Exigences de Cyber Essentials Canada

AB440

Version 3.0 | Janvier 2019

Table des matières

1 But

Le présent document est conçu pour servir de guide visant à expliquer brièvement aux organisations les mesures de sécurité qu'elles doivent s'attendre à mettre en œuvre pour répondre aux exigences du programme Cyber Essentials Canada. Ces mesures de sécurité de base permettront d'atténuer les menaces les plus courantes qui visent les organisations par l'intermédiaire d'Internet, et elles respectent les normes exhaustives bien établies en matière de cybersécurité.

1.1 Qui doit utiliser ce document?

Les thèmes concernant les mesures de contrôle abordés dans le présent document s'adressent aux organisations de toute taille.

On s'attend à ce que les organisations de grande taille disposent d'ores et déjà de connaissances ou d'expérience en matière de cybersécurité. Cependant, les entreprises plus petites présentent en général une capacité plus réduite pour mettre en œuvre l'ensemble des contrôles nécessaires leur permettant d'obtenir une protection solide contre les cybermenaces.

Il pourrait être nécessaire que les petites organisations (y compris celles qui ne comptent qu'un seul employé), et même quelques entreprises de taille moyenne, aient besoin d'un soutien et de conseils supplémentaires de manière à veiller à ce que les contrôles techniques abordés dans les présentes exigences puissent être mis en œuvre de manière adéquate.

1.2 Quels éléments de l'organisation ces exigences permettent-elles de protéger?

Les éléments technologiques d'une organisation qui sont généralement exposés aux cyberattaques fréquentes comprennent les dispositifs qui présentent une connexion Internet, y compris les ordinateurs de bureau, les ordinateurs portatifs, les tablettes et les téléphones intelligents, ainsi que les serveurs connectés à Internet, y compris les serveurs de messagerie, les serveurs Web et les serveurs d'applications.

2 Exigences pour l'infrastructure des TI

Il s'agit de préciser les contrôles techniques requis pour l'infrastructure de TI, aux fins d'évaluation dans le cadre du programme Cyber Essentials Canada.
Nous déterminons les exigences en fonction de cinq aspects de contrôle technique :

- Pare-feu frontaliers et passerelles Internet
- Configuration sécurisée
- Contrôle de compte d'utilisateur
- Protection contre les maliciels
- Gestion des correctifs

En tant que candidat au programme Cyber Essentials Canada, vous devez veiller à ce que votre organisation respecte l'ensemble des exigences. Vous devrez également présenter plusieurs formes de preuve à l'organisme de certification sélectionné avant de pouvoir recevoir la certification voulue.
Procédez comme suit :

1. Déterminez le **périmètre de la portée** pour votre organisation, et définissez la **portée au sein de cette limite**.

2. Examinez chacun des cinq **aspects de contrôle technique** ainsi que les **mesures de contrôle qu'ils comportent à titre d'exigences**.
3. Prenez les mesures nécessaires afin de vous **assurer que votre organisation respecte chaque exigence** au sein de la portée que vous avez déterminée.

Définitions

- Les **logiciels** comprennent les systèmes d'exploitation, les applications commerciales grand public, les modules d'extension, les interpréteurs, les scripts, les bibliothèques, les logiciels réseau et les micrologiciels.
- Les **dispositifs** comprennent tous les types d'hôtes, le matériel de mise en réseau, les serveurs, les réseaux et l'équipement des utilisateurs finaux, tels que les ordinateurs de bureau, les ordinateurs portatifs, les tablettes et les téléphones mobiles (téléphones intelligents), qu'ils soient physiques ou virtuels.
- Le **candidat** correspond à l'organisation qui cherche à obtenir la certification, ou parfois à la personne-ressource, selon le contexte.

https://www.cyberessentials.ncsc.gov.uk/requirements-for-it-infrastructure
https://www.cyberessentials.ncsc.gov.uk/requirements-for-it-infrastructure

3 Portée des activités

Aperçu de la portée

L'évaluation et la certification peuvent englober l'ensemble de l'infrastructure des TI du candidat, ou seulement une partie de celle-ci. Dans les deux cas, il faut clairement définir le périmètre de la portée en précisant l'unité fonctionnelle responsable, la limite du réseau et l'emplacement matériel. Le candidat et l'organisme de certification doivent s'entendre sur la portée avant le début de l'évaluation.

