gc.ca
- (613) 949-7048 ou 1-833-CYBER-88.

Date d'entrée en vigueur

Le présent document entre en vigueur le 2 avril 2025.

Historique des révisions

Révision	Modifications	Date
1	Première version.	2 avril 2025
2	Version 2	28 octobre 2025

D96-124/2024F-PDF
978-0-660-74645-6

Vue d'ensemble

La protection de l'information désignée revêt une importance capitale pour les ministères et organismes du gouvernement du Canada (GC) et peut avoir une incidence directe sur la capacité du GC de réaliser ses missions et ses fonctions essentielles avec succès. Cette publication offre aux ministères et aux organismes du GC des exigences de sécurité recommandées afin de protéger la confidentialité de l'information désignée se trouvant dans des organisations et des systèmes ne relevant pas du GC. Ces exigences s'appliquent aux composants des systèmes ne relevant pas du GC qui gèrent, traitent, stockent ou transmettent de l'information désignée ou qui protègent de tels composants. Les exigences de sécurité sont destinées à l'usage des ministères et organismes du GC dans des contrats ou d'autres ententes établis avec des organisations ne relevant pas du GC.

Le présent document est une version canadienne de la publication du National Institute of Standards and Technology intitulée *NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (en anglais seulement). Le Centre pour la cybersécurité produira une publication complémentaire à utiliser conjointement avec le document intitulé *NIST SP 800-171A Assessing Security Requirements for Controlled Unclassified Information* (en anglais seulement). Ce document fournira un ensemble complet de procédures pour évaluer les exigences de sécurité. Dans l'intervalle, le document NIST SP 800-171A (en anglais seulement) pourra servir de référence.

Mentions

Le Centre pour la cybersécurité souhaite remercier Victoria Pillitteri et Ron Ross (PhD) de la division de sécurité informatique du NIST d'avoir permis à l'équipe des Conseils en matière de cybersécurité (CSG pour *Cyber Security Guidance*) d'utiliser leurs conseils et de les modifier afin de les adapter au contexte canadien.

Table des matières

Liste des tableaux

Liste des annexes

1 Introduction

Cette publication est la version canadienne du document *NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (en anglais seulement). Il n'y a pas de changements techniques importants entre le présent document et le document NIST SP 800-171 (en anglais seulement). Les principales modifications concernent les différences entre les lois, les politiques, les directives, les normes et les lignes directrices. Autrement dit, les changements tiennent compte du contexte réglementaire et de conformité propre au Canada; aucun changement n'a été apporté au contexte technique sous-jacent.

Ces contrôles sont alignés sur le *Catalogue des activités d'assurance et des contrôles de sécurité et de confidentialité* (ITSP.10.033), qui est une version adaptée au contexte canadien du document *NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations* (en anglais seulement).

L'**information désignée** comprend toute information autre que classifiée qu'une autorité du GC désigne et mentionne dans un contrat comme devant faire l'objet d'une sauvegarde. L'information protégée, y compris les exigences de protection et de diffusion connexes, est définie par le Secrétariat du Conseil du Trésor du Canada (SCT) dans la *Directive sur la gestion de la sécurité – Annexe J : Norme sur la catégorisation de sécurité* du SCT et codifiée dans la *Politique sur la protection de la vie privée* du SCT. Nous employons le terme « information désignée » à la place du terme anglais « controlled unclassified information » (CUI) utilisé dans le document américain, et dont l'équivalent français est « information non classifiée contrôlée ».

Les ministères et organismes du GC doivent suivre les politiques et les directives publiées par le SCT lorsqu'ils utilisent des systèmes fédéraux pour gérer, traiter, stocker ou transmettre de l'information[1].

La responsabilité des ministères et des organismes du GC de protéger l'information désignée demeure la même lorsqu'elle communique une telle information à des organisations ne relevant pas du GC. Par conséquent, un niveau de protection similaire est nécessaire lorsque des organisations à l'extérieur du GC utilisent des systèmes ne relevant pas du GC pour gérer, traiter, stocker ou transmettre de l'information désignée. Afin d'assurer un niveau de protection uniforme, les exigences de sécurité pour la protection de l'information désignée dans les organisations et les systèmes ne relevant pas du GC doivent être conformes aux politiques du SCT suivantes : *Politique sur la sécurité du gouvernement*, *Politique sur les services et le numérique* et *Politique sur la protection de la vie privée*.

Les contrôles et les activités de sécurité présentés dans cette publication prennent en considération les exigences associées aux contrats fédéraux.

Le présent document n'intègre pas tous les ensembles de contrôles et d'activités associés à la protection de la vie privée décrits dans l'ITSP.10.033. Il présente plutôt un sous-ensemble des contrôles associés à la protection de la vie privée qui sont communs avec les contrôles de confidentialité.

[1] Système utilisé ou exploité par un ministère ou un organisme du GC, par une entrepreneure ou un entrepreneur, ou par une autre organisation au nom d'un ministère ou d'un organisme. Le terme « système », tel qu'il est utilisé dans cette publication, comprend les personnes, les processus et les technologies qui interviennent dans la gestion, le traitement, le stockage ou la transmission de l'information désignée. Les systèmes peuvent inclure les technologies opérationnelles (TO), les technologies de l'information (TI), les dispositifs de l'Internet des objets (IdO), les dispositifs de l'Internet industriel des objets (IIdO), les systèmes spécialisés, les cybersystèmes physiques, les systèmes embarqués et les capteurs.

1.1 Objectif

La présente publication présente aux ministères et aux organismes du GC des exigences de sécurité recommandées visant à protéger la confidentialité de l'information désignée lorsque l'information se trouve dans des systèmes et des organisations ne relevant pas du GC et lorsqu'il n'existe pas d'autres exigences de protection particulières imposées par des lois, la réglementation ou des politiques s'appliquant à l'échelle gouvernementale pour la catégorie d'information désignée.

Les exigences de sécurité dans la présente publication ne s'appliquent qu'aux composants[2] des systèmes ne relevant pas du GC qui gèrent, traitent, stockent ou transmettent de l'information désignée *ou* qui protègent de tels composants. Ces exigences serviront aux ministères et aux organismes du GC dans le cadre de contrats ou d'autres ententes établies avec des organisations ne relevant pas du GC.

Il est important d'établir adéquatement la portée des exigences imposées aux organisations ne relevant pas du GC lors des décisions d'investissement en matière de protection et de la gestion des risques liés à la sécurité. Dans le cadre des activités de conception associées aux composants de systèmes pour la gestion, le traitement, le stockage ou la transmission de l'information désignée, les organisations ne relevant pas du gouvernement du Canada peuvent limiter la portée des exigences de sécurité qui s'appliquent grâce à l'isolation des composants de systèmes dans un domaine de sécurité séparé. L'isolation est possible grâce à des concepts architecturaux et de conception (par exemple, la mise en œuvre de sous-réseaux dotés de pare-feu ou d'autres dispositifs de protection de périmètre et l'utilisation de mécanismes de contrôle de flux d'information). Les domaines de sécurité peuvent utiliser une séparation physique, une séparation logique ou une combinaison des deux. Une telle approche peut fournir une sécurité adéquate pour l'information désignée, tout en évitant d'augmenter la posture de sécurité d'une organisation ne relevant pas du GC au-delà du niveau requis afin de protéger ses missions, ses opérations et ses actifs.

1.2 Public cible

Cette publication est destinée à de nombreuses personnes et organisations des secteurs publics et privés, y compris :

- les ministères et organismes du gouvernement du Canada responsables de la gestion et de la protection de l'information désignée;
- les organismes ne relevant pas du GC responsables de la protection de l'information désignée;
- les personnes ayant des responsabilités en matière de cycle de développement de systèmes (CDS);
- les personnes ayant des responsabilités liées à l'acquisition ou à l'approvisionnement;
- les personnes ayant des responsabilités associées à la gestion et à la surveillance des systèmes, de la sécurité, de la confidentialité ou des risques;
- les personnes ayant des responsabilités associées à l'évaluation et à la surveillance de la sécurité ou de la confidentialité.

[2] Les composants incluent les postes de travail, les serveurs, les ordinateurs blocs-notes, les téléphones intelligents, les tablettes, les dispositifs d'entrée-sortie, les composants réseau, les systèmes d'exploitation, les machines virtuelles, les systèmes de gestion de base de données et les applications.

1.3 Structure de la publication

La suite de cette publication sera structurée comme suit :

- La section 2, Principes de base décrit les hypothèses et la méthodologie utilisées pour la mise au point des exigences de sécurité qui visent à protéger la confidentialité de l'information désignée. Elle présente également le format des exigences et les critères d'adaptation appliqués aux lignes directrices du Centre pour la cybersécurité pour obtenir les exigences.
- La section 3, Exigences énumère les exigences de sécurité pour la protection de la confidentialité de l'information désignée dans les organisations et les systèmes ne relevant pas du GC.

Les sections suivantes fournissent des renseignements supplémentaires pour appuyer la protection de l'information désignée :

- Annexe A : Critères d'adaptation
- Annexe B : Paramètres définis par l'organisation

2 Principes de base

La présente section décrit les hypothèses et la méthodologie utilisées pour mettre au point les exigences visant à protéger la confidentialité de l'information désignée dans les organisations et les systèmes ne relevant pas du GC. Elle comprend également les critères d'adaptation appliqués aux contrôles dans l'ITSP.10.033.

2.1 Hypothèses concernant les exigences de sécurité

Les exigences de sécurité dans la présente publication sont basées sur les hypothèses suivantes :

- l'information du GC désignée comme étant de l'information désignée a toute la même valeur, peu importe si elle réside sur des systèmes relevant ou ne relevant pas du GC;
- les exigences législatives et réglementaires relatives à la protection de l'information désignée sont uniformes dans les organisations et les systèmes relevant et ne relevant pas du GC;
- les mesures de protection mises en œuvre afin de protéger l'information désignée sont uniformes dans les organisations et les systèmes relevant et ne relevant pas du GC;
- la valeur d'incidence sur la confidentialité pour l'information désignée n'est pas inférieure à faible, mais sera moyenne pour la plupart des jeux de données de grande taille du GC;
- les organisations ne relevant pas du GC peuvent mettre en œuvre directement une variété de solutions de sécurité potentielles ou avoir recours à des fournisseurs de services externes afin de répondre aux exigences de sécurité.

2.2 Méthodologie d'élaboration des exigences de sécurité

En commençant par les contrôles de l'ITSP.10.033 dans le profil d'incidence moyenne de l'ITSP.10.033-01, les contrôles ont été adaptés afin d'éliminer les contrôles ou les parties de contrôles qui :

- relèvent principalement du GC;
- ne sont pas directement liés à la protection de la confidentialité de l'information désignée;
- sont déjà abordés adéquatement par d'autres contrôles;
- ne s'appliquent pas.

Les exigences de sécurité de l'ITSP.10.171 représentent un sous-ensemble des contrôles nécessaires à la protection de la confidentialité de l'information désignée. Les exigences de sécurité sont organisées en 17 familles, tel qu'il est illustré dans le tableau 1. Chaque famille contient les exigences associées au sujet de sécurité d'ordre général qu'elle aborde. Certaines familles de l'ITSP.10.033 n'ont pas été incluses dans la présente, car elles ne contribuent pas directement à la confidentialité. Par exemple, les activités de la famille Traitement des renseignements personnels et transparence (PT) ne sont pas incluses, car elles portent sur le traitement de renseignements personnels et non leur confidentialité. La famille Gestion des programmes (PM) n'est pas incluse, car elle n'est pas associée à la confidentialité. Enfin, la famille Planification d'urgence (CP) n'est pas incluse, car elle traite de la disponibilité de l'information.

La liste qui suit donne les familles d'exigences de sécurité :

- Contrôle d'accès
- Sensibilisation et formation
- Vérification et responsabilisation
- Gestion des configurations
- Identification et authentification
- Intervention en cas d'incident
- Maintenance
- Protection des supports
- Sécurité du personnel
- Protection physique
- Évaluation des risques
- Évaluation de sécurité et surveillance
- Protection des systèmes et des communications
- Intégrité de l'information et des systèmes
- Planification
- Acquisition des systèmes et des services
- Gestion des risques liés à la chaîne d'approvisionnement

Les paramètres définis par l'organisation (ODP pour *Organization-defined Parameter*) sont inclus dans certaines exigences de sécurité. Les ODP offrent une meilleure souplesse avec l'utilisation d'affectations et de sélections permettant aux ministères et organismes du GC, ainsi qu'aux organisations ne relevant pas du GC, de spécifier des valeurs pour les paramètres désignés dans les exigences. Les affectations et les sélections servent à adapter les exigences de sécurité en fonction de besoins particuliers en matière de protection. L'établissement des valeurs des ODP peut être guidé et informé par des lois, des décrets, des directives, une réglementation, des politiques, des normes, des lignes directrices ou des besoins liés à la mission et aux activités. Une fois spécifiées, les valeurs des ODP font partie intégrante de l'exigence. Des crochets qui se trouvent dans un énoncé de contrôle ou d'activité indiquent que la lectrice ou le lecteur doit insérer une valeur d'ODP afin de permettre à l'organisation d'adapter le contrôle à son contexte particulier.

Les ODP sont une partie importante de la spécification d'une exigence de sécurité. Ils offrent aux organisations la souplesse et la spécificité nécessaires pour définir clairement leurs exigences en matière de sécurité pour la protection de l'information désignée, en fonction de leur mission, de leurs activités, de leurs environnements opérationnels et de leur tolérance au risque. De plus, les ODP permettent d'assurer l'uniformité des évaluations de sécurité qui visent à déterminer si les exigences de sécurité spécifiées ont été satisfaites ou non. Si un ministère ou organisme du GC, ou encore un groupe de ministères ou d'organismes, ne précise pas de valeur ou d'intervalle de valeurs pour un ODP, les organisations ne relevant pas du GC devront affecter la ou les valeurs afin de satisfaire à l'exigence de sécurité.

Chaque exigence comprend une section de discussion découlant des sections de discussion qui se trouvent dans le document NIST SP 800-53 (en anglais seulement). Ces sections offrent des renseignements supplémentaires afin de faciliter la mise en œuvre et l'évaluation des exigences. Elles sont informatives, et non normatives. Les sections de discussion ne sont pas destinées à étendre la portée d'une exigence ni à influencer les solutions adoptées par les organisations pour satisfaire à une exigence. Les exemples fournis sont notionnels, non exhaustifs et ne présentent pas toutes les options offertes aux organisations. La section « Références » présente les sources pour les contrôles ou les activités d'assurance tirées de l'ITSP.10.033 et énumère les publications pertinentes permettant d'obtenir des renseignements supplémentaires sur le sujet décrit dans l'exigence.

Le présent document est la première version de la publication canadienne. Ainsi, les contrôles du document NIST SP 800-171 (en anglais seulement), révision 3, qui n'ont pas été inclus dans la présente publication portent la mention « Non affecté » afin de conserver la numérotation aux fins d'interopérabilité.

La structure et le contenu d'une exigence de sécurité type sont illustrés ci-dessous à titre d'exemple.

Le terme « organisation » est employé dans un grand nombre d'exigences de sécurité et sa signification peut varier en fonction du contexte. Par exemple, dans une exigence de sécurité comportant un ODP, une organisation peut désigner soit le ministère ou organisme du GC, soit l'organisation ne relevant pas du GC qui doit établir les valeurs de paramètre pour l'exigence.

L'annexe A décrit les critères d'adaptation des contrôles de sécurité qui servent à élaborer les exigences de sécurité et les résultats du processus d'adaptation. Elle offre une liste des contrôles et des activités tirés de l'ITSP.10.033 qui appuient les exigences, ainsi que les contrôles et les activités qui ont été éliminés du profil d'incidence moyenne, conformément aux critères d'adaptation.

3 Exigences

Cette section décrit les 17 familles d'exigences de sécurité visant à protéger la confidentialité de l'information désignée dans les organisations et les systèmes ne relevant pas du GC. Dans la présente section, le terme « système » fait référence aux systèmes ou aux composants de systèmes ne relevant pas du GC qui gèrent, traitent, stockent ou transmettent de l'information désignée ou qui offrent une protection pour de tels systèmes ou composants. Les exigences de sécurité ne mentionnent pas toutes l'information désignée de manière explicite. Les exigences qui ne mentionnent pas l'information désignée de manière explicite sont incluses, car elles ont une incidence directe sur la protection d'une telle information lors du traitement, du stockage ou de la transmission de ce type d'information.

Il peut y avoir des limites quant à la façon dont certains systèmes, y compris les systèmes spécialisés (par exemple, les systèmes de contrôle industriels ou de processus, les dispositifs médicaux ou les machines à commande numérique par ordinateur) peuvent appliquer certaines exigences de sécurité. Pour tenir compte de ces limites, le plan de sécurité du système (tel qu'il est indiqué dans l'exigence Plan de sécurité du système 03.15.02) est utilisé afin de décrire toutes les exceptions durables aux exigences de sécurité. De plus, les plans d'action et des jalons servent à gérer les lacunes individuelles, isolées ou temporaires (tel qu'il est indiqué dans l'exigence Plan d'action et des jalons 03.12.02).

Les exigences de sécurité dans cette section ne s'appliquent qu'aux composants des systèmes ne relevant pas du GC qui traitent, stockent ou transmettent de l'information désignée ou qui offrent une protection pour de tels composants.

3.1 Contrôle d'accès

Les contrôles dans la famille Contrôle d'accès permettent d'autoriser ou de refuser l'accès des utilisatrices et utilisateurs à des ressources dans le système.

03.01.01 Gestion des comptes

A. Définir les types de comptes système autorisés et interdits.

B. Créer, activer, modifier, désactiver et retirer les comptes système conformément aux stratégies, aux procédures, aux conditions préalables et aux critères de l'organisation.

C. Préciser :

1. les utilisatrices et utilisateurs autorisés du système;
2. les membres des groupes et des rôles;
3. les autorisations d'accès (c'est-à-dire les privilèges) pour chaque compte.

D. Autoriser l'accès au système en fonction de ce qui suit :

1. une autorisation d'accès valide;
2. l'utilisation prévue du système.

E. Surveiller l'utilisation des comptes système.

F. Désactiver les comptes système dans les circonstances suivantes :

1. les comptes sont expirés;
2. les comptes sont inactifs depuis [Affectation : durée définie par l'organisation];
3. les comptes ne sont plus associés à une utilisatrice ou un utilisateur, ou à une personne;
4. les comptes contreviennent à une stratégie organisationnelle;
5. des risques importants liés à des personnes sont découverts.

G. Aviser les gestionnaires de compte et le personnel ou les rôles désignés dans :

1. [Affectation : période définie par l'organisation] lorsque les comptes ne sont plus requis;
2. [Affectation : période définie par l'organisation] lorsque les utilisatrices et utilisateurs quittent leur emploi ou sont transférés;
3. [Affectation : période définie par l'organisation] lorsque l'utilisation du système ou le besoin de connaître d'une personne change.

H. Exiger que les utilisatrices et utilisateurs se déconnectent du système après [Affectation : période définie par l'organisation] d'inactivité ou lors de [Affectation : circonstances définies par l'organisation].

Discussion

La présente exigence s'applique à la gestion des comptes pour les systèmes et les applications. La définition et l'application des autorisations d'accès, autres que celles déterminées par le type de compte (par exemple, les accès privilégiés ou non privilégiés) sont énoncées dans l'exigence Application de l'accès 03.01.02. Les types de comptes incluent les comptes individuels, les comptes de groupe, les comptes temporaires, les comptes système, les comptes d'invité, les comptes anonymes, les comptes d'urgence, les comptes de développeur et les comptes de service. Les utilisatrices et utilisateurs nécessitant des privilèges administratifs pour les comptes système font l'objet d'un examen plus approfondi de la part des responsables appropriées et appropriés de l'organisation chargés d'approuver ces comptes et les accès privilégiés. Les types de comptes que les organisations peuvent interdire en raison d'un risque de sécurité accru incluent les comptes de groupe, d'urgence, d'invité, anonymes et temporaires.

Les organisations peuvent choisir de définir les privilèges d'accès ou d'autres attributs en fonction du compte, du type de compte ou d'une combinaison des deux. Les autres attributs requis pour autoriser l'accès incluent les restrictions en fonction du moment de la journée, du jour de la semaine et du point d'origine. Lors de la définition des autres attributs de compte, les organisations doivent considérer les exigences système (par exemple, les mises à niveau du système et la maintenance planifiée) et les exigences ayant trait à la mission et aux activités (par exemple, les différences de fuseau horaire et l'accès à distance pour faciliter les déplacements).

Les utilisatrices et utilisateurs qui présentent un risque important pour la sécurité et/ou l'atteinte à la vie privée comprennent les personnes pour lesquelles des preuves fiables indiquent l'intention d'utiliser un accès autorisé au système afin de causer des dommages ou de permettre à des adversaires de causer des dommages par leur entremise. Une collaboration étroite entre les gestionnaires des ressources humaines, les responsables de la mission ou des activités, les administratrices et administrateurs de système et le personnel juridique est essentielle à la désactivation des comptes système des personnes présentant un risque élevé. Les délais pour aviser le personnel ou les rôles désignés de l'organisation peuvent varier.

La fermeture de session en cas d'inactivité peut être basée sur des comportements ou sur des stratégies, et nécessite que les utilisatrices et utilisateurs effectuent une opération physique afin de fermer leur session s'ils prévoient d'être inactifs sur le système pendant une période dépassant la période définie. L'application automatique de la fermeture de session en cas d'inactivité est abordée dans l'exigence Verrouillage d'appareil 03.01.10.

Références

Sources des contrôles : AC-02, AC-02(03), AC-02(05) et AC-02(13)
Publications connexes :

- Centre pour la cybersécurité, *Gestion et contrôle des privilèges administratifs* (ITSAP.10.094)
- Centre pour la cybersécurité, *Comment protéger votre organisation contre les menaces internes* (ITSAP.10.003)

03.01.02 Application de l'accès

Appliquer les autorisations approuvées pour l'accès logique à l'information désignée et aux ressources système conformément aux stratégies de contrôle d'accès applicables.

Discussion

Les stratégies de contrôle d'accès contrôlent l'accès entre des entités ou sujets actifs (c'est-à-dire les utilisatrices et utilisateurs ou les processus système agissant au nom des utilisatrices et utilisateurs) et des entités ou objets passifs (comme les dispositifs, les fichiers, les documents et les domaines) dans les systèmes organisationnels. Les types d'accès au système incluent l'accès distant et l'accès aux systèmes qui communiquent à l'aide de réseaux externes, comme Internet. Les mécanismes d'application de l'accès peuvent également être utilisés au niveau des applications et des services afin de fournir une meilleure protection de l'information désignée. Ces mécanismes permettent de reconnaître que les systèmes peuvent héberger de nombreuses applications et de nombreux services

afin d'appuyer la mission et les activités. Les stratégies de contrôle d'accès sont définies dans l'exigence Stratégie et procédures 03.15.01.

Références

Source du contrôle : AC-03
Publications connexes : Centre pour la cybersécurité, *Gestion et contrôle des privilèges administratifs* (ITSAP.10.094)

03.01.03 Application du contrôle de flux d'information

Appliquer des autorisations approuvées pour contrôler le flux de l'information désignée dans le système et entre les systèmes interconnectés.

Discussion

Le contrôle de flux d'information détermine où l'information désignée peut transiter au sein d'un système et entre des systèmes (par opposition aux personnes autorisées à accéder à l'information), quels que soient les accès subséquents à cette information. Les restrictions de contrôle de flux comprennent notamment : empêcher la transmission de l'information désignée en clair sur Internet, bloquer le trafic entrant qui prétend provenir de l'intérieur de l'organisation, restreindre les demandes d'accès à Internet qui ne proviennent pas du serveur mandataire Web interne et limiter le transfert de l'information désignée entre les organisations en fonction des structures de données et du contenu.

Les organisations utilisent souvent des stratégies de contrôle de flux d'information et des mécanismes d'application pour contrôler le flux de l'information désignée entre des sources et des destinations données (par exemple, des réseaux, des personnes et des dispositifs) dans des systèmes et entre des systèmes interconnectés. Le contrôle de flux est basé sur les caractéristiques de l'information ou sur le chemin d'accès de l'information. Le contrôle de flux s'applique aux dispositifs de protection de périmètre (par exemple, tunnels chiffrés, routeurs, passerelles et pare-feu) qui ont recours à des ensembles de règles ou qui établissent des paramètres de configuration pour restreindre les services d'un système, pour fournir des capacités de filtrage des paquets selon les données d'en-tête ou pour fournir des capacités de filtrage des messages en fonction du contenu du message (par exemple, mise en œuvre des recherches par mots-clés ou utilisation des caractéristiques du document). Les organisations doivent également considérer la fiabilité des mécanismes de filtrage et d'inspection (c'est-à-dire les composants matériels, micrologiciels et logiciels) qui sont essentiels à l'application du contrôle de flux d'information.

Le transfert de l'information désignée entre des organisations peut nécessiter une entente indiquant comment le flux d'information sera appliqué (voir l'exigence Échange d'information 03.12.05). Le transfert de l'information désignée entre des systèmes associés à des domaines de sécurité différents et à des stratégies de sécurité différentes comporte un risque de contravention à une ou à plusieurs stratégies de sécurité des domaines. Dans de telles situations, les dépositaires de l'information doivent fournir des directives aux points désignés d'application des stratégies entre les systèmes interconnectés. Les organisations doivent examiner la possibilité d'imposer des solutions architecturales particulières lorsqu'elles appliquent des stratégies de sécurité précises. Ces solutions peuvent comprendre l'interdiction de transférer de l'information désignée entre des systèmes interconnectés (c'est-à-dire autoriser seulement l'accès à l'information), l'utilisation de mécanismes matériels pour appliquer un flux d'information unidirectionnel et la mise en œuvre de mécanismes remaniés de confiance pour réassigner les attributs et étiquettes de sécurité.

Références

Source du contrôle : AC-04
Publications connexes :

- Centre pour la cybersécurité, *Exigences de base en matière de sécurité pour les zones de sécurité de réseau* (ITSP.80.022)

- Centre pour la cybersécurité, *Nettoyage des supports de TI* (ITSP.40.006)

03.01.04 Séparation des tâches

A. Établir les tâches des personnes devant être séparées.

B. Définir les autorisations d'accès au système afin d'appuyer la séparation des tâches.

Discussion

La séparation des tâches permet d'éliminer l'abus possible des privilèges autorisés et réduit le risque d'activités malveillantes sans collusion. Les mécanismes de séparation des tâches comprennent notamment : la division des fonctions liées à la mission et des fonctions de soutien entre les personnes ou rôles, l'exécution de fonctions de soutien liées au système par différentes personnes ou différents rôles (par exemple, l'assurance de la qualité, la gestion de la configuration, la gestion du système, les évaluations, la programmation et la sécurité réseau) et l'assurance que le personnel qui administre les fonctions de contrôle d'accès n'administre pas également les fonctions de vérification. Puisque les violations de séparation des tâches peuvent s'étendre sur plusieurs systèmes et domaines d'application, les organisations doivent prendre en considération l'ensemble de leurs systèmes et de leurs composants de systèmes lors de l'élaboration des stratégies sur la séparation des tâches. Cette exigence est appliquée par l'exigence Application de l'accès 03.01.02.

Références

Source du contrôle : AC-05
Publications connexes :

- *NIST SP 800-162 Guide to Attribute Based Access Control (ABAC) Definition and Considerations* (en anglais seulement)
- *NIST SP 800-178 A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications: Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC)* (en anglais seulement)

03.01.05 Droit d'accès minimal

A. Permettre uniquement les accès autorisés au système pour les utilisatrices et utilisateurs (ou les processus exécutés en leur nom) qui sont nécessaires pour accomplir les tâches organisationnelles assignées.

B. Autoriser l'accès aux [Affectation : fonctions de sécurité définies par l'organisation] et à [Affectation : information liée à la sécurité définie par l'organisation].

C. Examiner les privilèges attribués aux rôles ou aux classes d'utilisateur tous les [Affectation : fréquence définie par l'organisation] afin de valider la nécessité de détenir ces privilèges.

D. Réattribuer ou retirer les privilèges, au besoin.

Discussion

Les organisations doivent avoir recours au principe de droit d'accès minimal pour des tâches précises et les accès autorisés pour les utilisatrices et utilisateurs et les processus système. Le principe de droit d'accès minimal s'applique au développement, à la mise en œuvre et à l'exploitation du système. Les organisations doivent envisager de créer des processus, des rôles et des comptes système supplémentaires afin de répondre à ce principe. Les fonctions de sécurité comprennent notamment l'établissement de comptes système, l'attribution de privilèges, l'installation de logiciels, la configuration des autorisations d'accès, la configuration des paramètres pour les événements qui seront vérifiés, l'établissement des paramètres d'analyse des vulnérabilités, l'établissement des paramètres de détection d'intrusion et la gestion de l'information de vérification. L'information liée à la sécurité comprend notamment l'information sur les menaces et les vulnérabilités, les règles de filtrage pour les routeurs et

les pare-feu, les paramètres de configuration pour les services de sécurité, l'architecture de sécurité, l'information de gestion des clés cryptographiques, les listes de contrôle d'accès et l'information de vérification.

Références

Sources des contrôles : AC-06, AC-06(01), AC-06(07) et AU-09(04)
Publications connexes : Aucune

03.01.06 Droit d'accès minimal – Comptes privilégiés

A. Restreindre les comptes privilégiés sur le système à [Affectation : personnel ou rôles définis par l'organisation].

B. Exiger que les utilisatrices et utilisateurs (ou les rôles) associés à des comptes privilégiés utilisent des comptes non privilégiés lorsqu'ils accèdent à des fonctions ou à de l'information qui ne sont pas liées à la sécurité.

C. Exiger que les opérations d'administration ou de superutilisateur soient réalisées à partir d'un poste de travail physique dédié à ces tâches précises et isolées des autres fonctions et réseaux. En particulier, la station ne devrait pas avoir accès à Internet.

Discussion

Les comptes privilégiés désignent les comptes associés à des privilèges élevés pour accéder à des ressources (y compris les fonctions de sécurité ou l'information liée à la sécurité) qui sont autrement restreintes pour les comptes non privilégiés. Les comptes privilégiés sont normalement décrits comme des comptes d'administrateur de système ou des comptes de surpeutilisateur. Par exemple, un compte privilégié est souvent requis pour réaliser des fonctions privilégiées, comme l'exécution de commandes pouvant modifier le comportement du système. La restriction des comptes privilégiés au personnel ou aux rôles désignés permet d'empêcher que des utilisatrices et utilisateurs non privilégiés accèdent à des fonctions de sécurité ou à de l'information liée à la sécurité. L'exigence d'utiliser des comptes non privilégiés pour accéder à des fonctions ou à de l'information qui ne sont pas liées à la sécurité limite l'exposition lors de l'utilisation de comptes privilégiés.

Un poste de travail administratif dédié est typiquement constitué d'un terminal d'utilisateur et d'une très petite sélection de logiciels conçus pour interfacer avec le système cible. Aux fins du présent contrôle, un poste de travail est considéré comme étant le système à partir duquel les tâches d'administration sont réalisées, par opposition au système cible.

