CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

AC-07

Tentatives d’ouverture de session infructueuses

Juill. 2026

Votre gouvernement

Québec

AC

Gestion des droits d'accès aux systèmes et données

Access Control

AC-07 — Tentatives d'ouverture de session infructueuses (PaF-) (Obligatoire)

Énoncés :

a. Appliquer une limite de [Affectation : nombre défini par l'organisation] tentatives d'ouverture de session non valides consécutives par l'utilisatrice ou utilisateur sur une période de [Affectation : délais définis par l'organisation];
b. [Sélection (un choix ou plus) : Verrouiller le compte ou le noeud pendant {Affectation : délais définis par l'organisation}; verrouiller le compte ou le noeud jusqu'à ce qu'une administratrice ou un administrateur le libère; retarder la prochaine invite d'ouverture de session selon {Affectation : algorithme de temporisation défini par l'organisation}; aviser l'administratrice ou administrateur de système; effectuer une autre {Affectation : opération définie par l'organisation}] automatiquement lorsque le nombre maximal de tentatives infructueuses est dépassé.

Paramètres :

Spécifique aux appareils mobiles :
a. maximum 5; à définir par l'organisme
b. verrouiller l'accès à l'application

Responsable : OP

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

Discussion :

La nécessité d'une limite de tentatives d'ouverture de session infructueuses et les mesures à prendre lorsque le nombre maximal est atteint s'appliquent peu importe si la connexion a été établie localement ou par l'intermédiaire d'un réseau. En raison des risques de déni de service, les verrouillages automatiques effectués par les systèmes sont habituellement temporaires et annulés automatiquement après un délai prédéterminé établi par l'organisation. Dans le cas où elle a choisi un algorithme de temporisation, l'organisation peut utiliser différents algorithmes pour différents composants du système, selon les capacités de ces composants. Les réponses aux tentatives d'ouverture de session infructueuses peuvent être mises en oeuvre tant au niveau du système d'exploitation qu'au niveau des applications. Les opérations définies par l'organisation qui peuvent être effectuées lorsque le nombre autorisé de tentatives d'ouverture de session infructueuses est atteint comprennent notamment l'affichage d'un message invitant l'utilisatrice ou utilisateur à répondre à une question secrète en plus d'entrer son nom d'utilisateur et son mot de passe, l'utilisation d'un mode de confinement avec des capacités limitées pour les utilisatrices et utilisateurs (plutôt qu'un verrouillage complet), permettre aux utilisatrices et utilisateurs de se connecter uniquement à partir de certaines adresses de protocole Internet (IP pour Internet Protocol) précises, l'utilisation d'un test captcha pour éviter les attaques automatisées ou l'application de profils d'utilisateur qui font intervenir d'autres paramètres, comme l'emplacement, le moment de la journée, l'adresse IP, l'appareil ou l'adresse de contrôle d'accès au support (MAC pour Media Access Control). Si le verrouillage automatique du système ou l'exécution d'un algorithme de temporisation n'est pas mis en oeuvre pour soutenir l'objectif en matière de disponibilité, l'organisation considère une combinaison de mesures alternatives pour aider à prévenir les attaques par force brute. En plus de ce qui précède, l'organisation peut inviter les utilisatrices ou utilisateurs à répondre à une question secrète avant que le nombre maximal de tentatives d'ouverture de session infructueuses soit atteint. Il n'est généralement pas permis de déverrouiller automatiquement un compte après une période donnée. Des exceptions peuvent toutefois être nécessaires selon la mission ou les besoins opérationnels.