Il est fortement recommandé que la portée englobe dans la mesure du possible l'ensemble de l'infrastructure des TI afin d'offrir une protection optimale.

Les exigences s'appliquent à tous les appareils et logiciels qui se trouvent au sein de ce périmètre et qui répondent aux conditions qui suivent :

- Acceptent les connexions réseau entrantes d'hôtes non sécurisés connectés à Internet;
- Établissent des connexions sortantes effectuées par des utilisateurs à des dispositifs arbitraires par le truchement d'Internet;
- Contrôlent le flux de données entre l'un des dispositifs mentionnés précédemment et Internet.

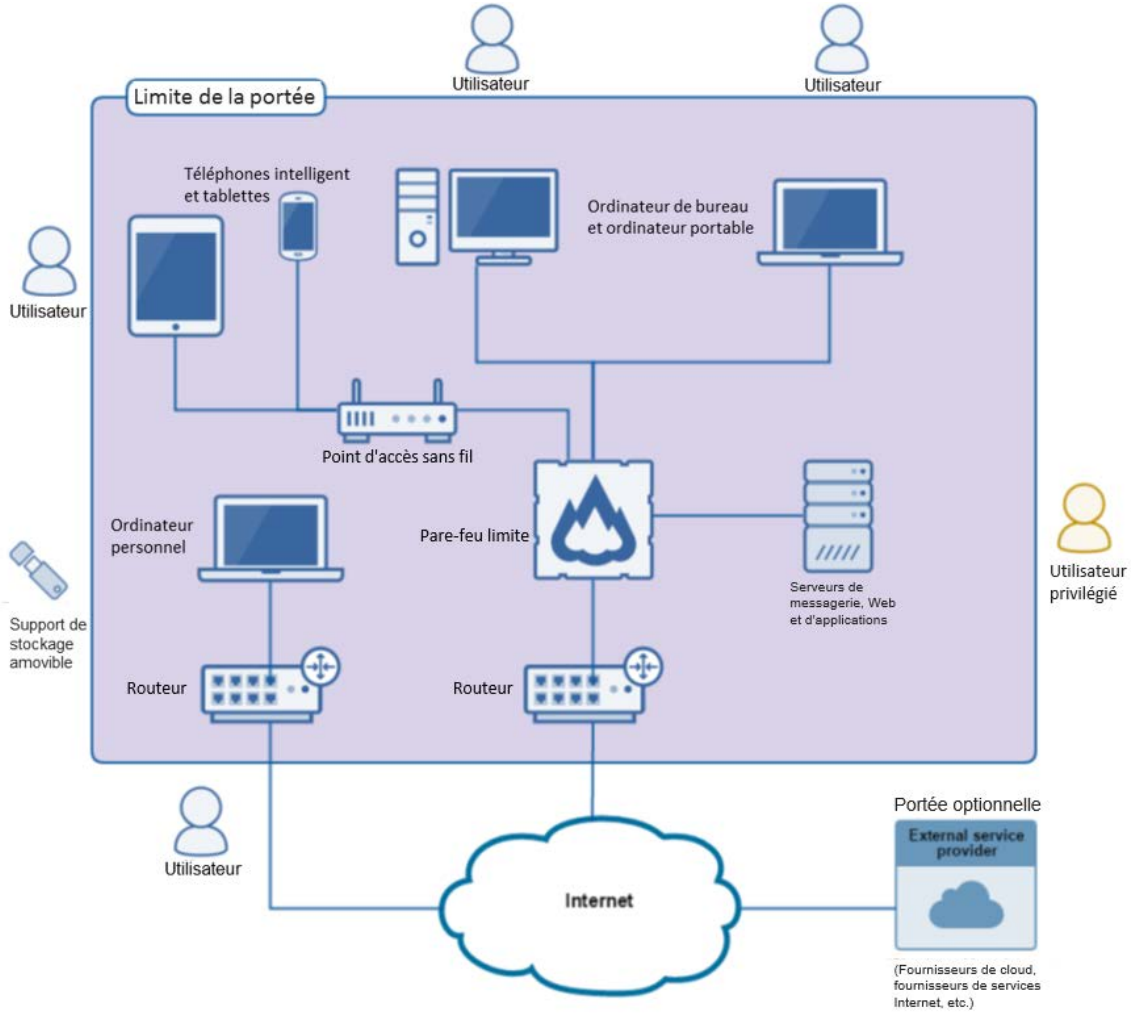

Figure 1. Portée des exigences pour l'infrastructure des TI.

Politique sur l'apport de votre équipement personnel de communication (AVEC)
En plus des appareils mobiles et des périphériques à distance dont l'organisation est propriétaire, les dispositifs qui appartiennent aux utilisateurs et qui ont également accès aux données ou aux services de l'organisation font également **partie de la portée**.

Auparavant, les appareils des utilisateurs étaient gérés par l'intermédiaire d'une administration centralisée, de manière à assurer l'uniformité au sein de l'organisation. Dans de tels cas, la certification des contrôles de sécurité est simple puisqu'il existe une version normalisée ou une référence pouvant être évaluée.

La politique AVEC complique les choses, puisque les utilisateurs ont la possibilité de personnaliser leur équipement, ce qui rend plus ardue la mise en place de mesures de contrôle uniformes.

Dispositifs sans fil
Les dispositifs sans fil (y compris les points d'accès sans fil) sont :

- Compris **dans la portée** s'ils peuvent communiquer avec d'autres dispositifs par Internet;
- **Exclus de la portée** si un assaillant ne peut pas attaquer directement par Internet (le programme Cyber Essentials Canada ne tient pas compte des attaques qui peuvent être uniquement lancées au sein de la portée des signaux de l'appareil sans fil).

