CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

AC-23

Protection contre l'exploration de données

Juill. 2026

Votre gouvernement

Québec

AC

Gestion des droits d'accès aux systèmes et données

Access Control

AC-23 — Protection contre l'exploration de données (Pb--)

Énoncés :

Employer des [Affectation : techniques de détection et de prévention de l'exploration de données définies par l'organisation] pour les [Affectation : objets de stockage de données définis par l'organisation] pour détecter l'exploration de données et protéger les systèmes contre celle-ci.

Responsable : Aucun

Discussion :

L'exploration de données est un processus analytique qui tente de trouver des corrélations ou des tendances dans de grands ensembles de données aux fins de découverte de données ou de connaissances, et à l'occasion qui fait correspondre l'information concernant une personne entre les jeux de données (correspondance de données). Les objets de stockage de données comprennent les enregistrements de base de données et les champs de base de données. L'information sensible peut être extraite des opérations d'exploration de données. Lorsque l'information consiste en des renseignements personnels, elle peut conduire à des révélations inattendues sur les personnes et engendrer des risques d'atteinte à la vie privée. Avant toute activité d'exploration de données, ces risques doivent être identifiés, gérés et, le cas échéant, atténués. Avant de mener les activités d'exploration de données, les organisations déterminent si de telles activités sont autorisées par la loi. Les techniques de détection et de prévention d'exploration de données incluent de limiter le nombre et la fréquence des requêtes de base de données afin d'augmenter le facteur de travail requis pour déterminer le contenu de telles bases de données, de limiter les types de réponses fournis aux requêtes de base de données, d'appliquer des techniques de protection de la vie privée différentielle ou de chiffrement homomorphique, et d'aviser le personnel lorsque des requêtes de base de données ou des accès irréguliers ont lieu. Aviser le personnel approprié lorsque des requêtes de base de données ou des accès irréguliers ont lieu est essentiel, car ils sont susceptibles de constituer une atteinte à la vie privée ou une violation de la sécurité. La protection contre l'exploration de données met l'accent sur la protection de l'information de l'organisation lorsque l'information est conservée dans des magasins de données. À l'inverse, le contrôle AU-13 porte sur la surveillance de diffusions inappropriées de l'information organisationnelle qui pourrait avoir été explorée ou obtenue de magasins de données et qui est maintenant offerte comme de l'information de sources ouvertes.