CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SI-03

Protection contre les programmes malveillants

Juill. 2026

Votre gouvernement

Québec

SI

Intégrité des systèmes et des données

System and Information Integrity

SI-03 — Protection contre les programmes malveillants (-F-) (Obligatoire)

Énoncés :

a. Mettre en oeuvre des mécanismes de protection contre les programmes malveillants [Sélection (un choix ou plus) : basés sur les signatures; non basés sur les signatures] aux points d'entrée et de sortie du système afin de détecter et d'éliminer le code malveillant
b. Mettre à jour automatiquement les mécanismes de protection contre les programmes malveillants dès que de nouvelles versions sont disponibles, conformément à la stratégie et aux procédures organisationnelles de gestion des configurations
c. Configurer les mécanismes de protection contre les programmes malveillants de façon à :
- **1.** effectuer des analyses périodiques du système [Affectation : fréquence définie par l'organisation] et des analyses en temps réel des fichiers de sources externes aux [Sélection (un choix ou plus) : points d'extrémité; point d'entrée ou sortie du réseau] lors de leur téléchargement, de leur ouverture ou de leur exécution, conformément à la stratégie organisationnelle
- **2.** [Sélection (un choix ou plus) : bloquer le code malveillant; mettre en quarantaine le code malveillant; effectuer {Affectation : action définie par l'organisation}]; et envoyer une alerte à [Affectation : personnel ou rôles définis par l'organisation] suivant la détection de code malveillant

d. Traiter les faux positifs résultant de la détection et de l'élimination de code malveillant et leurs répercussions potentielles sur la disponibilité des systèmes

Paramètres :

a. non basé sur la signature "Non-signature based" c.
- **1.** hebdomadaire; points d'extrémité ("endpoints") c.
- **2.** bloquer le code malveillant, mettre en quarantaine le code malveillant et effectuer une action à définir par l'organisation au besoin; personne responsable de la cyberdéfense au niveau opérationnel (ex.: analyste, COMSI, etc.)

aaQC. antivirus avec fonctionnalités EDR; serveurs et postes de travail

Responsable : OP

Date limite de mise en oeuvre : 2021-06-30

Discussion :

Les points d'entrée et de sortie du système comprennent les pare-feu, les serveurs d'accès à distance, les stations de travail, les serveurs de messagerie, les serveurs Web, les serveurs mandataires, les ordinateurs blocs-notes et les appareils mobiles. Le code malveillant comprend les virus, les vers, les chevaux de Troie et les logiciels espions. Le code malveillant peut également être codé 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 inséré dans les systèmes de différentes façons, notamment par courriel, par Internet et au moyen de dispositifs de stockage portatifs. Les insertions de code malveillant surviennent lors de l'exploitation de vulnérabilités du système. Il existe une variété de technologies et de méthodes pour limiter ou éliminer les effets des attaques de code malveillant. Les mécanismes de protection contre le code malveillant comprennent des technologies basées ou non sur les signatures. Les mécanismes de détection non fondés sur les signatures comprennent des techniques d'IA utilisant des données heuristiques pour détecter, analyser et décrire les caractéristiques ou les comportements de programmes malveillants, et pour trouver des moyens de contrôler ces programmes en l'absence de signature ou si les signatures existantes ne sont pas efficaces. Le code malveillant polymorphique (c'est-à-dire le code pour lequel les signatures sont modifiées lors de la réplication) est un des cas où les signatures actives sont inexistantes ou inefficaces. Les technologies basées sur la réputation sont un exemple de mécanismes qui ne sont pas fondés sur les signatures. En plus des technologies mentionnées précédemment, la gestion omniprésente des configurations, les contrôles complets d'intégrité des logiciels et les logiciels anti-exploitation peuvent être efficaces pour empêcher l'exécution de code non autorisé. Le code malveillant peut être présent dans des logiciels COTS et dans des logiciels conçus sur mesure. Il peut comprendre des bombes logiques, des portes dérobées et d'autres types d'attaques susceptibles d'avoir des répercussions sur les fonctions liées à la mission et aux activités de l'organisation. Dans les situations où le code malveillant ne peut pas être détecté par les méthodes ou les technologies de détection, l'organisation doit miser sur d'autres types de contrôles, comme des pratiques de codage sécurisé, la gestion et le contrôle des configurations, les processus d'approvisionnement fiable et les pratiques de surveillance, pour s'assurer que le logiciel n'effectue que les fonctions prévues. Les organisations peuvent décider de prendre différentes mesures en réponse à la détection de code malveillant. Par exemple, les organisations peuvent définir des mesures à prendre lors de la détection d'un code malveillant dans le cadre d'une analyse périodique, de la détection de téléchargements malveillants ou de la détection d'éléments malveillants lors de l'ouverture ou de l'exécution de fichiers.