Références

Sources des contrôles : AC-06(02), AC-06(05) et SI-400
Publications connexes : Aucune

03.01.07 Droit d'accès minimal – Fonctions privilégiées

A. Empêcher les utilisatrices et utilisateurs non privilégiés d'exécuter des fonctions privilégiées.

B. Journaliser l'exécution de fonctions privilégiées.

Discussion

Les fonctions privilégiées comprennent notamment l'établissement de comptes système, les vérifications de l'intégrité du système, l'application de correctifs et les activités de gestion des clés cryptographiques. Les utilisatrices et utilisateurs non privilégiés ne détiennent pas les autorisations nécessaires pour exécuter les fonctions privilégiées. Le contournement des mécanismes de détection et de prévention d'intrusion et les mécanismes de protection contre les programmes malveillants sont des exemples de fonctions privilégiées qui ne doivent pas être exécutées par des utilisatrices et utilisateurs non privilégiés. Cette exigence représente une condition devant être respectée en vertu de la définition des privilèges autorisés de l'exigence Gestion des comptes 03.01.01 et de l'application des privilèges de l'exigence Application de l'accès 03.01.02.

Une mauvaise utilisation des fonctions privilégiées, qu'elle soit intentionnelle ou non, par des utilisatrices et utilisateurs autorisés ou par des entités externes non autorisées ayant compromis des comptes système est une préoccupation constante et sérieuse qui peut avoir des répercussions négatives importantes sur les organisations. La journalisation de l'utilisation des fonctions privilégiées est une méthode permettant de détecter les mauvaises utilisations et d'atténuer les risques liés aux menaces persistantes avancées et aux menaces internes.

Références

Sources des contrôles : AC-06(09) et AC-06(10)
Publications connexes : Aucune

03.01.08 Tentatives d'ouverture de session infructueuses

A. Limiter le nombre de tentatives d'ouverture de session infructueuses à [Affectation : nombre défini par l'organisation] en moins de [Affectation : période définie par l'organisation].

B. [Sélection (un ou plusieurs) : Verrouiller le compte ou le nœud pendant [Affectation : période définie par l'organisation]; verrouiller le compte ou le nœud jusqu'à ce qu'une administratrice ou un administrateur le libère; retarder la prochaine invite d'ouverture de session; aviser l'administratrice ou administrateur de système; effectuer une autre opération] automatiquement lorsque le nombre maximal de tentatives infructueuses est dépassé.

Discussion

En raison des possibilités de déni de service, le verrouillage automatique du système est, dans la plupart des cas, temporaire et un rétablissement automatique survient normalement après une période prédéterminée établie par l'organisation (c'est-à-dire au moyen d'un algorithme de temporisation). Les organisations peuvent avoir recours à différents algorithmes de temporisation pour différents composants du système en fonction des capacités des composants respectifs. Les réponses aux tentatives d'ouverture de session système infructueuses peuvent être mises en œuvre au niveau du système ou de l'application.

Les opérations définies par l'organisation qui peuvent être effectuées comprennent notamment l'affichage d'un message invitant l'utilisatrice ou utilisateur à répondre à une question secrète en plus d'entrer son nom d'utilisateur et son mot de passe, l'utilisation d'un mode de confinement avec des capacités limitées pour les utilisatrices et utilisateurs (plutôt qu'un verrouillage complet), permettre aux utilisatrices et utilisateurs de se connecter uniquement à partir de certaines adresses de protocole Internet (IP pour *Internet Protocol*) précises, l'utilisation d'un test captcha pour éviter les attaques automatisées ou l'application de profils d'utilisateur qui font intervenir d'autres paramètres, comme l'emplacement, le moment de la journée, l'adresse IP, l'appareil ou l'adresse de contrôle d'accès au support (MAC pour *Media Access Control*).

Références

Source du contrôle : AC-07
Publications connexes :

- Centre pour la cybersécurité, *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information* (ITSP.30.031)
- *NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise* (en anglais seulement)

03.01.09 Avis d'utilisation système

Afficher un message d'avis d'utilisation du système qui comprend des énoncés de confidentialité et de sécurité qui sont conformes aux règles liées à l'information désignée applicables, avant d'accorder l'accès au système.

Discussion

Les avis concernant l'utilisation du système peuvent être mis en œuvre au moyen de messages d'avertissement ou de bannières. Ces messages sont affichés avant que les personnes se connectent au système. Les avis d'utilisation système sont utilisés lors de l'accès au moyen d'interfaces d'ouverture de session avec utilisatrices et utilisateurs humains et ne sont pas requis lorsque de telles interfaces n'existent pas. Les organisations doivent déterminer si un avis d'utilisation secondaire est nécessaire pour accéder à des applications ou à d'autres ressources système après la connexion initiale au réseau. Des affiches ou d'autres documents imprimés peuvent également être utilisés au lieu d'un message système automatisé. Cette exigence est associée à l'exigence Règles de conduite 03.15.03.

Références

Source du contrôle : AC-08
Publications connexes : Aucune

03.01.10 Verrouillage d'appareil

A. Empêcher l'accès au système [Sélection (un ou plusieurs) : en procédant à un verrouillage d'appareil après [Affectation : période définie par l'organisation] d'inactivité; en exigeant que l'utilisatrice ou utilisateur procède à un verrouillage d'appareil avant de laisser le système sans surveillance].

B. Préserver le verrouillage d'appareil jusqu'à ce que l'utilisatrice ou utilisateur rétablisse l'accès au moyen des procédures d'identification et d'authentification établies.

C. Masquer, au moyen d'un verrouillage d'appareil, l'information auparavant visible à l'écran en utilisant une image visible.

Discussion

Les verrouillages d'appareil sont des mesures temporaires servant à empêcher l'accès au système lorsque les utilisatrices et utilisateurs ne se trouvent pas à proximité du système et qu'ils préfèrent ne pas se déconnecter en raison de la nature temporaire de leur absence. Le verrouillage peut être mis en œuvre au niveau du système d'exploitation ou de l'application. Le verrouillage d'appareil est initié par l'utilisatrice ou utilisateur. Il peut s'agir d'une opération basée sur des comportements ou des stratégies et nécessite que l'utilisatrice ou utilisateur effectue une opération physique pour verrouiller son appareil. Les verrouillages d'appareil ne remplacent pas la fermeture de session sur le système (par exemple, l'organisation peut exiger que les utilisatrices et utilisateurs ferment leur session à la fin de leur journée de travail). Les images visibles peuvent inclure des images statiques ou dynamiques, comme celles générées par les économiseurs d'écran, des photographies, des couleurs solides, une horloge, un indicateur de la charge de la pile ou un écran vide, ce qui assure que l'information désignée n'est pas affichée.

Références

Sources des contrôles : AC-11 et AC-11(01)

Publications connexes : Aucune

03.01.11 Fin de session

Mettre automatiquement fin à une session utilisateur après [Affectation : conditions ou événements déclenchant une déconnexion définis par l'organisation].

Discussion

Cette exigence concerne la fin d'une session logique initiée par l'utilisatrice ou utilisateur, par opposition à la fin d'une connexion réseau qui est associée à une session de communication (c'est-à-dire une déconnexion réseau) présentée dans l'exigence Déconnexion réseau 03.13.09. Une session logique est lancée chaque fois qu'une

utilisatrice ou un utilisateur (ou un processus exécuté en son nom) accède à un système. Il est possible de mettre fin aux sessions logiques (ce qui met fin à l'accès de l'utilisatrice ou utilisateur) sans mettre fin aux sessions réseau. La fin d'une session arrête tous les processus système associés à une session logique d'utilisateur, à l'exception des processus qui ont été créés par l'utilisatrice ou utilisateur (c'est-à-dire la ou le responsable de la session) et qui sont destinés à se poursuivre lorsque la session est terminée. Les conditions ou les événements déclenchant la fin automatique d'une session peuvent inclure les périodes d'inactivité de l'utilisateur définies par l'organisation, des restrictions liées au moment de la journée pour l'utilisation du système et des réponses ciblées à certains types d'incidents.

Références

Source du contrôle : AC-12
Publications connexes : Aucune

03.01.12 Accès à distance

A. Établir les restrictions d'utilisation ainsi que les exigences en matière de configuration et de connexion pour chaque type d'accès distant au système pouvant être autorisé.

B. Autoriser chaque type d'accès distant au système avant d'établir une telle connexion.

C. Acheminer l'accès distant au système au moyen de points de contrôle d'accès autorisés et gérés.

D. Autoriser l'exécution distante des commandes privilégiées et les accès distants à l'information liée à la sécurité.

Discussion

Un accès à distance (ou accès distant) est l'accès des utilisatrices et utilisateurs (ou des processus exécutés en leur nom) aux systèmes au moyen de réseaux externes, comme Internet. Les méthodes de surveillance et de contrôle d'accès à distance permettent aux organisations de détecter les attaques et d'assurer la conformité aux stratégies d'accès à distance. L'acheminement de l'accès distant au moyen de points de contrôle d'accès gérés améliore le contrôle explicite de telles connexions et réduit la probabilité d'accès non autorisé au système, ce qui réduit également la probabilité de divulgation non autorisée de l'information désignée.

L'accès distant à un système représente une vulnérabilité potentielle importante pouvant être exploitée par des adversaires. La restriction des commandes et des accès privilégiés à l'information liée à la sécurité au moyen d'un accès à distance réduit l'exposition des organisations et leur vulnérabilité aux menaces provenant des adversaires. Une commande privilégiée est une commande lancée par un humain et exécutée sur un système impliquant le contrôle, la surveillance ou l'administration du système, y compris les fonctions de sécurité ou l'information liée à la sécurité. L'information liée à la sécurité constitue de l'information susceptible d'influer sur l'exécution des fonctions de sécurité ou la prestation des services de sécurité, de telle façon qu'elle nuirait à l'application des stratégies de sécurité du système ou à l'isolation du code et des données. Les commandes privilégiées permettent aux personnes d'exécuter des fonctions sensibles, essentielles à la sécurité ou liées à la sécurité du système.

Références

Sources des contrôles : AC-17, AC-17(03) et AC-17(04)
Publications connexes :

- *NIST SP 800-46 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (en anglais seulement)
- *NIST SP 800-77 Guide to IPsec VPNs* (en anglais seulement)
- *NIST SP 800-113 Guide to SSL VPNs* (en anglais seulement)
- *NIST SP 800-114 User's Guide to Telework and Bring Your Own Device (BYOD) Security* (en anglais

seulement)
- *NIST SP 800-121 Guide to Bluetooth Security* (en anglais seulement)

03.01.13 Non affecté

Retiré par le NIST.

03.01.14 Non affecté

Retiré par le NIST.

03.01.15 Non affecté

Retiré par le NIST.

03.01.16 Accès sans fil

A. Établir les restrictions d'utilisation ainsi que les exigences en matière de configuration et de connexion pour chaque type d'accès sans fil au système.

B. Autoriser chaque type d'accès sans fil au système avant d'autoriser de telles connexions.

C. Désactiver, lorsqu'on ne prévoit pas les utiliser, les capacités de réseautage sans fil avant leur remise et leur déploiement.

D. Protéger l'accès sans fil au système au moyen de mécanismes d'authentification et de chiffrement.

Discussion

Les capacités de réseau sans fil représentent une vulnérabilité potentielle importante pouvant être exploitée par des adversaires. L'établissement de restrictions d'utilisation ainsi que les exigences en matière de configuration et de connexion pour l'accès sans fil au système offrent des critères permettant d'appuyer les décisions d'autorisation d'accès. Ces restrictions et exigences réduisent la possibilité des accès système non autorisés par des technologies sans fil. Les réseaux sans fil utilisent des protocoles d'authentification afin de fournir une protection au moyen de justificatifs d'identité et d'une authentification mutuelle. Les organisations authentifient les personnes et les dispositifs afin de protéger les accès sans fil au système. Une attention particulière doit être accordée à la variété des appareils dotés d'un accès sans fil au système, y compris les appareils mobiles de petite taille (par exemple, les téléphones intelligents, les tablettes et les montres intelligentes). Les capacités de réseau sans fil intégrées aux composants de systèmes représentent une vulnérabilité potentielle importante pouvant être exploitée par des adversaires. Un mécanisme rigoureux d'authentification des utilisatrices et utilisateurs et des appareils, un chiffrement robuste et la désactivation des capacités sans fil non nécessaires à la mission ou aux activités peuvent réduire sensiblement les menaces que font peser les adversaires exploitant des technologies sans fil.

Références

Sources des contrôles : AC-18, AC-18(01) et AC-18(03)
Publications connexes :
- Centre pour la cybersécurité, *Exigences de sécurité liées aux réseaux locaux sans fil* (ITSG-41)
- Centre pour la cybersécurité, *Conseils sur la configuration sécurisée des protocoles réseau* (ITSP.40.062)
- *NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)* (en anglais seulement)
- *NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise* (en anglais seulement)

03.01.17 Non affecté

Retiré par le NIST.

03.01.18 Contrôle d'accès pour les appareils mobiles

A. Établir des restrictions d'utilisation ainsi que les exigences en matière de configuration et de connexion pour les appareils mobiles.

B. Autoriser les connexions d'appareil mobile au système.

C. Mettre en œuvre un chiffrement complet des appareils ou un chiffrement des contenants afin de protéger la confidentialité de l'information désignée sur les appareils mobiles.

Discussion

Un appareil mobile est un dispositif informatique de petite taille qui peut facilement être transporté par une personne. Il est conçu pour fonctionner sans connexion physique, il dispose d'un stockage de données local, fixe ou amovible. Il comprend également une source d'alimentation autonome. Les fonctionnalités des appareils mobiles peuvent également comprendre des capacités de communication vocale, des capteurs embarqués permettant aux appareils de recueillir des données et/ou des fonctions intégrées de synchronisation de données locales avec des emplacements distants. Les téléphones intelligents, les montres intelligentes et les tablettes sont des exemples d'appareils mobiles. Les appareils mobiles sont typiquement associés à une seule personne. Les capacités de traitement, de stockage et de transmission des appareils mobiles peuvent être comparables à un sous-ensemble d'ordinateurs blocs-notes ou d'ordinateurs de bureau, selon la nature et l'utilisation prévue de l'appareil. La protection et le contrôle des appareils mobiles sont basés sur les comportements et les stratégies et nécessitent que les utilisatrices et utilisateurs effectuent des opérations physiques afin de protéger et de contrôler leurs appareils lorsqu'ils se trouvent à l'extérieur des zones contrôlées. Les zones contrôlées sont des espaces dans lesquels les organisations fournissent des contrôles physiques ou procéduraux afin de respecter les exigences établies pour la protection de l'information désignée.

En raison de la grande variété d'appareils mobiles, y compris leur vaste gamme de caractéristiques et de capacités, les restrictions organisationnelles peuvent varier en fonction des classes ou des types d'appareils. Les restrictions d'utilisation ainsi que les exigences en matière de configuration et de connexion imposées aux appareils mobiles comprennent notamment la gestion de la configuration, l'identification et l'authentification des appareils, la mise en œuvre obligatoire de logiciels de protection, l'analyse des appareils afin de détecter les programmes malveillants, la mise à jour des logiciels antivirus, la recherche des mises à jour et des correctifs critiques, la vérification de l'intégrité du système d'exploitation de base et possiblement d'autres logiciels, et la désactivation du matériel qui n'est pas nécessaire. Sur les appareils mobiles, des contenants sécurisés offrent une isolation logicielle des données destinée à segmenter les applications et données organisationnelles, et les applications et données personnelles. Des contenants peuvent présenter différentes interfaces utilisateur, l'une des plus courantes étant une application mobile agissant à titre de portail vers une suite d'applications de productivité des activités, comme le courriel, les contacts et le calendrier. Les organisations peuvent utiliser un chiffrement complet des appareils ou un chiffrement des contenants afin de protéger la confidentialité de l'information désignée sur les appareils mobiles.

Références

Sources des contrôles : AC-19 et AC-19(05)
Publications connexes :

- *NIST SP 800-46 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (en anglais seulement)
- *NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise* (en anglais seulement)

- *NIST SP 800-114 User's Guide to Telework and Bring Your Own Device (BYOD) Security* (en anglais seulement)

03.01.19 Non affecté

Retiré par le NIST.

03.01.20 Utilisation de systèmes externes

A. Empêcher l'utilisation de systèmes externes, sauf si ceux-ci sont explicitement autorisés.

B. Établir les modalités, les conditions et les exigences de sécurité suivantes, que les systèmes externes doivent satisfaire avant de permettre aux personnes autorisées de les utiliser ou d'y accéder : [Affectation : exigences de sécurité définies par l'organisation]

C. Permettre aux personnes autorisées d'utiliser un système externe afin d'accéder au système de l'organisation ou afin de traiter, de stocker ou de transmettre de l'information désignée seulement après les opérations suivantes :

   1. vérifier la satisfaction des exigences de sécurité du système externe, telles qu'elles sont énoncées dans les plans de sécurité et de confidentialité du système de l'organisation;

   2. conserver les ententes approuvées de connexion au système ou de traitement avec les entités organisationnelles qui hébergent les systèmes externes.

D. Restreindre l'utilisation de dispositifs de stockage portatifs contrôlés par l'organisation aux personnes autorisées pour les systèmes externes.

Discussion

Les systèmes externes sont des systèmes qui sont utilisés par l'organisation, mais qui ne font pas partie de celle-ci. Ces systèmes comprennent notamment les systèmes, les composants de systèmes ou les dispositifs personnels; les dispositifs de traitement et de communication appartenant à une entreprise privée dans des installations commerciales ou publiques; les systèmes détenus ou contrôlés par des organisations non fédérales; et les systèmes gérés par des entrepreneurs. Les organisations ont l'option d'interdire l'utilisation de tous les types de systèmes externes ou de certains types de systèmes externes (par exemple, interdire l'utilisation de systèmes externes qui n'appartiennent pas à l'organisation). Les conditions générales doivent être conformes aux relations de confiance établies avec les entités qui possèdent, utilisent ou maintiennent les systèmes externes, et doivent comprendre une description des responsabilités partagées.

Les personnes autorisées comprennent notamment le personnel de l'organisation, les entrepreneures et entrepreneurs ou toute autre personne autorisée à accéder au système organisationnel et à qui l'organisation est en droit d'imposer des règles de conduite précises concernant l'accès au système. Les restrictions que les organisations peuvent imposer aux personnes autorisées peuvent dépendre des relations de confiance entre l'organisation et les entités externes. Les organisations doivent avoir l'assurance que les systèmes externes satisfont aux exigences de sécurité afin qu'ils ne compromettent pas ou n'endommagent pas le système de l'organisation, ou encore qu'ils ne nuisent pas au système. Cette exigence est associée à l'exigence Services de systèmes externes 03.16.03.

Références

Sources des contrôles : AC-20, AC-20(01) et AC-20(02)
Publications connexes : Aucune

03.01.21 Non affecté

Retiré par le NIST.

03.01.22 Contenu à accès public

A. Former les personnes autorisées afin de s'assurer que l'information accessible au public ne contient aucune information désignée.

B. Vérifier périodiquement le contenu des systèmes à accès public afin de s'assurer qu'il ne contient aucune information désignée et retirer une telle information, le cas échéant.

Discussion

Conformément aux lois, aux décrets, aux directives, aux politiques, à la réglementation, aux normes et aux lignes directrices applicables, le grand public n'est pas autorisé à accéder à de l'information non publique, y compris l'information désignée.

Références

Source du contrôle : AC-22
Publications connexes : Aucune

3.2 Sensibilisation et formation

Les contrôles de sensibilisation et de formation concernent la sensibilisation des utilisatrices et utilisateurs à la sécurité du système.

03.02.01 Formation et sensibilisation en matière de sécurité

A. Fournir de la formation sur la sécurité et la protection de la vie privée aux utilisatrices et utilisateurs système :

1. dans le cadre d'une formation de base pour les nouvelles utilisatrices et nouveaux utilisateurs, et tous les [Affectation : fréquence définie par l'organisation] par la suite;
2. lors de changements apportés au système ou à la suite de [Affectation : événements définis par l'organisation];
3. pour reconnaître et signaler les indicateurs de menace interne, de piratage psychologique et de l'exploration de données dans les médias sociaux.

B. Mettre à jour le contenu de formation en matière de sécurité et de protection de la vie privée tous les [Affectation : fréquence définie par l'organisation] et à la suite de [Affectation : événements définis par l'organisation].

Discussion

Les organisations doivent fournir de la formation de base et avancée en matière de sécurité et confidentialité aux utilisatrices et utilisateurs du système (y compris les gestionnaires, la haute direction, les administratrices et administrateurs de système et les entrepreneures et entrepreneurs) ainsi que des mesures pour tester les connaissances des utilisatrices et utilisateurs. Les organisations doivent établir le contenu de la formation en fonction de leurs exigences organisationnelles particulières, des systèmes auxquels le personnel a accès et des environnements de travail (par exemple, le télétravail). Le contenu devrait comprendre une présentation des besoins de sécurité et les mesures que doivent prendre les utilisatrices et utilisateurs afin de maintenir la sécurité et d'intervenir en cas d'incident. Le contenu devrait inclure les mesures nécessaires en matière de sécurité opérationnelle et de traitement de l'information désignée.

Les techniques de sensibilisation à la sécurité et à la protection de la vie privée comprennent des affiches, des objets affichant des rappels de sécurité, des messages au moment de la connexion, des avis envoyés par courriel ou de la part des responsables de l'organisation et des événements de sensibilisation au moyen de balados, de vidéos ou de webinaires. La formation sur la sécurité et la protection de la vie privée doit être menée à une fréquence conforme aux lois, aux directives, à la réglementation et aux politiques applicables. La mise à jour périodique du contenu de formation permet de s'assurer que le contenu reste pertinent. Les événements qui peuvent précipiter une mise à jour du contenu de la formation comprennent les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des chargements apportés aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables.

Les indicateurs potentiels et les possibles signes précurseurs de menace interne peuvent comprendre des comportements comme les suivants : des comportements excessifs, de l'insatisfaction de longue durée liée au travail, des tentatives d'accès à de l'information qui n'est pas nécessaire pour la réalisation du travail, un accès inexpliqué à des ressources financières, de l'intimidation ou du harcèlement sexuel envers des collègues, de la violence en milieu de travail et d'autres manquements graves aux politiques, aux procédures, aux règles, aux directives ou aux pratiques de l'organisation. Les organisations peuvent adapter le sujet de la sensibilisation aux menaces internes en fonction du rôle (par exemple, la formation des gestionnaires peut se concentrer sur les changements particuliers dans les comportements des membres de l'équipe, alors que la formation des employées et employés peut porter sur des observations plus générales).

Le piratage psychologique vise à tromper une personne pour l'inciter à révéler de l'information ou à faire une opération pouvant servir à s'introduire dans un système, à le compromettre ou à nuire à un système. Le piratage psychologique comprend l'hameçonnage, le faux-semblant, l'usurpation d'identité, l'appâtage, l'arnaque de la contrepartie, le détournement de chaînes de courriels, l'exploitation des médias sociaux et le talonnage. L'exploration de données dans les médias sociaux vise à recueillir de l'information à propos de l'organisation qui pourrait servir à appuyer des attaques à venir. La formation en matière de sécurité et de protection de la vie privée porte notamment sur la façon dont les membres du personnel et de la direction peuvent communiquer leurs préoccupations concernant des indicateurs potentiels de menace interne et des instances réelles et potentielles de piratage psychologique et d'exploration de données, au moyen des voies de communication appropriées de l'organisation, conformément aux stratégies et aux procédures établies.

Références

Sources des contrôles : AT-02, AT-02(02) et AT-02(03)
Publications connexes :

- Centre pour la cybersécurité, *Offrir aux employés une formation sur mesure en cybersécurité* (ITSAP.10.093)
- *NIST SP 800-160-2 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach* (en anglais seulement)

03.02.02 Formation selon le rôle

A. Fournir de la formation sur la sécurité et la confidentialité au personnel de l'organisation selon le rôle :

   1. avant d'autoriser l'accès au système ou à de l'information désignée, avant la réalisation des tâches attribuées et tous les [Affectation : fréquence définie par l'organisation] par la suite;

   2. lors de changements apportés au système ou à la suite de [Affectation : événements définis par l'organisation];

B. Mettre à jour le contenu de la formation offerte selon le rôle tous les [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation].

Discussion

Les organisations doivent déterminer le contenu et la fréquence des formations relatives à la sécurité et à la

confidentialité en fonction des tâches, des rôles et des responsabilités des personnes ainsi que des exigences en matière de sécurité et de confidentialité des systèmes auxquels le personnel autorisé peut accéder. De plus, les organisations doivent fournir une formation technique sur la sécurité adaptée à chacun des rôles suivants : développeuses et développeurs de système, architectes d'entreprise, architectes de la sécurité, agentes et agents de protection de la vie privée, développeuses et développeurs de logiciels, intégratrices et intégrateurs de systèmes, responsables de l'acquisition et de l'approvisionnement, administratrices et administrateurs de système et de réseau, personnel responsable des activités de gestion de la configuration et de vérification, personnel réalisant des vérifications et des validations indépendantes, évaluatrices et évaluateurs de la sécurité et personnel doté d'un accès logiciel de niveau système.

Une formation complète axée sur les rôles permet de tenir compte des rôles et responsabilités gestionnels, opérationnels et techniques et présente des contrôles physiques, techniques et s'appliquant au personnel. Une telle formation peut porter sur les stratégies, les procédures, les outils et les artéfacts qui sont adaptés aux rôles de sécurité et de confidentialité. Dans le cadre de leur programme de sécurité de l'information, les organisations doivent également fournir la formation nécessaire afin que les personnes puissent s'acquitter de leurs responsabilités en matière de sécurité des opérations et de la chaîne d'approvisionnement.

Références

Source du contrôle : AT-03
Publications connexes :

- *NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (en anglais seulement)
- *NIST SP 800-181 Workforce Framework for Cybersecurity (NICE Framework)* (en anglais seulement)

03.02.03 Non affecté

Retiré par le NIST.

3.3 Vérification et responsabilisation

Les contrôles de vérification et de responsabilisation permettent de recueillir, d'analyser et de stocker les enregistrements de vérification associés aux opérations des utilisatrices et utilisateurs réalisées sur le système.

03.03.01 Journalisation d'événements

A. Préciser les types d'événements suivants qui sont sélectionnés pour la journalisation dans le système : [Affectations : types d'événements définis par l'organisation].

B. Vérifier et mettre à jour les types d'événements sélectionnés pour la journalisation tous les [Affectation : fréquence définie par l'organisation].

Discussion

Un événement est une occurrence observable dans un système, y compris toute activité système illicite ou non autorisée. Les organisations doivent établir les types d'événements pour lesquels la fonctionnalité de journalisation est requise, notamment les événements qui sont liés à la sécurité des systèmes, à la protection de la vie privée des individus et aux environnements dans lesquels ces systèmes sont exploités, afin de répondre à des besoins précis et continus en matière de vérification. Les types d'événements peuvent comprendre les changements de mot de passe, l'exécution de fonctions privilégiées, les tentatives non réussies de connexion ou d'accès associées aux systèmes, l'utilisation de privilèges d'administrateur ou l'utilisation de justificatifs d'identité de tierce partie. Lors de l'établissement des types d'événements à journaliser, les organisations doivent considérer les activités de

surveillance et de vérification du système qui sont appropriées pour chaque exigence de sécurité. Pour définir les types d'événements, les organisations doivent considérer la journalisation nécessaire pour couvrir les événements connexes, comme les étapes dans les processus distribués basés sur une transaction (par exemple, les processus qui sont distribués parmi plusieurs organisations) ou encore les opérations qui surviennent dans les architectures orientées services ou basées sur le nuage.

Les exigences de surveillance et de vérification peuvent être équilibrées avec d'autres besoins du système. Par exemple, les organisations peuvent déterminer que les systèmes doivent avoir la capacité de journaliser tous les accès aux fichiers, qu'ils soient réussis ou non, mais d'activer cette capacité seulement dans des circonstances particulières pour ne pas nuire au rendement du système. Les types d'événements qui sont journalisés par les organisations peuvent changer au fil du temps. La vérification et la mise à jour des types d'événements journalisés sont nécessaires afin de s'assurer qu'ils demeurent pertinents.

Références

Source du contrôle : AU-02
Publications connexes :

- Centre pour la cybersécurité, *Journalisation et surveillance de la sécurité de réseau* (ITSAP.80.085)
- *NIST SP 800-92 Guide to Computer Security Log Management* (en anglais seulement)

03.03.02 Contenu des enregistrements de vérification

A. Inclure le contenu suivant dans les enregistrements de vérification :

1. type d'événement qui s'est produit;
2. moment auquel l'événement s'est produit;
3. endroit où l'événement s'est produit;
4. source de l'événement;
5. résultat de l'événement;
6. identité des personnes, des sujets, des objets ou des entités associés à l'événement.

B. Fournir des renseignements supplémentaires pour les enregistrements de vérification, au besoin.

Discussion

Le contenu des enregistrements de vérification pouvant être nécessaire pour appuyer la fonction de vérification comprend l'horodatage, l'adresse source et l'adresse de destination, les identificateurs d'utilisateur et de processus, la description des événements, le nom des fichiers et les règles de contrôle d'accès ou de contrôle de flux invoquées. Les résultats d'événements peuvent comprendre des indicateurs de réussite ou d'échec de l'événement et des résultats propres à l'événement (par exemple, l'état de sécurité du système après l'événement). Les renseignements détaillés que les organisations peuvent considérer dans les enregistrements de vérification peuvent comprendre un enregistrement plein texte des commandes privilégiées ou les identités individuelles des utilisatrices et utilisateurs appartenant à un compte de groupe.

Références

Sources des contrôles : AU-03 et AU-03(01)
Publications connexes : Aucune

03.03.03 Génération d'enregistrements de vérification

A. Générer les enregistrements de vérification pour les types d'événements sélectionnés et le contenu des enregistrements de vérification indiqué dans les exigences Journalisation d'événements 03.03.01 et Contenu des enregistrements de vérification 03.03.02

B. Conserver les enregistrements de vérification pendant la période correspondant à la stratégie de conservation des dossiers.

Discussion

Les enregistrements de vérification peuvent être créés à différents niveaux d'abstraction, y compris au niveau des paquets lorsque l'information traverse le réseau. La sélection du bon niveau d'abstraction est un aspect essentiel des capacités de journalisation des données de vérification et peut aider à déterminer les causes profondes des problèmes. La capacité d'ajouter l'information générée dans les enregistrements de vérification dépend des fonctionnalités du système permettant de configurer le contenu des enregistrements de vérification. Les organisations peuvent considérer ajouter de l'information supplémentaire dans les enregistrements de vérification, y compris les règles de contrôle d'accès et de contrôle de flux invoquées et les identités individuelles des utilisatrices et utilisateurs appartenant à un compte de groupe. Les organisations peuvent également envisager de limiter l'information supplémentaire à ajouter aux enregistrements de vérification en incluant seulement celle qui est nécessaire aux exigences de vérification. Si les enregistrements générés pour le processus de vérification contiennent des renseignements personnels qui ne sont pas requis pour le processus de vérification, les renseignements personnels doivent être retirés ou caviardés avant la conservation.

Si les enregistrements de vérification se fondent sur des renseignements personnels et si ces renseignements sont utilisés pour prendre une décision administrative, la période de conservation minimale standard est d'au moins deux ans suivant la date à laquelle les renseignements personnels ont été utilisés le plus récemment à des fins administratives, à moins que l'élimination soit explicitement autorisée par la personne concernée.

Références

Sources des contrôles : AU-11 et AU-12
Publications connexes : *NIST SP 800-92 Guide to Computer Security Log Management* (en anglais seulement)

03.03.04 Intervention en cas de défaillance du processus de journalisation des données de vérification

A. Alerter le personnel ou les rôles désignés de l'organisation dans une période de [Affectation : période définie par l'organisation] en cas de défaillance d'un processus de journalisation des données de vérification.

