CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

IA-05(01)

Authentification basée sur mot de passe

Juill. 2026

Votre gouvernement

Québec

IA

Contrôle de l’identité et de l’authentification

Identification and Authentication

IA-05(01) — Authentification basée sur mot de passe (PaF-)

Énoncés :

Pour l'authentification basée sur mot de passe :
a. créer une liste des mots de passe couramment utilisés, attendus ou compromis et la mettre à jour tous les [Affectation : fréquence définie par l'organisation] et lorsque l'on soupçonne que les mots de passe de l'organisation ont été compromis, directement ou indirectement
b. lorsque les utilisatrices et utilisateurs créent ou mettent à jour des mots de passe, vérifier que les mots de passe ne figurent pas sur la liste des mots de passe couramment utilisés, attendus ou compromis figurant au contrôle IA-05(01)a
c. transmettre les mots de passe uniquement par des canaux protégés par chiffrement
d. stocker les mots de passe au moyen de la fonction de dérivation de clé avec sel, de préférence avec hachage de clé
e. exiger la sélection immédiate d'un mot de passe dès la récupération du compte
f. autoriser les utilisatrices et utilisateurs à choisir de longs mots de passe et phrases de passe, y compris les espaces et les caractères imprimables
g. utiliser des outils automatisés pour aider l'utilisatrice ou utilisateur à sélectionner des authentifiants de mots de passe robustes
h. appliquer les règles de composition et de complexité suivantes : [Affectation : règles de composition et de complexité définies par l'organisation]

Paramètres :

a. en continu
h. : - sensible à la casse, 12 caractères minimum, 1 majuscule, 1 minuscule, 1 nombre et 1 caractère spécial - interdire la réutilisation des mots de passe pendant 24 générations

Responsable : OP

Discussion :

L'authentification basée sur mot de passe s'applique aux mots de passe, peu importe qu'ils soient utilisés pour l'authentification à un seul facteur ou multifacteur. Les longs mots de passe ou les phrases de passe sont préférables à des mots de passe courts. L'application de règles de composition offre certains avantages pour la sécurité, mais réduit l'utilisabilité. Les organisations peuvent choisir d'établir certaines règles pour la génération de mots de passe (par exemple, le nombre minimal de caractères pour les longs mots de passe) dans certaines circonstances et d'appliquer cette exigence au contrôle IA-05(01)(h). Par exemple, un mot de passe oublié peut mener à une récupération de compte. Des mots de passe protégés par chiffrement comprennent le hachage cryptographique unidirectionnel salé des mots de passe. La liste des mots de passe couramment utilisés, compromis ou attendus comprend les mots de passe provenant des corpus de violations précédentes, les mots du dictionnaire et les caractères répétitifs ou séquentiels. Cette liste comprend des mots s'appliquant au contexte, comme le nom du service, le nom de l'utilisateur et des dérivations de ces éléments. Les questions liées à la récupération demandent souvent aux utilisatrices et utilisateurs de fournir des renseignements personnels. Afin de considérer le concept de la nécessité du point de vue de la protection de la vie privée par rapport à sa proportionnalité, les organisations doivent collecter juste assez de renseignements personnels pour garantir une authentification précise. Le recours à des jetons de connaissance n'est pas recommandé pour la récupération d'un compte.