OBJECTIFS RELATIFS À L'ÉTAT DE PRÉPARATION EN MATIÈRE DE CYBERSÉCURITÉ

BOÎTE À OUTILS DES OBJECTIFS INTERSECTORIELS

VERSION 1.0

Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Communications Security Establishment Canada
Canadian Centre for Cyber Security

Canada

Objectifs relatifs à l’état de préparation en matière de cybersécurité : Boîte à outils des objectifs intersectoriels

D96-121/2024F-PDF
978-0-660-73263-3

La Boîte à outils des objectifs intersectoriels est liée à la publication des Objectifs relatifs à l'état de préparation en matière de cybersécurité (OEPC) du Centre pour la cybersécurité. La Boîte à outils des objectifs intersectoriels comprend 36 OEPC pour appuyer les propriétaires et exploitants d'infrastructures essentielles (IE) du Canada œuvrant dans n'importe quel secteur afin qu'ils priorisent des investissements en cybersécurité et renforcent leur posture de cybersécurité. Le tableau ci-dessous présente les objectifs, le résultat escompté de chaque objectif, les mesures recommandées à prendre pour chaque objectif, ainsi que les risques que l'objectif permet d'atténuer, tels que les tactiques, techniques et procédures (TTP) du cadre MITRE ATT&CK (https://attack.mitre.org/) (en anglais seulement). Le tableau comprend également des liens vers des documents de conseils du Centre pour la cybersécurité et des références au NIST Cybersecurity Framework (CSF) 2.0 (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf) (en anglais seulement).

Pour plus de contexte sur les OEPC, consultez la publication intitulée *Objectifs relatifs à l'état de préparation en matière de cybersécurité* (https://www.cyber.gc.ca/fr/objectifs-relatifs-letat-preparation-matiere-cybersecurite/objectifs-relatifs-letat-preparation-matiere-cybersecurite-securiser-systemes-plus-essentiels) sur le site Web du Centre pour la cybersécurité.

Le Centre pour la cybersécurité fournit la présente boîte à outils afin d'aider les organisations à renforcer leur posture de cybersécurité. Ce document PDF est un formulaire à remplir qui permet aux organisations de documenter les progrès réalisés dans l'atteinte des OEPC. L'information enregistrée dans ce formulaire n'est pas recueillie par le Centre pour la cybersécurité. Le formulaire ne doit donc pas être envoyé au Centre pour la cybersécurité, et toute information connexe transmise au Centre pour la cybersécurité sera supprimée.

GOUVERNANCE [0]

Leadership en matière de respect de la vie privée [0.0]

Résultat Une ou un leader, ou une équipe, est responsable et imputable de la gestion des risques d'atteinte à la vie privée qui touchent à la cybersécurité.

Mesures recommandées

Déterminer un rôle ou un titre précis qui sera responsable et imputable du programme de gestion des risques d'atteinte à la vie privée de l'organisation. La personne ou l'équipe responsable établit les politiques et procédures nécessaires afin que l'organisation :

- tienne compte de l'ensemble complet des obligations en matière de respect de la vie privée et des risques d'atteinte à la vie privée en matière de cybersécurité, y compris les lois applicables sur la protection de la vie privée;
- applique cette analyse pour appuyer les décisions opérationnelles.

Le programme de gestion des risques d'atteinte à la vie privée pourrait comprendre le maintien d'un répertoire des renseignements personnels ainsi que des politiques visant à limiter la collecte et la conservation des renseignements personnels.

TTP ou risques

Responsabilisation, investissement ou efficacité insuffisants.

Références

GV.OC-03, GV.RM-06

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Processus et politiques de signalement des incidents liés à la chaîne d'approvisionnement [0.1]

Résultat Les organisations sont informées plus rapidement des incidents et des atteintes touchant les autres fournisseurs et prestataires de services, et peuvent y intervenir plus rapidement.

Mesures recommandées

Veiller à ce que le programme de gestion des risques liés à la chaîne d'approvisionnement en cybersécurité de l'organisation stipule que les fournisseurs et/ou les prestataires de services doivent aviser les clientes et clients d'incidents de sécurité. La notification doit être réalisée dans un délai proportionnel aux risques, établi par l'organisation, et doit être documentée dans les documents et contrats d'approvisionnement, tels que les accords sur les niveaux de service.

TTP ou risques

Compromissions de la chaîne d'approvisionnement (techniques [T] 1195, systèmes de contrôle industriels [ICS] T0862).

Références

GV.SC-01, GV.SC-05

Protéger votre organisation contre les menaces de la chaîne d'approvisionnement des logiciels (ITSM.10.071) (https://www.cyber.gc.ca/fr/orientation/proteger-votre-organisation-contre-les-menaces-de-la-chaine-dapprovisionnement-des-logiciels-itsm10071)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Exigences en matière de cybersécurité des fournisseurs [0.2]

Résultat Réduit les risques en se procurant des produits et des services plus sécurisés, de fournisseurs plus sécurisés.

Mesures recommandées

Inclure les exigences et les questions en matière de cybersécurité dans les documents d'approvisionnement des organisations.
Veiller à ce que les réponses soient évaluées dans la sélection des fournisseurs de manière à privilégier, entre deux options à prix et fonctions similaires, l'option et/ou le fournisseur offrant une meilleure sécurité ou, dans la mesure du possible, à privilégier l'option la plus sécurisée même si elle est plus coûteuse.

TTP ou risques

Compromission de la chaîne d'approvisionnement (T1195, ICS T0862).

Références

GV.SC-05

Protéger votre organisation contre les menaces de la chaîne d'approvisionnement des logiciels (ITSM.10.071) (https://www.cyber.gc.ca/fr/orientation/proteger-votre-organisation-contre-les-menaces-de-la-chaine-dapprovisionnement-des-logiciels-itsm10071)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Leadership en matière de cybersécurité organisationnel et des technologies opérationnelles [0.3]

Résultat Une ou un leader est responsable et imputable de la cybersécurité au sein d'une organisation. Le cas échéant, une ou un leader est responsable et imputable de la cybersécurité liée aux technologies opérationnelles (TO) dans une organisation détenant des biens de TO. Dans certaines organisations, une personne peut être responsable des deux leaderships.

Mesures recommandées

Déterminer un rôle ou un titre précis qui sera responsable et imputable de la planification, des ressources et de l'exécution des activités de cybersécurité.
Ce rôle peut entreprendre des activités, telles que gérer les opérations de cybersécurité au niveau de la haute direction, demander et obtenir les ressources budgétaires ou diriger la stratégie pour informer le positionnement futur. Déterminer également un rôle ou un titre précis qui sera responsable des ressources et de l'exécution des activités de cybersécurité s'appliquant aux TO. Dans certaines organisations, les rôles associés au leadership en matière de cybersécurité et au leadership en matière de TO peuvent être assumés par la même personne.