Services gérés à l'externe – nuage
Si le candidat peut facilement mettre en œuvre les exigences en ce qui concerne ses services infonuagiques, ces services doivent être inclus dans la portée.

Exemple
L'entreprise Acme Corporation s'est procuré une infrastructure comme service (IaaS) auprès d'un fournisseur de services infonuagiques. Acme dispose du contrôle sur les systèmes d'exploitation de l'infrastructure et est en mesure de mettre en œuvre les exigences. Acme inclura donc ce service à la portée.

À l'heure actuelle, le logiciel comme service (SaaS) et la plateforme comme service (PaaS) ne font **pas partie de la portée** – les exigences actuelles ne peuvent pas leur être appliquées.

Services gérés à l'externe – autres
Lorsque le candidat utilise d'autres services gérés à l'externe (comme l'administration à distance), il pourrait être dans l'incapacité de répondre directement à toutes les exigences. Le candidat peut **choisir** d'inclure ces services dans la portée, en fonction de la faisabilité.

S'ils font partie de la portée, le candidat doit être en mesure d'attester que les exigences qui se trouvent hors de son contrôle sont respectées de manière adéquate par le fournisseur de services. Des éléments probants existants pourraient être pris en compte (par exemple ceux liés à la certification PCI d'un service infonuagique ou les certifications en vertu de la norme ISO 27001 dont la portée est pertinente).

Applications Web
Les applications Web commerciales créées par des entreprises de développement (plutôt que par des développeurs internes) et qui sont publiquement accessibles sur Internet font par défaut **partie de la portée**.

Les éléments sur mesure et personnalisés des applications Web sont **exclus de la portée**. Pour réduire les vulnérabilités de telles applications, la première mesure consiste à effectuer un développement et des essais approfondis qui respectent les pratiques commerciales exemplaires, telles que les normes OWASP (Open Web Application Security Project).