B. Prendre les mesures supplémentaires suivantes : [Affectation : mesures supplémentaires définies par l'organisation].

Discussion

L'échec du processus de journalisation des données de vérification inclut les erreurs logicielles et matérielles, l'échec des mécanismes de saisie des journaux de vérification et l'atteinte ou le dépassement de la capacité de stockage du journal de vérification. Les mesures d'intervention comprennent notamment l'écrasement des journaux de vérification plus anciens, la fermeture du système et l'arrêt de la génération des enregistrements de vérification. Les organisations peuvent choisir de définir des mesures supplémentaires associées aux défaillances du processus de journalisation des données de vérification en fonction du type, de l'emplacement et de la gravité de la défaillance, ou encore une combinaison de ces facteurs. Lorsque l'échec du processus de journalisation est associé au stockage, l'intervention doit s'appliquer au dépôt de stockage des journaux de vérification (c'est-à-dire le composant d'un système particulier où les journaux de vérification sont stockés), au système sur lequel les journaux de vérification se trouvent, à la capacité de stockage totale de l'organisation pour les journaux de vérification (c'est-à-

dire tous les dépôts de stockage de journaux de vérification) ou à ces trois éléments. Les organisations peuvent décider de ne pas prendre de mesures supplémentaires après avoir avisé les rôles ou le personnel désignés.

Références

Source du contrôle : AU-05
Publications connexes : Aucune

03.03.05 Examen, analyse et production de rapports liés aux enregistrements de vérification

A. Examiner et analyser les enregistrements de vérification du système tous les [Affectation : fréquence définie par l'organisation] afin de repérer les indications et les répercussions potentielles d'activités inappropriées ou inhabituelles.

B. Signaler les résultats au personnel ou aux rôles désignés de l'organisation.

C. Analyser et mettre en correspondance les enregistrements de vérification provenant de différents dépôts afin d'établir une connaissance de la situation à l'échelle de l'organisation.

Discussion

Les activités d'examen, d'analyse et de production de rapports liées aux enregistrements de vérification portent sur la journalisation des données relatives à la sécurité et à la confidentialité effectuée par les organisations et peuvent inclure la journalisation de données découlant de la surveillance de l'utilisation des comptes, des accès distants, des connexions sans fil, des paramètres de configuration, de l'utilisation d'outils de maintenance (locaux ou non locaux), de l'inventaire des composants de systèmes, des connexions d'appareils mobiles, de l'installation ou du retrait d'équipement, des accès physiques, de la température et de l'humidité, des communications au niveau des interfaces du système et de l'utilisation de code mobile. Les résultats peuvent être communiqués aux entités organisationnelles, comme l'équipe d'intervention en cas d'incident, le service de dépannage et le bureau de la sécurité ou de la protection de la vie privée. Si les organisations ne sont pas autorisées à examiner et à analyser les enregistrements de vérification ou si elles sont incapables de mener de telles activités, les activités d'examen et d'analyse peuvent être menées par les organisations disposant d'une telle autorité. La portée, la fréquence et/ou la précision de l'examen, de l'analyse et de la production de rapports liés aux enregistrements de vérification peuvent être ajustées afin de répondre aux besoins organisationnels, en fonction de l'information nouvelle reçue. La mise en correspondance des processus d'examen, d'analyse et de production de rapports liés aux enregistrements de vérification permet de s'assurer que ces processus, collectivement, brossent un tableau plus complet des événements.

Références

Sources des contrôles : AU-06 et AU-06(03)
Publications connexes :

- *NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response* (en anglais seulement)
- *NIST SP 800-101 Guidelines on Mobile Device Forensics* (en anglais seulement)

03.03.06 Réduction des enregistrements de vérification et génération de rapports

A. Mettre en œuvre des capacités de réduction des enregistrements de vérification et de génération de rapports pour répondre aux exigences en matière d'examen, d'analyse et de production de rapports ainsi qu'aux enquêtes sur les incidents.

B. Conserver le contenu original et la chronologie des enregistrements de vérification.

Discussion

Les enregistrements de vérification sont générés dans l'exigence Génération d'enregistrements de vérification 03.03.03. La réduction des enregistrements de vérification et la génération de rapports surviennent après la génération des enregistrements de vérification. La réduction des enregistrements de vérification est un processus qui transforme les données de vérification recueillies et les condense afin d'en accroître la valeur pour les analystes. Les capacités de réduction des enregistrements de vérification et de génération de rapports ne proviennent pas toujours du même système ou des mêmes entités organisationnelles qui mènent les activités de vérification. Les capacités de réduction des enregistrements de vérification peuvent inclure, par exemple, des techniques d'exploration de données modernes comportant des filtres de données évolués afin de détecter les comportements anormaux dans les enregistrements de vérification. Les capacités de génération de rapports fournies par le système peuvent aider à générer des rapports personnalisables. Le classement chronologique des enregistrements de vérification peut être un problème important si la granularité de l'horodatage des enregistrements est insuffisante.

Références

Source du contrôle : AU-07
Publications connexes : Aucune

03.03.07 Horodatage

A. Utiliser les horloges internes du système pour horodater les enregistrements de vérification.

B. Consigner l'horodatage des enregistrements de vérification correspondant à [Affectation : granularité de mesure du temps définie par l'organisation] et utilisant le temps universel coordonné (UTC), un décalage fixe par rapport à l'UTC correspondant à l'heure locale, ou encore en incluant le décalage local dans les données d'horodatage.

Discussion

L'horodatage généré par le système comprend la date et l'heure. L'heure est souvent exprimée selon l'UTC ou selon l'heure locale qui est un décalage par rapport à l'UTC. La granularité des mesures temporelle fait référence au degré de synchronisation entre les horloges du système et des horloges de référence (par exemple, la synchronisation des horloges avec une précision d'un centième ou d'un millième de seconde). Les organisations peuvent définir des granularités temporelles différentes pour les divers composants du système. Le service d'heure peut être essentiel à d'autres capacités de sécurité (par exemple, le contrôle d'accès ainsi que l'identification et l'authentification), selon la nature des mécanismes utilisés pour appuyer ces capacités

Références

Source du contrôle : AU-08
Publications connexes : Aucune

03.03.08 Protection de l'information de vérification

A. Protéger l'information de vérification et les outils de journalisation des données de vérification contre les accès non autorisés, les modifications et les suppressions.

B. Autoriser l'accès pour la gestion de la fonctionnalité de journalisation des données de vérification uniquement à un sous-ensemble d'utilisatrices et utilisateurs ou de rôles privilégiés.

Discussion

L'information de vérification comprend les renseignements nécessaires pour mener à bien la vérification des activités du système, notamment les enregistrements de vérification, les paramètres de journalisation des données de vérification, les rapports de vérification et les renseignements personnels. Les outils de journalisation des données de vérification sont des programmes et des dispositifs servant à mener les activités de vérification et de consignation. La protection de l'information de vérification se concentre sur la protection physique et empêche des

personnes non autorisées d'accéder à des outils de journalisation des données de vérification et de les exécuter. La protection physique de l'information de vérification est abordée par les exigences de protection physique et des supports.

Les personnes ou les rôles dotés d'un accès privilégié à un système et qui sont également l'objet d'une vérification par ce système peuvent affecter la fiabilité de l'information de vérification en bloquant les activités de vérification ou en modifiant les enregistrements de vérification. Le fait d'exiger un accès privilégié mieux défini en ce qui concerne les privilèges associés aux vérifications et les autres privilèges limite le nombre d'utilisatrices et utilisateurs ou de rôles qui détiennent les privilèges associés aux vérifications.

Références

Sources des contrôles : AU-09 et AU-09(04)
Publications connexes : Aucune

03.03.09 Non affecté

Retiré par le NIST.

3.4 Gestion des configurations

Les contrôles de gestion des configurations appuient la gestion et le contrôle de tous les composants du système, comme le matériel, les logiciels et les éléments de configuration.

03.04.01 Configuration de référence

A. Élaborer et tenir à jour, dans le cadre du contrôle des configurations, une configuration de référence du système.

B. Examiner et mettre à jour la configuration de référence du système tous les [Affectation : fréquence définie par l'organisation] et lorsque des composants de systèmes sont installés ou modifiés.

Discussion

Les configurations de référence pour les systèmes et les composants des systèmes incluent les éléments associés à la connectivité, à l'utilisation et aux communications. Les configurations de référence sont des spécifications des systèmes ou des éléments de configuration connexes documentés dont on a convenu et qui font l'objet d'un examen officiel. Les configurations de référence servent de fondement pour les éditions, les versions ou les changements à venir du système et comprennent des renseignements à propos des composants du système, des procédures opérationnelles, de la topologie de réseau et de la disposition des composants au sein de l'architecture du système. La tenue à jour des configurations de référence nécessite de créer de nouvelles bases de référence à mesure que le système évolue au fil du temps. Les configurations de référence des systèmes tiennent compte de l'architecture d'entreprise actuelle. Si le système facilite la collecte ou l'utilisation de renseignements personnels, les configurations de référence devraient inclure un énoncé sur la protection de la vie privée fourni aux utilisatrices et utilisateurs.

Références

Source du contrôle : CM-02
Publications connexes :

- *NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise* (en anglais seulement)

- *NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems* (en anglais seulement)

03.04.02 Paramètres de configuration

A. Établir, documenter et mettre en œuvre les paramètres de configuration suivants pour le système afin de refléter le mode le plus restrictif selon les exigences opérationnelles : [Affectation : paramètres de configuration définis par l'organisation].

B. Déterminer, documenter et approuver toute déviation des paramètres de configuration établis.

Discussion

Les paramètres de configuration représentent l'ensemble des paramètres pouvant être modifiés dans les composants matériels, logiciels ou micrologiciels du système et qui affectent la posture de sécurité ou de confidentialité ou encore le fonctionnement du système. Les paramètres de configuration liés à la sécurité peuvent être définis pour les systèmes (par exemple, les serveurs et postes de travail), les dispositifs d'entrée-sortie (par exemple, les numériseurs, photocopieurs et imprimantes), les composants réseau (par exemple, les pare-feu, routeurs, passerelles, commutateurs voix-données, points d'accès sans fil, appareils réseau et capteurs), les systèmes d'exploitation, les logiciels médiateurs et les applications.

Les paramètres de sécurité ont une incidence sur l'état de sécurité du système et incluent les paramètres nécessaires pour répondre à d'autres exigences de sécurité. Les paramètres de sécurité comprennent notamment les paramètres de registre, les paramètres d'autorisation pour les comptes, les fichiers et les répertoires (c'est-à-dire les privilèges) et les paramètres pour les fonctions, les ports, les protocoles et les connexions distantes. Les paramètres de confidentialité sont les paramètres qui ont une incidence sur la posture de confidentialité des systèmes, y compris ceux nécessaires pour répondre à d'autres contrôles de confidentialité. Les paramètres de confidentialité incluent les exigences liées au contrôle d'accès, aux renseignements personnels, à la précision des données, aux capacités de manipulation des données, aux préférences de traitement des données et aux permissions de traitement et de rétention de l'information. Les organisations doivent établir des paramètres de configuration à l'échelle de l'organisation et par la suite des paramètres de configuration particuliers pour le système. Les paramètres établis deviennent une partie intégrante de la configuration de référence du système.

Les configurations sécurisées communes (que l'on appelle également les listes de vérification concernant la configuration de sécurité, les guides de confinement et de renforcement, les guides de référence pour la sécurité et les guides techniques de mise en œuvre de la sécurité [STIG pour *Security Technical Implementation Guide*]) fournissent des points de repère reconnus, normalisés et établis qui stipulent les paramètres de configuration sécurisée associés à des plateformes ou à des produits de technologies de l'information (TI) particuliers ainsi que des instructions pour la configuration de ces composants de systèmes afin de répondre aux exigences opérationnelles. Diverses organisations peuvent développer des configurations sécurisées communes, y compris les développeurs de produits TI, les fabricants, les fournisseurs, les consortiums, le milieu universitaire, l'industrie, les ministères et organismes fédéraux ainsi que d'autres organisations des secteurs public et privé.

Références

Source du contrôle : CM-06
Publications connexes :

- Centre pour la cybersécurité, *Exigences de base en matière de sécurité pour les zones de sécurité de réseau (ITSP.80.022)*
- *NIST SP 800-70 National Checklist Program for IT Products: Guidelines for Checklist Users and Developers* (en anglais seulement)
- *NIST SP 800-126 The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3* (en anglais seulement)
- *NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems* (en anglais

seulement)

03.04.03 Contrôle des changements de configuration

A. Définir les types de changements apportés au système qui sont contrôlés par la configuration.

B. Examiner les changements proposés au système qui sont contrôlés par la configuration et les approuver ou les refuser en tenant compte explicitement des répercussions sur la sécurité.

C. Mettre en œuvre et documenter les changements approuvés au système qui sont contrôlés par la configuration.

D. Surveiller et examiner les activités associées aux changements contrôlés par la configuration visant le système.

Discussion

Le contrôle des changements de configuration fait référence aux activités de suivi, d'examen, d'approbation, de refus et de journalisation des changements au système. Ce contrôle comprend la proposition, la justification, la mise en œuvre, la mise à l'essai, l'examen et l'application systématiques de changements au système, y compris les mises à niveau et les modifications du système. Le contrôle des changements de configuration inclut les changements aux configurations de référence pour les composants de systèmes (par exemple, les systèmes d'exploitation, applications, pare-feu, routeurs et appareils mobiles) et aux éléments de configuration du système, les changements aux paramètres de configuration, les changements non planifiés et non autorisés, et les changements visant à corriger des vulnérabilités. Cette exigence est associée à l'exigence Analyses des répercussions 03.04.04.

Références

Source du contrôle : CM-03
Publications connexes :

- *NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise* (en anglais seulement)
- *NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems* (en anglais seulement)

03.04.04 Analyses des répercussions

A. Analyser les répercussions sur la sécurité et la confidentialité des changements apportés au système, avant la mise en œuvre.

B. Vérifier que les exigences de sécurité du système continueront d'être satisfaites après la mise en œuvre des changements.

Discussion

Le personnel de l'organisation ayant des responsabilités en matière de sécurité et confidentialité doit mener des analyses des répercussions qui comprennent les éléments suivants : examiner les plans, les stratégies et les procédures de sécurité et de confidentialité afin de comprendre les exigences de sécurité et de confidentialité; examiner la documentation de conception et les procédures opérationnelles du système afin de comprendre les répercussions que peuvent entraîner les changements apportés au système sur l'état de sécurité et de confidentialité du système; examiner les répercussions que peuvent entraîner les changements de partenaires de la chaîne d'approvisionnement sur les parties prenantes; déterminer la manière dont les changements potentiels apportés au système peuvent créer de nouveaux risques pour la vie privée des personnes et établir la capacité à atténuer ces risques. Les analyses des répercussions incluent également les évaluations des risques afin de comprendre les répercussions des changements et de déterminer si des exigences de sécurité ou de confidentialité supplémentaires sont nécessaires. Les changements apportés au système peuvent avoir une incidence sur les mesures de protection et les contre-mesures qui ont été mises en œuvre précédemment. Cette exigence est

associée à l'exigence Contrôle des changements de configuration 03.04.03. Les changements au système ne sont pas tous contrôlés par la configuration.

Références

Sources des contrôles : CM-04 et CM-04(02)
Publications connexes : *NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems* (en anglais seulement)

03.04.05 Restriction d'accès pour les changements

Définir, documenter, approuver et appliquer les restrictions d'accès physiques et logiques associées aux changements apportés au système.

Discussion

Les changements apportés aux composants matériels, logiciels ou micrologiciels du système ou aux procédures opérationnelles associées au système peuvent avoir des répercussions importantes sur la sécurité du système ou la vie privée des personnes. Les organisations doivent donc accorder l'accès au système seulement aux personnes qualifiées et autorisées et seulement pour effectuer les changements. Les restrictions d'accès incluent les contrôles d'accès physiques et logiques, les bibliothèques de logiciels, l'automatisation de flux de travaux, les médiathèques, les couches abstraites (c'est-à-dire les changements mis en œuvre dans les interfaces externes plutôt que directement dans le système) et les fenêtres de changement (c'est-à-dire les changements sont appliqués seulement à des moments précis).

Références

Source du contrôle : CM-05
Publications connexes :

- *NIST FIPS 140-3 Security Requirements for Cryptographic Modules* (en anglais seulement)
- *NIST FIPS 186-5, Digital Signature Standard (DSS)* (en anglais seulement)
- *NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems* (en anglais seulement)

03.04.06 Fonctionnalité minimale

A. Configurer le système afin qu'il fournisse uniquement les capacités essentielles à la mission.

B. Interdire ou restreindre l'utilisation des fonctions, des ports, des protocoles, des connexions et des services suivants : [Affectation : fonctions, ports, protocoles, connexions et services définis par l'organisation].

C. Examiner le système tous les [Affectation : fréquence définie par l'organisation] afin d'établir les fonctions, les ports, les protocoles, les connexions et les services non nécessaires.

D. Désactiver ou retirer les fonctions, les ports, les protocoles, les connexions et les services qui ne sont pas nécessaires ou non sécurisés.

Discussion

Les systèmes peuvent fournir une grande variété de fonctions et de services. Il se peut que certaines fonctions et certains services fournis régulièrement par défaut ne soient pas nécessaires pour appuyer la mission, les fonctions ou les opérations essentielles de l'organisation. Il peut être pratique de fournir plusieurs services à partir de composants individuels du système. Toutefois, cette façon de faire augmente les risques comparativement au fait de limiter les services fournis à partir d'un seul composant. Dans la mesure du possible, les organisations doivent limiter la fonctionnalité à une seule fonction par composant.

Les organisations doivent examiner les fonctions et les services fournis par le système ou les composants du système afin de déterminer ceux qui peuvent être éliminés. Les organisations doivent également désactiver les protocoles et les ports physiques et logiques inutilisés ou qui ne sont pas nécessaires afin d'empêcher les connexions non autorisées des appareils, les transferts d'information et la tunnellisation. Les organisations peuvent utiliser des outils d'analyse de réseau, des solutions de détection et de prévention d'intrusion et des solutions de protection des points d'extrémité (par exemple, des pare-feu et des systèmes de détection d'intrusion sur l'hôte) afin de détecter et de prévenir l'utilisation de fonctions, de ports, de protocoles, de connexions système et de services non autorisés. Bluetooth, FTP (*File Transfer Protocol*) et l'interconnexion de réseaux d'égal à égal sont des exemples de protocoles que les organisations doivent envisager d'éliminer, de restreindre ou de désactiver.

Références

Sources des contrôles : CM-07 et CM-07(01)
Publications connexes :

- Centre pour la cybersécurité, *Liste d'applications autorisées* (ITSAP.10.095)
- Centre pour la cybersécurité, *Les 10 mesures de sécurité des TI : No 10, Mettre en place une liste d'applications autorisées* (ITSM.10.095)
- *NIST SP 800-160-1 Engineering Trustworthy Secure Systems* (en anglais seulement)
- Centre pour la cybersécurité, *Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes* (ITSP.10.037)

03.04.07 Non affecté

Retiré par le NIST.

03.04.08 Logiciels autorisés – Autorisation par exception

A. Déterminer les programmes logiciels autorisés à être exécutés sur le système.

B. Mettre en œuvre une stratégie de refus par défaut, autorisation par exception pour l'exécution des programmes logiciels sur le système.

C. Examiner et mettre à jour la liste des programmes logiciels autorisés tous les [Affectation : fréquence définie par l'organisation].

Discussion

S'ils détiennent les privilèges nécessaires, les utilisatrices et utilisateurs peuvent installer des logiciels sur les systèmes organisationnels. Afin de garder le contrôle sur les logiciels installés, les organisations doivent déterminer les opérations permises et interdites concernant l'installation de logiciels. Les installations de logiciels autorisées comprennent les mises à jour et l'application de correctifs de sécurité aux logiciels existants, ainsi que le téléchargement de nouvelles applications à partir des magasins d'application approuvés par l'organisation. Les stratégies sélectionnées pour régir les logiciels installés par les utilisatrices et utilisateurs peuvent être développées par l'organisation ou fournies par une entité externe. Les méthodes d'application des stratégies peuvent inclure des méthodes procédurales et des méthodes automatisées.

Les programmes logiciels autorisés peuvent être limités à des versions ou à des sources particulières. Afin de favoriser un processus complet de gestion des logiciels autorisés et de renforcer la protection contre les attaques qui contournent les logiciels autorisés au niveau de l'application, les programmes logiciels peuvent être décomposés en différents niveaux de détail et surveillés. Ces niveaux incluent les applications, les interfaces de programmation d'applications, les modules d'application, les scripts, les processus système, les services système, les fonctions noyau, les registres, les pilotes et les bibliothèques de liens dynamiques.

Références

Source du contrôle : CM-07(05)
Publications connexes :

- Centre pour la cybersécurité, *Liste d'applications autorisées* (ITSAP.10.095)
- Centre pour la cybersécurité, *Les 10 mesures de sécurité des TI : No 10, Mettre en place une liste d'applications autorisées* (ITSM.10.095)
- *NIST SP 800-160-1 Engineering Trustworthy Secure Systems* (en anglais seulement)

03.04.09 Non affecté

Retiré par le NIST.

03.04.10 Inventaire des composants du système

A. Élaborer et documenter un inventaire des composants du système.

B. Examiner et mettre à jour l'inventaire des composants du système tous les [Affectation : fréquence définie par l'organisation].

C. Mettre à jour l'inventaire des composants du système dans le cadre des activités d'installation, de retrait et de mise à jour du système.

Discussion

Les composants du système sont des actifs discrets et identifiables (c'est-à-dire le matériel, les logiciels et les micrologiciels) qui composent un système. Les organisations peuvent mettre en œuvre des inventaires de composants de systèmes centralisés qui comprennent des composants de tous les systèmes. Dans de telles situations, les organisations doivent s'assurer que les inventaires comportent de l'information propre au système requise pour la comptabilisation des composants. L'information nécessaire pour une comptabilisation efficace des composants du système comprend le nom du système, les propriétaires des logiciels, les numéros de version des logiciels, les spécifications de l'inventaire du matériel, l'information sur les licences de logiciels, les composants réseau, les noms des machines et les adresses réseau pour tous les protocoles mis en œuvre (par exemple, IPv4 et IPv6). Les spécifications de l'inventaire doivent comprendre le type de composant, l'emplacement physique, la date de réception, le fabricant, le coût, le modèle, le numéro de série et des données sur le fournisseur.

Références

Sources des contrôles : CM-08 et CM-08(01)
Publications connexes :

- *NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise* (en anglais seulement)
- *NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems* (en anglais seulement)

03.04.11 Emplacement de l'information

A. Établir et documenter l'emplacement de l'information désignée et des composants de systèmes où l'information est traitée et stockée.

B. Documenter les changements d'emplacement sur le système ou les composants du système où l'information désignée est traitée et stockée.

Discussion

L'emplacement de l'information répond au besoin de bien comprendre les composants du système où l'information désignée est traitée et stockée ainsi que les utilisatrices et utilisateurs qui ont accès à l'information désignée, afin de pouvoir fournir les mécanismes de protection qui conviennent, y compris les contrôles de flux d'information, les contrôles d'accès et la gestion de l'information.

Références

Source du contrôle : CM-12
Publications connexes : Aucune

03.04.12 Configuration des systèmes et des composants pour des zones à risque élevé

A. Remettre des systèmes ou des composants de systèmes dotés des configurations suivantes aux personnes qui voyagent dans des lieux à risque élevé : [Affectation : configurations système définies par l'organisation].

B. Appliquer les exigences de sécurité suivantes aux systèmes ou aux composants de systèmes lorsque les personnes reviennent de voyage : [Affectation : exigences de sécurité définies par l'organisation].

Discussion

Lorsque l'on sait qu'un système ou qu'un composant de système se trouvera dans une zone à risque élevé, des exigences de sécurité supplémentaires peuvent être nécessaires afin de contrer les menaces accrues. Les organisations peuvent mettre en œuvre des mesures de protection sur les systèmes ou les composants de systèmes qui sont utilisés par des personnes qui partent en voyage et qui en reviennent. Les mesures comprennent déterminer les lieux préoccupants, définir les configurations requises pour les composants, s'assurer que les composants sont configurés adéquatement avant le voyage et réaliser prendre d'autres mesures au retour du voyage. Par exemple, les systèmes qui se trouveront dans des zones à risque élevé peuvent être configurés avec des disques durs préalablement nettoyés, un nombre limité d'applications ou encore des paramètres de configuration plus stricts. Les mesures appliquées aux appareils mobiles au retour du voyage comprennent un examen de l'appareil afin de détecter des signes physiques de tentatives de modification, le nettoyage de la mémoire ou la recréation de l'image de la mémoire de l'appareil.

Références

Source du contrôle : CM-02(07)
Publications connexes :

- *NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise* (en anglais seulement)
- *NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems* (en anglais seulement)

3.5 Identification et authentification

Les contrôles d'identification et d'authentification appuient l'identification unique des utilisatrices et utilisateurs, des processus agissant au nom des utilisatrices et utilisateurs et des dispositifs. Ils appuient également l'authentification ou la vérification des identités des utilisatrices et utilisateurs, des processus et des dispositifs comme condition préalable pour accorder l'accès aux systèmes organisationnels.

03.05.01 Identification, authentification et réauthentification des utilisatrices et utilisateurs

A. Identifier de manière unique et authentifier les utilisatrices et utilisateurs du système et associer un identificateur unique aux processus agissant en leur nom.

B. Réauthentifier les utilisatrices et utilisateurs lors de [Affectation : circonstances ou situations nécessitant une réauthentification définies par l'organisation].

Discussion

Les utilisatrices et utilisateurs de système incluent les personnes (ou les processus système agissant en leur nom) qui sont autorisées à accéder à un système. Normalement, les identificateurs d'individus correspondent aux noms d'utilisateur associés aux comptes système qui leur ont été attribués. Puisque les processus système sont exécutés au nom de groupes et de rôles, les organisations peuvent exiger l'identification individuelle de chacune des personnes comprises dans un compte de groupe aux fins de responsabilisation individuelle pour les activités réalisées sur le système. L'identification unique et l'authentification des utilisatrices et utilisateurs s'appliquent à tous les accès système. Les organisations peuvent avoir recours à des mots de passe, à des authentifiants physiques, à la biométrie ou à une combinaison de ces éléments pour l'authentification de l'identité des utilisatrices et utilisateurs. Les organisations peuvent procéder à une réauthentification des personnes dans certaines situations, y compris lors d'un changement lié aux rôles, aux authentifiants ou aux justificatifs d'identité, lors de l'exécution de fonctions privilégiées, après une période déterminée ou périodiquement.

Références

Sources des contrôles : IA-02 et IA-11
Publications connexes : Centre pour la cybersécurité, *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information* (ITSP.30.031)

03.05.02 Identification et authentification des dispositifs

Identifier de manière unique et authentifier les [Affectation : dispositifs ou types de dispositifs définis par l'organisation] avant d'établir une connexion au système.

Discussion

Les dispositifs qui exigent une identification et une authentification dispositif à dispositif unique sont définis en fonction du type, du dispositif ou d'une combinaison des deux. Les types de dispositifs définis par l'organisation incluent les dispositifs qui n'appartiennent pas à l'organisation. Les systèmes utilisent de l'information connue partagée (par exemple, des adresses Media Access Control [MAC] ou Transmission Control Protocol/Internet Protocol [TCP/IP]) pour l'identification des dispositifs ou encore des solutions d'authentification organisationnelles (par exemple, les protocoles Institute of Electrical and Electronics Engineers [IEEE] 802.1x et Extensible Authentication Protocol [EAP], un serveur RADIUS avec l'authentification EAP-Transport Layer Security [TLS] ou Kerberos) pour identifier et authentifier les dispositifs sur les réseaux locaux et étendus. Une infrastructure à clé publique (ICP) et une vérification de la révocation des certificats pour les certificats échangés peuvent également être intégrées dans le cadre de l'authentification des dispositifs.

Références

Source du contrôle : IA-03
Publications connexes : Centre pour la cybersécurité, *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information* (ITSP.30.031)

03.05.03 Authentification multifacteur

Mettre en œuvre des mécanismes robustes d'authentification multifacteur (AMF) pour l'accès aux comptes privilégiés et non privilégiés.

Discussion

Cette exigence s'applique aux comptes d'utilisateur. L'authentification multifacteur nécessite l'utilisation de deux facteurs différents ou plus pour l'authentification. Les facteurs d'authentification sont définis comme suit : quelque chose que l'utilisatrice ou utilisateur connaît (par exemple, un numéro d'identification personnel [NIP]), quelque chose en sa possession (par exemple, un authentifiant physique comme une clé cryptographique privée) ou quelque chose qui la ou le caractérise (par exemple, une authentification biométrique). Les solutions d'authentification multifacteur qui présentent des authentifiants physiques comprennent les authentifiants matériels qui fournissent des sorties à durée limitée ou de type défi-réponse ainsi que des cartes à puce. En plus d'authentifier les utilisatrices et utilisateurs au niveau du système, les organisations peuvent également avoir recours à des mécanismes d'authentification au niveau de l'application pour accroître la sécurité de l'information.

Références

Sources des contrôles : IA-02(01) et IA-02(02)
Publications connexes : Centre pour la cybersécurité, *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information* (ITSP.30.031)

03.05.04 Authentification résistant à la réinsertion

Mettre en œuvre des mécanismes d'authentification résistant à la réinsertion pour l'accès aux comptes privilégiés et non privilégiés.

Discussion

Les processus d'authentification résistent aux attaques par réinsertion lorsqu'il n'est pas pratique de réaliser une authentification réussie en enregistrant ou en réinsérant un message d'authentification antérieur. Les techniques résistant à la réinsertion incluent les protocoles qui utilisent des nonces ou des défis, comme des authentifiants à usage unique synchrones ou défi-réponse.

Références

Source du contrôle : IA-02(08)
Publications connexes : Centre pour la cybersécurité, *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information* (ITSP.30.031)

03.05.05 Gestion des identifiants

A. Recevoir une autorisation du personnel ou des rôles de l'organisation pour attribuer un identifiant à une personne, à un groupe, à un rôle, à un service ou à un dispositif.

B. Sélectionner et attribuer un identifiant qui identifie une personne, un groupe, un rôle, un service ou un dispositif.

C. Prévenir la réutilisation d'identifiant pendant [Affectation : délai défini par l'organisation].

D. Gérer les identifiants personnels en identifiant de façon unique chaque personne à titre de [Affectation : caractéristique définie par l'organisation identifiant le statut de la personne].

Discussion

Les identifiants sont fournis aux utilisatrices et utilisateurs, les processus agissant en leur nom et aux dispositifs. Le fait d'empêcher la réutilisation d'identifiant empêche d'attribuer à une autre entité des identifiants utilisés

précédemment par une personne, un groupe, un rôle, un service ou un dispositif.

Les caractéristiques qui identifient le statut d'un individu comprennent les utilisatrices et utilisateurs entrepreneurs, de nationalité étrangère et non organisationnels. L'identification du statut d'un individu au moyen de ces caractéristiques offre des renseignements à propos des personnes avec lesquelles le personnel de l'organisation communique. Par exemple, il peut être utile pour une employée ou un employé de savoir que l'une des personnes dans la liste des destinataires d'un courriel est une entrepreneure ou un entrepreneur.

Références

Sources des contrôles : IA-04 et IA-04(04)
Publications connexes : Centre pour la cybersécurité, *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information* (ITSP.30.031)

03.05.06 Non affecté

Retiré par le NIST.

03.05.07 Gestion des mots de passe

A. Créer une liste des mots de passe couramment utilisés, attendus ou compromis et la mettre à jour tous les [Affectation : fréquence définie par l'organisation] et lorsque l'on soupçonne que les mots de passe de l'organisation ont été compromis.

B. Vérifier que les mots de passe ne figurent pas sur la liste des mots de passe couramment utilisés, attendus ou compromis lorsque les utilisatrices et utilisateurs créent ou modifient leurs mots de passe.