TTP ou risques

Responsabilisation, investissement ou efficacité insuffisants dans les programmes de cybersécurité ou de cybersécurité des TO.

Références

GV.RR-02, GV.PO-01, GV.PO-02

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Amélioration des partenariats en matière de cybersécurité des TI et TO [0.4]

Résultat Améliorer la cybersécurité des TO et intervenir plus rapidement et efficacement aux cyberincidents liés aux TO.

Mesures recommandées

Au moins une fois par année, parrainer une activité d'établissement de relations axée sur le renforcement des relations de travail entre le personnel de la sécurité des TI et des TO et qui ne constitue pas un événement de travail (comme fournir des repas pendant une intervention à un incident). Cette activité peut donner l'occasion au personnel dans le domaine des TI et des TO :

- de favoriser la communication;
- de permettre une compréhension commune de l'exposition aux menaces qui évolue;
- d'établir des priorités communes;
- de créer un plan de sécurité pour protéger les TO et les TI connexes.

TTP ou risques

De mauvaises relations de travail et un manque de compréhension mutuelle entre le personnel chargé de la cybersécurité des TI et des TO peuvent souvent augmenter le risque pour la cybersécurité des TO.

Références

GV.RR-02

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

IDENTIFICATION [1]

Répertoire des biens et topologie de réseau [1.0]

Résultat Permet de mieux identifier les biens connus, inconnus et non gérés, y compris les biens connectés au Web pour le nuage et les biens de données. Votre organisation peut ensuite détecter plus rapidement les nouvelles vulnérabilités, les corriger et assurer la continuité des services.

Mesures recommandées

Tenir un répertoire de tous les biens dans les réseaux de TI (y compris IPv6) et de TO de l'organisation (le cas échéant) et le mettre à jour régulièrement. Inclure dans le répertoire des documents fiables sur la topologie de réseau et sur les biens de données identifiés, plus particulièrement l'information sensible ou classifiée. Mettre à jour le répertoire régulièrement pour les TI et les TO, et ajouter immédiatement au répertoire tout nouveau bien qui est intégré à l'infrastructure de l'organisation.

TTP ou risques

Ajouts de matériel (T1200)

Applications exposées au public exploitables (T1190, ICS T0819)

Dispositif accessible par Internet (ICS T0883)

Références

ID.AM-01, ID.AM-02, ID.AM 03, ID.AM-04, DE.CM 01

Utilisation de la gestion des biens de technologies de l'information (GBTI) pour renforcer la cybersécurité (ITSM.10.004) (https://www.cyber.gc.ca/fr/orientation/utilisation-gestion-biens-technologies-linformation-gbti-renforcer-cybersecurite)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Atténuation des vulnérabilités connues [1.1]

Résultat Réduit la probabilité que des auteures et auteurs de menace exploitent les vulnérabilités connues pour s'introduire dans les réseaux de l'organisation.

Mesures recommandées

Dans un délai proportionnel aux risques, corriger toutes les vulnérabilités exploitées connues qui figurent dans le catalogue de la Cybersecurity and Infrastructure Security Agency (CISA), *Known Exploited Vulnerabilities Catalog* (https://www.cisa.gov/known-exploited-vulnerabilities-catalog) (en anglais seulement), et qui pourraient être présentes dans les systèmes connectés à Internet, en priorisant les biens essentiels. Identifier les vulnérabilités de sécurité dans vos systèmes en réalisant des tests de pénétration et en utilisant des outils automatisés d'analyse des vulnérabilités. Ces activités font partie d'une stratégie complète de gestion des vulnérabilités.

Pour les biens de TO auxquels il est impossible d'appliquer les correctifs nécessaires ou dont l'application de correctifs risquerait de compromettre considérablement la disponibilité ou la sécurité, appliquer des contrôles compensatoires (comme la segmentation ou la surveillance) et les consigner. Les contrôles adéquats rendent le bien inaccessible par Internet ou réduisent la capacité des auteures et auteurs de menace d'exploiter les vulnérabilités de ces biens.

Sélectionner minutieusement des outils automatisés de détection des vulnérabilités aux fins d'analyse rigoureuse des systèmes. Ces outils peuvent provoquer un comportement erratique des dispositifs, entraîner l'arrêt, une panne ou un redémarrage de ceux-ci, ou nécessiter une intervention manuelle pour retourner à un état opérationnel.

TTP ou risques

Analyse active : analyse des vulnérabilités (T1595.002)

Applications exposées au public exploitables (T1190, ICS T0819)

Exploitation de services distants (T1210, ICS T0866)

Compromission de la chaîne d'approvisionnement (T1195, ICS T0862)

Services externes distants (T1133, ICS T0822)

Références

ID.RA-01, ID.RA-08, ID.RA-06, PR.PS-02, PR.PS-03

Les 10 mesures de sécurité des TI : No 2, Appliquer des correctifs aux applications et aux systèmes d'exploitation (ITSM.10.096) (https://www.cyber.gc.ca/fr/orientation/les-10-mesures-de-securite-des-ti-no2-appliquer-les-correctifs-aux-systemes-dexploitation-et-aux-applications-itsm10096)

Les 10 mesures de sécurité des TI : No 5, Segmenter et séparer l'information (ITSM.10.092) (https://www.cyber.gc.ca/fr/orientation/10-mesures-securite-ti-5-segmenter-separer-information-itsm10092)

Application des mises à jour sur les dispositifs (ITSAP.10.096) (https://www.cyber.gc.ca/fr/orientation/application-des-mises-jour-sur-les-dispositifs-itsap10096)

Contrôles de cybersécurité de base pour les petites et moyennes organisations (https://www.cyber.gc.ca/fr/orientation/controles-de-cybersecurite-de-base-pour-les-petites-et-moyennes-organisations)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Validation de tierce partie de l'efficacité des contrôles de cybersécurité [1.2]

Résultat Identifie les TTP contre lesquelles les mesures de défense sont insuffisantes et établit une confiance dans les mesures de cyberdéfense de l'organisation.

Mesures recommandées

Des tierces parties possédant de l'expertise éprouvée en cybersécurité des TI et/ou des TO valident régulièrement l'efficacité et la couverture des mesures de cyberdéfense d'une organisation. Mener ces exercices annuellement, ce qui comprend des activités telles que des tests de pénétration, des primes de bogues, des simulations d'incident ou des exercices de simulation, et inclure des tests annoncés et non annoncés.

Les exercices tiennent compte de la capacité d'une ou un adversaire potentiel d'infiltrer le réseau de l'extérieur et des répercussions d'une telle infiltration, ainsi que la capacité d'une ou un adversaire dans le réseau (par exemple dans le cas d'une infiltration présumée) à se déplacer latéralement afin de démontrer l'incidence possible sur les systèmes essentiels, y compris les systèmes de technologies opérationnelles et les systèmes de contrôle industriels.

