CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

IA-02(01)

AMF robustes pour les comptes privilégiés

Juill. 2026

Votre gouvernement

Québec

IA

Contrôle de l’identité et de l’authentification

Identification and Authentication

IA-02(01) — AMF robustes pour les comptes privilégiés (PaF-) (Obligatoire)

Énoncés :

Appliquer des AMF robustes pour l'accès à des comptes privilégiés.

Paramètres :

aaQC. tout système exposé sur Internet

Responsable : OP

Date limite de mise en oeuvre : 2021-06-30

Discussion :

L'authentification multifactorielle (AMF) exige l'utilisation de deux facteurs différents ou plus aux fins d'authentification. Les facteurs d'authentification sont définis comme suit : une information connue (par exemple, un numéro d'identification personnel [NIP]), une possession (par exemple, un authentifiant physique comme une clé cryptographique privée) ou un attribut personnel (par exemple, une authentification biométrique). Les solutions d'AMF qui présentent des authentifiants physiques comprennent les authentifiants matériels qui fournissent des sorties à durée limitée ou de type défi-réponse ainsi que des cartes à puce. En plus de permettre l'authentification des utilisatrices et utilisateurs au niveau du système (c'est-à-dire, au moment de l'ouverture de session), les organisations peuvent utiliser des mécanismes d'authentification au niveau de l'application, à leur discrétion, pour accroître la sécurité. Quel que soit le type d'accès (c'est-à-dire, local, réseau, à distance), les comptes privilégiés sont authentifiés au moyen d'options d'authentification multifacteur adéquates pour le niveau de risque. Les organisations peuvent ajouter des mesures de sécurité, comme des mécanismes d'authentification supplémentaires et plus rigoureux pour des types d'accès spécifiques.