Communications Security Establishment | Centre de la sécurité des télécommunications

Guide d'initiation à la sécurité interdomaines

Bulletin de sécurité des TI à l'intention du gouvernement du Canada

ITSB-120 **Janvier 2016**

1 Introduction

Dans le cadre de leurs activités opérationnelles, les employés du gouvernement du Canada (GC) doivent constamment accéder à des réseaux ayant des niveaux de classification de sécurité différents afin d'y consulter et d'y transférer de l'information. L'accès aux données se trouvant sur des réseaux ou le déplacement de données d'un réseau à l'autre favorise la réalisation des activités opérationnelles, l'échange d'information et la prise de décisions.

Toutefois, tout déplacement d'information entre les réseaux est susceptible de les exposer à de nouvelles menaces et de compromettre la sécurité des fonds de renseignement. Quoique plusieurs méthodes puissent servir à déplacer l'information d'un réseau à l'autre (qu'on appelle aussi domaines de sécurité), seules les solutions interdomaines (SID) approuvées par le Centre de la sécurité des télécommunications (CST) devraient être utilisées pour transférer l'information dont le niveau de sécurité est supérieur à PROTÉGÉ B.

2 Objet

Le présent bulletin expose les deux types de SID les plus courants et les considérations connexes en matière de sécurité. Il est destiné aux cadres, aux gestionnaires opérationnels et aux intervenants en TI qui participent collectivement à l'évaluation des exigences liées à l'échange d'information au sein de leurs ministères respectifs.

3 Que sont les SID?

Les SID sont des solutions de technologies de l'information (TI) qui permettent d'avoir accès à de l'information qui se trouve dans deux domaines de sécurité ou plus, ou de transférer de l'information entre au moins deux domaines de sécurité. Les fonctionnalités, les composants et les processus varient d'une solution à l'autre. Toutefois, chaque solution applique des contrôles de sécurité pour réduire les risques au minimum tout en offrant des avantages, comme les suivants :

- ✓ des mécanismes de contrôle d'accès;
- ✓ la protection du réseau contre les intrusions;
- ✓ l'application du contrôle de flux de données.

Un système pleinement déployé doit être accompagné d'une formation des utilisateurs, de politiques et de processus élaborés au sein du ministère. Il existe deux principaux types de SID : les **solutions d'accès interdomaine** et les **solutions de transfert interdomaine**.

3.1 Solutions d'accès interdomaine

Les solutions d'accès interdomaine permettent aux utilisateurs de consulter l'information hébergée dans divers domaines de sécurité dont les politiques de sécurité sont différentes, et ce, à partir d'un seul poste de travail auquel on a appliqué des mesures appropriées de sécurité physique et de sécurité des TI. Cependant, ces solutions ne permettent pas le transfert d'information entre les domaines de sécurité (il est donc impossible de copier-coller de l'information d'une fenêtre à l'autre).

Les solutions d'accès interdomaine n'empêcheront pas la prolifération de nombreux réseaux isolés au sein du GC, mais elles favoriseront la consolidation des systèmes de bureau et amélioreront l'expérience de l'utilisateur. En consolidant les systèmes de bureau, on parvient habituellement à réduire les coûts d'achat et de soutien (soit le coût total de possession), l'espace nécessaire, ainsi que la consommation d'électricité.

3.2 Solutions de transfert interdomaine

Les solutions de transfert interdomaine permettent aux utilisateurs de transférer de l'information entre différents domaines de sécurité de manière sécurisée. Ces solutions se divisent en trois catégories :