Atténuer en temps opportun les conclusions à incidence élevée des tests antérieurs afin qu'elles ne soient plus observées lors de futurs tests.

TTP ou risques

Réduit le risque de lacunes sur le plan des mesures de cyberdéfense ou d'un faux sentiment de sécurité avec les mesures de protection existantes.

Références

ID.RA-01, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Plans d'intervention en cas d'incident [1.3]

Résultat Les organisations tiennent, mettent en pratique et mettent à jour des plans d'intervention en cas d'incident de cybersécurité pour les scénarios de menace pertinents.

Mesures recommandées

Élaborer, tenir, mettre à jour et mettre à l'essai régulièrement les plans d'intervention en cas d'incident de cybersécurité s'appliquant aux TI et aux TO pour les TTP et les scénarios de menace courants et propres à l'organisation (par secteur ou par site, par exemple). Envisager de collaborer avec les parties prenantes appropriées pour mener des exercices de simulation axés sur les attaques renforcées par l'intelligence artificielle.

Dans le cadre des tests ou des exercices, veiller à ce qu'ils soient le plus réalistes, faisables et conformes possible aux niveaux d'interruption acceptables de l'organisation. Mettre à l'essai rigoureusement les plans d'intervention en cas d'incident au moins une fois par année et les mettre à jour dans un délai proportionnel aux risques à la suite des leçons retenues des tests ou des exercices.

TTP ou risques

Incapacité à contenir, à atténuer et à communiquer rapidement et efficacement les incidents de cybersécurité.

Références

ID.IM-04, ID.IM-02

Élaborer un plan d'intervention en cas d'incident (ITSAP.40.003) (https://www.cyber.gc.ca/fr/orientation/elaborer-un-plan-dintervention-en-cas-dincident-itsap40003)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Déploiement de fichiers security.txt [1.4]

Résultat

Permet aux chercheuses et chercheurs en sécurité de soumettre plus rapidement les faiblesses ou les vulnérabilités découvertes.

Mesures recommandées

Veiller à ce que tous les domaines Web publics aient un fichier security.txt conforme aux recommandations du document RFC 9116.

TTP ou risques

Analyse active : Analyse des vulnérabilités (T1595.002)

Applications exposées au public exploitables (T1190, ICS T0819)

Exploitation de services distants (T1210, ICS T0866)

Compromission de la chaîne d'approvisionnement (T1195, ICS T0862)

Références

ID.RA-08

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Sélection d'un fournisseur de services infonuagiques de confiance [1.5]

Résultat

Si le nuage est utilisé et si une relation de confiance est établie avec un fournisseur de services infonuagiques (FSI) possédant des capacités techniques éprouvées, les organisations peuvent adopter des services infonuagiques en toute confiance pour bénéficier des avantages d'extensibilité, de souplesse et de rentabilité tout en assurant la protection de leurs biens sensibles.

Mesures recommandées

Veiller à ce que votre FSI offre le stockage sécurisé des données, le chiffrement et des contrôles d'accès, et confirmer que les pratiques et les capacités du FSI en matière de cybersécurité sont conformes aux normes et règlements de sécurité pertinents. Cette étape peut être réalisée en confirmant que le FSI respecte les régimes de conformité existants, lesquels peuvent varier selon les besoins opérationnels de l'organisation.

TTP ou risques

Réduit le risque d'attaque et/ou de compromission lié à un FSI inexpérimenté.

Compromission de la chaîne d'approvisionnement (T1195, ICS T0862)

Références

GV.OC-03, GV.SC-05, GV.SC 07, ID.AM-02

Les meilleures mesures pour renforcer la cybersécurité des petites et moyennes entreprises (ITSAP.10.035) (https://www.cyber.gc.ca/fr/orientation/les-meilleures-mesures-pour-renforcer-la-cybersecurite-des-petites-et-moyennes)

Contrôles de cybersécurité de base pour les petites et moyennes organisations (https://www.cyber.gc.ca/fr/orientation/controles-de-cybersecurite-de-base-pour-les-petites-et-moyennes-organisations)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

PROTECTION [2]

Changement de mots de passe par défaut [2.0]

Résultat

Empêche les auteures et auteurs de menace d'utiliser les mots de passe par défaut pour obtenir un accès initial à un réseau ou pour se déplacer latéralement dans un réseau.

Mesures recommandées

Appliquer un processus et/ou une politique à l'échelle de l'organisation qui exige que les mots de passe par défaut du fabricant soient changés pour tout le matériel, tous les logiciels et tous les micrologiciels avant de les intégrer à un réseau interne ou externe. Cette mesure s'applique entre autres aux biens de TI pour les TO, comme les pages Web d'administration des TO.

Dans les cas où il est impossible de changer les mots de passe par défaut (comme un système de contrôle avec un mot de passe codé en dur), mettre en œuvre des contrôles de sécurité compensatoires appropriés et les documenter. Surveiller également les journaux, particulièrement le trafic réseau et les tentatives d'ouverture de session sur ces dispositifs.

Appliquer une stratégie de changement des justificatifs d'identité par défaut pour tous les dispositifs futurs ou nouveaux, puisque le changement des mots de passe par défaut sur les TO existantes d'une organisation représente beaucoup plus de travail. Cette mesure est non seulement beaucoup plus facile à mettre en œuvre, elle réduit également le risque si l'adversaire modifie ses TTP.

TTP ou risques

Comptes valides : comptes par défaut (T1078.001)

Comptes valides (ICS T0859)

Références

PR.AA-01, PR.AA-05

Les 10 mesures de sécurité des TI : No 3, Gestion et contrôle des privilèges d'administrateur (ITSM.10.094) (https://www.cyber.gc.ca/fr/orientation/10-mesures-securite-ti-no-3-gestion-controle-privileges-itsm10094)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Robustesse minimale de mot de passe [2.1]

Résultat Les mots de passe organisationnels sont plus difficiles pour les auteures et auteurs de menace à deviner ou à craquer.

Mesures recommandées

Mettre en œuvre une stratégie appliquée par le système qui exige un mot de passe d'une longueur minimale de 15 caractères pour tous les biens de TI protégés par mot de passe et pour tous les biens de TO, si c'est possible sur le plan technique.**

Envisager d'utiliser des phrases de passe comptant au moins quatre mots et 15 caractères. Dans les situations convenables, utiliser des phrases de passe puisqu'elles sont plus longues, mais plus faciles à retenir qu'un mot de passe composé de divers caractères choisis au hasard.

Dans les cas où la longueur minimale des mots de passe ne peut pas être respectée pour des raisons techniques, appliquer des contrôles compensatoires et les documenter, et journaliser toutes les tentatives de connexion à ces biens. Prioriser la mise à niveau ou le remplacement des biens qui ne peuvent pas prendre en charge la longueur minimale recommandée pour les mots de passe.