4 Pare-feux

Applicabilité : pare-feu frontaliers, ordinateurs de bureau, ordinateurs portatifs, routeurs, serveurs.

Objectif
Veiller à ce que seuls les services sécuritaires et essentiels du réseau soient accessibles à partir d'Internet.

Introduction
Tous les dispositifs utilisent des services du réseau, ce qui crée une forme de communication avec les autres dispositifs et services. En restreignant l'accès à ces services, vous limitez votre exposition aux attaques. Cela peut être réalisé à l'aide de pare-feu et de périphériques réseaux équivalents.

Un pare-feu limite est un périphérique réseau qui peut limiter le trafic entrant et sortant du réseau lié aux services de son réseau d'ordinateurs et d'appareils mobiles. Cela permet de se protéger contre les cyberattaques en mettant en place des limites, également appelées règles du pare-feu, qui peuvent autoriser ou bloquer le trafic en fonction de la source, de la destination et du type de protocole de communication.

Il est également possible de configurer un pare-feu hôte sur un dispositif. Cela fonctionne de la même manière qu'un pare-feu limite, mais seul le dispositif sur lequel le pare-feu est configuré est protégé. Cette approche permet de mettre en place des règles plus personnalisées qui s'appliquent au dispositif dès que ce dernier est utilisé. Cependant, cette approche augmente les démarches administratives relatives à la gestion des règles des pare-feu.

Exigences dans le cadre de l'aspect de contrôle technique
Chaque dispositif se trouvant au sein de la portée doit être protégé par un pare-feu correctement configuré (ou un périphérique réseau équivalent).

Pour l'ensemble des pare-feu (ou des périphériques réseau équivalents), l'organisation du candidat doit effectuer régulièrement ce qui suit :

- Remplacer tous les mots de passe par défaut de l'administrateur par des mots de passe difficiles à deviner (voir la section Authentification par mot de passe), ou désactiver complètement l'accès à distance de l'administrateur;
- Empêcher tout accès à l'interface de l'administrateur (utilisée pour gérer la configuration des pare-feu) par Internet, à moins qu'il n'existe une justification opérationnelle et que l'interface soit protégée par l'une des mesures de contrôle suivantes :
    - Un deuxième moyen d'authentification, par exemple un jeton unique;
    - Une liste blanche des adresses IP qui limite l'accès à un nombre réduit d'adresses fiables;
- Bloquer par défaut les connexions entrantes non authentifiées;

- Veiller à ce que les règles du pare-feu concernant les connexions entrantes soient approuvées et documentées par une personne autorisée; la justification opérationnelle doit être mentionnée dans la documentation;
- Supprimer ou désactiver rapidement les règles de permission d'accès du pare-feu lorsqu'elles ne sont plus nécessaires;
- Utiliser un pare-feu hôte sur les dispositifs utilisés sur des réseaux non sécurisés, comme les points d'accès sans fil publics.

5 Configuration sécurisée

Applicabilité : serveurs de messagerie, serveurs Web et serveurs d'applications; ordinateurs de bureau; ordinateurs portatifs; tablettes; cellulaires; pare-feu; routeurs.

Objectif

S'assurer que les ordinateurs et les périphériques réseau sont configurés de manière à :

- Réduire le niveau des vulnérabilités inhérentes;
- Fournir uniquement les services requis pour remplir leur rôle.

Introduction

Les ordinateurs et les périphériques réseau ne sont pas toujours sécurisés en raison de leur configuration par défaut. Les configurations standard de série comprennent souvent un ou plusieurs points faibles, par exemple :

- Un compte administrateur comportant un mot de passe par défaut prédéterminé et connu de tous;
- Des comptes utilisateurs inutiles préconfigurés (parfois avec des privilèges d'accès spéciaux);
- Des applications ou services inutiles préinstallés.

