CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SI-14

Non-persistance

Juill. 2026

Votre gouvernement

Québec

SI

Intégrité des systèmes et des données

System and Information Integrity

SI-14 — Non-persistance (PcEE)

Énoncés :

Mettre en œuvre des [Affectation : composants du système et services désignés par l'organisation] non persistants initialisés dans un état connu et interrompus [Sélection (un choix ou plus) : à la fin de la période d'utilisation; périodiquement {Affectation : fréquence déterminée par l'organisation}].

Responsable : Aucun

Discussion :

La mise en œuvre de composants et de services non persistants atténue les risques liés aux menaces persistantes avancées (MPA) en réduisant considérablement la capacité de ciblage des adversaires (par exemple, les créneaux et la surface d'attaque) qui préparent et lancent des attaques. En appliquant le concept de non-persistance à des composants sélectionnés du système, l'organisation dispose de ressources informatiques fiables dont l'état est connu, et ce, pendant une période précise qui ne laisse pas le temps aux adversaires d'exploiter les vulnérabilités de ses systèmes ou de ses environnements d'exploitation. Puisque les MPA sont des menaces sophistiquées de pointe en ce qui a trait à leurs capacités, à leurs intentions et à l'établissement de cibles, les organisations présument qu'à long terme, certaines attaques seront fructueuses. Les composants et services non persistants du système sont activés au besoin à l'aide d'informations protégées et sont interrompus périodiquement ou à la fin de la session. La non-persistance accroît la somme de travail des adversaires qui tentent de compromettre ou de pénétrer les systèmes organisationnels. Des composants non persistants du système peuvent être mis en œuvre en restaurant des composants de systèmes, en effectuant un redéploiement périodique de l'image ou en utilisant différentes techniques courantes de virtualisation. Les services non persistants peuvent être mis en œuvre au moyen de techniques de virtualisation en tant que machines virtuelles ou comme nouvelles instances de processus dans des machines physiques (persistantes et non persistantes). L'avantage des restaurations périodiques des composantes de systèmes et des services est qu'elles n'exigent pas que les organisations déterminent d'abord si les composants ou les services ont été compromis (ce qui peut parfois être difficile à déterminer). Les composants et services sont changés à une fréquence suffisante pour prévenir le déploiement d'attaques tout en maintenant la stabilité du système. La restauration de composants et services essentiels peut être effectuée périodiquement afin d'empêcher les adversaires d'exploiter les vulnérabilités optimales du système.