Sommaire de l’évaluation 2016-2017 de la Stratégie de Cybersécurité du Canada (SCSC)

Contexte

- **Lancement:** 3 octobre 2010.
- **Objectifs:** Sécuriser les systèmes du gouvernement du Canada (GC), établir des partenariats pour protéger les cybersystèmes essentiels à l’extérieur du GC et aider les canadiens à se protéger en ligne.
- **Organisations participantes:** Sécurité Publique Canada, Centre de la sécurité des télécommunications du Canada, Services partagés Canada, Défense nationale, Secrétariat du conseil du trésor, Service canadien du renseignement de sécurité, Affaires mondiales Canada, Justice Canada, Gendarmerie royale du Canada.
- **Financement total pour 5 ans :** Plus de 198M$ sur 5 ans et 60M$/an (de façon continue)
- **Portée de l'évaluation** : 2010-2011 et 2015-2016.

Qu’avons-nous examiné

- L’efficacité de la structure de gouvernance à assurer la surveillance de la stratégie.
- La mise en œuvre des activités proposées par les ministères et agences partenaires.
- Dans quelle mesure les principaux objectifs de la stratégie ont été réalisés.

Qu’avons-nous constaté

Gouvernance

- Les comités de surveillance ont facilité la collaboration, coordination et le partage d’information entre les organisations participantes.
- Cependant, l’absence de comptes rendus réguliers des réunions, autre documents, n’a pas permis d’évaluer dans quelle mesure les comités de surveillance ont pu assumer ces responsabilités.
- Bien que les rôles et les responsabilités des différents acteurs aient été clarifiés et que le partage de l’information et le niveau de collaboration se soient améliorés, il reste encore des problèmes persistants à résoudre.

Mise en œuvre

- La plupart des activités financées par la Stratégie ont été mises en œuvre comme prévu, à l’exception de quatre activités.
- Trois organisations ont signalé ne pas avoir dépensé tous les fonds accordés, deux organisations ont dépensé plus, deux ont dépensé le montant exact et une organisation n’a pas été en mesure de faire le suivi des dépenses pertinentes; trois organisations ont éprouvé de la difficulté à pouvoir certains postes hautement techniques, surtout aux niveaux secret et très secret.

Performance

- Le GC a accru sa capacité à prévenir, détecter, réagir et à se rétablir des cyberattaques.
- Le nombre d’atteintes à la protection des données a chuté durant la mise en œuvre de la Stratégie.
- Le gouvernement peut dorénavant analyser et contenir plus rapidement qu’auparavant, les atteintes à la protection des données.
- Ces améliorations ont été réalisées en dépit d’une hausse des cyberactivités étatiques et non étatiques contre les réseaux du GC.
- Des partenariats plus étroits ont été établis avec les propriétaires et les exploitants d’infrastructures critiques et d’autres intervenants du secteur privé.
- Malgré les activités de sensibilisation conduites, il demeure difficile de cerner dans quelle mesure les Canadiens sont protégés en ligne.

Recommandations

En collaboration avec les organismes participants, la sous-ministre adjointe principale du Secteur de la sécurité et de la cybersécurité nationale de Sécurité publique Canada devrait envisager de prendre les mesures suivantes :

1. Renforcer la structure de gouvernance horizontale de la Stratégie de cybersécurité du Canada en procédant aux tâches suivantes :
    a) réévaluer la structure de gouvernance pour déterminer la nécessité et la demande en ce qui a trait à la configuration actuelle des comités et pour améliorer la participation;
    b) améliorer le soutien du secrétariat, notamment la coordination, la gestion de l’information et d’autres services administratifs;
    c) s’assurer que les comités de surveillance ont des mandats qui définissent clairement les rôles et les responsabilités des membres et les attentes envers ceux-ci;
    d) s’assurer que les comités de surveillance s’acquittent des rôles et des responsabilités définis dans leur mandat; et
    e) rédiger des comptes rendus de décision de façon systématique.
2. Renforcer les pratiques d’échange de renseignements liés à la cybersécurité en élaborant des politiques et des procédures claires et concevoir des outils qui permettront un échange de renseignements systématique et opportun avec les partenaires et les intervenants.
3. Renforcer les pratiques de mesure du rendement et de collecte de données en procédant aux tâches suivantes :
    a) recueillir des renseignements pertinents, fiables et axés sur les résultats, y compris des renseignements sur les dépenses de programme, de façon régulière et méthodique; et
    b) fournir les renseignements recueillis sur le rendement et les dépenses aux comités de surveillance pertinents de façon régulière pour favoriser un suivi efficace et la reddition de comptes.