Les installations par défaut des ordinateurs et des périphériques réseau peuvent offrir aux cyberassaillants plusieurs occasions d'accéder de manière non autorisée aux renseignements confidentiels d'une organisation, souvent très facilement.

En mettant en œuvre de simples mesures de contrôle technique lors de l'installation des ordinateurs et des périphériques réseau, il est possible de réduire au minimum les vulnérabilités et d'augmenter la protection face aux types de cyberattaques les plus fréquents.

Exigences dans le cadre de l'aspect de contrôle technique

Ordinateurs et périphériques réseau

Le candidat doit gérer de manière active les ordinateurs et les périphériques réseau. Il doit effectuer ce qui suit de manière régulière :

- Remplacer tous les mots de passe par défaut ou facilement devinables par des mots de passe moins évidents;
- Supprimer ou désactiver les comptes utilisateurs inutiles (tels que les comptes d'invités et les comptes administrateurs qui ne seront pas utilisés);
- Supprimer ou désactiver les logiciels inutiles (y compris les applications, les utilitaires du système et les services du réseau);
- Désactiver toute fonction d'exécution automatique qui permet d'exécuter un fichier sans l'autorisation de l'utilisateur (par exemple lors d'un téléchargement à partir d'Internet);
- Authentifier les utilisateurs avant de permettre un accès par Internet aux données personnelles ou commerciales confidentielles, ou aux données critiques pour le fonctionnement de l'organisation.

Authentification par mot de passe
Authentification par mot de passe

Le candidat doit faire bon usage des contrôles techniques à sa disposition avec les systèmes protégés par un mot de passe. Dans la mesure du possible, les contrôles techniques et les politiques doivent permettre de soulager le fardeau qui pèse sur les utilisateurs individuels et de moins compter sur leur connaissance et leur mise en application des pratiques exemplaires.

On attend cependant des utilisateurs qu'ils choisissent des mots de passe confidentiels.

En ce qui concerne l'authentification par mot de passe pour les services Internet, le candidat doit faire ce qui suit :

- Éviter que les mots de passe puissent être devinés en employant une technique de force brute, en appliquant au moins l'une des méthodes suivantes :
  - Verrouiller les comptes après **tout au plus** 10 tentatives de connexion infructueuses;
  - Limiter le nombre d'essais autorisés dans un délai donné à **tout au plus** 10 essais dans une période de 5 minutes.

En ce qui concerne l'authentification par mot de passe pour les services Internet et ceux non basés sur Internet, le candidat doit faire ce qui suit :

- Créer un mot de passe comprenant au **minimum** huit caractères;
- **Ne pas** limiter la longueur maximale du mot de passe;
- Changer les mots de passe rapidement lorsque le candidat sait ou suspecte qu'ils ont été compromis;
- Disposer d'une politique sur les mots de passe qui explique ce qui suit aux utilisateurs :
  - Éviter de choisir des mots de passe évidents (par exemple ceux qui s'appuient sur des renseignements qui peuvent être obtenus facilement, comme le nom d'un animal domestique);
  - Ne pas choisir de mots de passe communs (par exemple en définissant une liste noire de mots de passe);
  - Ne pas utiliser le même mot de passe partout, au travail ou à la maison;
  - Où et comment consigner les mots de passe afin de les conserver et de les récupérer au besoin, par exemple dans une enveloppe cachetée placée dans une armoire sécurisée;
  - La possibilité d'utiliser un logiciel de gestion des mots de passe (si oui, quel logiciel et de quelle manière s'en servir);
  - Les mots de passe qui doivent être absolument mémorisés et jamais inscrits quelque part.

Le candidat n'est **pas** tenu d'effectuer ce qui suit :

- Configurer l'expiration à intervalle régulier des mots de passe de n'importe quel compte (nous contre-indiquons cette marche à suivre; pour en savoir plus, consultez la section Problèmes liés à l'expiration à intervalle régulier des mots de passe;
- Mettre en œuvre des exigences liées à la complexité des mots de passe.

