CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

AC-04

Application du contrôle de flux d'information

Juill. 2026

Votre gouvernement

Québec

AC

Gestion des droits d'accès aux systèmes et données

Access Control

AC-04 — Application du contrôle de flux d'information (PaF-)

Énoncés :

Appliquer des autorisations approuvées pour contrôler le flux d'information dans le système et entre les systèmes reconnectés en fonction des [Affectation : stratégies de contrôle de flux d'information définies par l'organisation].

Paramètres :

à définir par l'organisme

Responsable : Partagée

Discussion :

Le contrôle de flux d'information régit le cheminement de l'information au sein d'un système et entre des systèmes (par opposition aux personnes autorisées à y accéder), quels que soient les accès subséquents à cette information. Les restrictions relatives au contrôle du flux d'information consistent notamment à bloquer le trafic externe qui prétend provenir de l'intérieur de l'organisation, éviter que l'information contrôlée pour exportation ne soit transmise en clair sur Internet, limiter les requêtes Web qui ne sont pas acheminées par l'intermédiaire du serveur mandataire Web interne et limiter les transferts d'information entre les organisations selon les structures et le contenu des données. Le transfert d'information entre des organisations peut nécessiter une entente indiquant comment le flux d'information sera appliqué (voir le contrôle CA-03). Le transfert d'information entre des systèmes associés à des domaines de sécurité ou de protection de la vie privée différents et faisant l'objet de stratégies de sécurité ou de protection de la vie privée différentes présente un risque qu'un tel transfert contrevienne à une ou à plusieurs stratégies de sécurité ou de protection de la vie privée des domaines. Dans de telles situations, les gardiennes et gardiens de l'information fournissent des directives aux points désignés d'application des stratégies entre les systèmes interconnectés. Les organisations considèrent le recours à des solutions architecturales particulières pour appliquer des stratégies de sécurité et de protection de la vie privée en particulier. L'application des contrôles comprend l'interdiction des transferts d'information entre les systèmes connectés (c'est-à-dire autoriser l'accès seulement), la vérification des autorisations en écriture avant d'accepter l'information provenant d'un autre domaine de sécurité ou de protection de la vie privée ou d'un système connecté, le recours à des mécanismes matériels pour appliquer des flux d'information dans une seule direction et la mise en place de mécanismes remaniés de confiance pour réassigner les attributs et les étiquettes de sécurité et de protection de la vie privée. Les responsables des fonds de renseignements personnels devraient s'assurer que la quantité minimale de renseignements personnels requis est échangée d'un système à l'autre et, dans la mesure du possible, veiller à ce que l'échange des renseignements personnels soit documenté dans un accord. Les organisations utilisent couramment les mécanismes d'application et les stratégies de contrôle de flux d'information pour contrôler le flux d'information entre des sources et des destinations précises à l'intérieur des systèmes et entre les systèmes interconnectés. Le contrôle de flux est fondé sur les caractéristiques de l'information et/ou sur son chemin. Il est appliqué, par exemple, aux dispositifs de protection des frontières qui font appel à des ensembles de règles ou qui mettent en place des paramètres de configuration qui restreignent les services de systèmes et permettent de filtrer les paquets de données en fonction de l'information comprise dans les en-têtes ou de filtrer les messages en fonction du contenu du message. Les organisations doivent également considérer la robustesse des mécanismes de filtrage et d'inspection (c'est-à-dire les composants matériels, micrologiciels et logiciels) qui sont essentiels à l'application du contrôle de flux d'information. Les améliorations 3 à 32 portent principalement sur les besoins en matière de solutions interdomaines, qui sont axés sur des techniques de filtrage avancées, une analyse approfondie et des mécanismes robustes d'application du contrôle de flux d'information mis en oeuvre dans les produits interdomaines, comme les mécanismes de protection à assurance élevée. De telles capacités ne sont généralement pas offertes dans des produits commerciaux sur étagère (COTS pour Commercial Off-The-Shelf). L'application du contrôle de flux d'information vise également le trafic du plan de contrôle (par exemple, le routage et le système de noms de domaine (DNS pour Domain Name System)).