Cybermenaces et menaces liées à l'approvisionnement visant le GC

Services partagés Canada - Calculateur haute performance

16 oct 2013

Carey Frey, Directeur du Bureau des relations stratégiques de la sécurité des TI
Centre de la sécurité des télécommunications Canada

Canada

Activités du CSTC

- Le CSTC est l'organisme national de cryptologie du Canada
- Son mandat
  - Renseignement électromagnétique à l'appui des politiques étrangères
  - Sécurité des TI
  - Soutien à l'accès légal
- Mandat « B »
  - Fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada.

Programme de sécurité des TI du CSTC

- Nous aidons à prévenir, à détecter et à contrer les menaces et les vulnérabilités relatives à la sécurité des TI.
- Le CSTC utilise son expertise et ses capacités techniques uniques, ainsi que ses renseignements classifiés, pour compléter les technologies de sécurité commerciales qui sont à la portée des praticiens de la sécurité des TI.
- Il utilise ses propres méthodes et opérations pour détecter et contrer les menaces qui ne relèvent pas du domaine public.

Effets des forces du marché sur les technologies

- Les forces du marché favorisent les technologies commerciales et personnelles plutôt que le respect des exigences relatives aux caractéristiques de sécurité.
- Notre société est presque entièrement dépendante des fournisseurs de logiciels et de matériel commerciaux du marché mondial.
- De nouveaux produits ou de nouvelles versions de produits sont rapidement mis au point.
- Aucun cadre réglementaire n'est en place relativement à la sécurité des logiciels et du matériel.
- Les processus et politiques traditionnelles du gouvernement imposent des exigences en matière de sécurité une fois que les produits et systèmes sont développés.
- Les développeurs de technologies commerciales sont peu motivés à investir dans la sécurité.

Vulnérabilités des technologies

- « Les gens développent des logiciels négligemment. Personne ne vérifie s'il y a des erreurs avant de les vendre. »
  - (traduction libre) Peiter Zatko (Mudge), sommet sur la cybersécurité de la Maison-Blanche (2000)

- Faiblesses ou vulnérabilité accidentelles
  - Défaillances au niveau de la conception
  - Erreurs de mise en œuvre

- **Cybermenace –** Un auteur de menace utilise Internet pour tirer profit d'une vulnérabilité connue d'un produit afin d'exploiter un réseau et l'information qui y circule.

- Faiblesses ou vulnérabilités intentionnelles
  - Implantation dans un produit de biens livrables prédéterminés, à la connaissance ou à l'insu de l'entreprise.

- **Menace liée à la chaîne d'approvisionnement –** Il est facile de saboter un produit dans la chaîne d'approvisionnement pour faciliter une cyberattaque subséquente qui permettra d'exploiter un réseau et l'information qui y circule.

Évolution de la cybermenace

- Aujourd'hui, des cyberactivités malveillantes ciblent le Canada et ses plus proches alliés chaque jour.

- Le degré de sophistication des agents de menace varie : il peut s'agir de pirates malfaisants, de groupes du crime organisé, de terroristes ou d'États.

- Les Canadiens font confiance au GC pour défendre la cybersouveraineté du Canada, et protéger et faire progresser la sécurité nationale et les intérêts économiques du pays.

Une question de sécurité nationale

- **Risques liés aux technologies vulnérables**
  - L'accès secret et persistant des auteurs de cybermenaces dans les centres de données canadiens/les infrastructures infonuages représente un danger pour la souveraineté de l'information du GC et la continuité des activités du gouvernement
  - Les auteurs de cybermenaces sont adroits à exploiter les technologies d'entreprises et les systèmes de gestion utilisés aux fins d'administration des centre de données et des infrastructures infonuages.
- **Risques liés à la chaîne d'approvisionnement**
  - La chaîne d'approvisionnement élargit les possibilités pour les auteurs de menace de contourner les mesures de sécurité mises en place par le GC
  - Il est plus difficile pour le GC de détecter ces risques et d'y remédier

Approvisionnements du GC

- **Le CSTC collaborent avec les départements du GC pour éliminer ou réduire de façon importante les risques que représentent les cybermenaces et les vulnérabilités de la chaîne d'approvisionnement mondiale pour le GC.**
- **Le CSTC proposera des séances d'information de suivi sur l'atténuation des risques émanant de la chaîne d'approvisionnement aux fournisseurs intéressés aux initiatives consolidés du GC.**
  - Les entreprises doivent être prêtes à signer une entente de non-divulgation avec le CSTC pour obtenir ces renseignements.
- **Les fournisseurs doivent satisfaire aux exigences de sécurité en matière de cyberprotection, de cyberdéfense et d'atténuation des risques associés à la chaîne d'approvisionnement afin que leur offre soit retenue dans le cadre des initiatives consolidés du GC.**
  - À titre de responsable de la sécurité des TI pour le GC, le CSTC cherchera à établir des partenariats à long terme avec les fournisseurs retenus.
  - Le CSTC assistera le Secrétariat du Conseil au Trésor du Canada (SCTB) et Travaux Public et Services Gouvernementaux Canada (PWGSC) dans l'analyse des liens qu'il est possible d'établir à partir renseignements fournis par les répondants concernant leur chaîne d'approvisionnement.
- **Vous pouvez trouver des exemples de ces exigences dans le site Web du CSTC sur la page *Conseils sur la chaîne d'approvisionnement des technologies*.**