6 Contrôle de compte d'utilisateur

Applicabilité : serveurs de messagerie, serveurs Web et serveurs d'applications; ordinateurs de bureau; ordinateurs portatifs; tablettes; cellulaires.

Objectifs
Veiller à ce que les comptes utilisateurs :

- Soient uniquement attribués à des personnes autorisées;
- Offrent uniquement un accès aux applications, ordinateurs et réseaux nécessaires pour que l'utilisateur puisse remplir son rôle.

Introduction
Chaque compte utilisateur actif de votre organisation permet d'accéder à des dispositifs et des applications, ainsi qu'à des renseignements opérationnels confidentiels. En vous assurant que seules les personnes autorisées disposent de comptes utilisateurs, et que ces comptes offrent seulement l'accès requis pour que les utilisateurs remplissent leur rôle, vous réduisez le risque que des renseignements soient volés ou endommagés.

Par rapport aux comptes utilisateurs normaux, les comptes qui présentent des privilèges d'accès spéciaux offrent un accès amélioré aux dispositifs, applications et renseignements. Lorsque de tels comptes sont compromis, il est possible de tirer parti de la plus grande liberté qu'ils offrent pour altérer les renseignements à grande échelle, interrompre les processus opérationnels et accéder sans autorisation à d'autres dispositifs de l'organisation.

Par exemple, les comptes administrateurs comportent de très nombreux privilèges. De tels comptes permettent généralement d'effectuer ce qui suit :

- Exécuter un logiciel qui peut apporter des modifications importantes au système d'exploitation en ce qui concerne la sécurité;
- Modifier le système d'exploitation pour certains utilisateurs ou la totalité d'entre eux;
- Créer de nouveaux comptes et leur attribuer des privilèges.

Tous les types d'administrateurs possèdent de tels comptes, y compris les administrateurs de domaine et les administrateurs locaux.

Il faut également garder à l'esprit que si un utilisateur ouvre une adresse URL ou une pièce jointe contenant un maliciel, ce dernier sera exécuté en conservant les mêmes privilèges que ceux associés au compte de l'utilisateur en question. Il faut donc faire preuve de prudence en ce qui concerne l'attribution des comptes présentant des privilèges.

Exemple
Jody est connectée à un compte administrateur. Si elle ouvre une adresse URL ou une pièce jointe contenant un maliciel, ce dernier profitera probablement de ses privilèges d'administrateur.

Malheureusement, c'est exactement ce qui se produit. En se servant des privilèges d'administrateur de Jody, un type de maliciel appelé logiciel rançonneur chiffre toutes les données du réseau et exige ensuite le versement d'une somme d'argent.

Le logiciel rançonneur a été en mesure de chiffrer beaucoup plus de données avec ces privilèges d'administrateur que ce qui aurait été le cas avec les privilèges associés à un compte utilisateur standard, ce qui n'a fait qu'empirer la situation.

Le candidat doit contrôler les comptes utilisateurs et les privilèges d'accès accordés à chaque compte utilisateur. Il doit également comprendre l'authentification des comptes utilisateurs et contrôler ce niveau d'authentification. Cela signifie que le candidat doit réaliser ce qui suit :

- Disposer d'un processus de création et d'approbation des comptes utilisateurs;
- Authentifier les utilisateurs avant de leur permettre d'accéder aux applications ou aux dispositifs en utilisant des données d'identification uniques (voir la section Authentification par mot de passe);
- Supprimer ou désactiver les comptes utilisateurs qui ne sont plus requis (lorsqu'un utilisateur quitte l'organisation ou après une période définie d'inactivité du compte, par exemple);
- Mettre en place une authentification en deux étapes dans la mesure du possible;
- Utiliser des comptes administrateurs pour effectuer **uniquement** des tâches administratives (pas de courriels, de navigation sur Internet ou d'autres activités possibles avec un compte standard qui pourraient exposer les privilèges d'administrateur à des risques pouvant être évités);
- Supprimer ou désactiver les privilèges d'accès spéciaux lorsqu'ils ne sont plus requis (lorsqu'un membre du personnel change de rôle, par exemple).