C. Transmettre les mots de passe uniquement par des canaux protégés par chiffrement.

D. Stocker les mots de passe sous forme chiffrée.

E. Sélectionner un nouveau mot de passe lors de la première utilisation à la suite d'une récupération de compte.

F. Appliquer aux mots de passe les règles de composition et de complexité suivantes : [Affectation : règles de composition et de complexité définies par l'organisation].

Discussion

L'authentification fondée sur un mot de passe s'applique aux mots de passe utilisés pour l'authentification à un seul facteur ou multifacteur. Les longs mots de passe ou les phrases de passe sont préférables aux mots de passe courts. L'application de règles de composition offre certains avantages pour la sécurité, mais réduit l'utilisabilité. Les organisations peuvent choisir d'établir et d'appliquer certaines règles pour la génération de mots de passe (notamment concernant le nombre minimal de caractères) dans certaines circonstances. Par exemple, un mot de passe oublié peut mener à une récupération de compte. Des mots de passe protégés par chiffrement comprennent le hachage cryptographique unidirectionnel salé des mots de passe. La liste des mots de passe couramment utilisés, compromis ou attendus comprend les mots de passe provenant des corpus de violations précédentes, les mots du dictionnaire et les caractères répétitifs ou séquentiels. Cette liste comprend des mots s'appliquant au contexte, comme le nom du service, le nom d'utilisateur et des dérivations de ces éléments. L'obligation de remplacer un mot de passe temporaire par un mot de passe permanent immédiatement après la connexion au système permet de s'assurer que les mécanismes d'authentification sont suffisamment robustes et mis en œuvre à la première occasion, ce qui permet de réduire les possibilités de compromission d'authentifiants. Il peut être possible d'utiliser de longs mots de passe ou des phrases de passe dans le but d'augmenter la complexité des mots de passe.

Références

Source du contrôle : IA-05(01)
Publications connexes : Centre pour la cybersécurité, *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information* (ITSP.30.031)

03.05.08 Non affecté

Retiré par le NIST.

03.05.09 Non affecté

Retiré par le NIST.

03.05.10 Non affecté

Retiré par le NIST.

03.05.11 Rétroaction d'authentification

Masquer la rétroaction d'information d'authentification durant le processus d'authentification.

Discussion

La rétroaction d'authentification n'offre pas d'information qui pourrait permettre à des personnes non autorisées de compromettre les mécanismes d'authentification. Par exemple, dans le cas des ordinateurs de bureau ou blocs-notes dotés d'un écran relativement grand, la menace peut être importante en raison de l'espionnage par-dessus l'épaule. Par contre, dans le cas des appareils mobiles à petit écran, cette menace peut être moins importante et contrebalancée par la possibilité accrue d'erreurs de saisie due aux claviers de petite taille. Les moyens pour masquer la rétroaction d'authentification doivent être sélectionnés en conséquence. Le masquage de la rétroaction comprend l'affichage d'astérisques au moment où l'utilisatrice ou utilisateur saisit son mot de passe sur l'appareil ou l'affichage d'une rétroaction seulement pendant une courte période avant l'application d'un masquage complet.

Références

Source du contrôle : IA-06
Publications connexes : Aucune

03.05.12 Gestion des authentifiants

A. Vérifier l'identité de la personne, du groupe, du rôle, du service ou du dispositif recevant l'authentifiant dans le cadre de la distribution initiale d'authentifiant.

B. Établir le contenu de l'authentifiant initial pour les authentifiants émis par l'organisation.

C. Établir et mettre en œuvre des procédures administratives pour la distribution initiale des authentifiants en cas de perte, de compromission, de corruption et de révocation.

D. Changer les authentifiants par défaut lors de la première utilisation.

E. Changer ou actualiser les authentifiants tous les [Affectation : fréquence définie par l'organisation] ou lorsque les événements suivants se produisent : [Affectation : événements définis par l'organisation].

F. Protéger le contenu des authentifiants contre les divulgations ou les modifications non autorisées.

Discussion

Les authentifiants comprennent les mots de passe, les dispositifs de chiffrement, la biométrie, les certificats, les dispositifs avec mot de passe à usage unique et les cartes d'identité. Le contenu de l'authentifiant initial correspond au contenu réel de l'authentifiant (par exemple, le mot de passe initial). Comparativement, les exigences pour le contenu de l'authentifiant contiennent des caractéristiques particulières. La gestion des authentifiants est prise en charge par des paramètres et des restrictions définis par l'organisation pour différentes caractéristiques d'authentifiant (par exemple, la complexité du mot de passe et les règles de composition, la fenêtre de validation des jetons synchrones à utilisation unique et le nombre de refus permis durant l'étape de vérification de l'authentification biométrique).

L'exigence de protéger les authentifiants individuels peut être mise en œuvre au moyen de l'exigence Règles de conduite 03.15.03 pour les authentifiants qui se trouvent dans la possession de personnes et par les exigences Gestion des comptes 03.01.01, Application de l'accès 03.01.02, Droit d'accès minimal 03.01.05 et Confidentialité lors de la transmission et du stockage 03.13.08 pour ceux qui sont stockés dans les systèmes organisationnels. Cela comprend les mots de passe stockés en format haché ou chiffré, ou les fichiers qui contiennent des mots de passe hachés ou chiffrés accessibles à l'aide de privilèges d'administrateur. Il est possible de mettre en œuvre des mesures pour protéger les authentifiants, y compris garder en sa possession les authentifiants, ne pas partager les authentifiants avec d'autres personnes et signaler immédiat la perte, le vol ou la compromission d'authentifiants.

Les développeuses et développeurs peuvent livrer des composants de systèmes avec les justificatifs d'authentification pour l'installation et la configuration initiales. Les justificatifs d'authentification par défaut sont souvent bien connus, faciles à découvrir et présentent un risque important. La gestion des authentifiants comprend l'émission et la révocation des authentifiants pour un accès temporaire, qui ne sera plus nécessaire par la suite. L'utilisation de longs mots de passe ou de phrases de passe peut remplacer le besoin d'avoir à changer périodiquement les authentifiants.

Références

Source du contrôle : IA-05
Publications connexes : Centre pour la cybersécurité, *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information* (ITSP.30.031)

3.6 Intervention en cas d'incident

Les contrôles d'intervention en cas d'incident appuient l'établissement de capacités de traitement d'incident opérationnel pour les systèmes organisationnels, y compris la préparation, la surveillance, la détection, l'analyse, le confinement, la reprise et l'intervention. Les incidents sont surveillés, documentés et signalés aux autorités et aux responsables organisationnels appropriés.

03.06.01 Traitement des incidents

Mettre en œuvre des capacités de traitement des incidents alignées sur le plan d'intervention en cas d'incident et y inclure les activités de préparation, de détection, d'analyse, de confinement, d'éradication et de reprise.

Discussion

L'information liée aux incidents peut provenir de différentes sources, y compris la surveillance des vérifications, des réseaux et des accès physiques, les rapports d'utilisateur et d'administrateur, et les événements signalés de la chaîne d'approvisionnement. L'efficacité des capacités de traitement des incidents dépendent de la coordination

entre différentes entités organisationnelles, y compris les propriétaires des activités et de la mission, les propriétaires des systèmes, les ressources humaines, les équipes de sécurité physique et du personnel, les services juridiques, le personnel des opérations et les responsables de l'approvisionnement.

Un incident touchant les renseignements personnels est considéré comme une atteinte à la vie privée. Une atteinte à la vie privée mène à une perte de contrôle, à une compromission, à une divulgation non autorisée, à une utilisation non autorisée, à une collecte illégale, à une conservation ou à une élimination inadéquate, ou à une occurrence similaire où une utilisatrice ou un utilisateur autorisé ou non autorisé accède ou accède potentiellement à une telle information à une fin qui n'est pas autorisée.

Si l'incident comprend une atteinte à la sécurité des renseignements personnels, il est nécessaire d'aviser le responsable du contrat.

Références

Source du contrôle : IR-04
Publications connexes :

- Centre pour la cybersécurité, *Élaborer un plan d'intervention en cas d'incident* (ITSAP.40.003)
- *NIST SP 800-61 Computer Security Incident Handling Guide* (en anglais seulement)
- *NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (en anglais seulement)

03.06.02 Surveillance des incidents, signalement des incidents et assistance en cas d'incident

A. Faire le suivi et documenter les incidents de sécurité du système.

B. Signaler les incidents soupçonnés à l'équipe d'intervention en cas d'incident de l'organisation dans une période de [Affectation : période définie par l'organisation].

C. Donner de l'information sur l'incident à [Affectation : autorités définies par l'organisation].

D. Fournir une ressource de soutien pour l'intervention en cas d'incident qui offre des conseils et de l'assistance aux utilisatrices et utilisateurs du système pour ce qui est du traitement et du signalement des incidents.

Discussion

La documentation des incidents comprend la tenue de dossiers au sujet de chaque incident, l'état de l'incident et toute autre information pertinente aux fins d'investigation informatique, ainsi que l'évaluation des détails, des tendances et du traitement des incidents. L'information relative à un incident peut provenir de diverses sources, y compris la surveillance réseau, les rapports d'incident, les équipes d'intervention en cas d'incident, les plaintes d'utilisatrices et utilisateurs, les partenaires de la chaîne d'approvisionnement, la surveillance des vérifications, la surveillance des accès physiques et les rapports d'utilisateur et d'administrateur. L'exigence Traitement des incidents 03.06.01 fournit de l'information sur les types d'incidents qui sont appropriés pour la surveillance. Les types d'incidents signalés, le contenu et la rapidité des signalements, ainsi que les autorités de signalement doivent refléter les lois, les décrets, les directives, la réglementation, les politiques, les normes et les lignes directrices applicables. Les renseignements sur l'incident informent les évaluations des risques, l'efficacité des évaluations de la sécurité et de la confidentialité, les exigences de sécurité pour l'acquisition et les critères de sélection pour les produits technologiques. Les ressources de soutien fournies par les organisations pour l'intervention en cas d'incident comprennent les services de dépannage, les groupes d'assistance, les systèmes automatisés de demandes de service pour l'ouverture et le suivi des demandes d'intervention en cas d'incident, et l'accès aux services d'investigation informatique ou aux services de recours des consommatrices et consommateurs, au besoin.

Références

Sources des contrôles : IR-05, IR-06 et IR-07
Publications connexes :

- *NIST SP 800-61 Computer Security Incident Handling Guide* (en anglais seulement)
- *NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response* (en anglais seulement)
- Centre pour la cybersécurité, *Élaborer un plan d'intervention en cas d'incident* (ITSAP.40.003)

03.06.03 Tests d'intervention en cas d'incident

Tester l'efficacité des capacités d'intervention en cas d'incident tous les [Affectation : fréquence définie par l'organisation].

Discussion

Les organisations doivent tester les capacités d'intervention en cas d'incident afin de déterminer leur efficacité et d'identifier les faiblesses ou les lacunes potentielles. Les tests d'intervention en cas d'incident incluent l'utilisation de listes de vérification, les exercices de revue générale, les exercices de table et les simulations. Les tests d'intervention en cas d'incident peuvent comprendre la détermination des effets de l'intervention en cas d'incident sur les opérations de l'organisation, les actifs organisationnels et les personnes. Des données qualitatives et quantitatives peuvent aider à déterminer l'efficacité des processus d'intervention en cas d'incident.

Références

Source du contrôle : IR-03
Publications connexes : *NIST SP 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* (en anglais seulement)

03.06.04 Formation d'intervention en cas d'incident

A. Fournir une formation pour intervenir en cas d'incident aux utilisatrices et utilisateurs du système en fonction des rôles et des responsabilités attribués :

   1. dans un délai de [Affectation : période définie par l'organisation] après avoir été affecté à un rôle ou à des responsabilités d'intervention en cas d'incident ou après avoir obtenu l'accès au système;
   2. lorsque des changements apportés au système l'exigent;
   3. tous les [Affectation : fréquence définie par l'organisation] par la suite.

B. Examiner et mettre à jour le contenu de la formation d'intervention en cas d'incident tous les [Affectation : fréquence définie par l'organisation] et à la suite de [Affectation : événements définis par l'organisation].

Discussion

La formation d'intervention en cas d'incident est associée à des responsabilités et à des rôles affectés au personnel de l'organisation afin d'assurer un contenu et un niveau de détails appropriés. Par exemple, les utilisatrices et utilisateurs peuvent avoir seulement besoin de connaître avec qui communiquer ou comment reconnaître un incident; les administratrices et administrateurs de système peuvent nécessiter de la formation supplémentaire sur le traitement des incidents; et les intervenantes et intervenants en cas d'incident pourraient recevoir de la formation sur les techniques d'investigation informatique, de collecte de données, de signalement, de reprise et de restauration des systèmes. La formation d'intervention en cas d'incident comprend la formation offerte aux utilisatrices et utilisateurs pour reconnaître et signaler les activités suspectes provenant de sources externes ou internes. La formation d'intervention en cas d'incident pour les utilisatrices et utilisateurs peut être fournie dans le cadre de l'exigence Formation selon le rôle 03.02.02. Les événements qui peuvent nécessiter une mise à jour du

contenu de la formation d'intervention en cas d'incident comprennent la mise à l'essai du plan d'intervention en cas d'incident, l'intervention à la suite d'un incident réel, les résultats d'une évaluation ou d'une vérification, ou les changements apportés aux lois, aux décrets, aux politiques, aux directives, à la réglementation, aux normes ou aux lignes directrices applicables.

Références

Source du contrôle : IR-02
Publications connexes :

- *NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response* (en anglais seulement)
- *NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (en anglais seulement)

03.06.05 Plan d'intervention en cas d'incident

A. Élaborer un plan d'intervention en cas d'incident qui :

1. fournit à l'organisation une feuille de route pour la mise en œuvre de ses capacités d'intervention en cas d'incident;
2. décrit la structure et l'organisation des capacités d'intervention en cas d'incident;
3. fournit une approche de haut niveau indiquant comment les capacités d'intervention en cas d'incident s'intègrent à l'organisation en général;
4. définit les incidents devant être signalés;
5. décrit les modalités d'échange d'information en cas d'incident;
6. désigne les responsabilités pour les entités, le personnel et les rôles organisationnels.

B. Distribuer des copies des plans d'intervention en cas d'incident au personnel responsable de l'intervention en cas d'incident désigné (identifié par nom ou rôle) et aux équipes organisationnelles.

C. Mettre à jour le plan d'intervention en cas d'incident afin de tenir compte des changements apportés aux systèmes et des changements organisationnels, ou encore des problèmes rencontrés durant la mise en œuvre, l'exécution ou la mise à l'essai du plan d'intervention.

D. Protéger le plan d'intervention en cas d'incident des divulgations non autorisées.

Discussion

Il est important que les organisations élaborent et mettent en œuvre une approche d'intervention coordonnée en cas d'incident. Les fonctions liées à la mission et aux activités de l'organisation déterminent la structure des capacités d'intervention en cas d'incident. Dans le cadre des capacités d'intervention en cas d'incident, les organisations doivent considérer la coordination et l'échange d'information avec des organisations externes, y compris des fournisseurs de services et d'autres organisations participant à la chaîne d'approvisionnement.

Références

Source du contrôle : IR-08
Publications connexes :

- Centre pour la cybersécurité, *Élaborer un plan d'intervention en cas d'incident* (ITSAP.40.003)
- Sécurité publique Canada, *Élaboration d'un plan d'intervention en cas d'incident de la technologie opérationnelle et de la technologie de l'information*
- Justice Canada, *Règlement sur les atteintes aux mesures de sécurité* (DORS/2018-64)

3.7 Maintenance

Les contrôles de maintenance appuient la maintenance périodique et opportune des systèmes organisationnels et fournissent des contrôles efficaces pour les outils, les techniques, les mécanismes et le personnel employés pour mener la maintenance des systèmes afin d'assurer leur disponibilité continue.

03.07.01 Non affecté

Retiré par le NIST.

03.07.02 Non affecté

Retiré par le NIST.

03.07.03 Non affecté

Retiré par le NIST.

03.07.04 Outils de maintenance

A. Approuver, contrôler et surveiller l'utilisation des outils de maintenance des systèmes.

B. Vérifier les supports où sont stockés les programmes de diagnostic et de test afin de détecter la présence de code malveillant, avant d'utiliser les supports dans les systèmes.

C. Prévenir le retrait d'équipement de maintenance de système qui pourrait contenir de l'information désignée et vérifier qu'il ne contient pas une telle information, en procédant à des opérations de nettoyage ou de destruction de l'équipement ou encore en conservant l'équipement dans l'installation.

Discussion

L'approbation, le contrôle, la surveillance et l'examen des outils de maintenance permettent de traiter les problèmes de sécurité en lien avec les outils servant aux activités de diagnostic et de réparation sur le système. Les outils de maintenance peuvent comprendre l'équipement de test et de diagnostic matériel ou logiciel, ainsi que les renifleurs de paquets. Les outils peuvent être préinstallés, transportés par le personnel de maintenance sur des supports, basés sur le nuage ou téléchargés à partir de sites Web. Les programmes de diagnostic et de test peuvent contenir du code malveillant et le livrer au système, intentionnellement ou non. Les supports peuvent être inspectés notamment en vérifiant le hachage cryptographique ou les signatures numériques des programmes de diagnostic et de test, ainsi que des supports.

Si les organisations, lors de l'inspection d'un support qui contient des programmes de diagnostic et de test, déterminent que le support contient également du code malveillant, l'incident doit être traité conformément aux stratégies et aux procédures de traitement des incidents. Un examen périodique des outils de maintenance peut mener au retrait de l'approbation d'outils désuets, non pris en charge, non pertinents ou inutilisés. Les outils de maintenance ne concernent pas les composants matériels et logiciels qui appuient la maintenance et sont considérés comme faisant partie du système.

Références

Sources des contrôles : MA-03, MA-03(01), MA-03(02) et MA-03(03)
Publications connexes : Centre pour la cybersécurité, *Nettoyage des supports de TI* (ITSP.40.006)

03.07.05 Maintenance non locale

A. Approuver et surveiller les activités de maintenance et de diagnostic non locales.

B. Mettre en œuvre des mécanismes d'authentification multifacteur et résistant à la réinsertion lors de l'établissement des sessions de maintenance et de diagnostic non locales.

C. Mettre fin aux sessions et aux connexions réseau lorsque la maintenance non locale est terminée.

Discussion

Les activités de maintenance et de diagnostic non locales sont menées par des personnes qui communiquent à partir de réseaux externes ou internes. Les activités de maintenance et de diagnostic locales sont menées par des personnes qui se trouvent physiquement à l'emplacement du système et qui ne communiquent pas au moyen d'une connexion réseau. Les techniques d'authentification servant à établir des sessions de maintenance et de diagnostic non locales sont traitées dans l'exigence Identification, authentification et réauthentification des utilisatrices et utilisateurs 03.05.01.

Références

Source du contrôle : MA-04
Publications connexes :

- Centre pour la cybersécurité, *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information* (ITSP.30.031)
- Centre pour la cybersécurité, *Nettoyage des supports de TI* (ITSP.40.006)
- Centre pour la cybersécurité, *Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA)* (ITSAP.30.018)

03.07.06 Personnel de maintenance

A. Établir un processus pour l'autorisation du personnel de maintenance.

B. Maintenir une liste des organisations ou du personnel autorisés pour la maintenance.

C. Vérifier que le personnel non accompagné réalisant des activités de maintenance sur le système dispose des autorisations d'accès nécessaires.

D. Désigner des membres du personnel de l'organisation qui possèdent les autorisations d'accès et les compétences techniques nécessaires pour superviser les activités de maintenance effectuées par le personnel qui ne possède pas les autorisations d'accès appropriées.

Discussion

Le personnel de maintenance fait référence aux personnes qui réalisent les activités de maintenance matérielle ou logicielle sur le système, et l'exigence Autorisations d'accès physique 03.10.01 traite de l'accès physique des personnes devant réaliser des activités de maintenance qui les placent dans le périmètre de protection physique du système. La compétence technique de supervision des personnes est liée à la maintenance réalisée sur le système, tandis que la possession des autorisations d'accès appropriées est liée à la maintenance sur ou près du système. Les personnes qui n'ont pas été identifiées précédemment comme faisant partie du personnel de maintenance autorisé (par exemple, les fabricants, les consultantes et consultants, les intégratrices et intégrateurs de systèmes et les fournisseurs) pourraient avoir besoin d'un accès privilégié au système, par exemple dans les cas où la maintenance doit être réalisée avec peu ou sans préavis. Les organisations peuvent choisir d'émettre des justificatifs d'identité temporaires à ces personnes, en fonction de leurs évaluations des risques. Ces justificatifs peuvent être octroyés pour un accès unique ou pour un délai très limité.

Références

Source du contrôle : MA-05
Publications connexes : Aucune

3.8 Protection des supports

Les contrôles de protection des supports appuient la protection des supports du système tout au long du cycle de vie. Ils permettent de limiter l'accès à l'information sur les supports du système aux utilisatrices et utilisateurs autorisés et exigent un nettoyage ou une destruction des supports avant leur élimination ou leur réutilisation.

03.08.01 Entreposage des supports

Contrôler physiquement les supports du système contenant de l'information désignée et les entreposer de façon sécurisée.

Discussion

Les supports du système comprennent les supports numériques et non numériques. Les supports numériques comprennent les disquettes, les disques à mémoire flash, les bandes magnétiques, les disques durs ou à entraînement magnétique externes ou amovibles, les disques compacts et les disques numériques polyvalents (DVD pour *Digital Versatile Disc*). Les supports non numériques incluent le papier et les microfilms. Le contrôle physique des supports stockés comprend la conduite d'inventaires, l'établissement de procédures afin de permettre aux personnes d'emprunter et de retourner des supports dans la bibliothèque et préserver la responsabilisation des supports stockés. Le stockage sécurisé comprend les tiroirs, les armoires et les bureaux verrouillés ainsi que les bibliothèques de supports contrôlées. Les zones contrôlées fournissent des contrôles physiques et procéduraux afin de répondre aux exigences établies pour la protection de l'information et des systèmes. Les techniques de nettoyage (par exemple, l'effacement, la destruction et la purge cryptographiques) préviennent la divulgation d'information désignée à des personnes non autorisées. Le processus de nettoyage retire l'information désignée des supports de façon à ce que l'information ne puisse pas être récupérée ou reconstruite.

Références

Source du contrôle : MP-04
Publications connexes :

- *NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices* (en anglais seulement)
- Centre pour la cybersécurité, *Nettoyage des supports de TI* (ITSP.40.006)

03.08.02 Accès aux supports

Restreindre l'accès à l'information désignée qui se trouve sur les supports du système au personnel ou aux rôles autorisés.

Discussion

Les supports du système comprennent les supports numériques et non numériques. L'accès à l'information désignée sur un support du système peut être restreint en contrôlant physiquement le support. Le contrôle physique des supports du système comprend la conduite d'inventaires, l'établissement de procédures afin de permettre aux personnes d'emprunter et de retourner des supports dans la bibliothèque et de préserver la responsabilisation des supports stockés. Dans le cas des supports numériques, l'accès à l'information désignée peut être restreint en ayant recours à des moyens de chiffrement. Le chiffrement de données stockées ou au repos est traité dans l'exigence Confidentialité lors de la transmission et du stockage 03.13.08.

Références

Source du contrôle : MP-02
Publications connexes : *NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices* (en anglais seulement)

03.08.03 Nettoyage des supports

Nettoyer les supports du système qui contiennent de l'information désignée avant leur élimination ou leur transfert hors du contrôle de l'organisation ou aux fins de réutilisation.

Discussion

Le nettoyage des supports s'applique aux supports numériques et non numériques sujets à une élimination ou à une réutilisation, qu'ils soient considérés comme amovibles ou non. Il peut s'agir, par exemple, de supports numériques qui se trouvent dans les numériseurs, les photocopieurs, les imprimantes, les ordinateurs blocs-notes, les postes de travail, les appareils mobiles, les composants réseau et les supports non numériques. Le processus de nettoyage retire l'information désignée des supports de façon à ce que l'information ne puisse pas être récupérée ou reconstruite. Les techniques de nettoyage (par exemple, l'effacement, la destruction et la purge cryptographiques) préviennent la divulgation d'information désignée à des personnes non autorisées lorsque les supports sont réutilisés ou transférés aux fins d'élimination. Le Centre pour la cybersécurité et la GRC soutiennent les normes pour le contrôle des processus de nettoyage des supports contenant de l'information désignée et peuvent exiger la destruction des supports lorsque d'autres méthodes ne peuvent pas être appliquées aux supports.

Références

Source du contrôle : MP-06
Publications connexes :

- Centre pour la cybersécurité, *Nettoyage des supports de TI* (ITSP.40.006)
- GRC, *Guide d'équipement de sécurité* (G1-001) (réservé au GC)

03.08.04 Marquage des supports

Marquer les supports du système contenant de l'information désignée afin d'indiquer les limites de distribution, les mises en garde concernant le traitement et les marquages applicables d'une telle information.

Discussion

Les supports du système comprennent les supports numériques et non numériques. Le marquage désigne l'utilisation ou l'application d'attributs de sécurité lisibles par les humains. L'étiquetage désigne l'utilisation d'attributs de sécurité liés aux structures de données internes du système. Les supports numériques comprennent les disquettes, les bandes magnétiques, les disques durs ou à entraînement magnétique externes ou amovibles, les disques à mémoire flash, les disques compacts et les disques numériques polyvalents (DVD). Les supports non numériques incluent le papier et les microfilms. L'information désignée comprend toute information autre que classifiée qu'une autorité du GC désigne et mentionne dans un contrat comme devant faire l'objet d'une sauvegarde.

Références

Source du contrôle : MP-03
Publications connexes : Aucune

03.08.05 Transport des supports

A. Protéger et contrôler les supports du système contenant de l'information désignée durant le transport à

l'extérieur des zones contrôlées.

B. Demeurer responsable des supports du système contenant de l'information désignée durant le transport à l'extérieur des zones contrôlées.

C. Documenter les activités associées au transport des supports du système contenant de l'information désignée.

Discussion

Les supports du système comprennent les supports numériques et non numériques. Les supports numériques incluent les disquettes, les disques à mémoire flash, les bandes magnétiques, les disques durs ou à entraînement magnétique externes ou amovibles, les disques compacts et les DVD. Les supports non numériques incluent le papier et les microfilms. Les zones contrôlées sont des espaces dans lesquels les organisations appliquent des mesures physiques ou procédurales afin de respecter les exigences établies pour la protection de l'information et des systèmes en particulier. La protection des supports durant le transport peut comprendre la cryptographie et/ou des contenants verrouillés. Les activités associées au transport des supports comprennent la remise des supports aux fins de transport, la vérification que les supports suivent les processus de transport adéquats et le transport en tant que tel. Le personnel autorisé responsable du transport et de la messagerie peut inclure des personnes de l'extérieur de l'organisation. Préserver la responsabilisation des supports durant le transport comprend la restriction des activités de transport au personnel autorisé et le suivi ou l'obtention des enregistrements officiels des activités de transport, à mesure que les supports se déplacent dans le système de transport, afin de prévenir et de détecter les pertes, les destructions ou les modifications. Cette exigence est associée aux exigences Confidentialité lors de la transmission et du stockage 03.13.08 et Protection cryptographique 03.13.11.

Références

Sources des contrôles : MP-05 et SC-28
Publications connexes : *NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices* (en anglais seulement)

03.08.06 Non affecté

Retiré par le NIST.

03.08.07 Utilisation des supports

A. Limiter ou interdire l'utilisation de [Affectation : types de supports définis par l'organisation].

B. Interdire l'utilisation de supports amovibles sans la présence d'un propriétaire identifiable.

Discussion

Contrairement à l'exigence Entreposage des supports 03.08.01, qui restreint l'accès des utilisatrices et utilisateurs aux supports, cette exigence limite ou interdit l'utilisation de certains types de supports, comme les disques durs externes, les disques à mémoire flash ou les écrans intelligents. Les organisations peuvent utiliser des mesures techniques et non techniques (par exemple, des stratégies, des procédures et des règles de conduite) afin de contrôler l'utilisation des supports du système. Par exemple, les organisations peuvent contrôler l'utilisation des dispositifs de stockage portatifs en installant des cages sur les postes de travail afin d'empêcher l'accès aux ports externes ou encore désactiver ou retirer la possibilité d'insertion, de lecture ou d'écriture de dispositifs.

Les organisations peuvent limiter l'utilisation des dispositifs de stockage portatifs à ceux approuvés, y compris les dispositifs fournis par l'organisation, les dispositifs fournis par d'autres organisations approuvées et les dispositifs qui n'appartiennent pas aux personnes. Les organisations peuvent aussi contrôler l'utilisation des dispositifs de stockage portatifs en fonction du type de dispositif, en empêchant l'utilisation de dispositifs portatifs inscriptibles, et mettre en œuvre cette restriction en désactivant ou en retirant la capacité d'écriture sur ces dispositifs. Les

limites ayant trait à l'utilisation des supports de systèmes contrôlés par l'organisation dans les systèmes externes incluent les restrictions sur la façon dont les supports peuvent être utilisés et les conditions associées. En attribuant des propriétaires identifiables (par exemple, des personnes, des organisations ou des projets) aux supports système amovibles, les organisations réduisent les risques liés à l'utilisation de ces technologies puisqu'ils savent à qui attribuer la responsabilité en cas de vulnérabilité connue des supports (par exemple, l'insertion de code malveillant).

Références

Source du contrôle : MP-07
Publications connexes : *NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices* (en anglais seulement)

03.08.08 Non affecté

Retiré par le NIST.

03.08.09 Sauvegarde du système – Protection cryptographique

A. Protéger la confidentialité de l'information sauvegardée.

B. Mettre en œuvre des mécanismes cryptographiques afin d'empêcher la divulgation non autorisée d'information désignée aux emplacements de stockage des sauvegardes.

Discussion

La sélection de mécanismes cryptographiques est fondée sur le besoin de protéger la confidentialité de l'information sauvegardée. Les dispositifs avec module de sécurité matériel (HSM pour *Hardware Security Module*) protègent et gèrent les clés cryptographiques et offrent des fonctions de traitement cryptographique. Les opérations cryptographiques (par exemple, le chiffrement, le déchiffrement, et la génération et la vérification de signature) sont typiquement hébergées sur le dispositif HSM, et plusieurs mises en œuvre offrent des mécanismes d'accélération par matériel pour les opérations cryptographiques. Cette exigence est associée à l'exigence Protection cryptographique 03.13.11.

Références

Sources des contrôles : CP-09 et CP-09(08)
Publications connexes :

- *NIST SP 800-34 Contingency Planning Guide for Federal Information Systems* (en anglais seulement)
- *NIST SP 800-130 A Framework for Designing Cryptographic Key Management Systems* (en anglais seulement)

3.9 Sécurité du personnel

Les contrôles de sécurité du personnel appuient les procédures requises pour s'assurer que le personnel ayant accès aux systèmes dispose des autorisations nécessaires et des niveaux d'habilitation de sécurité appropriés. Ils contribuent à protéger l'information organisationnelle et les systèmes durant et après les opérations du personnel, par exemple après une cessation d'emploi ou une mutation.

03.09.01 Filtrage de sécurité du personnel

A. Procéder au filtrage de sécurité des personnes avant de leur accorder l'accès au système.

B. Procéder à nouveau au filtrage de sécurité des personnes conformément à [Affectation : conditions nécessitant

un nouveau filtrage de sécurité définies par l'organisation].