Cet objectif est particulièrement important pour les organisations qui :

- ne peuvent pas mettre en œuvre, à grande échelle, l'authentification multifacteur (AMF) et des capacités pour se protéger contre les attaques par force brute (telles que des pare-feu d'applications Web et des réseaux de diffusion de contenu tiers);
- ne peuvent pas adopter de méthodes d'authentification sans mot de passe.

Remarque

* Les outils modernes employés par les attaquantes et attaquants peuvent craquer rapidement les mots de passe de huit caractères. La longueur est un facteur plus important et efficace en ce qui concerne la robustesse des mots de passe que la complexité ou les rotations fréquentes de mots de passe. Les longs mots de passe sont également plus faciles à créer et à retenir.

** La priorité doit être accordée aux biens de TO qui utilisent un mécanisme centralisé d'authentification (comme Active Directory). Des exemples de biens de TO à faible risque pour lesquels ces mesures ne sont peut-être pas possibles sur le plan technique comprennent ceux dans des emplacements éloignés tels que des éoliennes ou des plateformes de forage pétrolier en mer.

TTP ou risques

Force brute : supposition de mots de passe (T1110.001)

Force brute : cassage de mots de passe (T1110.002)

Force brute : rafale de mots de passe (T1110.003)

Force brute : bourrage d'identifiants (T1110.004)

Références

PR.AA-01, PR.AA-05

Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032) (https://www.cyber.gc.ca/fr/orientation/pratiques-exemplaires-de-creation-de-phrases-de-passe-et-de-mots-de-passeitsap30032)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Justificatifs d'identité uniques [2.2]

Résultat Les attaquantes et attaquants ne peuvent pas réutiliser les justificatifs d'identité compromis pour se déplacer latéralement dans l'organisation, particulièrement entre les réseaux de TI et de TO.

Mesures recommandées

Fournir des justificatifs d'identité uniques et distincts pour des services similaires et l'accès aux biens sur les réseaux de TI et de TO. S'assurer que les utilisatrices et utilisateurs ne peuvent pas réutiliser les mots de passe pour d'autres comptes, applications, services, etc. Exiger que les comptes de services et de machines aient des mots de passe uniques et différents de tous les comptes d'utilisateur.

TTP ou risques

Comptes valides (T1078, ICS T0859)

Force brute : Supposition de mots de passe (T1110.001)

Références

PR.AA-01, PR.AA-05

Les 10 mesures de sécurité des TI : No 3, Gestion et contrôle des privilèges d'administrateur (ITSM.10.094) (https://www.cyber.gc.ca/fr/orientation/10-mesures-securite-ti-no-3-gestion-controle-privileges-itsm10094)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Révocation des justificatifs des employées et employés quittant leur poste [2.3]

Résultat Empêcher l'accès non autorisé aux comptes ou aux ressources de l'organisation par d'anciennes et anciens membres du personnel.

Mesures recommandées

Pour tous les employées et employés quittant leur poste, appliquer un processus administratif défini et mis en œuvre avant la journée de leur départ qui :

- révoque tous les laissez-passer, cartes-clés, jetons physiques, etc. et permet de les retourner de manière sécurisée;
- désactive tous les comptes d'utilisateur et tous les accès aux ressources de l'organisation.

TTP ou risques

Comptes valides (T1078, ICS T0859)

Références

PR.AA-01, PR.AA-05, PR.AA-06, GV.RR-04

Les 10 mesures de sécurité des TI : No 3, Gestion et contrôle des privilèges d'administrateur (ITSM.10.094) (https://www.cyber.gc.ca/fr/orientation/10-mesures-securite-ti-no-3-gestion-controle-privileges-itsm10094)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Séparation des comptes d'utilisateur et privilégiés [2.4]

Résultat Rend la tâche plus difficile pour les auteures et auteurs de menace d'obtenir un accès aux comptes privilégiés ou d'administrateur, même lorsque les comptes d'utilisateur courants sont compromis.

Mesures recommandées

Les comptes d'utilisateur n'ont pas toujours des privilèges d'administrateur ou de superutilisateur. Les administratrices et administrateurs ont des comptes d'utilisateur séparés pour réaliser les activités qui ne sont pas liées au rôle d'administrateur (comme le courrier électronique et la navigation Web). Réévaluer les privilèges à un intervalle régulier pour vérifier que les différents ensembles d'autorisations sont toujours nécessaires.

TTP ou risques

Comptes valides (T1078, ICS T0859)

Références

PR.AA-05

Les 10 mesures de sécurité des TI : No 3, Gestion et contrôle des privilèges d'administrateur (ITSM.10.094) (https://www.cyber.gc.ca/fr/orientation/10-mesures-securite-ti-no-3-gestion-controle-privileges-itsm10094)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Segmentation réseau [2.5]

Résultat Réduit la probabilité que des auteures et auteurs de menace accèdent au réseau de TO après avoir compromis le réseau de TI.

Mesures recommandées

Toutes les connexions au réseau de TO sont refusées par défaut à moins qu'elles aient été explicitement autorisées (par exemple, pour une adresse IP et un port particuliers) à des fins de fonctionnement du système. Les voies de communication nécessaires entre les réseaux de TI et de TO doivent passer par un intermédiaire, tel qu'un pare-feu configuré adéquatement, un hôte bastion, un serveur intermédiaire ou une zone démilitarisée, qui est surveillé étroitement, saisit les journaux réseau et autorise seulement les connexions de biens approuvés.

TTP ou risques

Découverte de services réseau (T1046)

Relation de confiance (T1199)

Énumération de connexions réseau (ICS T0840)

Reniflage de réseau (T1040, ICS T0842)

Références

PR.IR-01, PR.AA-06

Les 10 mesures de sécurité des TI : No 5, Segmenter et séparer l'information (ITSM.10.092) (https://www.cyber.gc.ca/fr/orientation/10-mesures-securite-ti-5-segmenter-separer-information-itsm10092)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Détection des tentatives (automatisées) d'ouverture de session infructueuses [2.6]

Résultat Protège les organisations des attaques automatisées basées sur les justificatifs d'identité.

Mesures recommandées

Journaliser toutes les tentatives infructueuses et les envoyer à l'équipe de sécurité ou au système de journalisation pertinent de votre organisation. Veiller à ce que les équipes de sécurité soient avisées (au moyen d'une alerte, par exemple) lorsque le nombre maximal de tentatives consécutives d'ouverture de session infructueuses a été atteint dans un délai très court (par exemple, cinq tentatives infructueuses en deux minutes). Journaliser et conserver ces alertes dans le système de demandes de service ou de sécurité pertinent aux fins d'analyse rétroactive.

Pour les biens de TI, établir une stratégie appliquée par le système qui empêche les ouvertures de session futures provenant du compte suspect. Cette stratégie pourrait, par exemple, être mise en place pour une période minimale précise ou jusqu'à ce que le compte soit réactivé par une utilisatrice ou un utilisateur privilégié. Activer cette configuration sur un bien dans la mesure du possible. À titre d'exemple, Windows 11 peut verrouiller automatiquement les comptes pendant dix minutes à la suite de dix tentatives infructueuses d'ouverture de session dans un délai de dix minutes.