- **Transfert supérieur-inférieur :** Les utilisateurs transfèrent des données d'un domaine ayant une classification de sécurité supérieure (domaine supérieur) à un domaine ayant une classification inférieure (domaine inférieur) au moyen d'une solution interdomaine. Par exemple, afin de répondre aux demandes d'accès à l'information et de communication des renseignements personnels, il faut parfois démarquer de l'information classifiée, sensible ou personnelle avant de la transférer sur un système non classifié.
- **Transfert inférieur-supérieur :** Les utilisateurs transfèrent des données d'un domaine inférieur à un domaine supérieur au moyen d'une solution interdomaine. Il pourrait s'agir, par exemple, du transfert d'un rapport météorologique d'un système non classifié à un tableau de bord opérationnel qui se trouve sur un système classifié.
- **Transfert manuel de données :** Les utilisateurs transfèrent des données manuellement au moyen d'un support amovible, comme une clé USB, un CD-R ou un DVD. Il pourrait s'agir, par exemple, du transfert d'un correctif logiciel ou d'une mise à jour antivirus d'un support amovible à un domaine de sécurité isolé.

4 Considérations liées à la sécurité

Il existe des menaces inhérentes au transfert d'information entre des domaines de sécurité appliquant des politiques de sécurité différentes ou à l'affichage de nombreux domaines de sécurité sur un seul poste de travail. Certaines de ces menaces sont expliquées brièvement ci-dessous.

- **Fuites de données :** La fuite de données est la principale menace qui pèse sur une solution de transfert interdomaine supérieur-inférieur. Elle survient lorsque l'information classifiée est involontairement transférée d'un domaine de sécurité classifié à un niveau supérieur à un domaine de sécurité classifié à un niveau inférieur.
- **Code malveillant :** La principale menace envers une solution de transfert interdomaine inférieur-supérieur est la prolifération de codes malveillants ou d'autres logiciels non autorisés dans l'ensemble des domaines de sécurité.

- **Comportements inadéquats des utilisateurs :** Certains utilisateurs peuvent choisir de contourner les procédures de transfert adéquates et transférer l'information manuellement à l'aide d'un support amovible ou tenter d'utiliser d'autres méthodes inappropriées ou interdites pour transférer des données.

Les personnes autorisées des ministères du GC doivent bien comprendre que même si les SID amélioreront la sécurité, il y aura toujours un certain risque résiduel qu'il faut évaluer avant d'accorder une dispense de sécurité ou une autorisation d'exploiter, surtout lorsque le transfert d'information est considéré comme un impératif opérationnel qui l'emporte sur les risques liés à la sécurité.

5 Tenir compte des exigences

Lorsque vous planifiez, choisissez ou mettez en œuvre une SID, il importe :

- ✓ d'évaluer vos exigences opérationnelles et de déterminer vos besoins opérationnels;
- ✓ de comprendre le contexte de menaces et de risques (évaluation des menaces et des risques);
- ✓ d'élaborer de solides politiques, procédures et mesures de protection en matière de sécurité et de gestion de l'information (p. ex. marquage des données);
- ✓ de déterminer et de comprendre les pratiques exemplaires actuelles en matière de sécurité des TI en fonction des exigences opérationnelles, et de sélectionner les contrôles de sécurité appropriés.

Pour mettre en œuvre une solution qui réduira le risque (à un niveau acceptable) associé au transfert de données entre différents domaines de sécurité, il faut tenir compte de la conception et des exigences de sécurité de l'architecture d'entreprise du ministère.

6 Supports amovibles

Certains ministères pourraient trouver que la mise en œuvre d'une SID n'est pas une décision opérationnelle viable et que l'utilisation de supports amovibles pour transférer l'information répondrait mieux à leurs besoins opérationnels. Il est primordial de mettre en œuvre une solide politique sur les supports amovibles qui expose les nombreuses étapes à suivre pour atténuer les menaces, conformément à l'ITSB-112, *Questions de sécurité relatives à l'utilisation de supports amovibles pour les renseignements Protégé C et classifiés*.

7 Aide et renseignements

Le CST recommande de suivre le cadre de gestion des risques de sécurité de l'ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*. De plus, si les représentants de votre ministère ont déterminé qu'une SID répondrait à leurs besoins opérationnels et qu'ils souhaitent en savoir plus sur ces solutions, veuillez communiquer avec les Services à la clientèle de la STI du CST.

Services à la clientèle de la STI
Téléphone : 613-991-7654
Courriel : itsclientservices@cse-cst.gc.ca