Discussion

Les activités de filtrage de sécurité du personnel comprennent l'évaluation de la conduite, de l'intégrité, du jugement, de la loyauté, de la fiabilité et de la stabilité d'une personne (c'est-à-dire l'établissement de la fiabilité) avant d'accorder l'accès au système ou d'élever le niveau d'accès au système. Les activités de filtrage et de refiltrage de sécurité doivent refléter les lois, les décrets, les directives, les politiques, la réglementation et les critères fédéraux établis pour le niveau d'accès requis en fonction du poste concerné.

Références

Source du contrôle : PS-03
Publications connexes :

- *NIST SP 800-181 Workforce Framework for Cybersecurity (NICE Framework)* (en anglais seulement)
- SPAC, *Manuel de la sécurité des contrats*

03.09.02 Cessation d'emploi et mutation de personnel

A. Après la cessation d'emploi d'une personne :

1. désactiver l'accès au système dans une période de [Affectation : période définie par l'organisation];
2. mettre fin ou révoquer les authentifiants et les justificatifs d'identité associés à la personne;
3. récupérer les propriétés système associées à la sécurité.

B. Après la mutation d'une personne à un autre poste au sein de l'organisation :

1. examiner et confirmer le besoin opérationnel continu pour les autorisations d'accès logiques et physiques au système et aux installations;
2. modifier les autorisations d'accès afin de tenir compte des changements opérationnels nécessaires.

Discussion

Les propriétés système associées à la sécurité incluent les jetons d'authentification matériels, les manuels techniques d'administration de système, les clés, les cartes d'identité et les laissez-passer d'immeuble. Les entrevues de départ permettent de s'assurer que les personnes comprennent les contraintes de sécurité auxquelles elles doivent se soumettre à titre d'anciennes et anciens membres du personnel et leur responsabilité à l'égard des biens de l'organisation. Les sujets abordés lors des entrevues de départ incluent les rappels concernant les éventuelles limitations professionnelles dont ils pourraient faire l'objet et les ententes de non-divulgation. Il se peut qu'il soit impossible de procéder aux entrevues de départ pour certaines employées et certains employés, y compris dans les cas de non-disponibilité des superviseures et superviseurs, de maladie ou d'abandon de poste.

Une exécution rapide des mesures de cessation d'emploi est essentielle dans les cas de congédiement pour motif valable. Les organisations peuvent considérer la désactivation des comptes d'une personne qui a été congédiée avant d'en aviser la personne. Cette exigence s'applique dans les cas de réaffectation ou de mutation d'individus, lorsque la mesure est permanente ou si la durée est suffisamment longue pour nécessiter une protection. Les mesures de protection qui peuvent être requises en cas de mutation ou de réaffectation à un autre poste au sein de l'organisation incluent le retour des anciens laissez-passer, cartes d'identité et clés et l'émission de nouveaux laissez-passer d'immeuble, cartes d'identité et clés; le changement des autorisations d'accès au système (c'est-à-dire les privilèges); la fermeture des comptes système et l'établissement de nouveaux comptes; et le déblocage de l'accès aux documents officiels auxquels la personne avait accès à l'emplacement de travail précédent et des comptes système précédents.

Références

Sources des contrôles : PS-04 et PS-05
Publications connexes : Aucune

3.10 Protection physique

Les contrôles de protection matérielle appuient le contrôle de l'accès physique des personnes autorisées aux systèmes, à l'équipement et aux environnements d'exploitation respectifs. Ils favorisent la protection des installations physiques et des infrastructures des systèmes ainsi que la protection des systèmes contre les dangers environnementaux. Ils fournissent également des contrôles environnementaux appropriés pour les installations hébergeant des systèmes.

03.10.01 Autorisations d'accès physique

A. Développer, approuver et tenir une liste des personnes disposant d'un accès autorisé à l'emplacement physique où se trouvent les systèmes.

B. Émettre des justificatifs d'identité pour autoriser l'accès physique.

C. Examiner la liste d'accès physique tous les [Affectation : fréquence définie par l'organisation].

D. Retirer les personnes de la liste d'accès aux installations lorsqu'un tel accès n'est plus nécessaire.

Discussion

Une installation peut comprendre un ou plusieurs emplacements physiques hébergeant des systèmes ou des composants de systèmes servant à traiter, à stocker ou à transmettre de l'information désignée. Les autorisations d'accès physique s'appliquent au personnel, aux visiteuses et aux visiteurs. Les personnes avec des justificatifs d'identité d'autorisation d'accès physique permanents ne sont pas considérées comme des visiteuses et visiteurs. Les justificatifs d'autorisation comprennent les laissez-passer, les cartes d'identité et les cartes à puce. Les organisations doivent déterminer la force des justificatifs d'identité d'autorisation en fonction des lois, des décrets, des directives, de la réglementation, des politiques, des normes et des lignes directrices applicables. Il se peut que les autorisations d'accès physique ne soient pas nécessaires pour accéder à certaines zones dans les installations qui sont désignées comme zones d'accès public.

Références

Source du contrôle : PE-02
Publications connexes : Aucune

03.10.02 Surveillance de l'accès physique

A. Surveiller l'accès physique aux installations où se trouvent les systèmes afin de détecter et d'intervenir en cas d'incident de sécurité physique.

B. Examiner les journaux d'accès physique tous les [Affectation : fréquence définie par l'organisation] et à la suite de [Affectation : événements ou indications potentielles d'événement définis par l'organisation].

Discussion

Une installation peut comprendre un ou plusieurs emplacements physiques hébergeant des systèmes ou des composants de systèmes servant à traiter, à stocker ou à transmettre de l'information désignée. La surveillance de l'accès physique s'applique aux zones à accès public dans les installations de l'organisation. Elle peut être effectuée par des gardes de sécurité, de l'équipement de vidéosurveillance (c'est-à-dire les caméras) et des capteurs. L'examen des journaux d'accès physique peut aider à repérer les activités suspectes, les événements

anormaux ou les menaces. Les examens peuvent être appuyés par les contrôles de journalisation des données de vérification si les journaux d'accès font partie d'un système automatisé. Les capacités d'intervention en cas d'incident incluent les enquêtes associées aux incidents de sécurité physique et les interventions connexes. Les incidents incluent les violations de sécurité et les activités d'accès physique suspectes, comme les accès hors des heures normales de travail, les accès répétés aux zones auxquelles on n'accède pas normalement, les accès d'une durée anormalement longue et les accès ne respectant pas l'ordre établi.

Références

Source du contrôle : PE-06
Publications connexes : Aucune

03.10.03 Non affecté

Retiré par le NIST.

03.10.04 Non affecté

Retiré par le NIST.

03.10.05 Non affecté

Retiré par le NIST.

03.10.06 Autres lieux de travail

A. Déterminer les autres lieux où le personnel peut travailler.

B. Utiliser les exigences de sécurité suivantes pour les autres lieux de travail : [Affectation : exigences de sécurité définies par l'organisation].

Discussion

Les autres lieux de travail incluent les résidences privées des membres du personnel ou d'autres installations désignées par l'organisation. Les autres lieux de travail peuvent être des emplacements de travail facilement accessibles pour les opérations d'urgence. Les organisations peuvent définir des exigences de sécurité différentes pour d'autres lieux de travail ou types de lieux particuliers, en fonction des activités liées au travail menées sur ces lieux. Évaluer l'efficacité des exigences et fournir un moyen de communication des incidents aux autres lieux de travail permettront d'appuyer les activités de planification d'urgence des organisations.

Références

Source du contrôle : PE-17
Publications connexes :

- Centre pour la cybersécurité, *Sécurité des appareils des utilisateurs finaux pour les modèles de déploiement Prenez vos appareils personnels (PAP)* (ITSM.70.003)
- *NIST SP 800-46 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (en anglais seulement)
- *NIST SP 800-114 User's Guide to Telework and Bring Your Own Device (BYOD) Security* (en anglais seulement)

03.10.07 Contrôle d'accès physique

A. Appliquer les autorisations d'accès physique aux points d'entrée et de sortie des installations où se trouvent les systèmes au moyen de ce qui suit :

   1. vérification des autorisations d'accès physique avant d'accorder l'accès aux installations;
   2. contrôle des points d'entrée et de sortie au moyen de systèmes de contrôle d'accès physique, de dispositifs ou de gardes.

B. Tenir des journaux de vérification d'accès physique pour les points d'entrée et de sortie.

C. Accompagner les visiteuses et visiteurs et contrôler leurs activités.

D. Fournir des clés sécurisées, des cadenas ou d'autres dispositifs d'accès physique.

E. Contrôler l'accès physique des dispositifs de sortie afin d'empêcher les personnes non autorisées d'obtenir l'accès à l'information désignée.

Discussion

Cette exigence traite des emplacements physiques hébergeant des systèmes ou des composants de systèmes qui assurent le traitement, le stockage ou la transmission de l'information désignée. Les organisations doivent déterminer le type de garde nécessaire, y compris le personnel de sécurité professionnel ou le personnel administratif. Les dispositifs de contrôle d'accès physique comprennent les clés, les verrous, les cadenas, les lecteurs biométriques et les lecteurs de cartes. Les systèmes de contrôle d'accès physique doivent être conformes aux lois, aux décrets, aux directives, aux politiques, à la réglementation, aux normes et aux lignes directrices applicables. Les organisations peuvent employer les types de journaux de vérification de leur choix. Les journaux de vérification peuvent être procéduraux, automatisés ou une combinaison des deux. Les points d'accès physique peuvent inclure les points d'accès extérieurs, les points d'accès intérieurs aux systèmes qui exigent des contrôles d'accès supplémentaires ou les deux. Les contrôles d'accès physique s'appliquent au personnel, aux visiteuses et aux visiteurs. Les personnes avec des autorisations d'accès physique permanentes ne sont pas considérées comme des visiteuses et visiteurs.

Les contrôles de l'accès physique aux dispositifs de sortie incluent l'entreposage des dispositifs de sortie dans des pièces verrouillées ou d'autres zones sécurisées dotées d'un contrôle d'accès avec clavier numérique ou lecteur de cartes et auxquelles seules les personnes autorisées peuvent accéder, l'entreposage des dispositifs de sortie dans des emplacements pouvant être surveillés par le personnel, l'installation de filtres d'écran et l'utilisation de casques d'écoute. Les écrans, les imprimantes, les numériseurs, les télécopieurs, les dispositifs audio et les photocopieurs sont des exemples de dispositifs de sortie.

Références

Sources des contrôles : PE-03 et PE-05
Publications connexes : Aucune

03.10.08 Contrôle d'accès pour la transmission

Contrôler l'accès physique aux lignes de distribution et de transmission des systèmes dans les installations de l'organisation.

Discussion

Les mesures de protection appliquées aux lignes de distribution et de transmission des systèmes permettent de prévenir les dommages accidentels, les pannes et les modifications physiques. De telles mesures peuvent également être nécessaires afin d'éviter l'écoute clandestine ou la modification des transmissions non chiffrées. Les mesures de protection servant à contrôler l'accès physique aux lignes de distribution et de transmission des systèmes incluent la déconnexion ou le verrouillage des connecteurs non utilisés, le verrouillage des armoires de câblage, la protection du câblage par des conduits ou des chemins de câbles et l'écoute électronique des

capteurs.

Références

Source des contrôles et des activités : PE-04
Publications connexes : Aucune

3.11 Évaluation des risques

Les contrôles d'évaluation des risques appuient la conduite périodique d'évaluations des risques, y compris les évaluations des facteurs relatifs à la vie privée, qui peuvent découler de l'exploitation des systèmes organisationnels ou du traitement, du stockage ou de la transmission de données et d'information.

03.11.01 Évaluation des risques

A. Évaluer le risque (y compris les risques associés à la chaîne d'approvisionnement) de divulgation non autorisée résultant de la gestion, du traitement, du stockage ou de la transmission de l'information désignée.

B. Mettre à jour les évaluations des risques tous les [Affectation : fréquence définie par l'organisation].

Discussion

L'établissement du périmètre du système est une condition préalable pour évaluer les risques de divulgation non autorisée d'information désignée. Les évaluations des risques doivent prendre en compte les menaces, les vulnérabilités, les probabilités et les impacts sur les activités et les actifs organisationnels, en fonction de l'exploitation et de l'utilisation du système, et de la divulgation non autorisée d'information désignée. Les évaluations des risques doivent également considérer les risques provenant des parties externes (par exemple, les entrepreneurs exploitant les systèmes au nom de l'organisation, les fournisseurs de services, les personnes accédant aux systèmes et les sous-traitants). Elles peuvent être menées au niveau de l'organisation, des processus liés à la mission ou aux activités, ou des systèmes, ainsi qu'à n'importe quelle phase du cycle de développement des systèmes. Les évaluations des risques incluent les risques liés à la chaîne d'approvisionnement et associés aux fournisseurs ou aux entrepreneurs ainsi qu'au système, au composant de système ou au service connexe qu'ils fournissent.

Références

Sources des contrôles et des activités : RA-03, RA-03(01) et SR-06
Publications connexes :

- CST et GRC, *Méthodologie harmonisée d'évaluation des menaces et des risques (EMR-1)*
- Centre pour la cybersécurité, *La cybersécurité et la chaîne d'approvisionnement : évaluation des risques* (ITSAP.10.070)
- Centre pour la cybersécurité, *Sécurité de la chaîne d'approvisionnement pour les petites et moyennes organisations* (ITSAP.00.070)
- *NIST SP 800-30 Guide for Conducting Risk Assessments* (en anglais seulement)
- *NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (en anglais seulement)

03.11.02 Surveillance et analyse des vulnérabilités

A. Surveiller et analyser les vulnérabilités du système tous les [Affectation : fréquence définie par l'organisation] et lorsque de nouvelles vulnérabilités affectant le système sont identifiées.

B. Corriger les vulnérabilités du système dans une période de [Affectation : délais d'exécution définis par

l'organisation].

C. Mettre à jour la liste des vulnérabilités du système à analyser tous les [Affectation : fréquence définie par l'organisation] et lorsque de nouvelles vulnérabilités sont identifiées et signalées.

Discussion

Les organisations doivent déterminer l'analyse des vulnérabilités requise pour les composants du système et s'assurer que les sources potentielles de vulnérabilités (par exemple, les imprimantes, les numériseurs et les photocopieurs en réseau) ne sont pas ignorées. Les analyses de vulnérabilités des logiciels sur mesure peuvent nécessiter des mesures supplémentaires, comme des analyses statistiques, dynamiques ou binaires. Les organisations peuvent utiliser ces mesures dans les examens de code source et les outils (par exemple, les outils d'analyse statique, les analyseurs d'application Web et des analyseurs binaires). L'analyse des vulnérabilités comprend l'analyse des niveaux de correctifs; l'analyse des fonctions, des ports, des protocoles et des services qui ne doivent pas être accessibles aux utilisatrices et utilisateurs ou aux dispositifs; et l'analyse des mécanismes de contrôle de flux mal configurés ou défectueux.

Afin de faciliter l'interopérabilité, les organisations doivent considérer l'utilisation d'outils d'analyse qui expriment les vulnérabilités selon la convention d'appellation des vulnérabilités et expositions courantes (CVE pour *Common Vulnerabilities and Exposures*). Les sources d'information sur les vulnérabilités incluent la liste des lacunes courantes (CWE pour *Common Weakness Enumeration*), la base de données nationale sur les vulnérabilités (NVD pour *National Vulnerability Database*) et le système de notation des vulnérabilités courantes (CVSS pour *Common Vulnerability Scoring System*).

Références

Sources pour les activités : RA-05 et RA-05(02)
Publications connexes :

- *NIST SP 800-40 Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology* (en anglais seulement)
- *NIST SP 800-53A Assessing Security and Privacy Controls in Information Systems and Organizations* (en anglais seulement)
- *NIST SP 800-70 National Checklist Program for IT Products: Guidelines for Checklist Users and Developers* (en anglais seulement)
- *NIST SP 800-115 Technical Guide to Information Security Testing and Assessment* (en anglais seulement)
- *NIST SP 800-126 The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3* (en anglais seulement)
- Centre pour la cybersécurité, *Les 10 mesures de sécurité des TI : No 2, Appliquer les correctifs aux systèmes d'exploitation et aux applications* (ITSM.10.096)

03.11.03 Non affecté

Retiré par le NIST.

03.11.04 Réponse aux risques

Prendre des mesures à l'égard des résultats des évaluations, des activités de surveillance et des vérifications de la sécurité.

Discussion

Cette exigence traite le besoin de déterminer une réaction appropriée aux risques avant de générer une entrée dans le plan d'action et des jalons (PAJ). Il peut être possible d'atténuer les risques immédiatement de sorte que

l'entrée dans le PAJ ne soit pas nécessaire. Toutefois, une entrée dans le PAJ doit être générée si la réponse aux risques consiste à atténuer les risques identifiés, mais s'il n'est pas possible de procéder à une atténuation immédiate.

Références

Source de l'activité : RA-07
Publications connexes :

- Centre pour la cybersécurité , *Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée* (ITSP.10.036)
- Centre pour la cybersécurité, *Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes* (ITSP.10.037)
- *NIST SP 800-160-1 Engineering Trustworthy Secure Systems* (en anglais seulement)

3.12 Évaluation de sécurité et surveillance

Les contrôles d'évaluation de sécurité et de surveillance traitent des évaluations de sécurité et des mécanismes de surveillance du système.

03.12.01 Évaluation de sécurité

Évaluer les exigences de sécurité et de confidentialité du système et son environnement d'exploitation tous les [Affectation : fréquence définie par l'organisation] afin de déterminer si les exigences sont satisfaites.

Discussion

En évaluant les exigences de sécurité et de confidentialité, les organisations doivent déterminer si les mesures de protection et les contre-mesures nécessaires sont correctement mises en œuvre, si elles fonctionnent comme prévu et si elles produisent le résultat escompté. Les évaluations de sécurité identifient les faiblesses et les lacunes du système et fournissent les renseignements essentiels nécessaires pour prendre des décisions en fonction des risques. Les rapports d'évaluation de sécurité et de confidentialité documentent les résultats de l'évaluation à un niveau de détails jugé suffisant par l'organisation pour assurer l'exactitude et l'exhaustivité des rapports. Les résultats des évaluations de sécurité sont présentés aux personnes ou aux rôles appropriés pour les types d'évaluations menées.

Références

Source de l'activité : CA-02
Publications connexes :

- Centre pour la cybersécurité, *Catalogue des activités d'assurance et des contrôles de sécurité et de confidentialité* (ITSP.10.033)
- Centre pour la cybersécurité , *Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée* (ITSP.10.036)
- Centre pour la cybersécurité, *Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes* (ITSP.10.037)
- CST et GRC, *Méthodologie harmonisée d'évaluation des menaces et des risques (EMR-1)*
- *NIST SP 800-115 Technical Guide to Information Security Testing and Assessment* (en anglais seulement)
- *NIST SP 800-53A Assessing Security and Privacy Controls in Information Systems and Organizations* (en anglais seulement)

03.12.02 Plans d'action et des jalons

A. Élaborer un plan d'action et des jalons (PAJ) pour le système dans le but de :

1. documenter les mesures correctives prévues pour corriger les faiblesses ou les lacunes établies lors des évaluations de sécurité;
2. réduire ou éliminer les vulnérabilités connues du système.

B. Mettre à jour les PAJ existants en fonction des résultats provenant des activités suivantes :

1. les évaluations de sécurité;
2. les vérifications ou examens;
3. la surveillance continue.

Discussion

Les PAJ sont des documents importants des programmes organisationnels de sécurité et de confidentialité. Les organisations ont recours à des PAJ pour décrire comment les exigences de sécurité non satisfaites seront respectées et comment les mesures d'atténuation prévues seront mises en œuvre. Les organisations peuvent documenter les plans de sécurité des systèmes et les PAJ en utilisant des documents séparés ou combinés, peu importe le format.

Références

Source de l'activité : CA-05
Publications connexes : Centre pour la cybersécurité , *Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée* (ITSP.10.036)

03.12.03 Surveillance continue

Élaborer et mettre en œuvre une stratégie de surveillance continue des systèmes qui comprend des activités continues d'évaluation de la sécurité et de surveillance.

Discussion

La surveillance continue du système facilite une sensibilisation permanente de la posture de sécurité et de confidentialité du système afin d'appuyer les décisions relatives à la gestion des risques. Les termes *continu* et *permanent* signifient que les organisations évaluent et surveillent leurs systèmes à une fréquence suffisante pour appuyer les décisions en fonction des risques. Différents types d'exigence de sécurité et de confidentialité peuvent exiger des fréquences de surveillance différentes.

Références

Source du contrôle : CA-07
Publications connexes :

- Centre pour la cybersécurité , *Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée* (ITSP.10.036)
- *NIST SP 800-115 Technical Guide to Information Security Testing and Assessment* (en anglais seulement)
- *NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (en anglais seulement)
- *NIST SP 800-53A Assessing Security and Privacy Controls in Information Systems and Organizations* (en anglais seulement)

03.12.04 Non affecté

Retiré par le NIST.

03.12.05 Échange d'information

A. Approuver et gérer l'échange d'information désignée entre le système et d'autres systèmes au moyen de [Sélection (un ou plusieurs) : ententes sur la sécurité des interconnexions; ententes sur la sécurité de l'échange d'information; ententes ou protocoles d'entente; ententes sur l'échange d'information; accords sur les niveaux de service; ententes avec les utilisatrices et utilisateurs; accords de non-divulgation].

B. Documenter, dans le cadre des ententes d'échange, les caractéristiques d'interface, les exigences de sécurité et de confidentialité ainsi que les responsabilités liées à chacun des systèmes.

C. Examiner et mettre à jour les ententes d'échange tous les [Affectation : fréquence définie par l'organisation].

Discussion

L'échange d'information s'applique aux échanges d'information entre deux ou plusieurs systèmes de l'organisation ou à l'extérieur de l'organisation. Les organisations doivent considérer les risques associés aux menaces nouvelles ou grandissantes qui peuvent être introduites lorsque les systèmes échangent de l'information avec d'autres systèmes qui peuvent avoir des exigences ou des stratégies de sécurité différentes. Les types d'ententes doivent être sélectionnés en fonction de facteurs comme la relation entre les organisations qui échangent de l'information (par exemple, d'un organisme gouvernemental à un autre, d'un organisme gouvernemental à une entreprise, d'une entreprise à une autre, d'un organisme gouvernemental ou d'une entreprise à un fournisseur de services, d'un organisme gouvernemental ou d'une entreprise à personne) et le niveau d'accès au système organisationnel par les utilisatrices et utilisateurs de l'autre système. Les types d'ententes peuvent inclure des ententes sur la sécurité de l'échange d'information, des ententes sur la sécurité des interconnexions, des ententes ou protocoles d'entente, des ententes sur l'échange d'information, des accords sur les niveaux de service ou d'autres types d'ententes.

Les organisations peuvent intégrer l'information des ententes dans des contrats officiels, en particulier pour les échanges d'information entre des ministères et organismes fédéraux et des organisations non fédérales (par exemple, des prestataires de services, des entrepreneures et entrepreneurs, des développeuses et développeurs de systèmes et des intégratrices et intégrateurs de systèmes). Les renseignements qui se trouvent dans les ententes d'échange incluent les caractéristiques d'interface, les exigences de sécurité et de confidentialité, les contrôles et les responsabilités pour chaque système.

Références

Source du contrôle : CA-03
Publications connexes :

- Centre pour la cybersécurité, *Exigences de base en matière de sécurité pour les zones de sécurité de réseau* (ITSP.80.022)
- Centre pour la cybersécurité, *Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones* (ITSG-38)
- *NIST SP 800-47 Managing the Security of Information Exchanges* (en anglais seulement)

3.13 Protection des systèmes et des communications

Les contrôles de protection des systèmes et des communications appuient les activités de surveillance, de contrôle et de protection des systèmes ainsi que les communications internes et externes des systèmes.

03.13.01 Protection de périmètre

A. Surveiller et contrôler les communications des interfaces externes gérées vers le système et des principales interfaces internes gérées au sein du système.

B. Mettre en œuvre des sous-réseaux pour les composants de systèmes à accès public qui sont séparés physiquement ou logiquement des réseaux internes.

C. Assurer la connexion des systèmes externes seulement au moyen d'interfaces gérées constituées de dispositifs de protection de périmètre organisés conformément à l'architecture de sécurité de l'organisation.

Discussion

Les interfaces gérées incluent les passerelles, les routeurs, les pare-feu, les analyseurs réseau de code malveillant, les systèmes de virtualisation et les tunnels chiffrés mis en œuvre au sein d'une architecture de sécurité. Les sous-réseaux qui sont séparés physiquement ou logiquement des réseaux internes sont appelés communément des zones démilitarisées (ZD) ou DMZ (pour *Demilitarized Zones*). La restriction ou l'interdiction d'interfaces au sein des systèmes organisationnels comprend la restriction du trafic Web externe vers les serveurs Web désignés dans des interfaces gérées et l'interdiction de la mystification d'adresses (internes et externes) pour les protocoles franchissant le périmètre.

Références

Source du contrôle : SC-07
Publications connexes :

- Centre pour la cybersécurité, *Exigences de base en matière de sécurité pour les zones de sécurité de réseau* (ITSP.80.022)
- Centre pour la cybersécurité, *Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones* (ITSG-38)
- Centre pour la cybersécurité, *Conseils sur la configuration sécurisée des protocoles réseau* (ITSP.40.062)
- *NIST SP 800-189 Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation* (en anglais seulement)
- *NIST SP 800-41 Guidelines on Firewalls and Firewall Policy* (en anglais seulement)
- *NIST SP 800-160-1 Engineering Trustworthy Secure Systems* (en anglais seulement)
- *NIST SP 800-125B Secure Virtual Network Configuration for Virtual Machine (VM) Protection* (en anglais seulement)
- *NIST SP 800-207 Zero Trust Architecture* (en anglais seulement)

03.13.02 Non affecté

Retiré par le NIST.

03.13.03 Non affecté

Retiré par le NIST.

03.13.04 Information dans les ressources système partagées

Empêcher les transferts d'information non autorisés ou non prévus au moyen de ressources système partagées.

Discussion

Empêcher les transferts d'information non autorisés ou non prévus au moyen de ressources système partagées permet d'éviter que l'information produite par les opérations d'utilisatrices et utilisateurs ou de rôles antérieurs (ou les opérations de processus agissant au nom d'utilisatrices et utilisateurs ou de rôles antérieurs) soit disponible pour les utilisatrices et utilisateurs ou les rôles actuels (ou les processus actuels agissant au nom des utilisatrices et utilisateurs ou des rôles actuels) qui obtiennent l'accès aux ressources système partagées après que les ressources ont été retournées au système. L'information dans les ressources système partagées s'applique

également aux représentations chiffrées de l'information. Dans d'autres contextes, le contrôle de l'information dans les ressources système partagées est couramment appelé la réutilisation d'objets et la protection d'information résiduelle. L'information dans les ressources système partagées ne s'applique pas à la persistance d'information, qui fait référence à la représentation résiduelle des données qui ont été nominalement supprimées, ni aux canaux cachés (y compris les canaux de stockage et de temps) où les ressources système partagées sont manipulées de façon à enfreindre les restrictions relatives aux flux d'information, ni aux composants des systèmes qui sont associés à un seul utilisateur ou rôle.

Références

Source du contrôle : SC-04
Publications connexes : Aucune

03.13.05 Non affecté

Retiré par le NIST.

03.13.06 Communications réseau – Refus par défaut et autorisation par exception

Refuser par défaut le trafic de communications réseau et permettre le trafic de communications réseau au moyen d'exceptions.

Discussion

Cette exigence s'applique au trafic de communications réseau entrant et sortant dans le périmètre du système et aux points désignés au sein du système. Une stratégie de trafic de communications réseau de type « refus par défaut et autorisation par exception » permet de s'assurer que seules les connexions essentielles et approuvées sont permises.

Références

Source du contrôle : SC-07(05)
Publications connexes :

- *NIST SP 800-41 Guidelines on Firewalls and Firewall Policy* (en anglais seulement)
- *NIST SP 800-77 Guide to IPsec VPNs* (en anglais seulement)
- *NIST SP 800-189 Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation* (en anglais seulement)

03.13.07 Non affecté

Retiré par le NIST.

03.13.08 Confidentialité lors de la transmission et du stockage

Mettre en œuvre des mécanismes cryptographiques afin d'empêcher la divulgation non autorisée d'information désignée lors de la transmission et du stockage.

Discussion

Cette exigence s'applique aux réseaux internes et externes ainsi qu'à tous les composants du système qui peuvent transmettre de l'information désignée, y compris les serveurs, les ordinateurs blocs-notes, les ordinateurs de bureau, les appareils mobiles, les imprimantes, les photocopieurs, les numériseurs, les télécopieurs et les radios.

Les voies de communication non protégées sont vulnérables à l'interception et à la modification. Le chiffrement protège l'information désignée des divulgations non autorisées lors de la transmission et du stockage. Les mécanismes cryptographiques qui protègent la confidentialité de l'information désignée durant la transmission incluent les protocoles TLS et IPsec. L'information en stockage (c'est-à-dire l'information au repos) désigne l'état de l'information désignée lorsqu'elle n'est pas traitée ou en transit et qu'elle réside sur des dispositifs de stockage internes ou externes, sur des dispositifs de réseau de stockage et dans des bases de données. La protection de l'information désignée en stockage ne concerne pas le type de dispositif de stockage ni la fréquence d'accès au dispositif, mais plutôt l'état de l'information. Cette exigence est associée à l'exigence Protection cryptographique 03.13.11.

Références

Sources des contrôles : SC-08, SC-08(01), SC-28 et SC-28(01)
Publications connexes :

- Centre pour la cybersécurité, *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B* (ITSP.40.111)
- Centre pour la cybersécurité, *Conseils sur la configuration sécurisée des protocoles réseau* (ITSP.40.062)
- *NIST FIPS 140-3 Security Requirements for Cryptographic Modules* (en anglais seulement)
- *NIST FIPS 197 Advanced Encryption Standard* (en anglais seulement)
- *NIST SP 800-46 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (en anglais seulement)
- *NIST SP 800-52 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* (en anglais seulement)
- *NIST SP 800-56A Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography* (en anglais seulement)
- *NIST SP 800-56B Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography* (en anglais seulement)
- *NIST SP 800-56C Recommendation for Key-Derivation Methods in Key-Establishment Schemes* (en anglais seulement)
- *NIST SP 800-57-1 Recommendation for Key Management: Part 1 – General* (en anglais seulement)
- *NIST SP 800-57-2 Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations* (en anglais seulement)
- *NIST SP 800-57-3 Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance* (en anglais seulement)
- *NIST SP 800-77 Guide to IPsec VPNs* (en anglais seulement)
- *NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices* (en anglais seulement)
- *NIST SP 800-113 Guide to SSL VPNs* (en anglais seulement)
- *NIST SP 800-114 User's Guide to Telework and Bring Your Own Device (BYOD) Security* (en anglais seulement)
- Centre pour la cybersécurité, *Sécurité des appareils des utilisateurs finaux pour les modèles de déploiement Prenez vos appareils personnels (PAP)* (ITSM.70.003)
- *NIST SP 800-121 Guide to Bluetooth Security* (en anglais seulement)
- *NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise* (en anglais seulement)
- *NIST SP 800-177 Trustworthy Email* (en anglais seulement)

03.13.09 Déconnexion réseau

Mettre fin aux connexions réseau associées aux sessions de communication à la fin de la session ou après [Affectation : période définie par l'organisation] d'inactivité.

Discussion

Cette exigence s'applique aux réseaux internes et externes. L'interruption des connexions réseau associées aux sessions de communication comprend la désaffectation des adresses TCP/IP ou des paires de ports au niveau du système d'exploitation ou la désaffectation des attributions réseau au niveau de l'application si plusieurs sessions d'application utilisent une seule connexion réseau. Les périodes d'inactivité peuvent être établies par les organisations et comprennent des périodes par type d'accès réseau ou pour des accès réseau particuliers.