TTP ou risques

Force brute : supposition de mots de passe (T1110.001)

Force brute : cassage de mots de passe (T1110.002)

Force brute : rafale de mots de passe (T1110.003)

Force brute : bourrage d'identifiants (T1110.004)

Références

PR.AA-03, DE.CM-09

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Authentification multifacteur résistante à l'hameçonnage [2.7]

Résultat Ajoute une couche de sécurité additionnelle et essentielle pour protéger les comptes de biens dont les justificatifs d'identité ont été compromis.

Mesures recommandées

Mettre en œuvre l'AMF pour accéder aux biens en utilisant la méthode la plus robuste possible pour chaque bien (voir la portée ci-dessous).

Voici les options d'AMF classées par robustesse, de la plus robuste à la moins robuste :

1. AMF matérielle résistante à l'hameçonnage (par exemple, FIDO/WebAuthn ou basée sur l'infrastructure à clé publique [ICP]).
2. Si une telle AMF matérielle n'est pas possible, utiliser des jetons logiciels basés sur des applications mobiles (préférablement des notifications de type « pousser » avec correspondance des nombres) ou une technologie émergente telle que les clés d'accès FIDO.
3. Utiliser seulement l'AMF par message texte ou appel vocal lorsqu'aucune autre option n'est possible.

Veiller à ce que tous les comptes de TI aient recours à l'AMF pour accéder aux ressources de l'organisation. Prioriser les comptes qui posent le risque le plus élevé, tels que les comptes administratifs privilégiés pour les systèmes de TI importants.

Dans les environnements de TO, activer l'AMF pour tous les comptes et systèmes auxquels il est possible d'accéder à distance, y compris les comptes de fournisseurs ou de maintenance, les postes de travail d'ingénierie et d'utilisateur accessibles à distance et les interfaces homme-machine accessibles à distance.

TTP ou risques

Force brute (T1110)

Services distants : protocole RDP (T1021.001)

Protocole SSH pour services distants (T1021.004)

Comptes valides (T1078, ICS T0859)

Services externes distants (ICS T0822)

Références

PR.AA-01, PR.AA-03, PR.AA 05

Étapes à suivre pour déployer efficacement l'authentification multifacteur (AMF) (ITSAP.00.105) (https://www.cyber.gc.ca/fr/orientation/etapes-suivre-deployer-efficacement-lauthentification-multifacteur-amf-itsap00105)

Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030) (https://www.cyber.gc.ca/fr/orientation/securisez-vos-comptes-et-vos-appareils-avec-une-authentification-multifacteur)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Formation relative à la cybersécurité de base et des TO [2.8]

Résultat Les utilisatrices et utilisateurs de l'organisation apprennent à adopter des comportements plus sécuritaires. Le cas échéant, le personnel responsable de sécuriser les biens de TO reçoit de la formation spécialisée en cybersécurité axée sur les TO.

Mesures recommandées

Donner de la formation sur les concepts de base en matière de sécurité et de protection de la vie privée, tels que l'hameçonnage, les compromissions de courriel d'affaires, la sécurité opérationnelle de base, la sécurité des mots de passe et les atteintes à la vie privée, et promouvoir une culture interne de sécurité et de sensibilisation à la cybersécurité. Donner de la formation au moins annuellement à toutes les employées et à tous les employés, ainsi qu'à toutes les entrepreneures et à tous les entrepreneurs. Exiger que les nouvelles employées et nouveaux employés reçoivent une formation initiale en cybersécurité au moment de l'intégration, puis de façon récurrente au moins annuellement et au besoin à la suite de certains événements ou de certains changements de système.

Veiller à ce que les programmes axés sur la sécurité et la protection de la vie privée collaborent afin d'élaborer des procédures et politiques de formation et de sensibilisation.

En plus de la formation de base en matière de cybersécurité, s'assurer que le personnel qui entretient ou sécurise les TO dans le cadre de leurs tâches courantes reçoit de la formation en matière de cybersécurité propre aux TO au moins tous les ans.

TTP ou risques

Formation destinée aux utilisatrices et utilisateurs (M1017, ICS M0917).

Références

PR.AT-01, PR.AT-02

Offrir aux employés une formation sur mesure en cybersécurité (ITSAP.10.093) (https://www.cyber.gc.ca/fr/orientation/offrir-aux-employes-une-formation-sur-mesure-en-cybersecurite-itsap10093)

Les 10 mesures de sécurité des TI : No 6, Miser sur une formation sur mesure en matière de cybersécurité (ITSM.10.093) (https://www.cyber.gc.ca/fr/orientation/les-10-mesures-de-securite-des-ti-n0-6-miser-sur-une-formation-sur-mesure-en-matiere-de)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Chiffrement fort et agile : données en transit [2.9]

Résultat Chiffrement efficace déployé pour assurer la confidentialité des données sensibles et l'intégrité du trafic réseau transitant par des environnements de TI, de TO et infonuagiques.

Mesures recommandées

Utiliser un protocole SSL à jour et configuré adéquatement pour protéger les données en transit, lorsqu'il est possible de le faire sur le plan technique. Déterminer toute utilisation de chiffrement faible ou désuète, les mettre à jour pour utiliser des algorithmes suffisamment forts et envisager de gérer les implications relatives à la cryptographie post-quantique. Chiffrer les données en transit au moyen d'un chiffrement suffisamment fort et approuvé en fonction de la sensibilité des données.

Pour réduire au minimum l'incidence sur la latence et la disponibilité, utiliser le chiffrement dans la mesure du possible pour les communications des TO avec des biens externes ou distants.

TTP ou risques

Adversaire au milieu (T1557)

Collecte automatisée (T1119)

Reniflage de réseau (T1040, ICS T0842)

Compromission sans fil (ICS T0860)

Reniflage sans fil (ICS T0887)

Références

PR.DS-02

Utiliser le chiffrement pour assurer la sécurité des données sensibles (ITSAP.40.016) (https://www.cyber.gc.ca/fr/orientation/utiliser-le-chiffrement-pour-assurer-la-securite-des-donnees-sensibles-itsap40016)

Conseils sur la mise en œuvre de l'agilité cryptographique (ITSAP.40.018) (https://www.cyber.gc.ca/fr/orientation/conseils-sur-la-mise-en-oeuvre-de-lagilite-cryptographique-itsap40018)

Préparez votre organisation à la menace que pose l'informatique quantique pour la cryptographie (ITSAP.00.017) (https://www.cyber.gc.ca/fr/orientation/preparez-votre-organisation-la-menace-que-pose-linformatique-quantique-pour-la)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Données sensibles sécurisées : données au repos [2.10]

Résultat Protège l'information sensible des accès non autorisés.