7 Protection contre les maliciels

Applicabilité : ordinateurs de bureau; ordinateurs portatifs; tablettes; cellulaires.

Objectifs

Limiter l'exécution des maliciels connus et des logiciels non sécurisés afin d'empêcher que des codes malveillants endommagent des données sensibles ou y accèdent.

Introduction

L'exécution d'un logiciel téléchargé à partir d'Internet peut exposer un dispositif à une infection par un maliciel.

Les maliciels, tels que des virus informatiques, des vers et des logiciels espions, correspondent à des logiciels qui ont été conçus et délibérément distribués afin de réaliser des actions malveillantes. Les potentielles sources d'infection par un maliciel comprennent les pièces jointes des courriels, les téléchargements (y compris à partir des boutiques d'applications) et l'installation directe d'un logiciel non autorisé.

Si un système est infecté par un maliciel, votre organisation connaîtra sans doute des problèmes tels que des dysfonctionnements des systèmes, des pertes de données et une infection croissante qui reste non décelée jusqu'à ce qu'elle cause d'autres problèmes ailleurs.

Vous pouvez éviter en grande partie les dommages potentiels causés par un maliciel de la manière suivante :

- En décelant et en désactivant le maliciel avant qu'il ne cause de dommages (logiciel anti-maliciel);
- En exécutant uniquement les logiciels sécurisés (liste blanche);
- En exécutant les logiciels non sécurisés dans un environnement dans lequel l'accès aux autres données est contrôlé (bac à sable).

Exemple

L'entreprise Acme Corporation a mis en œuvre une procédure de signature du code ainsi qu'une règle permettant uniquement l'exécution sur les dispositifs des applications approuvées provenant de la boutique d'applications de l'appareil. Les applications non signées et non approuvées ne peuvent pas être exécutées sur les dispositifs. Le fait que les utilisateurs ne puissent installer que des applications sécurisées (liste blanche) permet de réduire les risques d'infection par un maliciel.

Exigences dans le cadre de l'aspect de contrôle technique

Le candidat doit mettre en place un mécanisme de protection contre les maliciels sur tous les dispositifs faisant partie de la portée. Pour chacun de ces dispositifs, le candidat doit utiliser au moins l'un des trois mécanismes indiqués ci-dessous :

Logiciel anti-maliciel

- Le logiciel (ainsi que tous les fichiers signature associés aux maliciels) doit être tenu à jour, et les fichiers signature doivent être mis à jour au moins une fois par jour. Cela peut être réalisé par l'intermédiaire de mises à jour automatiques, ou par l'intermédiaire d'un déploiement géré de manière centrale.

- Le logiciel doit être configuré de manière à balayer automatiquement les fichiers dès qu'on y accède. Cela comprend les fichiers téléchargés et ouverts, ainsi que les fichiers auxquels on accède à partir d'un dossier réseau.
- Le logiciel doit balayer automatiquement les pages Web lorsqu'on y accède à partir d'un navigateur Web (qu'il s'agisse d'un accès par un autre logiciel ou par le navigateur en tant que tel).
- Le logiciel doit empêcher toute connexion à des sites Web malveillants sur Internet (à l'aide d'une liste noire, par exemple), à moins qu'il existe un besoin opérationnel clairement justifié et que le candidat comprenne et accepte les risques connexes.

Liste blanche des applications

- Seules les applications approuvées, limitées par la signature du code, peuvent être exécutées sur les dispositifs. Le candidat doit effectuer ce qui suit :
    - Approuver de manière proactive les applications avant leur installation sur les dispositifs;
    - Tenir à jour une liste des applications approuvées;
    - Les utilisateurs ne doivent pas être en mesure d'installer une application non signée ou présentant une signature non valide.