Références

Source du contrôle : SC-10
Publications connexes : Aucune

03.13.10 Établissement et gestion des clés cryptographiques

Établir et gérer les clés cryptographiques dans le système conformément aux exigences de gestion de clés suivantes : [Affectation : exigences définies par l'organisation liées à la génération, à la distribution, au stockage, à l'accès et à la destruction des clés].

Discussion

L'établissement et la gestion des clés cryptographiques peuvent être effectués au moyen de procédures manuelles ou de mécanismes automatisés appuyés par des procédures manuelles. Les organisations doivent répondre aux exigences d'établissement et de gestion de clés conformément aux lois, aux décrets, aux politiques, aux directives, à la réglementation et aux normes applicables qui précisent les options, les niveaux et les paramètres appropriés. Cette exigence est associée à l'exigence Protection cryptographique 03.13.11.

Références

Source du contrôle : SC-12
Publications connexes :

- Centre pour la cybersécurité, *Conseils sur la configuration sécurisée des protocoles réseau* (ITSP.40.062)
- *NIST FIPS 140-3 Security Requirements for Cryptographic Modules* (en anglais seulement)
- *NIST SP 800-56A Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography* (en anglais seulement)
- *NIST SP 800-56B Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography* (en anglais seulement)
- *NIST SP 800-56C Recommendation for Key-Derivation Methods in Key-Establishment Schemes* (en anglais seulement)
- *NIST SP 800-57-1 Recommendation for Key Management: Part 1 – General* (en anglais seulement)
- *NIST SP 800-57-2 Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations* (en anglais seulement)
- *NIST SP 800-57-3 Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance* (en anglais seulement)

03.13.11 Protection cryptographique

Mettre en œuvre les types de cryptographie suivants pour protéger la confidentialité de l'information désignée : [Affectation : types de cryptographie définis par l'organisation].

Discussion

La cryptographie est mise en œuvre conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Une cryptographie validée selon la norme Federal Information Processing Standard (FIPS) est recommandée pour la protection de l'information désignée.

Références

Source du contrôle : SC-13
Publications connexes : *NIST FIPS 140-3 Security Requirements for Cryptographic Modules* (en anglais seulement)

03.13.12 Applications et appareils informatiques collaboratifs

A. Empêcher l'activation à distance d'applications et d'appareils informatiques collaboratifs, sauf pour les exceptions suivantes : [Affectation : exceptions définies par l'organisation pour lesquelles l'activation à distance doit être permise].

B. Indiquer de manière explicite l'utilisation permise pour les utilisatrices et utilisateurs physiquement à proximité des appareils.

Discussion

Les appareils informatiques collaboratifs incluent les tableaux blancs, les microphones et les caméras. Les ordinateurs blocs-notes, les téléphones intelligents, les écrans et les tablettes intégrant des caméras et des microphones sont considérés comme faisant partie des appareils informatiques collaboratifs lors de l'utilisation d'un logiciel de conférence. L'indication explicite d'utilisation comprend l'envoi d'un avis aux utilisatrices et utilisateurs (par exemple, un menu contextuel indiquant qu'un enregistrement est en cours ou que le microphone est activé) lorsque des appareils informatiques collaboratifs sont activés. Les systèmes de vidéoconférence dédiés, qui exigent normalement qu'une participante ou un participant appelle les autres personnes ou se connectent pour activer la vidéoconférence, sont exclus. Les solutions permettant d'empêcher l'utilisation d'appareils comprennent les bouchons pour caméras Web et les boutons pour désactiver les microphones.

Références

Source du contrôle : SC-15
Publications connexes : Aucune

03.13.13 Code mobile

A. Définir le code mobile et les technologies de code mobile acceptables.

B. Autoriser, surveiller et contrôler l'utilisation de code mobile.

Discussion

Le code mobile comprend des programmes informatiques ou des parties de programme obtenus de systèmes distants, transmis sur un réseau et exécutés sur un système local sans installation explicite ou exécution par la ou le destinataire. Les décisions concernant l'utilisation de code mobile reposent sur le degré de possibilité qu'une utilisation malveillante du code cause des dommages au système. Les technologies de code mobile incluent les applets Java, JavaScript, HTML5, VBScript et WebGL. Les restrictions d'utilisation et les lignes directrices sur la mise en œuvre s'appliquent à la sélection et à l'utilisation de code mobile installé sur les serveurs ainsi que le code mobile téléchargé et exécuté sur les postes de travail et les appareils individuels, y compris les ordinateurs blocs-notes, les téléphones intelligents et les dispositifs intelligents. Les stratégies et procédures liées au code mobile concernent les mesures prises afin d'empêcher le développement, l'acquisition et l'utilisation de code mobile non acceptable au sein du système, y compris exiger la signature numérique du

code mobile par une source de confiance.

Références

Source du contrôle : SC-18
Publications connexes : *NIST SP 800-28 Guidelines on Active Content and Mobile Code* (en anglais seulement)

03.13.14 Non affecté

Retiré par le NIST.

03.13.15 Authenticité des sessions

Protéger l'authenticité des sessions de communication.

Discussion

La protection de l'authenticité des sessions porte sur la protection des communications au niveau de la session plutôt qu'au niveau des paquets. Cette protection permet d'instaurer un niveau de confiance adéquat aux deux extrémités des sessions de communication quant à l'identité des autres parties et à la validité de l'information transmise. La protection de l'authenticité comprend la protection contre les attaques par interception, le détournement de session et l'insertion d'information erronée dans les sessions.

Références

Source du contrôle : SC-23
Publications connexes :

- Centre pour la cybersécurité, *Conseils sur la configuration sécurisée des protocoles réseau* (ITSP.40.062)
- *NIST SP 800-52 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* (en anglais seulement)
- *NIST SP 800-77 Guide to IPsec VPNs* (en anglais seulement)
- *NIST SP 800-95 Guide to Secure Web Services* (en anglais seulement)
- *NIST SP 800-113 Guide to SSL VPNs* (en anglais seulement)

03.13.16 Non affecté

Retiré par le NIST.

3.14 Intégrité de l'information et des systèmes

Les contrôles d'intégrité de l'information et des systèmes appuient la protection de l'intégrité des composants du système et des données traitées par le système. Ils permettent à l'organisation d'établir, de signaler et de corriger rapidement les défauts liés aux données et aux systèmes afin d'offrir une protection contre les programmes malveillants. Ils permettent également de surveiller les alertes et les avis de sécurité du système et d'intervenir de manière appropriée.

03.14.01 Correction des défauts

A. Établir, signaler et corriger les défauts du système.

B. Installer les mises à jour de sécurité appropriées des logiciels et des micrologiciels dans une période de [Affectation : période définie par l'organisation] suivant la date de publication des mises à jour.

Discussion

Les organisations doivent établir les systèmes qui sont touchés par les défauts logiciels et micrologiciels, y compris les vulnérabilités qui découlent de ces défauts, et signaler cette information au personnel responsable de la sécurité et de la confidentialité de l'information. Les mises à jour liées à la sécurité incluent les correctifs, les ensembles de modifications provisoires, les correctifs d'urgence et les signatures de logiciel antivirus. Les organisations doivent corriger les défauts découverts au cours des évaluations de sécurité, de la surveillance continue, des activités d'intervention en cas d'incident et du traitement des erreurs du système. Les organisations peuvent tirer parti des ressources offertes (par exemple, les bases de données CWE ou CVE) pour corriger les défauts des systèmes. Les périodes définies par l'organisation pour la mise à jour de sécurité des logiciels et des micrologiciels peuvent varier en fonction de divers facteurs, notamment la criticité de la mise à jour (c'est-à-dire la gravité de la vulnérabilité associée à la faille découverte). Certains types de correctifs peuvent nécessiter plus de mises à l'essai que d'autres.

Références

Source du contrôle : SI-02
Publications connexes :

- Centre pour la cybersécurité , *Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée* (ITSP.10.036)
- *NIST SP 800-40 Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology* (en anglais seulement)
- *NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems* (en anglais seulement)

03.14.02 Protection contre les programmes malveillants

A. Mettre en œuvre des mécanismes de protection contre les programmes malveillants aux points d'entrée et de sortie du système afin de détecter et d'éradiquer le code malveillant.

B. Mettre à jour les mécanismes de protection contre les programmes malveillants dès que de nouvelles versions sont disponibles, conformément aux stratégies et procédures de gestion des configurations.

C. Configurer les mécanismes de protection contre les programmes malveillants de façon à :

1. effectuer une analyse du système tous les [Affectation : fréquence définie par l'organisation] et des analyses en temps réel des fichiers de sources externes aux points d'extrémité ou aux points d'entrée et de sortie du système lorsque des fichiers sont téléchargés, ouverts ou exécutés;
2. bloquer ou mettre en quarantaine le code malveillant ou entreprendre d'autres mesures d'atténuation afin d'intervenir lors de la détection de code malveillant.

Discussion

Les insertions de code malveillant surviennent lors de l'exploitation de vulnérabilités du système. Le code malveillant peut être inséré dans le système de différentes façons, y compris par courriel, par Internet et par des dispositifs de stockage portatifs. Le code malveillant comprend les virus, les vers, les chevaux de Troie et les logiciels espions. Le code malveillant peut être encodé sous différents formats, contenu dans des fichiers compressés ou cachés, ou encore dissimulé dans des fichiers en utilisant des techniques comme la stéganographie. Le code malveillant peut être présent dans des logiciels commerciaux sur étagère et dans des logiciels conçus sur mesure et peut comprendre des bombes logiques, des portes dérobées et d'autres types d'attaques qui peuvent affecter la mission et les activités de l'organisation. Des analyses périodiques du système et des analyses en temps réel des fichiers provenant de sources externes lorsqu'ils sont téléchargés, ouverts ou exécutés peuvent faciliter la détection de code malveillant. Les mécanismes de protection contre les programmes malveillants peuvent également surveiller les systèmes afin de détecter les comportements anormaux ou

inattendus et prendre les mesures appropriées.

Ces mécanismes comprennent des technologies axées ou non sur les signatures. Les mécanismes de détection qui ne sont pas axés sur les signatures intègrent des techniques d'intelligence artificielle (IA) qui utilisent l'heuristique afin de détecter, d'analyser et de décrire les caractéristiques ou les comportements des programmes malveillants. Ils fournissent également des contrôles contre de tels programmes malveillants pour lesquels il n'existe pas encore de signature ou de telles signatures s'avèrent inefficaces. Les cas où les signatures sont inexistantes ou inefficaces incluent le code malveillant polymorphique (c'est-à-dire le code pour lequel les signatures sont modifiées lors de la réplication). Les mécanismes qui ne sont pas axés sur les signatures incluent les technologies basées sur la réputation. Une gestion omniprésente des configurations, des logiciels anti-exploitation et des contrôles d'intégrité logicielle peuvent également être efficaces pour empêcher l'exécution de code non autorisé.

S'il n'est pas possible de détecter le code malveillant à l'aide de méthodes ou de technologies de détection, les organisations peuvent miser sur des pratiques de codage sécurisées, le contrôle et la gestion des configurations, des processus d'approvisionnement de confiance et des pratiques de suivi pour veiller à ce que les logiciels n'exécutent que les fonctions prévues. Les organisations peuvent déterminer que d'autres mesures s'imposent en réponse à une détection de code malveillant. Par exemple, les organisations peuvent définir des mesures à prendre en réponse à une détection de code malveillant au cours d'analyses, de téléchargements malveillants ou d'activités malveillantes associés à une tentative d'ouverture ou d'exécution de fichier.

Références

Source du contrôle : SI-03
Publications connexes :

- Centre pour la cybersécurité, *Protéger votre organisation contre les maliciels* (ITSAP.00.057)
- Centre pour la cybersécurité, *Reconnaître les courriels malveillants* (ITSAP.00.100)
- *NIST SP 800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops* (en anglais seulement)
- *NIST SP 800-125B Secure Virtual Network Configuration for Virtual Machine (VM) Protection* (en anglais seulement)
- *NIST SP 800-177 Trustworthy Email* (en anglais seulement)

03.14.03 Alertes, avis et directives de sécurité

A. Recevoir régulièrement d'organisations externes des alertes, des avis et des directives de sécurité concernant les systèmes.

B. Générer et diffuser les alertes, les avis et les directives de sécurité internes concernant les systèmes, au besoin.

Discussion

Il existe de nombreuses sources publiques pour les alertes et les avis de sécurité des systèmes. Par exemple, le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) génère des alertes et des bulletins de sécurité pour assurer une connaissance de la situation au sein des organismes du GC et des organisations ne relevant pas du GC. Les fournisseurs de logiciels, les services d'abonnement et les centres ISAC (pour *Information Sharing and Analysis Centres*) de l'industrie peuvent également fournir des alertes et des avis de sécurité. La conformité aux directives de sécurité est essentielle en raison de la nature critique d'un grand nombre de ces directives et des effets néfastes immédiats possibles sur les opérations et les actifs organisationnels, sur les utilisatrices et utilisateurs, sur d'autres organisations et sur l'ensemble du pays dans l'éventualité où les directives ne sont pas mises en œuvre rapidement.

Références

Source du contrôle : SI-05

Publications connexes : *NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (en anglais seulement)

03.14.04 Non affecté

Retiré par le NIST.

03.14.05 Non affecté

Retiré par le NIST.

03.14.06 Surveillance du système

A. Surveiller le système afin de détecter :
   1. les attaques et les indicateurs d'attaques potentielles;
   2. les connexions non autorisées.

B. Détecter les utilisations non autorisées du système.

C. Surveiller le trafic de communications entrantes et sortantes afin de détecter les activités ou les conditions atypiques ou non autorisées.

Discussion

La surveillance du système comprend à la fois la surveillance interne et la surveillance externe. La surveillance interne comprend l'observation des événements qui surviennent dans le système. La surveillance externe comprend l'observation des événements qui se produisent à la frontière du système. Les organisations peuvent surveiller le système en observant les activités liées aux enregistrements de vérification en temps réel ou en observant d'autres aspects du système, comme les tendances d'accès, les caractéristiques d'accès et d'autres opérations. Les objectifs de la surveillance peuvent orienter la détermination des événements.

Les capacités de surveillance du système sont réalisées au moyen d'une variété d'outils et de techniques (par exemple, les logiciels de surveillance des enregistrements de vérification, les systèmes de détection d'intrusion, les systèmes de prévention d'intrusion, les logiciels de protection contre le code malveillant, les outils d'analyse et les logiciels de surveillance de réseau). Les dispositifs de surveillance sont déployés à des endroits stratégiques, notamment dans des emplacements du périmètre sélectionnés et près des grappes de serveurs qui prennent en charge des applications essentielles, et sont employés à titre d'interfaces système gérées. La granularité de la surveillance de l'information collectée est basée sur les objectifs de surveillance de l'organisation et la capacité du système à prendre en charge de tels objectifs.

Les connexions aux systèmes peuvent être de type réseau, distant ou local. Une connexion réseau est une connexion effectuée avec un appareil qui communique au moyen d'un réseau (par exemple, un réseau local, Internet). Une connexion distante est une connexion effectuée avec un appareil qui communique au moyen d'un réseau externe (par exemple, Internet). Les connexions réseau, distantes et locales peuvent être filaires ou sans fil.

Les activités ou conditions inusitées ou non autorisées associées au trafic de communications entrantes et sortantes comprennent le trafic interne qui indique la présence de code malveillant sur le système ou qui se propage entre les composants du système, l'exportation d'information non autorisée ou la signalisation vers des systèmes externes. Les preuves de code malveillant servent à déterminer la compromission potentielle du système. Les exigences en matière de surveillance du système, y compris la surveillance selon le type de système, peuvent se trouver dans d'autres exigences.

Références

Sources des contrôles : SI-04 et SI-04(04)
Publications connexes :

- *NIST SP 800-61 Computer Security Incident Handling Guide* (en anglais seulement)
- *NIST SP 800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops* (en anglais seulement)
- *NIST SP 800-92 Guide to Computer Security Log Management* (en anglais seulement)
- *NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)* (en anglais seulement)
- *NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (en anglais seulement)
- *NIST SP 800-177 Trustworthy Email* (en anglais seulement)

03.14.07 Non affecté

Retiré par le NIST.

03.14.08 Gestion et conservation de l'information

Gérer et conserver l'information désignée au sein du système et les sorties d'information désignée du système conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes, aux lignes directrices et aux exigences opérationnelles applicables.

Discussion

Les ministères et organismes fédéraux doivent tenir compte des exigences de conservation des données des organisations non fédérales. La conservation d'information désignée sur des systèmes non fédéraux à la fin de contrats ou d'ententes augmente la surface d'attaque de ces systèmes et les risques de compromission de l'information. Bibliothèque et Archives Canada fournit la politique et les directives fédérales concernant la conservation des documents et le calendrier de conservation.

Références

Source du contrôle : SI-12
Publications connexes : Aucune

03.14.09 Poste de travail administratif dédié

A. Exiger que les opérations d'administration ou de superutilisateur soient réalisées à partir d'un poste de travail physique dédié à ces tâches précises et isolées des autres fonctions et réseaux. Plus particulièrement, la station ne devrait pas avoir accès à Internet.

B. S'assurer que la connexion distante d'un poste de travail administratif dédié à un réseau cible utilise un réseau privé d'opérateur (par exemple, un service LAN privé virtuel [VPLS pour *Virtual Private LAN*] ou une commutation multiprotocole par étiquette [MPLS pour *Multiprotocol Label Switching*]) avec chiffrement de RPV.

C. Utiliser un client léger ou un poste de travail physique dédié et renforcé univalent à titre de poste de travail administratif dédié, qui n'est pas partagé entre les domaines de sécurité.

Discussion

Un poste de travail administratif dédié est typiquement constitué d'un terminal d'utilisateur et d'une très petite sélection de logiciels conçus pour interfacer avec le système cible. Aux fins du présent contrôle, un poste de

travail est un système à partir duquel les tâches d'administration sont réalisées, par opposition au système cible. Le poste de travail administratif dédié doit être renforcé pour le rôle afin de réduire la probabilité qu'un point d'extrémité de superutilisateur ou d'administrateur soit compromis par un auteur de menace (ce qui entraînerait logiquement la compromission du système cible). Les outils bureautiques typiques ne sont pas nécessaires sur le poste de travail administratif dédié. Toutes les applications et tous les services non essentiels doivent être supprimés. Les postes de travail administratifs dédiés n'ont pas de jonction de domaine, ne peuvent pas télécharger de correctif à partir d'Internet et ne peuvent pas mettre à jour la documentation dans les applications en réseau.

Le retrait de l'accès Internet public des postes de travail administratifs réduit considérablement les risques de compromission. Les passerelles RPV exposées à Internet ne sont pas privilégiées pour les activités d'administration à distance. Les opérateurs privés offrent une meilleure protection, mais nécessitent tout de même un chiffrement de RPV au sein de réseau. Le poste de travail administratif dédié ne doit pas devenir un moyen de déplacement latéral entre les domaines de sécurité.

Références

Sources des contrôles : SI-400, SI-400(02) et SI-400(05)
Publications connexes : Aucune

3.15 Planification

Les contrôles de planification et les activités d'assurance sont liés à l'élaboration, à la documentation, à la mise à jour et à la mise en œuvre des plans de sécurité et de confidentialité pour les systèmes organisationnels. Ces plans décrivent les contrôles de sécurité et de confidentialité ainsi que les activités d'assurance en place ou planifiées pour les systèmes. Ils intègrent également les règles de conduite pour les personnes ayant accès aux systèmes.

03.15.01 Stratégie et procédures

A. Élaborer, documenter et diffuser au personnel ou aux rôles de l'organisation les stratégies et les procédures nécessaires afin de satisfaire les exigences de sécurité pour la protection de l'information désignée.

B. Examiner et mettre à jour les stratégies et les procédures tous les [Affectation : fréquence définie par l'organisation].

Discussion

Cette exigence traite des stratégies et des procédures pour la protection de l'information désignée. Les stratégies et les procédures contribuent à l'assurance de la sécurité et doivent s'appliquer à chaque famille d'exigences de sécurité de l'information désignée. Les stratégies peuvent être incluses dans le cadre de la stratégie de sécurité de l'organisation ou être représentées par des stratégies séparées pour chacune des familles d'exigence. Les procédures décrivent comment les stratégies sont mises en œuvre et peuvent s'appliquer aux personnes ou aux rôles étant l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité du système ou dans un ou plusieurs documents séparés.

Références

Sources pour les activités : AC-01, AT-01, AU-01, CA-01, CM-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PS-01, RA-01, SA-01, SC-01, SI-01 et SR-01
Publications connexes :

- Centre pour la cybersécurité , *Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée* (ITSP.10.036)

- *NIST SP 800-12 An Introduction to Information Security* (en anglais seulement)
- *NIST SP 800-100 Information Security Handbook* (en anglais seulement)

03.15.02 Plan de sécurité du système

A. Élaborer un plan de sécurité et de confidentialité pour le système qui :

1. définit les composants constitutifs du système;
2. identifie les types d'informations traitées, stockées et transmises par le système;
3. décrit les menaces particulières pour le système qui sont préoccupantes pour l'organisation;
4. décrit l'environnement opérationnel du système ainsi que les dépendances ou les connexions à d'autres systèmes ou à d'autres composants du système;
5. fournit un aperçu des exigences de sécurité du système;
6. décrit les mesures de protection en place ou prévues pour répondre aux exigences de sécurité;
7. identifie les personnes qui assument des rôles et des responsabilités liés au système;
8. contient d'autres renseignements pertinents nécessaires à la protection de l'information désignée.

B. Examiner et mettre à jour le plan de sécurité du système tous les [Affectation : fréquence définie par l'organisation].

C. Protéger le plan de sécurité du système contre les divulgations non autorisées.

Discussion

Les plans de sécurité et de confidentialité du système offrent les caractéristiques clés du système concernant le traitement, le stockage et la transmission de l'information désignée, ainsi que la manière dont le système et l'information sont protégés. Les plans de sécurité et de confidentialité du système doivent contenir suffisamment d'information pour faciliter une conception et une mise en œuvre qui sont conformes, sans équivoque, à leurs objectifs et pour faciliter la détermination des risques si le plan est mis en œuvre comme prévu. Les plans de sécurité et de confidentialité du système peuvent être en ensemble de documents, y compris des documents qui existent déjà. Les plans de sécurité efficaces du système font référence à des stratégies, à des procédures et à des documents supplémentaires (par exemple, spécifications de conception) contenant de l'information détaillée. Ces références permettent de réduire les exigences en matière de documentation associées aux programmes de sécurité et de conserver l'information relative à la sécurité dans d'autres secteurs opérationnels ou de gestion établis en lien avec l'architecture d'entreprise, le cycle de développement des systèmes, l'ingénierie des systèmes et l'acquisition.

Références

Source de l'activité : PL-02
Publications connexes :

- Centre pour la cybersécurité , *Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée* (ITSP.10.036)
- *NIST SP 800-18 Guide for Developing Security Plans for Federal Information Systems* (en anglais seulement)

03.15.03 Règles de conduite

A. Établir des règles qui décrivent les responsabilités et le comportement attendu pour l'utilisation du système et la protection de l'information désignée.

B. Fournir des règles aux personnes devant accéder au système.

C. Obtenir des personnes devant accéder au système une attestation documentée selon laquelle elles ont lu et compris le document et acceptent de respecter les règles de conduite avant d'obtenir l'accès autorisé à l'information désignée et au système.

D. Examiner et mettre à jour les règles de conduite tous les [Affectation : fréquence définie par l'organisation].

Discussion

Les règles de conduite représentent un type d'entente d'accès pour les utilisatrices et utilisateurs du système. Les organisations doivent prévoir des règles de conduite pour le traitement de l'information désignée en fonction des rôles et des responsabilités des utilisatrices et utilisateurs, et faire la distinction entre les règles s'appliquant aux utilisatrices et utilisateurs privilégiés et les règles s'appliquant aux utilisatrices et utilisateurs généraux.

Références

Source de l'activité : PL-04
Publications connexes :

- Centre pour la cybersécurité , *Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée* (ITSP.10.036)
- *NIST SP 800-18 Guide for Developing Security Plans for Federal Information Systems* (en anglais seulement)

3.16 Acquisition des systèmes et des services

Les contrôles pour l'acquisition des systèmes et des services s'appliquent à la passation de marchés pour l'acquisition des produits et des services nécessaires afin de soutenir la mise en œuvre et l'exploitation des systèmes organisationnels. Ils permettent de s'assurer que des ressources suffisantes sont affectées à la protection des systèmes organisationnels et ils appuient les processus relatifs au cycle de développement des systèmes qui intègrent des considérations de sécurité.

03.16.01 Principes d'ingénierie de la sécurité

Appliquer les principes d'ingénierie de la sécurité des systèmes suivants pour le développement ou la modification des systèmes et des composants de systèmes : [Affectation : principes d'ingénierie de la sécurité des systèmes définis par l'organisation].

Discussion

Les organisations doivent appliquer des principes d'ingénierie de la sécurité des systèmes aux nouveaux systèmes en développement. Dans le cas des systèmes existants, les organisations doivent appliquer des principes d'ingénierie de la sécurité des systèmes aux modifications des systèmes autant que possible, en tenant compte de l'état actuel des composants matériels, logiciels et micrologiciels. L'application de principes d'ingénierie de la sécurité des systèmes favorise le développement de systèmes dignes de confiance, sécurisés et résilients, et réduit la susceptibilité des organisations aux interruptions, aux risques et aux menaces. Des exemples de ces principes comprennent le développement de mesures de protection en couche; l'établissement de stratégies, d'architectures et de contrôles de sécurité comme base de la conception des systèmes; l'intégration d'exigences de sécurité au cycle de développement des systèmes; la délimitation des frontières de sécurité physiques et logiques; l'assurance que les développeuses et développeurs sont formés pour concevoir des logiciels sécurisés et dignes de confiance; la modélisation des menaces afin d'établir les cas d'utilisation, les agents de menace, les vecteurs et les schémas d'attaque, les schémas de conception et les contrôles compensatoires nécessaires pour atténuer les risques. Les organisations qui appliquent des principes d'ingénierie de la sécurité peuvent faciliter le développement de systèmes, de composants de systèmes et de services connexes sécurisés et fiables, réduire les risques à des niveaux acceptables et prendre des décisions informées en matière de gestion des risques.

Références

Source du contrôle : SA-08
Publications connexes :

- Centre pour la cybersécurité, *Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes* (ITSP.10.037)
- *NIST SP 800-160-1 Engineering Trustworthy Secure Systems* (en anglais seulement)
- *NIST SP 800-160-2 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach* (en anglais seulement)

03.16.02 Composants de systèmes non pris en charge

A. Remplacer les composants des systèmes lorsque les développeuses, les développeurs, les fournisseurs ou les fabricants ne prennent plus en charge ces composants.

B. Fournir des options pour l'atténuation des risques ou d'autres sources pour bénéficier d'un soutien continu des composants non pris en charge si les composants ne peuvent pas être remplacés.

Discussion

La prise en charge (ou le soutien) des composants de systèmes comprend les correctifs logiciels, les mises à jour de micrologiciels, les remplacements de pièces et les contrats de maintenance. Les exemples de composants non pris en charge comprennent les circonstances où les fournisseurs ne produisent plus de correctifs logiciels critiques ou de mises à jour pour les produits, ce qui peut mener à des possibilités pour les adversaires d'exploiter les faiblesses ou les lacunes des composants installés. Les exceptions au remplacement des composants de systèmes non pris en charge comprennent les systèmes qui fournissent des capacités essentielles à la mission ou aux activités lorsque des technologies plus récentes ne sont pas disponibles ou lorsque les systèmes sont tellement isolés que l'installation de composants de remplacement n'est pas une option.

Les autres sources de soutien permettent de répondre au besoin de fournir un soutien continu pour les composants de systèmes qui ne sont plus pris en charge par les fabricants d'origine, les développeurs ou les fournisseurs lorsque ces composants sont essentiels à la mission et aux activités de l'organisation. Au besoin, les organisations peuvent établir un soutien interne en développant des correctifs sur mesure pour les composants logiciels critiques ou avoir recours à des services de fournisseurs externes qui pourront fournir, au moyen de relations contractuelles, du soutien continu pour les composants qui ne sont plus pris en charge. Ces relations contractuelles peuvent comprendre des fournisseurs de logiciels libres à valeur ajoutée. Le risque accru d'utilisation de composants de systèmes non pris en charge peut être atténué en empêchant la connexion de ces composants aux réseaux publics ou non contrôlés ou en mettant en œuvre d'autres formes d'isolation.

Références

Source du contrôle : SA-22
Publications connexes : Aucune

03.16.03 Services de systèmes externes

A. Exiger que les fournisseurs de services de systèmes externes utilisés pour le traitement, le stockage ou la transmission de l'information désignée respectent les exigences de sécurité suivantes : [Affectation : exigences de sécurité définies par l'organisation].

B. Définir et documenter les rôles et les responsabilités d'utilisateur concernant les services de système externe, y compris les responsabilités partagées avec les fournisseurs de services externes.

C. Mettre en œuvre des processus, des méthodes et des techniques pour surveiller la conformité aux exigences de sécurité des fournisseurs de services externes sur une base continue.

Discussion

Les services de système externe sont fournis par des fournisseurs de services externes. Les organisations peuvent établir des relations avec des fournisseurs de services externes de nombreuses façons, y compris au moyen de partenariats, de contrats, d'ententes entre les organisations, d'ententes liées aux secteurs d'activités, d'accords de licence, de coentreprises et d'échanges de chaîne d'approvisionnement. L'organisation devant protéger l'information désignée demeure responsable de la gestion des risques liés à l'utilisation de services de système externe. Les accords sur les niveaux de service définissent les attentes de rendement, décrivent les résultats mesurables et déterminent les mesures de correction, les mesures d'atténuation et les exigences en matière d'intervention pour les cas de non-conformité. L'information provenant de fournisseurs de services externes concernant les fonctions, les ports, les protocoles et les services particuliers utilisés pour la prestation de tels services peut être utile pour comprendre les compromis associés à la restriction de certaines fonctions et de certains services ou au blocage de certains ports et protocoles. Cette exigence est associée à l'exigence Utilisation de systèmes externes 03.01.20.

Références

Source du contrôle : SA-09
Publications connexes :

- *NIST SP 800-160-1 Engineering Trustworthy Secure Systems* (en anglais seulement)
- *NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (en anglais seulement)

3.17 Gestion des risques liés à la chaîne d'approvisionnement

Les contrôles de gestion des risques liés à la chaîne d'approvisionnement appuient l'atténuation des risques de cybersécurité dans toutes les phases de la chaîne d'approvisionnement.

03.17.01 Plan de gestion des risques liés à la chaîne d'approvisionnement

A. Élaborer un plan pour gérer les risques liés à la chaîne d'approvisionnement associés à la recherche, au développement, à la conception, à la fabrication, à l'acquisition, à la livraison, à l'intégration, à l'exploitation, à la maintenance et à l'élimination des systèmes, des composants de systèmes ou des services qui s'y rapportent.

B. Examiner et mettre à jour le plan de gestion des risques liés à la chaîne d'approvisionnement tous les [Affectation : fréquence définie par l'organisation].