Mesures recommandées

Veiller à ce que les données sensibles, y compris les justificatifs d'identité, ne soient pas conservées en clair dans l'organisation et que seuls des utilisateurs et utilisatrices autorisés et authentifiés puissent y accéder. Conserver les justificatifs d'identité de manière sécurisée, par exemple à l'aide d'un coffre-fort ou d'un gestionnaire de mots de passe ou de justificatifs d'identité, ou de toute autre solution de gestion de comptes privilégiés. Chiffrer les données sensibles au repos à l'aide d'un chiffrement suffisamment fort et approuvé en fonction de la sensibilité des données.

TTP ou risques

Justificatifs d'identité non sécurisés (T1552)

Tickets Kerberos volés ou forgés (T1558)

Vidage de justificatifs d'identité de système d'exploitation (T1003)

Données de dépôts d'information (T1213, ICS T0811)

Vol d'information opérationnelle (T0882)

Références

PR.DS-01

Conseils de sécurité sur les gestionnaires de mots de passe (ITSAP.30.025) (https://www.cyber.gc.ca/fr/orientation/conseils-de-securite-sur-les-gestionnaires-de-mots-de-passeitsap30025)

Notes d'évaluation

◯ Non commencé Date : _____
◯ Défini Date : _____
◯ En cours Date : _____
◯ Mis en œuvre Date : _____

Remarques

Sécurité des courriels [2.11]

Résultat Réduit les risques liés aux menaces courantes par courriel, telles que la mystification, l'hameçonnage et l'interception.

Mesures recommandées

Dans l'ensemble de l'infrastructure de courriel de l'organisation :

- activer STARTTLS;
- activer les protocoles SPF (pour *Sender Policy Framework*) et DKIM (pour *DomainKeys Identified Mail*);
- activer le protocole DMARC (pour *Domain-based Message Authentication, Reporting, and Conformance*) et le régler à « rejeter ».

Utiliser également un chiffrement de courriels réglé au niveau approprié et approuvé selon la sensibilité du contenu des courriels.

TTP ou risques

Hameçonnage (T1566)

Compromission du courriel d'affaires

Références

PR.DS-01, PR.DS-02, PR.DS-10, PR.AA-03

Directives de mise en œuvre – protection du domaine de courrier (ITSP.40.065) (https://www.cyber.gc.ca/fr/orientation/directives-de-mise-en-oeuvre-protection-du-domaine-de-courrier)

Notes d'évaluation

◯ Non commencé Date : _____
◯ Défini Date : _____
◯ En cours Date : _____
◯ Mis en œuvre Date : _____

Remarques

Macros désactivées par défaut [2.12]

Résultat Réduit le risque lié aux macros intégrées et au code d'exécution similaire, une TTP d'auteure et auteur de menace très courante et efficace.

Mesures recommandées

Établir une stratégie appliquée par le système qui désactive par défaut sur tous les dispositifs les macros de Microsoft Office ou le code similaire intégré. Si les macros doivent être activées dans des circonstances précises, établir une stratégie pour que les utilisatrices et utilisateurs autorisés puissent demander à ce que les macros soient activées sur des biens précis.

TTP ou risques

Hameçonnage : pièce jointe de harponnage (T1566.001)

Exécution par l'utilisatrice ou utilisateur : fichier malveillant (T1204.002)

Références

PR.PS-01, ID.RA-07

Protection d'un organisme contre les macros malveillantes (ITSAP.00.200) (https://www.cyber.gc.ca/fr/orientation/protection-dun-organisme-contre-les-macros-malveillantes-itsap00200)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Processus d'approbation du matériel et des logiciels [2.13]

Résultat Assure une meilleure visibilité des biens de technologies déployés et réduit la probabilité de violation de la sécurité par les utilisatrices et utilisateurs qui installent du matériel, des micrologiciels ou des logiciels non approuvés.

Mesures recommandées

Mettre en œuvre une stratégie administrative ou un processus automatisé qui exige une approbation avant l'installation ou le déploiement d'une nouvelle version logicielle ou d'un nouveau logiciel, micrologiciel ou matériel. Tenir une liste de matériel, de micrologiciels et de logiciels autorisés en fonction du risque qui comprend des versions précises approuvées, lorsqu'il est possible de le faire sur le plan technique. Pour les biens de TO en particulier, aligner ces mesures sur les activités définies de tests et de contrôle des changements.

TTP ou risques

Compromission de la chaîne d'approvisionnement (T1195, ICS T0862)

Ajouts de matériel (T1200)

Extensions de navigateur (T1176)

Bien numérique temporaire (ICS T0864)

Références

PR.PS-01, ID.RA-07

Listes d'applications autorisées (ITSAP.10.095) (https://www.cyber.gc.ca/fr/orientation/liste-dapplications-autorisees-itsap10095)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Sauvegardes et redondance de système [2.14]

Résultat Réduit la probabilité et la durée de la perte de données pour les opérations ou la prestation de service d'une organisation.

Mesures recommandées

Effectuer régulièrement des sauvegardes de tous les systèmes nécessaires aux opérations. Déterminer au cas par cas les systèmes qui doivent faire l'objet d'une sauvegarde et la fréquence précise à laquelle la sauvegarde doit être faite, car tous les systèmes auront différentes exigences en matière de sauvegarde et de récupération des données. Conserver les sauvegardes séparément des systèmes sources et effectuer des tests régulièrement au moins annuellement. Veiller à ce que l'information conservée pour les biens de TO comprenne, au minimum :

- les configurations;
- les rôles;
- les automates programmables industriels (API);
- les dessins techniques;
- les outils.

Mettre en œuvre les redondances appropriées (établies par l'organisation), comme les composants réseau et le stockage de données. S'assurer que le système secondaire redondant n'est pas situé au même endroit que le système principal et qu'il peut être activé sans perte d'information ou perturbation des opérations.

TTP ou risques

Destruction de données (T1485, ICS T0809)

Données chiffrées pour réduire l'incidence (T1486)

Effacement de disque (T1561)

Récupération des systèmes interdite (T11490)

Déni de contrôle (ICS T0813)

Déni ou perte de vue (ICS T0815, T0829)

Perte de disponibilité (T0826)

Perte ou manipulation de contrôle (T0828, T0831)

Références

PR.DS-11

Sauvegarder et récupérer vos données (ITSAP.40.002) (https://www.cyber.gc.ca/fr/orientation/sauvegarder-et-recuperer-vos-donnees-itsap40002)

Contrôles de cybersécurité de base pour les petites et moyennes organisations (https://www.cyber.gc.ca/fr/orientation/controles-de-cybersecurite-de-base-pour-les-petites-et-moyennes-organisations)

Les meilleures mesures pour renforcer la cybersécurité des petites et moyennes entreprises (ITSAP.10.035) (https://www.cyber.gc.ca/fr/orientation/les-meilleures-mesures-pour-renforcer-la-cybersecurite-des-petites-et-moyennes)

Les 10 mesures de sécurité des TI : No 7, Protéger l'information au niveau de l'organisme (ITSM.10.097) (https://www.cyber.gc.ca/fr/orientation/10-mesures-securite-ti-no-7-proteger-information-niveau-organisme-itsm10097)

Facteurs à considérer en matière de cybersécurité pour votre site Web (ITSM.60.005) (https://www.cyber.gc.ca/fr/orientation/facteurs-considerer-en-matiere-de-cybersecurite-pour-votre-site-web-itsm60005)

Notes d'évaluation

◯ Non commencé Date : _____
◯ Défini Date : _____
◯ En cours Date : _____
◯ Mis en œuvre Date : _____

Remarques

Collecte des journaux [2.15]

Résultat Permet d'obtenir une meilleure visibilité pour détecter les cyberattaques et y intervenir efficacement.

