CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SA-08(23)

Valeurs par défaut sécurisées

Juill. 2026

Votre gouvernement

Québec

SA

Acquisition sécurisée des systèmes/services

System and Services

SA-08(23) — Valeurs par défaut sécurisées (PbMM)

Énoncés :

Mettre en place le principe de conception sécurisée des valeurs par défaut sécurisées dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe des valeurs par défaut sécurisées repose sur le fait que la configuration par défaut d'un système (y compris ses sous-systèmes, ses composants et ses mécanismes sous-jacents) constitue une application restrictive et conservatrice de la stratégie de sécurité. Le principe des valeurs par défaut sécurisées s'applique à la configuration initiale (c'est-à-dire par défaut) d'un système, ainsi qu'à l'ingénierie et à la conception de sécurité du contrôle de l'accès et des autres fonctions de sécurité qui suivent une stratégie consistant à tout refuser à l'exclusion de ce qui est explicitement autorisé. L'aspect initial de la configuration de ce principe exige que toute configuration d'usine d'un système, d'un sous-système ou d'un composant de système n'aide pas à contrevenir à la stratégie de sécurité et puisse empêcher le système de s'exécuter dans la configuration par défaut dans les cas où la stratégie de sécurité à propre dit exige que l'utilisatrice ou utilisateur opérationnel procède à la configuration. Les valeurs par défaut restrictives font en sorte que le système s'exécute comme en usine avec l'autoprotection adéquate et soit en mesure d'éviter les atteintes à la sécurité avant que la stratégie de sécurité et la configuration du système aient été établies. Dans les cas où la protection fournie par le produit d'usine est inadéquate, les parties prenantes évaluent le risque posé par l'utilisation du produit en question avant d'établir un état sécurisé initial. Le respect du principe des valeurs par défaut sécurisées permet de garantir qu'un système est dans un état sécurisé au moment de terminer son initialisation. Dans les situations où le système n'arrive pas à terminer l'initialisation, il exécutera une opération demandée au moyen des valeurs par défaut sécurisées ou n'exécutera aucune opération. Il convient de se référer aux principes de protection continue et de défaillance et reprise sécurisées qui sont similaires à ce principe pour fournir la capacité de détecter les défaillances et d'assurer la reprise par la suite. L'approche en matière d'ingénierie de la sécurité relative à ce principe repose sur le fait que les mécanismes de sécurité refusent les requêtes à moins qu'on puisse établir qu'elles ont été formées adéquatement et qu'elles respectent la stratégie de sécurité. L'option sécurisée est d'autoriser une requête dans la mesure où l'on peut établir qu'elle respecte la stratégie. Dans un large système, les conditions à respecter pour accepter une demande qui est refusée par défaut sont souvent plus concises et complètes que celles qu'il faudrait vérifier pour refuser une demande autorisée par défaut.