C. Protéger le plan de gestion des risques liés à la chaîne d'approvisionnement des divulgations non autorisées.

Discussion

La dépendance aux produits, aux systèmes et aux services de fournisseurs externes ainsi que la nature des relations avec ces fournisseurs présentent un niveau accru de risque pour une organisation. Les menaces pouvant augmenter les risques liés à la sécurité ou à la confidentialité incluent la production non autorisée, la falsification, la modification, les mauvaises pratiques de développement et de fabrication dans la chaîne d'approvisionnement, le vol ainsi que l'insertion de logiciel, de micrologiciel ou de matériel malveillant. Les risques liés à la chaîne d'approvisionnement peuvent être endémiques ou systémiques au sein d'un système, d'un composant ou d'un service. La gestion des risques liés à la chaîne d'approvisionnement est une tâche complexe à plusieurs facettes nécessitant des efforts coordonnés au sein d'une organisation afin d'établir des relations de confiance et de communiquer avec les parties prenantes internes et externes.

Les activités de gestion des risques liés à la chaîne d'approvisionnement (GRCA) comprennent l'identification et l'évaluation des risques, la détermination des mesures appropriées de réponse aux risques, l'élaboration de plans de GRCA visant à documenter les mesures de réponse et la surveillance du rendement par rapport aux plans. Les

plans de GRCA au niveau du système dépendent de la mise en œuvre particulière du système et fournissent une mise en œuvre, des exigences, des contraintes et des implications au sujet des stratégies. Ce plan peut être indépendant ou intégré aux plans de sécurité et de confidentialité du système. Les plans de GRCA portent sur la gestion, la mise en œuvre et la surveillance des contrôles de GRCA ainsi que le développement ou le maintien des systèmes pendant le cycle de développement des systèmes afin de soutenir la mission et les activités. Puisque les chaînes d'approvisionnement peuvent varier considérablement au sein d'une même organisation et d'une organisation à l'autre, les plans de GRCA sont adaptés aux programmes individuels ainsi qu'aux contextes organisationnels et opérationnels.

Références

Source de l'activité : SR-02
Publications connexes :

- CST et GRC, *Méthodologie harmonisée d'évaluation des menaces et des risques (EMR-1)*
- Centre pour la cybersécurité , *Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée* (ITSP.10.036)
- Centre pour la cybersécurité, *Protéger votre organisation contre les menaces de la chaîne d'approvisionnement des logiciels* (ITSM.10.071)
- Centre pour la cybersécurité, *La cybersécurité et la chaîne d'approvisionnement : évaluation des risques* (ITSAP.10.070)
- Centre pour la cybersécurité, *Sécurité de la chaîne d'approvisionnement pour les petites et moyennes organisations* (ITSAP.00.070)
- *NIST SP 800-160-1 Engineering Trustworthy Secure Systems* (en anglais seulement)
- *NIST SP 800-181 Workforce Framework for Cybersecurity (NICE Framework)* (en anglais seulement)

03.17.02 Stratégies, outils et méthodes d'acquisition

Élaborer et mettre en œuvre des stratégies d'acquisition, des outils de contrats et des méthodes d'approvisionnement afin de déterminer, de contrer et d'atténuer les risques associés à la chaîne d'approvisionnement.

Discussion

Les processus d'acquisition fournissent un véhicule important pour la protection de la chaîne d'approvisionnement. Il existe de nombreux outils et de nombreuses techniques, y compris le masquage de l'utilisation finale d'un système ou d'un composant du système, l'achat à l'aveugle, l'exigence d'un emballage protégé contre les modifications ou l'utilisation d'une distribution de confiance ou contrôlée. Les résultats d'une évaluation des risques liés à la chaîne d'approvisionnement peuvent informer le choix des stratégies, des outils et des méthodes qui conviennent le mieux à la situation. Les outils et les techniques peuvent fournir une protection contre la production non autorisée, le vol, la modification, la contrefaçon, l'insertion de code malveillant ou de porte dérobée et les mauvaises pratiques de développement tout au long du cycle de vie du système.

Les organisations peuvent également penser à offrir des mesures incitatives pour les fournisseurs afin de mettre en œuvre des contrôles et de favoriser la transparence des processus et des pratiques de sécurité. Elles peuvent également fournir un libellé de contrat qui traite de l'interdiction d'utiliser des composants contaminés ou contrefaits et restreindre les achats des fournisseurs qui ne sont pas dignes de confiance. Les organisations doivent considérer fournir des programmes de formation et de sensibilisation pour le personnel concernant les risques liés à la chaîne d'approvisionnement, les stratégies d'atténuation disponibles et les circonstances appropriées pour utiliser les programmes. Les méthodes pour examiner et protéger les plans de développement, la documentation et les preuves doivent être appropriées selon les exigences de sécurité de l'organisation. Les contrats peuvent également préciser les exigences concernant la protection des documents.

Références

Source du contrôle : SR-05
Publications connexes :

- CST et GRC, *Méthodologie harmonisée d'évaluation des menaces et des risques (EMR-1)*
- *NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (en anglais seulement)

03.17.03 Exigences et processus de la chaîne d'approvisionnement

A. Établir un processus pour identifier et corriger les faiblesses ou les lacunes établies dans les éléments et les processus de la chaîne d'approvisionnement.

B. Appliquer les exigences de sécurité suivantes pour offrir une protection contre les risques liés à la chaîne d'approvisionnement pour les systèmes, les composants de systèmes ou les services système ainsi que pour limiter les conséquences ou les dommages potentiels associés aux événements de la chaîne d'approvisionnement : [Affectation : exigences de sécurité définies par l'organisation].

Discussion

Les éléments de la chaîne d'approvisionnement incluent les organisations, les entités ou les outils qui servent à la recherche, au développement, à la conception, à la fabrication, à l'acquisition, à la livraison, à l'intégration, aux opérations, à la maintenance et à l'élimination des systèmes et des composants de systèmes. Les processus de la chaîne d'approvisionnement incluent les processus de développement du matériel, des logiciels, des micrologiciels et des systèmes; les procédures d'expédition et de traitement; les programmes de sécurité physique; les programmes de sécurité du personnel; les outils, les techniques et les mesures de gestion des configurations pour le maintien de la provenance; ou les autres programmes, processus ou procédures associés au développement, à l'acquisition, à la maintenance et à l'élimination des systèmes et des composants de systèmes. Les éléments et les processus de la chaîne d'approvisionnement peuvent être fournis par les organisations, les intégratrices et intégrateurs de systèmes ou les fournisseurs externes. Les faiblesses ou les lacunes des éléments ou des processus de la chaîne d'approvisionnement représentent des vulnérabilités potentielles qui peuvent être exploitées par des adversaires afin de nuire à l'organisation et à sa capacité de réaliser sa mission ou ses activités.

Références

Source du contrôle : SR-03
Publications connexes :

- CST et GRC, *Méthodologie harmonisée d'évaluation des menaces et des risques (EMR-1)*
- *NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (en anglais seulement)

Annexe A Critères d'adaptation

La présente annexe décrit les critères pour adapter les contrôles de sécurité utilisés pour élaborer les exigences de sécurité de l'information désignée. Le tableau 2 énumère les options d'adaptation disponibles ainsi que les symboles abrégés connexes. Les tableaux 3 à 22 énoncent les mesures d'adaptation qui s'appliquent aux contrôles du profil d'incidence moyenne dans l'ITSP.10.033-01 afin d'obtenir les exigences de sécurité de la section 3. Les contrôles, les activités d'assurance et les améliorations contiennent un hyperlien vers l'entrée correspondante dans l'ITSP.10.033.

Les critères d'adaptation des contrôles de sécurité sont les suivants :

- **NCO [Non confidentiel]** : le contrôle n'est pas directement lié à la protection de la confidentialité de l'information désignée;
- **GC [Gouvernement du Canada]** : le contrôle relève principalement du gouvernement du Canada;
- **ACC [Autre contrôle connexe]** : le résultat du contrôle associé à la protection de la confidentialité de l'information désignée est traité adéquatement par d'autres contrôles connexes;
- **s.o.** : le contrôle est sans objet;
- **C [Confidentiel]** : le contrôle est directement lié à la protection de la confidentialité de l'information désignée.

Tableau 1 : Contrôle d'accès (AC)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
AC-01	Stratégie et procédures de contrôle d'accès	C	Stratégie et procédures 03.15.01
AC-02	Gestion des comptes	C	Gestion des comptes 03.01.01
AC-02(01)	Gestion des comptes : Gestion automatisée des comptes système	NCO	Aucune
AC-02(02)	Gestion des comptes : Gestion automatisée des comptes temporaires et des comptes d'urgence	NCO	Aucune
AC-02(03)	Gestion des comptes : Désactivation des comptes	C	Gestion des comptes 03.01.01
AC-02(04)	Gestion des comptes : Opérations automatisées de vérification	NCO	Aucune
AC-02(05)	Gestion des comptes : Fermeture de session en cas d'inactivité	C	Gestion des comptes 03.01.01
AC-02(07)	Gestion des comptes : Comptes d'utilisateur privilégiés	NCO	Aucune
AC-02(13)	Gestion des comptes : Désactivation des comptes des personnes à risque élevé	C	Gestion des comptes 03.01.01
AC-03	Application de l'accès	C	Application de l'accès 03.01.02
AC-03(02)	Application de l'accès : Double autorisation	NCO	Aucune
AC-03(04)	Application de l'accès : Contrôle d'accès discrétionnaire	ACC	Aucune

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
AC-03(09)	Application de l'accès : Diffusion contrôlée	ACC	Aucune
AC-04	Application du contrôle de flux d'information	C	Application du contrôle de flux d'information 03.01.03
AC-05	Séparation des tâches	C	Séparation des tâches 03.01.04
AC-06	Droit d'accès minimal	C	Droit d'accès minimal 03.01.05
AC-06(01)	Droit d'accès minimal : Autorisation de l'accès aux fonctions de sécurité	C	Droit d'accès minimal 03.01.05
AC-06(02)	Droit d'accès minimal : Accès non privilégié aux fonctions non liées à la sécurité	C	Droit d'accès minimal – Comptes privilégiés 03.01.06
AC-06(05)	Droit d'accès minimal : Comptes privilégiés	C	Droit d'accès minimal – Comptes privilégiés 03.01.06
AC-06(07)	Droit d'accès minimal : Examen des privilèges d'utilisateur	C	Droit d'accès minimal 03.01.05
AC-06(09)	Droit d'accès minimal : Journalisation de l'utilisation des fonctions privilégiées	C	Comptes privilégiés – Fonctions privilégiées 03.01.07
AC-06(10)	Droit d'accès minimal : Interdiction aux utilisatrices et utilisateurs non privilégiés d'exécuter des fonctions privilégiées	C	Comptes privilégiés – Fonctions privilégiées 03.01.07
AC-07	Tentatives d'ouverture de session infructueuses	C	Tentatives d'ouverture de session infructueuses 03.01.08
AC-08	Avis d'utilisation système	C	Avis d'utilisation système 03.01.09
AC-11	Verrouillage d'appareil	C	Verrouillage d'appareil 03.01.10
AC-11(01)	Verrouillage d'appareil : Masquage de l'affichage au moyen d'une image	C	Verrouillage d'appareil 03.01.10
AC-12	Fin de session	C	Fin de session 03.01.11
AC-14	Opérations permises sans identification ni authentification	GC	Aucune
AC-16	Attributs de sécurité et de confidentialité	ACC	Aucune
AC-16(02)	Attributs de sécurité et de confidentialité : Changements aux valeurs d'attribut par des personnes autorisées	ACC	Aucune
AC-16(05)	Attributs de sécurité et de confidentialité : Affichage d'attributs des objets transmis à des dispositifs de sortie	ACC	Aucune

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
AC-17	Accès à distance	C	Application de l'accès 03.01.02
AC-17(01)	Accès à distance : Surveillance et contrôle	NCO	Aucune
AC-17(02)	Accès à distance : Protection de la confidentialité et de l'intégrité au moyen du chiffrement	C	Tentatives d'ouverture de session infructueuses 03.01.08
AC-17(03)	Accès à distance : Points de contrôle d'accès gérés	C	Accès à distance 03.01.12
AC-17(04)	Accès à distance : Commandes et accès privilégiés	C	Accès à distance 03.01.12
AC-17(400)	Accès à distance : Accès à distance à des comptes privilégiés	ACC	Aucune
AC-18	Accès sans fil	C	Accès sans fil 03.01.16
AC-18(01)	Accès sans fil : Authentification et chiffrement	C	Accès sans fil 03.01.16
AC-18(03)	Accès sans fil : Désactivation du réseautage sans fil	C	Accès sans fil 03.01.16
AC-18(04)	Accès sans fil : Restriction des configurations par les utilisatrices et utilisateurs	ACC	Aucune
AC-19	Contrôle d'accès pour les appareils mobiles	C	Contrôle d'accès pour les dispositifs mobiles 03.01.18
AC-19(05)	Contrôle d'accès pour les dispositifs mobiles : Chiffrement complet des appareils ou chiffrement des contenants	C	Contrôle d'accès pour les dispositifs mobiles 03.01.18
AC-20	Utilisation de systèmes externes	C	Utilisation de systèmes externes 03.01.20
AC-20(01)	Utilisation de systèmes externes : Limites relatives à l'utilisation autorisée	C	Utilisation de systèmes externes 03.01.20
AC-20(02)	Utilisation de systèmes externes : Dispositifs de stockage portatifs – Utilisation restreinte	C	Utilisation de systèmes externes 03.01.20
AC-20(04)	Utilisation de systèmes externes : Dispositifs de stockage accessibles par réseau – Utilisation restreinte	ACC	Aucune
AC-21	Échange d'information	GC	Aucune
AC-21(400)	Échange d'information : Entente sur l'échange d'information	GC	Aucune
AC-21(401)	Échange d'information : Accord sur l'échange d'information	GC	Aucune
AC-22	Contenu à accès public	C	Contenu accessible au public 03.01.22

Tableau 2 : Sensibilisation et formation (AT)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adaptation	Exigence de sécurité
AT-01	Stratégie et procédures de sensibilisation et de formation	C	Stratégie et procédures 03.15.01
AT-02	Formation et sensibilisation en matière de sécurité	C	Formation et sensibilisation en matière de sécurité 03.02.01
AT-02(02)	Formation et sensibilisation en matière de sécurité : Menace interne	C	Formation et sensibilisation en matière de sécurité 03.02.01
AT-02(03)	Formation et sensibilisation en matière de sécurité : Piratage psychologique et exploration de données	C	Formation et sensibilisation en matière de sécurité 03.02.01
AT-03	Formation selon le rôle	C	Formation selon le rôle 03.02.02
AT-04	Dossiers de formation	NCO	Aucune

Tableau 3 : Vérification et responsabilisation (AU)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adaptation	Exigence de sécurité
AU-01	Stratégie et procédures de vérification et de responsabilisation	C	Stratégie et procédures 03.15.01
AU-02	Journalisation d'événements	C	Journalisation d'événements 03.03.01
AU-03	Contenu des enregistrements de vérification	C	Contenu des enregistrements de vérification 03.03.02
AU-03(01)	Information de vérification supplémentaire	C	Contenu des enregistrements de vérification 03.03.02
AU-04	Capacité de stockage des journaux de vérification	NCO	Aucune
AU-04(01)	Capacité de stockage des journaux de vérification : Transfert vers une autre capacité de stockage	NCO	Aucune

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
AU-05	Intervention en cas de défaillance du processus de journalisation des données de vérification	C	Intervention en cas d'échec du processus de journalisation des données de vérification 03.03.04
AU-05(01)	Intervention en cas d'échec du processus de journalisation des données de vérification : Avertissement de capacité de stockage	NCO	Aucune
AU-06	Examen, analyse et production de rapports liés aux enregistrements de vérification	C	Examen, analyse et production de rapports liés aux enregistrements de vérification 03.03.05
AU-06(01)	Examen, analyse et production de rapports liés aux enregistrements de vérification : Intégration de processus automatisés	NCO	Aucune
AU-06(03)	Examen, analyse et production de rapports liés aux enregistrements de vérification : Correspondance des dépôts pour les enregistrements de vérification	C	Examen, analyse et production de rapports liés aux enregistrements de vérification 03.03.05
AU-06(04)	Examen, analyse et production de rapports liés aux enregistrements de vérification : Analyses et examens centralisés	NCO	Aucune
AU-07	Réduction des enregistrements de vérification et génération de rapports	C	Réduction des enregistrements de vérification et génération de rapports 03.03.06
AU-07(01)	Réduction des enregistrements de vérification et génération de rapports : Traitement automatique	NCO	Aucune
AU-08	Horodatage	C	Horodatage 03.03.07
AU-09	Protection de l'information de vérification	C	Protection de l'information de vérification 03.03.08
AU-09(02)	Protection de l'information de vérification : Stockage sur un système ou un composant physique séparé	NCO	Aucune
AU-09(04)	Protection de l'information de vérification : Accès par un sous-ensemble d'utilisateurs privilégiés	C	Protection de l'information de vérification 03.03.08
AU-09(06)	Protection de l'information de vérification : Accès en lecture seule	NCO	Aucune
AU-11	Conservation des enregistrements de vérification	C	Génération d'enregistrements de vérification 03.03.03
AU-12	Génération d'enregistrements de vérification	C	Génération d'enregistrements de vérification 03.03.03

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adaptation	Exigence de sécurité
AU-12(01)	Génération d'enregistrements de vérification : Piste de vérification à l'échelle du système et corrélée dans le temps	NCO	Aucune

Tableau 4 : Évaluation, autorisation et surveillance (CA)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adaptation	Exigence de sécurité
CA-01	Stratégies et procédures d'évaluation, d'autorisation et de surveillance	C	Stratégie et procédures 03.15.01
CA-02	Évaluations de contrôle	C	Évaluation de sécurité 03.12.01
CA-02(01)	Évaluations de contrôle : Évaluatrices et évaluateurs indépendants	NCO	Aucune
CA-03	Échange d'information	C	Échange d'information 03.12.05
CA-05	Plans d'action et des jalons	C	Plan d'action et des jalons 03.12.02
CA-06	Autorisation	GC	Aucune
CA-07	Surveillance continue	C	Surveillance continue 03.12.03
CA-07(01)	Surveillance continue : Évaluation indépendante	NCO	Aucune
CA-07(04)	Surveillance continue : Surveillance des risques	NCO	Aucune
CA-09	Connexions des systèmes internes	NCO	Aucune
CA-09(01)	Connexions des systèmes internes : Vérifications de la conformité	ACC	Aucune

Tableau 5 : Gestion des configurations (CM)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adaptation	Exigence de sécurité
CM-01	Stratégie et procédures de gestion des configurations	C	Stratégie et procédures 03.15.01
CM-02	Configuration de référence	C	Configuration de référence 03.04.01
CM-02(02)	Configuration de référence : Automatisation du soutien aux fins d'exactitude et d'actualité	NCO	Aucune
CM-02(03)	Configuration de référence : Conservation des configurations antérieures	NCO	Aucune
CM-02(06)	Configuration de référence : Environnements de test et de développement	NCO	Aucune

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
CM-02(07)	Configuration de référence : Configuration des systèmes et des composants pour des zones à risque élevé	C	Configuration des systèmes et des composants pour des zones à risque élevé 03.04.12
CM-03	Contrôle des changements de configuration	C	Contrôle des changements de configuration 03.04.03
CM-03(02)	Contrôle des changements de configuration : Tests, validation et documentation des changements	NCO	Aucune
CM-03(04)	Contrôle des changements de configuration : Représentantes et représentants de la sécurité et de la protection de la vie privée	NCO	Aucune
CM-04	Analyses des répercussions	C	Analyses des répercussions 03.04.04
CM-04(01)	Analyses des répercussions : Environnements de test distincts	NCO	Aucune
CM-04(02)	Analyses des répercussions : Vérification des contrôles	C	Analyses des répercussions 03.04.04
CM-05	Restriction d'accès pour les changements	C	Restriction d'accès pour les changements 03.04.05
CM-06	Paramètres de configuration	C	Paramètres de configuration 03.04.02
CM-07	Fonctionnalité minimale	C	Fonctionnalité minimale 03.04.06
CM-07(01)	Fonctionnalité minimale : Examen périodique	C	Fonctionnalité minimale 03.04.06
CM-07(02)	Fonctionnalité minimale : Prévention de l'exécution des programmes	ACC	Aucune
CM-07(05)	Fonctionnalité minimale : Logiciels autorisés – Autorisation par exception	C	Logiciels autorisés – Autorisation par exception 03.04.08
CM-08	Inventaire des composants du système	C	Inventaire des composants du système 03.04.10
CM-08(01)	Inventaire des composants du système : Mises à jour durant l'installation et le retrait	C	Inventaire des composants du système 03.04.10
CM-08(03)	Inventaire des composants du système : Détection automatisée de composants non autorisés	NCO	Aucune
CM-08(04)	Inventaire des composants du système : Information sur la comptabilisation	NCO	Aucune

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adaptation	Exigence de sécurité
CM-08(06)	Inventaire des composants du système : Configurations évaluées et écarts approuvés	NCO	Aucune
CM-09	Plan de gestion des configurations	NCO	Aucune
CM-10	Restrictions relatives à l'utilisation des logiciels	NCO	Aucune
CM-11	Logiciels installés par les utilisatrices et utilisateurs	ACC	Aucune
CM-11(02)	Logiciels installés par les utilisatrices et utilisateurs : Installation de logiciels avec statut privilégié	ACC	Aucune
CM-12	Emplacement de l'information	C	Emplacement de l'information 03.04.11
CM-12(01)	Emplacement de l'information : Outils automatisés associés à l'emplacement de l'information	NCO	Aucune

Tableau 6 : Planification d'urgence (CP)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adaptation	Exigence de sécurité
CP-01	Stratégie et procédures de planification d'urgence	NCO	Aucune
CP-02	Plan d'urgence	NCO	Aucune
CP-02(01)	Plan d'urgence : Coordination avec les plans connexes	NCO	Aucune
CP-02(02)	Plan d'urgence : Planification de la capacité	NCO	Aucune
CP-02(03)	Plan d'urgence : Reprise de la mission et des activités	NCO	Aucune
CP-02(08)	Plan d'urgence : Désignation des actifs essentiels	NCO	Aucune
CP-03	Formation sur les mesures d'urgence	NCO	Aucune
CP-04	Tests relatifs au plan d'urgence	NCO	Aucune
CP-04(01)	Tests relatifs au plan d'urgence : Coordination avec les plans connexes	NCO	Aucune
CP-06	Autre site de stockage	NCO	Aucune
CP-06(01)	Autre site de stockage : Séparation du site principal	NCO	Aucune
CP-06(03)	Autre site de stockage : Accessibilité	NCO	Aucune
CP-07	Autre site de traitement	NCO	Aucune
CP-07(01)	Autre site de traitement : Séparation du site principal	NCO	Aucune
CP-07(02)	Autre site de traitement : Accessibilité	NCO	Aucune
CP-07(03)	Autre site de traitement : Priorité de service	NCO	Aucune
CP-07(04)	Autre site de traitement : Préparation en vue de l'utilisation	NCO	Aucune
CP-07(06)	Autre site de traitement : Impossibilité de retourner au site principal	NCO	Aucune

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
CP-08	Services de télécommunications	NCO	Aucune
CP-08(01)	Services de télécommunications : Dispositions de priorité de service	NCO	Aucune
CP-08(02)	Services de télécommunications : Points de défaillance uniques	NCO	Aucune
CP-08(03)	Services de télécommunications : Séparation des fournisseurs principaux et autres	NCO	Aucune
CP-08(05)	Services de télécommunications : Test des services de télécommunications de secours	NCO	Aucune
CP-09	Sauvegarde du système	C	Sauvegarde du système – Protection cryptographique 03.08.09
CP-09(01)	Sauvegarde du système : Tests de fiabilité et d'intégrité	NCO	Aucune
CP-09(03)	Sauvegarde du système : Stockage distinct pour l'information essentielle	NCO	Aucune
CP-09(05)	Sauvegarde du système : Transfert vers un autre site de stockage	NCO	Aucune
CP-09(07)	Sauvegarde du système : Double autorisation pour la suppression ou la destruction	NCO	Aucune
CP-09(08)	Sauvegarde du système : Protection cryptographique	C	Sauvegarde du système – Protection cryptographique 03.08.09
CP-10	Reprise et reconstitution du système	NCO	Aucune
CP-10(02)	Reprise et reconstitution du système : Reprise des transactions	NCO	Aucune
CP-10(04)	Reprise et reconstitution du système : Restauration dans les délais précisés	NCO	Aucune
CP-10(06)	Reprise et reconstitution du système : Protection des composants	NCO	Aucune

Tableau 7 : Identification et authentification (IA)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
IA-01	Stratégie et procédures d'identification et d'authentification	C	Stratégie et procédures 03.15.01

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
IA-02	Identification et authentification (utilisatrices et utilisateurs de l'organisation)	C	Identification, authentification et réauthentification des utilisatrices et utilisateurs 03.05.01
IA-02(01)	Identification et authentification (utilisatrices et utilisateurs de l'organisation) : Authentification multifacteur pour les comptes privilégiés	C	Authentification multifacteur 03.05.03
IA-02(02)	Identification et authentification (utilisatrices et utilisateurs de l'organisation) : Authentification multifacteur pour les comptes non privilégiés	C	Authentification multifacteur 03.05.03
IA-02(08)	Identification et authentification (utilisatrices et utilisateurs de l'organisation) : Accès aux comptes – Résistant à la réinsertion	C	Authentification résistant à la réinsertion 03.05.04
IA-02(10)	Identification et authentification (utilisatrices et utilisateurs de l'organisation) : Authentification unique	NCO	Aucune
IA-02(12)	Identification et authentification (utilisatrices et utilisateurs de l'organisation) : Utilisation de jeton matériel du GC basé sur des justificatifs d'identité d'ICP	GC	Aucune
IA-03	Identification et authentification des dispositifs	C	Identification et authentification des dispositifs 03.05.02
IA-04	Gestion des identifiants	C	Gestion des identifiants 03.05.05
IA-04(04)	Gestion des identifiants : Établissement du statut d'une utilisatrice ou un utilisateur	C	Gestion des identifiants 03.05.05
IA-05	Gestion des authentifiants	C	Gestion des authentifiants 03.05.12
IA-05(01)	Gestion des authentifiants : Authentification basée sur mot de passe	C	Gestion des mots de passe 03.05.07
IA-05(02)	Gestion des authentifiants : Authentification basée sur clé publique	GC	Aucune
IA-05(06)	Gestion des authentifiants : Protection des authentifiants	GC	Aucune
IA-05(07)	Gestion des authentifiants : Aucun authentifiant statique intégré non chiffré	NCO	Aucune
IA-05(08)	Gestion des authentifiants : Comptes de systèmes multiples	NCO	Aucune
IA-05(09)	Gestion des authentifiants : Gestion des justificatifs d'identité fédérés	GC	Aucune
IA-05(13)	Gestion des authentifiants : Expiration d'authentifiants en mémoire cache	ACC	Aucune
IA-05(14)	Gestion des authentifiants : Gestion du contenu des magasins de confiance d'ICP	GC	Aucune

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
IA-06	Rétroaction d'authentification	C	Rétroaction d'authentification 03.05.11
IA-07	Authentification du module cryptographique	GC	Aucune
IA-08	Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation)	GC	Aucune
IA-08(01)	Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) : Acceptation des justificatifs d'identité d'ICP d'autres organismes	GC	Aucune
IA-08(02)	Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) : Acceptation des authentifiants externes	GC	Aucune
IA-08(04)	Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) : Utilisation de profils définis	GC	Aucune
IA-11	Réauthentification	C	Identification, authentification et réauthentification des utilisatrices et utilisateurs 03.05.01
IA-12	Confirmation de l'identité	GC	Aucune
IA-12(02)	Confirmation de l'identité : Preuve d'identité	GC	Aucune
IA-12(03)	Confirmation de l'identité : Validation et vérification de preuve d'identité	GC	Aucune
IA-12(04)	Confirmation de l'identité : Validation et vérification en personne	GC	Aucune
IA-12(05)	Confirmation de l'identité : Confirmation d'adresse	GC	Aucune

Tableau 8 : Intervention en cas d'incident (IR)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
IR-01	Stratégie et procédure d'intervention en cas d'incident	C	Stratégie et procédures 03.15.01
IR-02	Formation d'intervention en cas d'incident	C	Formation d'intervention en cas d'incident 03.06.04
IR-03	Tests d'intervention en cas d'incident	C	Tests d'intervention en cas d'incident 03.06.03
IR-03(02)	Tests d'intervention en cas d'incident : Coordination avec les plans connexes	NCO	Aucune

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
IR-04	Traitement des incidents	C	Traitement des incidents 03.06.01
IR-04(03)	Traitement des incidents : Continuité des opérations	NCO	Aucune
IR-04(08)	Traitement des incidents : Corrélation avec des organisations externes	NCO	Aucune
IR-04(09)	Traitement des incidents : Capacités d'intervention dynamique	NCO	Aucune
IR-05	Surveillance des incidents	C	Surveillance des incidents, signalement des incidents et assistance en cas d'incident 03.06.02
IR-06	Signalement des incidents	C	Surveillance des incidents, signalement des incidents et assistance en cas d'incident 03.06.02
IR-06(01)	Signalement des incidents : Signalement automatisé	NCO	Aucune
IR-06(02)	Signalement des incidents : Vulnérabilités liées aux incidents	NCO	Aucune
IR-06(03)	Signalement des incidents : Coordination avec la chaîne d'approvisionnement	NCO	Aucune
IR-07	Assistance en cas d'incident	C	Surveillance des incidents, signalement des incidents et assistance en cas d'incident 03.06.02
IR-07(01)	Assistance en cas d'incident : Soutien automatisé concernant la disponibilité de l'information et du soutien	NCO	Aucune
IR-08	Plan d'intervention en cas d'incident	C	Plan d'intervention en cas d'incident 03.06.05

Tableau 9 : Maintenance (MA)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
MA-01	Stratégie et procédures de maintenance des systèmes	C	Stratégie et procédures 03.15.01
MA-02	Maintenance contrôlée	NCO	Aucune

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adaptation	Exigence de sécurité
MA-03	Outils de maintenance	C	Outils de maintenance 03.07.04
MA-03(01)	Outils de maintenance : Inspection des outils	C	Outils de maintenance 03.07.04
MA-03(02)	Outils de maintenance : Inspection des supports	C	Outils de maintenance 03.07.04
MA-03(03)	Outils de maintenance : Prévention des retraits non autorisés	C	Outils de maintenance 03.07.04
MA-04	Maintenance non locale	C	Maintenance non locale 03.07.05
MA-04(01)	Maintenance non locale : Journalisation et examen	NCO	Aucune
MA-04(03)	Maintenance non locale : Sécurité et nettoyage comparables	ACC	Aucune
MA-04(04)	Maintenance non locale : Authentification et séparation des sessions de maintenance	ACC	Aucune
MA-04(05)	Maintenance non locale : Approbations et avis	ACC	Aucune
MA-04(06)	Maintenance non locale : Protection cryptographique	ACC	Aucune
MA-05	Personnel de maintenance	C	Personnel de maintenance 03.07.06
MA-05(01)	Personnel de maintenance : Personnes ne détenant pas l'accès approprié	ACC	Aucune
MA-06	Maintenance opportune	NCO	Aucune

Tableau 10 : Protection des supports (MP)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adaptation	Exigence de sécurité
MP-01	Stratégie et procédures de protection des supports	C	Stratégie et procédures 03.15.01
MP-02	Accès aux supports	C	Accès aux supports 03.08.02
MP-03	Marquage des supports	C	Marquage des supports 03.08.04
MP-04	Entreposage des supports	C	Entreposage des supports 03.08.01
MP-05	Transport des supports	C	Transport des supports 03.08.05

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
MP-06	Nettoyage des supports	C	Nettoyage des supports 03.08.03
MP-06(03)	Nettoyage des supports : Techniques non destructives	ACC	Aucune
MP-06(08)	Nettoyage des supports : Purge ou nettoyage à distance de l'information	ACC	Aucune
MP-07	Utilisation des supports	C	Utilisation des supports 03.08.07
MP-08	Déclassement des supports	ACC	Aucune
MP-08(03)	Déclassement des supports : Information protégée	ACC	Aucune