Bac à sable pour les applications

- Tous les codes d'origine inconnue doivent être exécutés dans un « bac à sable » afin de limiter l'accès aux autres ressources, à moins qu'une autorisation explicite ne soit accordée par l'utilisateur. Il s'agit notamment :
    - D'autres applications exécutées dans un bac à sable;
    - D'entrepôts de données, tels que ceux qui contiennent des documents et des photos;
    - De périphériques confidentiels, tels que les caméras, microphones et GPS;
    - D'accès au réseau local.

8 Gestion des correctifs

Applicabilité : serveurs de messagerie, serveurs Web et serveurs d'applications; ordinateurs de bureau; ordinateurs portatifs; tablettes; cellulaires; pare-feu; routeurs.

Objectifs
Veiller à ce que les appareils et les logiciels ne soient pas vulnérables aux problèmes de sécurité connus pour lesquels existent des correctifs.

Introduction
Tout dispositif sur lequel est exécuté un logiciel présente des défauts de sécurité, appelés vulnérabilités.

Des vulnérabilités sont fréquemment découvertes dans toutes sortes de logiciels. Une fois qu'elles sont décelées, des personnes ou des groupes malveillants agissent rapidement pour exploiter ces vulnérabilités afin d'attaquer les ordinateurs et les réseaux des organisations qui présentent ces défauts.

Les fournisseurs des produits proposent des correctifs pour résoudre les vulnérabilités décelées dans leurs produits pour lesquels ils offrent toujours un soutien; il s'agit de mises à jour du logiciel appelées correctifs. Les correctifs sont offerts immédiatement aux clients ou proposés sous la forme de publication régulière (par exemple mensuelle).

Les fournisseurs de produits n'offrent généralement pas de correctifs pour les produits pour lesquels ils ont cessé de fournir un soutien, même pas pour résoudre des vulnérabilités.

Exigences dans le cadre de l'aspect de contrôle technique :
Le candidat doit tenir tous ses logiciels à jour. Les logiciels doivent :

- Faire l'objet d'une licence et être pris en charge;
- Être supprimés des dispositifs lorsqu'ils ne sont plus pris en charge;
- Recevoir un correctif dans les 14 jours qui suivent sa publication, lorsque le correctif résout une vulnérabilité que le fournisseur du produit décrit comme critique ou présentant un risque élevé*.

*Si le fournisseur utilise des termes différents pour décrire la gravité des vulnérabilités, se reporter à la définition précise du Système commun de notation des vulnérabilités (CVSS).

Dans le cadre du programme Cyber Essentials Canada, les vulnérabilités critiques ou présentant un niveau de risque élevé comportent les caractéristiques suivantes :

- Vecteur d'attaque : réseau seulement
- Complexité de l'attaque : faible seulement
- Privilèges requis : aucun uniquement
- Interaction avec les utilisateurs : aucune uniquement
- Exploitation de la maturité du code : fonctionnelle ou élevée
- Niveau de confiance signalé : confirmé ou élevé

Certains fournisseurs proposent sous la forme d'une seule mise à jour des correctifs pour plusieurs problèmes présentant différents niveaux de gravité. Si une telle mise à jour permet de résoudre des enjeux critiques ou présentant un risque élevé, elle doit être installée dans un délai de 14 jours.

Il est important dans toutes les organisations que la haute direction participe à la cybersécurité de l'entreprise; c'est pourquoi il est obligatoire qu'un membre du Conseil (ou équivalent) approuve les renseignements transmis à un organisme de certification.

9 Historique des versions

Version	Date	Auteur	Type de changement
1.0	8 mars 2017	Brendan Dunphy	Création du document
2.0	15 juillet 2017	Brendan Dunphy	Ajout de nouvelles exigences
2.1	16 juillet 2018	Jessica Hamilton	Formatage, orthographe, grammaire, nouvelle image de marque
2.2	14 août 2018	Jessica Hamilton	Révisions et insertion de l'historique des versions
2.3	28 août 2018	Geneviève Law	Révisions, mise à jour de la date et de l'en-tête
3.0	07 janvier 2019	Brendan Dunphy	Corrections et révisions