CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SC-05

Protection contre les dénis de service

Juill. 2026

Votre gouvernement

Québec

SC

Sécurité des communications et des systèmes

System and Communications Protection

SC-05 — Protection contre les dénis de service (--F) (Obligatoire)

Énoncés :

a. [Sélection (un choix) : Protéger contre; Limiter] les effets des types d'attaques par déni de service suivants : [Affectation : types d'attaque par déni de service définis par l'organisation]
b. Employer les contrôles suivants pour atteindre l'objectif de déni de service : [Affectation : contrôles définis par l'organisation par types d'attaque par déni de service]

Paramètres :

a. Protéger contre; robots logiciels dans les formulaires Web exposés à Internet (incluant les pages d'authentification)
b. Dispositif antirobot devant : - Bloquer les tentatives venant de sources réputées malicieuses; - Déterminer si l'utilisateur est un humain ou un robot et s'il faut envoyer un défi ou non; - Éviter les demandes de défis récurrents dans les mêmes conditions (adresse IP, « user agent », comportement...) si l'utilisateur a déjà résolu un premier défi; - Offrir la possibilité de mettre des exceptions pour exclure ce qui est jugé légitime (ex. : faux positifs) par l'OP; - Être intégré à même le formulaire de saisie de données; - Être en fonction avant l'envoi de données; - Le dispositif antirobot visé au premier alinéa doit également être conforme à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ,
c. A-2.1), notamment : - en respectant le critère de nécessité applicable en lien avec la fin recherchée pour laquelle des renseignements personnels ont été recueillis, à savoir la sécurisation des sites Web; - en permettant un consentement éclairé de l'utilisateur en énonçant de manière claire et précise le type de données recueillies ainsi que leur utilisation finale.

Responsable : OP

Date limite de mise en oeuvre : 2026-06-30

Discussion :

Les événements liés à des dénis de service peuvent survenir en raison de plusieurs causes internes et externes, comme une attaque menée par un adversaire ou le manque de planification pour soutenir les besoins organisationnels en matière de capacité et de bande passante. De telles attaques peuvent survenir par l'intermédiaire d'une vaste gamme de protocoles réseau (par exemple, IPv4, IPv6). Il existe une variété de technologies pour limiter ou éliminer l'origine et les effets des événements liés à des dénis de service. Par exemple, les mécanismes de protection des frontières peuvent filtrer certains types de paquets pour empêcher les composants d'un système faisant partie de l'un des réseaux internes d'être directement visés par des attaques par déni de service ou d'en être la source. Combinée à la redondance des services, l'utilisation d'une capacité réseau et d'une bande passante accrues peut également réduire la sensibilité à certaines attaques par déni de service.