Tableau 11 : Protection physique et environnementale (PE)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
PE-01	Stratégie et procédures de protection physique et environnementale	C	Stratégie et procédures 03.15.01
PE-02	Autorisations d'accès physique	C	Autorisations d'accès physique 03.10.01
PE-02(400)	Autorisations d'accès physique : Exigences des cartes d'identité	GC	Aucune
PE-03	Contrôle d'accès physique	C	Contrôle d'accès physique 03.10.07
PE-03(400)	Contrôle d'accès physique : Inspections de sécurité	GC	Aucune
PE-04	Contrôle d'accès pour la transmission	C	Contrôle d'accès pour la transmission 03.10.08
PE-05	Contrôle d'accès aux dispositifs de sortie	C	Contrôle d'accès physique 03.10.07
PE-06	Surveillance de l'accès physique	C	Surveillance de l'accès physique 03.10.02
PE-06(01)	Surveillance de l'accès physique : Alarmes de détection d'intrusion et équipement de surveillance	NCO	Aucune
PE-08	Registre des accès des visiteuses et visiteurs	NCO	Aucune
PE-09	Équipement et câblage d'alimentation	NCO	Aucune
PE-10	Arrêt d'urgence	NCO	Aucune
PE-11	Alimentation d'urgence	NCO	Aucune
PE-12	Éclairage d'urgence	NCO	Aucune
PE-13	Protection contre les incendies	NCO	Aucune
PE-13(01)	Protection contre les incendies : Systèmes de détection – Activation et avis automatiques	NCO	Aucune
PE-13(04)	Protection contre les incendies : Inspections	NCO	Aucune

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adaptation	Exigence de sécurité
PE-13(400)	Protection contre les incendies : Services d'urgence	NCO	Aucune
PE-14	Contrôles environnementaux	NCO	Aucune
PE-15	Protection contre les dégâts d'eau	NCO	Aucune
PE-16	Livraison et retrait	NCO	Aucune
PE-17	Autres lieux de travail	C	Autres lieux de travail 03.10.06
PE-400	Environnements à distance et de télétravail	GC	Aucune
PE-400(01)	Environnements à distance et de télétravail : Entreposage physique d'information et d'actifs	GC	Aucune
PE-400(02)	Environnements à distance et de télétravail : Travail à distance et télétravail à l'étranger	GC	Aucune
PE-401	Centre des opérations de sécurité	NCO	Aucune

Tableau 12 : Planification (PL)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adaptation	Exigence de sécurité
PL-01	Stratégie et procédures de planification	C	Stratégie et procédures 03.15.01
PL-02	Plans de sécurité et de confidentialité du système	C	Plan de sécurité du système 03.15.02
PL-04	Règles de conduite	C	Règles de conduite 03.15.03
PL-04(01)	Règles de conduite : Restriction d'utilisation des médias sociaux et des sites et applications externes	NCO	Aucune
PL-08	Architectures de sécurité et de confidentialité	NCO	Aucune
PL-10	Sélection de base	GC	Aucune
PL-11	Adaptation de base	GC	Aucune

Tableau 13 : Gestion des programmes (PM)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adaptation	Exigence de sécurité
PM-01	Plan du programme de sécurité de l'information	s.o.	Aucune
PM-02	Rôle de leadership pour le programme de sécurité de l'information	s.o.	Aucune
PM-03	Ressources de sécurité et de confidentialité de l'information	s.o.	Aucune

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
PM-04	Processus du plan d'action et des jalons	s.o.	Aucune
PM-05	Inventaire des systèmes et des programmes	s.o.	Aucune
PM-05(01)	Inventaire des systèmes : Inventaire des renseignements personnels	s.o.	Aucune
PM-06	Mesures du rendement	s.o.	Aucune
PM-07	Architecture d'entreprise	s.o.	Aucune
PM-07(01)	Architecture d'entreprise : Déchargement	s.o.	Aucune
PM-08	Plan pour les infrastructures essentielles	s.o.	Aucune
PM-09	Stratégie de gestion des risques	s.o.	Aucune
PM-10	Processus d'autorisation	s.o.	Aucune
PM-11	Définition des processus liés à la mission et aux activités	s.o.	Aucune
PM-12	Programme de protection contre la menace interne	s.o.	Aucune
PM-13	Effectif de sécurité et de confidentialité	s.o.	Aucune
PM-14	Tests, formation et surveillance	s.o.	Aucune
PM-15	Groupes et associations de sécurité et de confidentialité	s.o.	Aucune
PM-16	Programme de sensibilisation aux menaces	s.o.	Aucune
PM-16(01)	Programme de sensibilisation aux menaces : Moyens automatisés pour l'échange de renseignement sur les menaces	s.o.	Aucune
PM-17	Protection de l'information désignée sur les systèmes externalisés	s.o.	Aucune
PM-18	Plan du programme de confidentialité	s.o.	Aucune
PM-19	Rôle de leadership du programme de confidentialité	s.o.	Aucune
PM-20	Communication des principaux services de confidentialité	s.o.	Aucune
PM-20(01)	Communication des principaux services de confidentialité : Politiques de confidentialité pour les sites Web, les applications et les services numériques	s.o.	Aucune
PM-21	Maintien d'un registre des divulgations	s.o.	Aucune
PM-22	Gestion de la qualité des renseignements personnels	s.o.	Aucune
PM-23	Comité de gouvernance des données	s.o.	Aucune
PM-24	Conseil de l'intégrité des données	s.o.	Aucune
PM-25	Réduction des renseignements personnels utilisés dans les tests, la formation et la recherche	s.o.	Aucune
PM-26	Gestion des plaintes	s.o.	Aucune
PM-27	Génération de rapports concernant la protection de la vie privée	s.o.	Aucune
PM-28	Cadrage des risques	s.o.	Aucune
PM-29	Rôles de leadership pour le programme de gestion des risques	s.o.	Aucune
PM-30	Stratégie de gestion des risques liés à la chaîne d'approvisionnement	s.o.	Aucune
PM-30(01)	Stratégie de gestion des risques liés à la chaîne d'approvisionnement : Fournisseurs d'articles critiques ou essentiels à la mission	s.o.	Aucune
PM-31	Stratégie de surveillance continue	s.o.	Aucune
PM-32	Définition de l'objectif	s.o.	Aucune

Tableau 14 : Sécurité du personnel (PS)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
PS-01	Stratégie et procédures de sécurité du personnel	C	Stratégie et procédures 03.15.01
PS-02	Analyse de sécurité des postes	GC	Aucune
PS-03	Filtrage de sécurité du personnel	C	Filtrage de sécurité du personnel 03.09.01
PS-04	Cessation d'emploi	C	Cessation d'emploi et mutation de personnel 03.09.02
PS-05	Mutation de personnel	C	Cessation d'emploi et mutation de personnel 03.09.02
PS-06	Ententes d'accès	NCO	Aucune
PS-07	Sécurité du personnel externe	NCO	Aucune
PS-08	Sanctions imposées au personnel	NCO	Aucune
PS-09	Descriptions de poste	GC	Aucune

Tableau 15 : Traitement des renseignements personnels et transparence (PT)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
PT-01	Stratégie et procédures de traitement des renseignements personnels et de transparence	s.o.	Aucune
PT-02	Pouvoir en matière de collecte et d'utilisation de renseignements personnels	s.o.	Aucune
PT-02(01)	Pouvoir en matière de collecte et d'utilisation de renseignements personnels : Étiquetage des données	s.o.	Aucune
PT-02(02)	Pouvoir en matière de collecte et d'utilisation de renseignements personnels : Automatisation	s.o.	Aucune
PT-03	Traitement, utilisation et divulgation de renseignements personnels	s.o.	Aucune
PT-03(01)	Traitement, utilisation et divulgation de renseignements personnels : Étiquetage des données	s.o.	Aucune
PT-03(02)	Traitement, utilisation et divulgation de renseignements personnels : Automatisation	s.o.	Aucune
PT-04	Consentement	s.o.	Aucune
PT-04(01)	Consentement : Consentement adapté au gouvernement du Canada	s.o.	Aucune

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adaptation	Exigence de sécurité
PT-04(02)	Consentement : Consentement opportun	s.o.	Aucune
PT-04(03)	Consentement : Révocation	s.o.	Aucune
PT-04(400)	Consentement : Consentement adapté au secteur privé	s.o.	Aucune
PT-05	Énoncé sur la protection de la vie privée	s.o.	Aucune
PT-05(01)	Énoncé sur la protection de la vie privée : Énoncés sur la protection de la vie privée en temps opportun	s.o.	Aucune
PT-05(02)	Énoncé sur la protection de la vie privée : Énoncés sur la protection de la vie privée	s.o.	Aucune
PT-06	Fichiers de renseignements personnels	s.o.	Aucune
PT-06(01)	Fichiers de renseignements personnels : Utilisations et divulgations compatibles	s.o.	Aucune
PT-06(02)	Fichiers de renseignements personnels : Fichiers inconsultables	s.o.	Aucune
PT-07	Renseignements personnels particulièrement sensibles	s.o.	Aucune
PT-07(01)	Renseignements personnels particulièrement sensibles : Numéros d'assurance sociale	s.o.	Aucune
PT-07(02)	Renseignements personnels particulièrement sensibles : *Charte canadienne des droits et libertés*	s.o.	Aucune
PT-07(400)	Renseignements personnels particulièrement sensibles : Secteur privé	s.o.	Aucune
PT-08	Exigences de correspondance de données	s.o.	Aucune

Tableau 16 : Évaluation des risques (RA)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adaptation	Exigence de sécurité
RA-01	Stratégie et procédures d'évaluation des risques	C	Stratégie et procédures 03.15.01
RA-02	Catégorisation de sécurité	GC	Aucune
RA-03	Évaluation des risques	C	Évaluation des risques 03.11.01
RA-03(01)	Évaluation des risques : Évaluation des risques liés à la chaîne d'approvisionnement	C	Évaluation des risques 03.11.01
RA-05	Surveillance et analyse des vulnérabilités	C	Surveillance et analyse des vulnérabilités 03.11.02
RA-05(02)	Surveillance et analyse des vulnérabilités : Mise à jour de la liste de vulnérabilités à analyser	C	Surveillance et analyse des vulnérabilités 03.11.02
RA-05(05)	Surveillance et analyse des vulnérabilités : Accès privilégiés	ACC	Aucune

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
RA-05(11)	Surveillance et analyse des vulnérabilités : Programme de divulgation publique	NCO	Aucune
RA-07	Réponse aux risques	C	Réponse aux risques 03.11.04
RA-09	Analyse de criticité	NCO	Aucune

Tableau 17 : Acquisition des systèmes et des services (SA)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
SA-01	Stratégie et procédures d'acquisition des systèmes et des services	C	Stratégie et procédures 03.15.01
SA-02	Affectation des ressources	NCO	Aucune
SA-03	Cycle de développement des systèmes	NCO	Aucune
SA-04	Processus d'acquisition	NCO	Aucune
SA-04(01)	Processus d'acquisition : Propriétés fonctionnelles des contrôles	NCO	Aucune
SA-04(09)	Processus d'acquisition : Fonctions, ports, protocoles et services utilisés	NCO	Aucune
SA-04(10)	Processus d'acquisition : Utilisation de produits de justificatifs d'identité numériques approuvés	GC	Aucune
SA-04(12)	Processus d'acquisition : Propriété des données	GC	Aucune
SA-05	Documentation relative aux systèmes	NCO	Aucune
SA-08	Principes d'ingénierie de la sécurité et de la confidentialité	C	Principes d'ingénierie de la sécurité 03.16.01
SA-09	Services de systèmes externes	C	Services de systèmes externes 03.16.03
SA-09(01)	Services de systèmes externes : Évaluations des risques et approbations organisationnelles	NCO	Aucune
SA-09(02)	Services de systèmes externes : Établissement des fonctions, des ports, des protocoles et des services	ACC	Aucune
SA-10	Gestion des configurations par les développeuses et développeurs	NCO	Aucune
SA-10(01)	Gestion des configurations par les développeuses et développeurs : Vérification de l'intégrité des logiciels et des micrologiciels	NCO	Aucune
SA-11	Tests et évaluations effectués par les développeuses et développeurs	NCO	Aucune
SA-15	Processus, normes et outils de développement	NCO	Aucune
SA-15(03)	Processus, normes et outils de développement : Analyse de criticité	NCO	Aucune
SA-16	Formation offerte par la développeuse ou le développeur	NCO	Aucune
SA-17	Architecture et conception de la sécurité et de la confidentialité de la développeuse ou du développeur	NCO	Aucune

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adaptation	Exigence de sécurité
SA-22	Composants de systèmes non pris en charge	C	Composants de systèmes non pris en charge 03.16.02

Tableau 18 : Protection des systèmes et des communications (SC)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adaptation	Exigence de sécurité
SC-01	Stratégie et procédures de protection des systèmes et des communications	C	Stratégie et procédures 03.15.01
SC-02	Séparation des fonctionnalités des utilisatrices, des utilisateurs et du système	ACC	Aucune
SC-04	Information dans les ressources système partagées	C	Information dans les ressources système partagées 03.13.04
SC-05	Protection contre les dénis de service	NCO	Aucune
SC-05(02)	Protection contre les dénis de service : Capacité, bande passante et redondance	NCO	Aucune
SC-05(03)	Protection contre les dénis de service : Détection et surveillance	NCO	Aucune
SC-07	Protection de périmètre	C	Protection de périmètre 03.13.01
SC-07(03)	Protection de périmètre : Points d'accès	ACC	Aucune
SC-07(04)	Protection de périmètre : Services de télécommunications externes	ACC	Aucune
SC-07(05)	Protection de périmètre : Refus par défaut – Autorisation par exception	C	Communications réseau – Refus par défaut – Autorisation par exception 03.13.06
SC-07(07)	Protection de périmètre : Tunnellisation partagée pour les appareils distants	ACC	Aucune
SC-07(08)	Protection de périmètre : Acheminement du trafic vers des serveurs mandataires authentifiés	ACC	Aucune
SC-07(09)	Protection de périmètre : Restriction du trafic de communications malveillant sortant	NCO	Aucune
SC-07(11)	Protection de périmètre : Trafic de communications entrant	NCO	Aucune
SC-07(12)	Protection de périmètre : Protection au niveau de l'hôte	ACC	Aucune
SC-07(13)	Protection de périmètre : Isolation des outils de sécurité, des mécanismes et des composants de soutien	NCO	Aucune

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
SC-08	Confidentialité et intégrité des transmissions	C	Confidentialité lors de la transmission et du stockage 03.13.08
SC-08(01)	Confidentialité et intégrité des transmissions : Protection cryptographique	C	Confidentialité lors de la transmission et du stockage 03.13.08
SC-10	Déconnexion réseau	C	Déconnexion réseau 03.13.09
SC-12	Établissement et gestion des clés cryptographiques	C	Établissement et gestion des clés cryptographiques 03.13.10
SC-12(01)	Établissement et gestion des clés cryptographiques : Disponibilité	NCO	Aucune
SC-13	Protection cryptographique	C	Protection cryptographique 03.13.11
SC-15	Applications et appareils informatiques collaboratifs	C	Applications et appareils informatiques collaboratifs 03.13.12
SC-15(03)	Applications et appareils informatiques collaboratifs : Désactivation et retrait dans les zones de travail sécurisées	GC	Aucune
SC-17	Certificats d'infrastructure à clé publique	GC	Aucune
SC-18	Code mobile	C	Code mobile 03.13.13
SC-18(01)	Code mobile : Établissement du code inadéquat et application de mesures correctives	NCO	Aucune
SC-18(02)	Code mobile : Acquisition, développement et utilisation	NCO	Aucune
SC-18(03)	Code mobile : Prévention du téléchargement et de l'exécution	NCO	Aucune
SC-18(04)	Code mobile : Prévention de l'exécution automatique	NCO	Aucune
SC-18(05)	Code mobile : Autorisation d'exécution seulement dans les environnements clos	NCO	Aucune
SC-20	Service sécurisé de résolution de nom ou d'adresse (source faisant autorité)	NCO	Aucune
SC-21	Service sécurisé de résolution de nom ou d'adresse (résolveur récursif ou cache)	NCO	Aucune
SC-22	Architecture et prestation de services de résolution de nom ou d'adresse	NCO	Aucune
SC-23	Authenticité des sessions	C	Authenticité des sessions 03.13.15
SC-23(01)	Authenticité des sessions : Annulation de la validation des identificateurs de session lors de la fermeture de session	ACC	Aucune

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adaptation	Exigence de sécurité
SC-23(03)	Authenticité des sessions : Identificateurs de session uniques générés par le système	ACC	Aucune
SC-28	Protection de l'information au repos	C	Confidentialité lors de la transmission et du stockage 03.13.08
SC-28(01)	Protection de l'information au repos : Protection cryptographique	C	Confidentialité lors de la transmission et du stockage 03.13.08
SC-29	Hétérogénéité	NCO	Aucune
SC-39	Isolation des processus	NCO	Aucune

Tableau 19 : Intégrité de l'information et des systèmes (SI)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adaptation	Exigence de sécurité
SI-01	Stratégie et procédures d'intégrité de l'information et des systèmes	C	Stratégie et procédures 03.15.01
SI-02	Correction des défauts	C	Correction des défauts 03.14.01
SI-02(02)	Correction des défauts : État automatisé de la correction des défauts	NCO	Aucune
SI-02(06)	Correction des défauts : Retrait des versions antérieures des logiciels et des micrologiciels	NCO	Aucune
SI-03	Protection contre les programmes malveillants	C	Protection contre les programmes malveillants 03.14.02
SI-03(04)	Protection contre les programmes malveillants : Mises à jour effectuées seulement par les utilisatrices et utilisateurs privilégiés	NCO	Aucune
SI-04	Surveillance du système	C	Surveillance des systèmes 03.14.06
SI-04(02)	Surveillance du système : Outils et mécanismes automatisés aux fins d'analyse en temps réel	NCO	Aucune
SI-04(04)	Surveillance du système : Trafic de communications entrant et sortant	C	Surveillance des systèmes 03.14.06
SI-04(05)	Surveillance du système : Alertes générées par le système	NCO	Aucune
SI-04(10)	Surveillance du système : Visibilité des communications chiffrées	NCO	Aucune
SI-04(11)	Surveillance du système : Analyse des anomalies du trafic de communications	NCO	Aucune
SI-04(12)	Surveillance du système : Alertes automatisées générées par l'organisation	NCO	Aucune

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
SI-04(13)	Surveillance du système : Analyse du trafic et des tendances des événements	NCO	Aucune
SI-04(14)	Surveillance du système : Détection d'intrusion sans fil	NCO	Aucune
SI-04(15)	Surveillance du système : Communications entre un réseau sans fil et un réseau filaire	NCO	Aucune
SI-05	Alertes, avis et directives de sécurité	C	Alertes, avis et directives de sécurité 03.14.03
SI-07	Intégrité des logiciels, des micrologiciels et de l'information	NCO	Aucune
SI-07(01)	Intégrité des logiciels, des micrologiciels et de l'information : Vérifications de l'intégrité	NCO	Aucune
SI-07(02)	Intégrité des logiciels, des micrologiciels et de l'information : Automatisation des avis d'atteinte à l'intégrité	NCO	Aucune
SI-07(03)	Intégrité des logiciels, des micrologiciels et de l'information : Outils de vérification de l'intégrité gérés de façon centralisée	NCO	Aucune
SI-07(07)	Intégrité des logiciels, des micrologiciels et de l'information : Intégration de la détection et de l'intervention	NCO	Aucune
SI-08	Protection contre les pourriels	ACC	Aucune
SI-08(02)	Protection contre les pourriels : Mises à jour automatiques	NCO	Aucune
SI-10	Validation de la saisie d'information	NCO	Aucune
SI-11	Traitement des erreurs	NCO	Aucune
SI-12	Gestion et conservation de l'information	C	Gestion et conservation de l'information 03.14.08
SI-16	Protection de la mémoire	NCO	Aucune
SI-400	Poste de travail administratif dédié	C	Station de travail administrative dédiée 03.14.09

Tableau 20 : Gestion des risques liés à la chaîne d'approvisionnement (SR)

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
SR-01	Stratégie et procédures de gestion des risques liés à la chaîne d'approvisionnement	C	Stratégie et procédures 03.15.01
SR-02	Plan de gestion des risques liés à la chaîne d'approvisionnement	C	Plan de gestion des risques liés à la chaîne d'approvisionnement 03.17.01

No de contrôle ou d'activité	Profil d'incidence moyenne dans l'ITSP.10.033-01	Critères d'adapta-tion	Exigence de sécurité
SR-02(01)	Plan de gestion des risques liés à la chaîne d'approvisionnement : Établissement des équipes de GRCA	NCO	Aucune
SR-03	Contrôles et processus de la chaîne d'approvisionnement	C	Exigences et processus de la chaîne d'approvisionnement 03.17.03
SR-05	Stratégies, outils et méthodes d'acquisition	C	Stratégies, outils et méthodes d'acquisition 03.17.02
SR-06	Évaluations et examens des fournisseurs	C	Évaluation des risques 03.11.01
SR-08	Ententes de notification	NCO	Aucune
SR-10	Inspection des systèmes ou des composants	NCO	Aucune
SR-11	Authenticité des composants	NCO	Aucune
SR-11(01)	Authenticité des composants : Formation anticontrefaçon	NCO	Aucune
SR-11(02)	Authenticité des composants : Contrôle des configurations pour l'entretien et la réparation des composants	NCO	Aucune
SR-12	Mise hors service des composants	ACC	Aucune

Annexe B Paramètres définis par l'organisation

Cette annexe énumère les paramètres définis par l'organisation (ODP) qui sont inclus dans les exigences de sécurité de la section 3. Les ODP sont énumérés de façon séquentielle en fonction de la famille d'exigences, en commençant par la première exigence contenant un ODP dans la famille Contrôle d'accès (AC) et en terminant par la dernière exigence contenant un ODP dans la famille Gestion des risques liés à la chaîne d'approvisionnement (SR).

Tableau 21 : Paramètres définis par l'organisation

Exigence de sécurité	Paramètre défini par l'organisation
Gestion des comptes 03.01.01.F.02	[Affectation : période définie par l'organisation]
Gestion des comptes 03.01.01.G.01	[Affectation : période définie par l'organisation]
Gestion des comptes 03.01.01.G.02	[Affectation : période définie par l'organisation]
Gestion des comptes 03.01.01.G.03	[Affectation : période définie par l'organisation]
Gestion des comptes 03.01.01.H	[Affectation : période définie par l'organisation]
Gestion des comptes 03.01.01.H	[Affectation : circonstances définies par l'organisation]
Droit d'accès minimal 03.01.05.B	[Affectation : fonctions de sécurité définies par l'organisation]
Droit d'accès minimal 03.01.05.B	[Affectation : information liée à la sécurité définie par l'organisation]
Droit d'accès minimal 03.01.05.C	[Affectation : fréquence définie par l'organisation]
Droit d'accès minimal – Comptes privilégiés 03.01.06.A	[Affectation : personnel ou rôles définis par l'organisation]
Tentatives d'ouverture de session infructueuses 03.01.08.A	[Affectation : nombre défini par l'organisation]
Tentatives d'ouverture de session infructueuses 03.01.08.A	[Affectation : période définie par l'organisation]
Tentatives d'ouverture de session infructueuses 03.01.08.B	[Sélection (un choix ou plus) : verrouiller le compte ou le nœud pendant [Affectation : période définie par l'organisation]; verrouiller le compte ou le nœud jusqu'à ce qu'une administratrice ou un administrateur le libère; retarder la prochaine invite d'ouverture de session; aviser l'administratrice ou administrateur de système; effectuer une autre opération]
Verrouillage d'appareil 03.01.10.A	[Sélection (un choix ou plus) : en procédant à un verrouillage d'appareil après [Affectation : période définie par l'organisation] d'inactivité; en exigeant que l'utilisatrice ou utilisateur procède à un verrouillage d'appareil avant de laisser le système sans surveillance]
Fin de session 03.01.11	[Affectation : conditions ou événements déclenchant une déconnexion définis par l'organisation]
Utilisation de systèmes externes 03.01.20.B	[Affectation : exigences de sécurité définies par l'organisation]
Formation et sensibilisation en matière de sécurité 03.02.01.A.01	[Affectation : fréquence définie par l'organisation]
Formation et sensibilisation en matière de sécurité 03.02.01.A.02	[Affectation : événements définis par l'organisation]
Formation et sensibilisation en matière de sécurité 03.02.01.B	[Affectation : fréquence définie par l'organisation]

Exigence de sécurité	Paramètre défini par l'organisation
Formation et sensibilisation en matière de sécurité 03.02.01.B	[Affectation : événements définis par l'organisation]
Formation selon le rôle 03.02.02.A.01	[Affectation : fréquence définie par l'organisation]
Formation selon le rôle 03.02.02.A.02	[Affectation : événements définis par l'organisation]
Formation selon le rôle 03.02.02.B	[Affectation : fréquence définie par l'organisation]
Formation selon le rôle 03.02.02.B	[Affectation : événements définis par l'organisation].
Journalisation d'événements 03.03.01.A	[Affectations : types d'événements définis par l'organisation]
Journalisation d'événements 03.03.01.B	[Affectation : fréquence définie par l'organisation]
Intervention en cas de défaillance du processus de journalisation des données de vérification 03.03.04.A	[Affectation : période définie par l'organisation]
Intervention en cas de défaillance du processus de journalisation des données de vérification 03.03.04.B	[Affectation : mesures supplémentaires définies par l'organisation]
Examen, analyse et production de rapports liés aux enregistrements de vérification 03.03.05.A	[Affectation : fréquence définie par l'organisation]
Horodatage 03.03.07.B	[Affectation : granularité de mesure du temps définie par l'organisation]
Configuration de référence 03.04.01.B	[Affectation : fréquence définie par l'organisation]
Paramètres de configuration 03.04.02.A	[Affectation : paramètres de configuration définis par l'organisation]
Fonctionnalité minimale 03.04.06.B	[Affectation : fonctions, ports, protocoles, connexions et/ou services définis par l'organisation]
Fonctionnalité minimale 03.04.06.C	[Affectation : fréquence définie par l'organisation]
Logiciels autorisés – Autorisation par exception 03.04.08.C	[Affectation : fréquence définie par l'organisation]
Inventaire des composants du système 03.04.10.B	[Affectation : fréquence définie par l'organisation]
Configuration des systèmes et des composants pour des zones à risque élevé 03.04.12.A	[Affectation : configurations système définies par l'organisation]
Configuration des systèmes et des composants pour des zones à risque élevé 03.04.12.B	[Affectation : exigences de sécurité définies par l'organisation].
Identification, authentification et réauthentification des utilisatrices et utilisateurs 03.05.01.B	[Affectation : circonstances ou situations nécessitant une réauthentification définies par l'organisation]

Exigence de sécurité	Paramètre défini par l'organisation
Identification et authentification des dispositifs 03.05.02	[Affectation : dispositifs ou types de dispositifs définis par l'organisation]
Gestion des identifiants 03.05.05.C	[Affectation : période définie par l'organisation]
Gestion des identifiants 03.05.05.D	[Affectation : caractéristique définie par l'organisation identifiant le statut des individus]
Gestion des mots de passe 03.05.07.A	[Affectation : fréquence définie par l'organisation]
Gestion des mots de passe 03.05.07.F	[Affectation : règles de composition et de complexité définies par l'organisation].
Gestion des authentifiants 03.05.12.E	[Affectation : fréquence définie par l'organisation]
Gestion des authentifiants 03.05.12.E	[Affectation : événements définis par l'organisation]
Surveillance des incidents, signalement des incidents et assistance en cas d'incident 03.06.02.B	[Affectation : période définie par l'organisation]
Surveillance des incidents, signalement des incidents et assistance en cas d'incident 03.06.02.C	[Affectation : autorités définies par l'organisation]
Tests d'intervention en cas d'incident 03.06.03	[Affectation : fréquence définie par l'organisation]
Formation d'intervention en cas d'incident 03.06.04.A.01	[Affectation : période définie par l'organisation]
Formation d'intervention en cas d'incident 03.06.04.A.03	[Affectation : fréquence définie par l'organisation]
Formation d'intervention en cas d'incident 03.06.04.B	[Affectation : fréquence définie par l'organisation]
Formation d'intervention en cas d'incident 03.06.04.B	[Affectation : événements définis par l'organisation]
Utilisation des supports 03.08.07.A	[Affectation : types de supports définis par l'organisation]
Filtrage de sécurité du personnel 03.09.01.B	[Affectation : conditions nécessitant un nouveau filtrage de sécurité définies par l'organisation]
Cessation d'emploi et mutation de personnel 03.09.02.A.01	[Affectation : période définie par l'organisation]
Autorisations d'accès physique 03.10.01.C	[Affectation : fréquence définie par l'organisation]
Surveillance de l'accès physique 03.10.02.B	[Affectation : fréquence définie par l'organisation]
Surveillance de l'accès physique 03.10.02.B	[Affectation : événements ou indications potentielles d'événement définis par l'organisation]

Exigence de sécurité	Paramètre défini par l'organisation
Autres lieux de travail 03.10.06.B	[Affectation : exigences de sécurité définies par l'organisation]
Évaluation des risques 03.11.01.B	[Affectation : fréquence définie par l'organisation]
Surveillance et analyse des vulnérabilités 03.11.02.A	[Affectation : fréquence définie par l'organisation]
Surveillance et analyse des vulnérabilités 03.11.02.B	[Affectation : délais d'exécution définis par l'organisation]
Surveillance et analyse des vulnérabilités 03.11.02.C	[Affectation : fréquence définie par l'organisation]
Évaluation de sécurité 03.12.01	[Affectation : fréquence définie par l'organisation]
Échange d'information 03.12.05.A	[Sélection (un choix ou plus) : ententes sur la sécurité des interconnexions; ententes sur la sécurité de l'échange d'information; ententes ou protocoles d'entente; accords sur les niveaux de service; ententes avec les utilisatrices et utilisateurs; accords de non-divulgation; autres types d'ententes]
Échange d'information 03.12.05.C	[Affectation : fréquence définie par l'organisation]
Déconnexion réseau 03.13.09	[Affectation : période définie par l'organisation]
Établissement et gestion des clés cryptographiques 03.13.10	[Affectation : exigences définies par l'organisation pour l'établissement et la gestion des clés]
Protection cryptographique 03.13.11	[Affectation : types de cryptographie définis par l'organisation]
Applications et appareils informatiques collaboratifs 03.13.12.A	[Affectation : exceptions définies par l'organisation pour lesquelles l'activation à distance doit être permise]
Correction des défauts 03.14.01.B	[Affectation : période définie par l'organisation]
Protection contre les programmes malveillants 03.14.02.C.01	[Affectation : fréquence définie par l'organisation]
Stratégie et procédures 03.15.01.B	[Affectation : fréquence définie par l'organisation]
Plan de sécurité du système 03.15.02.B	[Affectation : fréquence définie par l'organisation]
Règles de conduite 03.15.03.D	[Affectation : fréquence définie par l'organisation]
Principes d'ingénierie de la sécurité 03.16.01	[Affectation : principes d'ingénierie de la sécurité des systèmes définis par l'organisation]
Services de systèmes externes 03.16.03.A	[Affectation : exigences de sécurité définies par l'organisation].
Plan de gestion des risques liés à la chaîne d'approvisionnement 03.17.01.B	[Affectation : fréquence définie par l'organisation]
Exigences et processus de la chaîne d'approvisionnement 03.17.03.B	[Affectation : exigences de sécurité définies par l'organisation]