CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SA-400

Souveraineté et juridiction

Juill. 2026

Votre gouvernement

Québec

SA

Acquisition sécurisée des systèmes/services

System and Services

SA-400 — Souveraineté et juridiction (PaFF)

Énoncés :

Exiger que les fonctions opérationnelles de l'organisation respectent un processus d'évaluation des menaces et des risques en matière de souveraineté et de juridiction au [Sélection (un choix ou plus) : niveau de l'organisation; niveau de la mission et des activités; niveau du système] qui consiste à :
a. procéder à l'évaluation des préjudices pour déterminer les préjudices potentiels maximaux qui pourraient être causés par une contrainte légale externe imposée aux fonctions organisationnelles ou aux ressources informationnelles en :
    1. considérant les besoins opérationnels en matière de sécurité, y compris les lois ou la réglementation qui exigent que les données ne soient pas divulguées ou compromises
    2. mettant à jour la catégorisation de la sécurité des fonctions organisationnelles ou des ressources informationnelles
    3. documentant les conséquences négatives de la contrainte légale
b. procéder à l'évaluation des menaces propres à la juridiction pour établir la probabilité d'être pris pour cible
c. effectuer une évaluation des vulnérabilités pour déterminer les moyens potentiels que la juridiction externe pourrait utiliser pour exploiter les fonctions organisationnelles ou les ressources informationnelles
d. procéder à l'évaluation des risques propres à la juridiction

Responsable : Aucun

Discussion :

La souveraineté des données concerne le droit du Québec de contrôler l'accès à l'information numérique qui est assujetti à un contrôle prévu par la loi et la divulgation d'une telle information. Par résidence des données, on entend l'emplacement physique ou géographique des données au repos d'une organisation. Par juridiction, on entend le domaine d'autorité qui, dans ce contexte, fait référence à la capacité d'imposer la conformité des entités dans ce domaine comme menace principale. L'hébergement de données dans une juridiction étrangère suscite des préoccupations dans la mesure où ces données pourraient être observées, modifiées ou refusées dans le cadre d'une contrainte légale, alors que ça ne devrait pas être le cas lorsqu'une organisation jouit de la souveraineté de ses données. L'exposition d'une fonction organisationnelle à une compétence juridique différente peut en fait éliminer les barrières juridiques souveraines qui protègent contre la compromission dans la juridiction d'origine. Par exemple, la protection de la vie privée des citoyennes et citoyens n'est souvent pas accordée aux non-citoyennes et non-citoyens, et les fournisseurs de services peuvent être légalement tenus de fournir l'accès à des données ou à des services qui seraient protégés par la loi dans la juridiction d'origine. Dans le cas des fonctions organisationnelles, on peut donner en exemple la technologie opérationnelle qui contrôle les infrastructures essentielles hébergées dans un nuage qui est modifié ou mis hors service par une juridiction étrangère hostile. Les techniques employées peuvent être très sophistiquées et seront généralement exécutées avec tous les privilèges d'administrateur des initiées et initiés. La contrainte légale imposée par des juridictions dotées de moyens sophistiqués est extrêmement efficace pour ce qui est de contourner les autres contrôles. Plusieurs juridictions peuvent s'appliquer, par exemple une administration municipale, une ville, un comté, une réserve, un district, une région, une province, un État, un canton, un territoire ou une nation. Tous les niveaux doivent être identifiés pour évaluer les capacités d'imposer des contraintes. D'autres juridictions peuvent forcer la compromission des fonctions opérationnelles en matière de confidentialité, d'intégrité ou de disponibilité. Une évaluation des préjudices doit documenter les conséquences négatives de la contrainte légale, notamment tout besoin opérationnel en matière de sécurité (par exemple, les lois ou la réglementation qui exigent que les données ne soient pas compromises). Une organisation pourrait ne pas être en mesure d'adopter une approche à la gestion des risques (notamment en raison d'un mandat prescrit par la loi ou de la souveraineté des données nationales) et devoir éviter d'emblée tout scénario de risque.