Communications Security Establishment | Centre de la sécurité des télécommunications

Questions de sécurité relatives à l'utilisation de supports amovibles pour les renseignements Protégé C et classifiés

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

ITSB-112 **Août 2014**

1 Objet

Les ministères du gouvernement du Canada (GC) ont recours à des systèmes d'information pour soutenir leurs activités opérationnelles. Plusieurs ministères et organismes utilisent des supports amovibles pour faciliter le stockage ou l'échange de renseignements entre les ordinateurs ou les réseaux. Cependant, les supports amovibles représentent une menace aux actifs d'information du GC en raison de leur petite taille, de leur portabilité, de leur capacité de stockage et de leur capacité à exécuter des applications propres à un dispositif. Les ministères et les organismes doivent s'assurer que leurs supports amovibles offrent des mesures de protection adéquates afin de bloquer les tentatives d'accès non autorisées aux renseignements du GC.

Ce bulletin complète l'Avis de mise en œuvre de la Politique sur la technologie de l'information 2014-01 (AMPTI : 2014-01) du Secrétariat du Conseil du Trésor du Canada. L'avis, publié en mai 2014, décrit les risques liés au stockage temporaire de renseignements du GC sur des supports amovibles, ainsi que les moyens d'atténuer ces risques. Le présent bulletin est destiné à la haute direction, aux gestionnaires des risques liés à la sécurité des TI et aux professionnels de la sécurité des systèmes informatiques.

2 Répercussions

Les supports amovibles sont habituellement utilisés pour stocker temporairement des renseignements ou transférer des données par voie électronique d'un système à l'autre. Le transfert de données permet la collaboration entre les employés et les organismes, mais l'utilisation inappropriée des supports amovibles représente un risque important à la confidentialité des ressources d'information des ministères. Une gestion inappropriée de ces dispositifs augmente la probabilité que des renseignements du GC soient exposés à des risques inacceptables (p. ex., un dispositif pourrait être perdu, volé ou utilisé pour introduire un code malveillant).

3 Stratégies d'atténuation

Appliquées conjointement, les mesures de protection suivantes définissent les recommandations de l'ITPIN 2014-01 relatives aux dispositifs de stockage contenant des renseignements Protégé C et classifiés :

- Le dispositif doit être encodé à l'aide d'un module approuvé par le Programme de validation des modules cryptographiques (PVMC) **exploité selon les normes du Federal Information Processing Standards (FIPS)**.
- Le dispositif doit être manipulé avec les mêmes précautions que celles requises par la cote de sécurité la plus élevée détenue à quelque moment que ce soit par les renseignements contenus sur le dispositif **avant leur encodage**. Le dispositif doit également être manipulé avec les mêmes précautions que celles requises par la classification de sécurité la plus élevée du réseau **auquel il sera connecté à quelque moment que ce soit**.

4 Mise en application

Certains aspects des solutions de ce domaine seront laissés à la discrétion des ministères en tant que décisions relatives à la gestion des risques. Cependant, les spécifications relatives à l'encodage ou à d'autres mesures de sécurité pour la manipulation électronique de renseignements Protégé C et classifiés sont la responsabilité du CST, conformément à la section 16.4.4 de la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information du SCT (GSTI).

4.1 Sécurité cryptographique

Les dispositifs doivent être encodés à l'aide d'un module approuvé par le PVMC, exploité en mode FIPS seulement. Les modules d'encodage qui ne fonctionnent pas en mode FIPS n'ont pas été approuvés. L'encodage de tout renseignement du GC sur un support amovible à l'aide de modules PVMC ne fonctionnant pas en mode FIPS n'est pas recommandé par le CST. En plus des solutions validées au titre du PVMC, il existe des produits d'assurance élevée qui conviennent à la manipulation de renseignements Protégé C et classifiés. L'utilisation de ces produits diminue le nombre de mesures de protection nécessaires au stockage et à la manipulation des renseignements. Pour obtenir plus d'information sur les produits à assurance élevée, communiquez avec comsecclientservices@cse-cst.gc.ca.

4.2 Sécurité physique

Les ministères doivent s'assurer d'avoir des politiques et des procédures adéquates de manutention physique en place pour protéger les renseignements Protégé C et classifiés. Pour de plus amples détails sur le marquage, l'entreposage et le transport des supports amovibles, veuillez consulter le Guide d'équipement de sécurité (G1-1001) et le guide Transport et transmission de renseignements protégés ou classifiés (G1-009) de la Gendarmerie royale du Canada.

4.3 Considérations interdomaines

Les ministères et organismes du GC qui doivent transférer des données électroniquement d'un domaine de sécurité à un autre doivent toujours utiliser une solution interdomaine (SID) approuvée. Cependant, si une SID n'est pas disponible, il pourrait être nécessaire d'effectuer le transfert de données au moyen d'un support amovible. Selon les niveaux de classification des réseaux impliqués et la direction du transfert, plusieurs contrôles de sécurité spécifiques pourraient être envisagés et mis en place dans le cadre d'une politique ministérielle des TI

régissant le transfert manuel des données. Le choix des mesures de sécurité est particulièrement important quand vient le temps de transférer des données hors des réseaux classifiés. Ces mesures permettent d'éviter les fuites d'information ou l'introduction de données comportant des maliciels ou des virus qui pourraient compromettre les environnements classifiés.

Le CST est en mesure d'aider les ministères à mettre en place une politique rigoureuse en matière de SID. Pour en savoir plus, veuillez envoyer un courriel à itsclientservices@cse-cst.gc.ca.

5 Conclusion

Il est impératif que les ministères du GC mettent des mesures de sécurité en place afin d'assurer la protection, la disponibilité et l'intégrité de leurs renseignements et de leurs actifs liés aux TI. Les supports amovibles commerciaux sont conformes aux recommandations du CST s'ils sont validés au titre du PVMC et fonctionnent en mode FIPS. Avant que des données ne soient versées dans les dispositifs, il est impératif ces derniers soient manipulés conformément aux mesures de sécurité physique mises en place pour protéger les renseignements qui y sont ou y seront stockés. Pour de plus amples renseignements sur ce bulletin, le Programme de validation des modules cryptographiques ou d'autres produits certifiés, communiquez avec itsclientservices@cse-cst.gc.ca.

6 Aide et renseignements

Numéro de téléphone du service à la clientèle de la STI : 613-991-7654
Courriel : itsclientservices@cse-cst.gc.ca