CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SC-07(10)

Prévention de l’exfiltration

Juill. 2026

Votre gouvernement

Québec

SC

Sécurité des communications et des systèmes

System and Communications Protection

SC-07(10) — Prévention de l'exfiltration (Pa--)

Énoncés :

a. Prévenir l'exfiltration de l'information
b. Procéder à des tests d'exfiltration [Affectation : fréquence définie par l'organisation]

Paramètres :

b. annuellement ou après tout changement significatif

Responsable : OP

Discussion :

La prévention de l'exfiltration s'applique à l'exfiltration d'information intentionnelle et accidentelle. Les techniques utilisées pour prévenir l'exfiltration d'information des systèmes peuvent être mises en oeuvre aux points d'extrémité internes, aux frontières externes et à travers les interfaces gérées. Elles comprennent également l'adhésion aux formats de protocoles, la surveillance du balisage malveillant en provenance des systèmes, la déconnexion des interfaces réseau externes, sauf lorsqu'elles sont explicitement requises, l'analyse des profils de trafic visant à détecter tout écart par rapport au volume et aux types de trafic attendus au sein des organisations, les procédures de rappel vers les centres de commande et de contrôle, la réalisation de tests d'intrusion, la surveillance de la stéganographie, le désassemblage et le réassemblage d'en-têtes de paquet, et l'utilisation d'outils de prévention de la perte et de la fuite de données. Parmi les dispositifs servant à imposer le respect rigoureux des formats de protocole, on retrouve les pare-feu d'inspection approfondie des paquets et les passerelles d'interface XML (Extensible Markup Language). Les dispositifs vérifient le respect des spécifications et des formats de protocoles au niveau de la couche application et permettent de relever les vulnérabilités indétectables au moyen de dispositifs fonctionnant au niveau des couches réseau ou transport. La prévention de l'exfiltration est similaire à la prévention de la perte ou de la fuite de données et est étroitement liée aux solutions interdomaines et aux mécanismes de protection de systèmes qui appliquent les exigences relatives aux flux d'information.