Mesures recommandées

Recueillir et conserver les journaux pour les utiliser dans les activités de détection et d'intervention en cas d'incident (comme les enquêtes numériques), y compris les journaux suivants :

- axés sur l'accès et la sécurité (comme les systèmes de détection et de prévention d'intrusion);
- pare-feu;
- prévention de la perte de données;
- réseaux privés virtuels (RPV).

Aviser les équipes de sécurité lorsqu'une source de journaux essentielle est désactivée, comme la journalisation des événements Windows.

Pour les biens de TO dont les journaux ne sont pas standards ou disponibles, recueillir le trafic réseau et les communications entre ces biens et d'autres biens.

TTP ou risques

Capacité retardée, insuffisante ou incomplète à détecter les cyberincidents et à y intervenir.

Défenses affaiblies (T1562)

Références

PR.PS-04

Journalisation et surveillance de la sécurité de réseau (ITSAP.80.085) (https://www.cyber.gc.ca/fr/orientation/journalisation-surveillance-securite-reseau-itsap80085)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Stockage des journaux sécurisé et central [2.16]

Résultat Les journaux de sécurité des organisations sont protégés contre tout accès et toute modification non autorisés.

Mesures recommandées

Veiller à ce que les journaux soient conservés dans un système central, comme un outil de gestion des informations et des événements de sécurité (GIES) ou une base de données centrale, et que seuls les utilisateurs et utilisatrices autorisés et authentifiés puissent y accéder et les modifier. Conserver les journaux pendant une période déterminée en fonction des risques ou des lignes directrices règlementaires pertinentes.

TTP ou risques

Retrait d'indicateur sur l'hôte : suppression des journaux d'événement Windows (T1070.001)

Retrait d'indicateur sur l'hôte : suppression des journaux système Linux ou Mac (T1070.002)

Retrait d'indicateur sur l'hôte : détection de fichier (T1070.004)

Retrait d'indicateur sur l'hôte (ICS T0872)

Références

PR.PS-04

Journalisation et surveillance de la sécurité de réseau (ITSAP.80.085) (https://www.cyber.gc.ca/fr/orientation/journalisation-surveillance-securite-reseau-itsap80085)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Connexion interdite de dispositifs non autorisés [2.17]

Résultat Empêche les auteures et auteurs de menace d'obtenir un accès initial ou d'exfiltrer des données à l'aide de supports amovibles non autorisés.

Mesures recommandées

Appliquer des politiques et des processus pour veiller à ce que le matériel et les supports non autorisés ne soient pas connectés aux biens de TI et de TO, par exemple en limitant l'utilisation de dispositifs USB et de supports amovibles, ou en désactivant le lancement automatique.

Établir des procédures pour retirer, désactiver ou sécuriser les ports physiques dans les environnements de TO de façon à empêcher la connexion de dispositifs non autorisés, ou établir des procédures pour accorder l'accès au moyen d'exceptions approuvées.

TTP ou risques

Ajouts de matériel (T1200)

Duplication par support amovible (T1091, ICS T0847)

Références

PR.AA-05, PR.PS-01, PR.DS-01

Défense contre les menaces d'exfiltration de données (ITSM.40.110) (https://www.cyber.gc.ca/fr/orientation/defense-contre-menaces-dexfiltration-donnees-itsm40110)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Limitation des connexions de TO à l'Internet public [2.18]

Résultat Réduit le risque que des auteures et auteurs de menace exploitent ou interrompent des biens de TO connectés à l'Internet public.

Mesures recommandées

S'assurer qu'aucun bien de TO n'est connecté à l'Internet public, à moins que la connexion soit explicitement requise pour le fonctionnement. Exiger que les exceptions soient justifiées et documentées, et que des mesures de protection additionnelles soient mises en place pour les biens exclus afin d'empêcher et de détecter les tentatives d'exploitation (comme la journalisation, l'AMF, l'accès obligatoire par serveur mandataire ou autre intermédiaire).

TTP ou risques

Analyse active : analyse des vulnérabilités (T1595.002)

Applications exposées au public exploitables (T1190, ICS T0819)

Exploitation de services distants (T1210, ICS T0866)

Services externes distants (T1133, ICS T0822)

Références

PR.IR-01

Protéger vos technologies opérationnelles (ITSAP.00.051) (https://www.cyber.gc.ca/fr/orientation/proteger-vos-technologies-operationnelles-itsap00051)

Facteurs relatifs à la sécurité à considérer pour les systèmes de contrôle industriels (ITSAP.00.050) (https://www.cyber.gc.ca/fr/orientation/facteurs-relatifs-la-securite-considerer-pour-les-systemes-de-controle-industriels)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Documentation des configurations de dispositifs [2.19]

Résultat Améliore l'efficacité de la gestion des cyberattaques contre l'organisation, de l'intervention et de la reprise, et assure la continuité des services.

Mesures recommandées

Tenir des documents fiables qui décrivent les détails de configuration actuels et de base de tous les biens de TI et de TO essentiels pour faciliter des activités de gestion des vulnérabilités, d'intervention et de reprise plus efficaces. Effectuer des mises à jour et des examens périodiques, et en assurer le suivi.

TTP ou risques

Capacité retardée, insuffisante ou incomplète à maintenir les services et la fonctionnalité des dispositifs essentiels, ou à les rétablir.

Références

PR.PS-01

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Aucun service exploitable sur Internet [2.20]

Résultat Les utilisatrices et utilisateurs non autorisés ne peuvent pas obtenir un accès initial aux systèmes en exploitant des faiblesses connues dans les biens exposés au public.

Mesures recommandées

S'assurer que les biens dans l'Internet public n'exposent aucun service exploitable, tel que le protocole RDP. Lorsque ces services doivent être exposés, mettre en œuvre des contrôles compensatoires appropriés pour prévenir les formes courantes d'abus et d'exploitation. Désactiver tous les protocoles réseau et toutes les applications de système d'exploitation qui ne sont pas nécessaires sur les biens connectés à Internet.

