CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SA-08(19)

Protection continue

Juill. 2026

Votre gouvernement

Québec

SA

Acquisition sécurisée des systèmes/services

System and Services

SA-08(19) — Protection continue (PbMM)

Énoncés :

Mettre en place le principe de conception sécurisée de la protection continue dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de protection continue repose sur le fait que les composants et les données servant à appliquer la stratégie de sécurité sont soumis à une protection interrompue qui est conforme à la stratégie de sécurité et aux hypothèses de l'architecture de sécurité. On ne peut offrir aucune assurance que le système est en mesure de protéger la protection de la vie privée, l'intégrité et la disponibilité de sa capacité de conception s'il y a des lacunes dans la protection. Toute assurance quant à la capacité de sécuriser une fonctionnalité fournie exige que les données et l'information fassent l'objet d'une protection continue. Cela signifie qu'il n'y a aucune période au cours de laquelle les données et l'information sont laissées sans protection alors qu'elles sont sous le contrôle du système (c'est-à-dire au cours de la création, du stockage, du traitement ou de la communication des données et de l'information, ainsi que lors de l'initialisation, de l'exécution, de la défaillance, de l'interruption et de l'arrêt du système). Une protection continue exige l'adoption des principes du concept de contrôleur de référence selon lequel chaque requête est validée par le contrôleur de référence, faisant en sorte que ce dernier soit en mesure de se protéger contre le trafiquage et qu'il soit possible d'établir une assurance suffisante de l'exactitude et de l'exhaustivité du mécanisme à partir de l'analyse et des tests. De plus, elle exige l'adoption du principe de défaillance et de reprise sécurisées (à savoir la préservation d'un état sécurisé lors d'une erreur, d'un défaut, d'une défaillance et d'une attaque fructueuse; la préservation d'un état sécurisé lors d'une reprise à des modes opérationnels normaux, dégradés ou autres). Une protection continue s'applique également aux systèmes conçus pour s'exécuter dans différentes configurations, y compris celles qui fournissent une capacité opérationnelle totale et les configurations en mode dégradé qui fournissent une capacité opérationnelle partielle. Le principe de protection continue exige que les changements apportés aux stratégies de sécurité du système puissent être retracés jusqu'au besoin opérationnel qui guide la configuration et être vérifiés (c'est-à-dire pouvoir s'assurer que les changements proposés ne poussent pas le système à passer à un état non sécurisé). Une traçabilité et une vérification insuffisantes peuvent mener à des états irréguliers ou à une discontinuité de la protection en raison de la nature complexe et indécidable du problème. L'utilisation de définitions de configuration prévérifiées qui reflètent la nouvelle stratégie de sécurité permet de réaliser l'analyse nécessaire pour déterminer si la transition des anciennes stratégies aux nouvelles est essentiellement atomique et s'il est garanti que les effets résiduels de l'ancienne stratégie n'entreront pas en conflit avec la nouvelle stratégie. La capacité de démontrer une protection continue est fondée sur une articulation claire des besoins de protection du cycle de vie en tant qu'exigences des parties prenantes en matière de sécurité.