TTP ou risques

Analyse active : analyse des vulnérabilités (T1595.002)

Applications exposées au public exploitables (T1190, ICS T0819)

Exploitation de services distants (T1210, ICS T0866)

Services externes distants (T1113, ICS T0822)

Services distants : Protocole RDP (T1021.001)

Références

PR.AA-03, PR.AA-05, PR.IR 01

Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089) (https://www.cyber.gc.ca/fr/orientation/les-10-mesures-de-securite-des-ti-visant-proteger-les-reseaux-internet-et-0)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

Poste de travail administratif sécurisé [2.21]

Résultat

Les postes de travail administratifs sécurisés (SAW pour *Secure Administrative Workstation*) dédiés à usage limité réduisent les risques pour la cybersécurité liés aux maliciels, à l'hameçonnage et aux attaques de type « Pass-the-Hash ». Ils permettent aux administratrices et administrateurs (comme les utilisatrices et utilisateurs détenant un accès privilégié) de se connecter de façon sécurisée au réseau de l'organisation.

Mesures recommandées

Les organisations fournissent des SAW aux administratrices et administrateurs pour réaliser leurs tâches administratives. Créer des SAW sécurisés et renforcés comme suit :

- isoler les SAW du réseau de TI public et, le cas échéant, du plan de données;
- désactiver la capacité d'installer d'autres logiciels;
- limiter l'accès à Internet ou aux services de courriel.

Pour l'administration du nuage à partir de ce poste de travail dédié, s'assurer qu'un RPV ou des listes d'applications autorisées sont nécessaires afin d'accéder à l'architecture du nuage.

TTP ou risques

Vidage de justificatifs d'identité (T1003)

Utilisation d'une autre méthode d'authentification (T1550)

Exploitation pour l'élévation des privilèges (T1068)

Exploitation pour l'élévation des privilèges (SCI) (T0890)

Comptes valides (T1078)

Services distants (T1021)

Interpréteur de commandes et de scripts (T1059)

Données du système local (T1005)

Exploitation pour l'évasion des défenses (T1211)

Découverte de compte (T1087)

Reniflage de réseau (T1040)

Références

PR.AA-05, PR.PS-01, PR.PS 02, PR.PS-03, PR.PS 04, PR.PS-05

Les 10 mesures de sécurité des TI : No 3, Gestion et contrôle des privilèges d'administrateur (ITSM.10.094) (https://www.cyber.gc.ca/fr/orientation/10-mesures-securite-ti-no-3-gestion-controle-privileges-itsm10094)

Mesures de cybersécurité de base à l'intention des petites organisations (ITSAP.10.300) (https://www.cyber.gc.ca/fr/orientation/foundational-cyber-security-actions-small-organizations-itsap10300)

Notes d'évaluation

◯ Non commencé Date : _____
◯ Défini Date : _____
◯ En cours Date : _____
◯ Mis en œuvre Date : _____

Remarques

DÉTECTION [3]

Détection de menace pertinente et de TTP [3.0]

Résultat Les organisations sont au courant des menaces et des TTP et sont en mesure de les détecter en temps opportun.

Mesures recommandées

Documenter une liste de menaces et de TTP des auteures et auteurs de cybermenace qui s'applique à l'organisation (par exemple, en fonction de l'industrie ou du secteur) et être capable de détecter ces principales menaces (par exemple, à l'aide de règles, d'alertes ou de systèmes commerciaux de détection et de prévention).

TTP ou risques

Sans connaître les menaces pertinentes et sans avoir la capacité de les détecter, les organisations risquent que les auteures et auteurs de menace soient présents dans leurs réseaux pendant de longues périodes sans être détectés.

Références

ID.RA-02, ID.RA-03, DE.CM-01, DE.CM-03, DE.CM-06

Pratiques exemplaires sur la mise en place d'un centre des opérations de sécurité (COS) (ITSAP.00.500) (https://www.cyber.gc.ca/fr/orientation/pratiques-exemplaires-mise-place-dun-centre-operations-securite-cos-itsap00500)

Journalisation et surveillance de la sécurité de réseau (ITSAP.80.085) (https://www.cyber.gc.ca/fr/orientation/journalisation-surveillance-securite-reseau-itsap80085)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

INTERVENTION [4]

Signalement des incidents [4.0]

Résultat Aide le Centre pour la cybersécurité et d'autres organisations à comprendre l'ampleur d'une cyberattaque afin d'être en mesure de fournir une assistance appropriée.

Mesures recommandées

Avoir en place des politiques et procédures codifiées sur la façon de signaler tous les cyberincidents confirmés aux entités externes appropriées.

Signaler les incidents connus au Centre pour la cybersécurité et à d'autres parties dans les délais prescrits par les lignes directrices règlementaires applicables ou, en l'absence de lignes directrices, dès qu'il est possible de le faire en toute sécurité.

TTP ou risques

Sans signalement opportun des incidents, l'assistance offerte aux organisations touchées par le Centre pour la cybersécurité et d'autres groupes est moins efficace en raison du manque de renseignements essentiels relatifs à l'environnement global de menaces (par exemple si une attaque plus vaste est orchestrée contre un secteur précis).

Références

RS.CO-02, RS.CO-03, RS.MA-01, RS.MA-02, RS.MA-04

Signaler un cyberincident (https://www.cyber.gc.ca/fr/cyberincidents)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques

REPRISE [5]

Planification en cas d'incident et état de préparation [5.0]

Résultat Les organisations sont en mesure d'assurer la reprise des activités de façon efficace et en toute sécurité à la suite d'un incident de cybersécurité.

Mesures recommandées

Élaborer, tenir à jour et exécuter des plans visant à assurer la reprise et la restauration des activités et des systèmes ou biens essentiels à la mission qui pourraient avoir été touchés par un cyberincident.

En cas de cyberincident, exécuter une analyse de l'incident après la reprise afin de déterminer les leçons retenues et d'empêcher de futurs incidents. Intégrer les leçons retenues aux améliorations apportées aux processus de gouvernance et/ou au plan d'intervention en cas d'incident.

TTP ou risques

Perturbation de la disponibilité d'un bien, d'un service ou d'un système.

Références

RC.RP-01, ID.IM-02, ID.IM-03, ID.IM-04

Élaborer un plan d'intervention en cas d'incident (ITSAP 40.003) (https://www.cyber.gc.ca/fr/orientation/elaborer-un-plan-dintervention-en-cas-dincident-itsap40003)

Élaboration d'un plan de reprise informatique personnalisé (ITSAP.40.004) (https://www.cyber.gc.ca/fr/orientation/elaboration-dun-plan-de-reprise-informatique-personnalise-itsap40004)

Notes d'évaluation

- ◯ Non commencé Date : _____
- ◯ Défini Date : _____
- ◯ En cours Date : _____
- ◯ Mis en œuvre Date : _____

Remarques