Sécurité des dispositifs mobiles - Sécuriser le gouvernement du Canada

JUIN 2016 | SERIE HAUTS DIRIGEANTS | ITSE.80.001

Les dispositifs mobiles, comme les téléphones intelligents et les tablettes, se sont rapidement répandus à l'échelle du gouvernement du Canada (GC), et bien qu'ils permettent d'augmenter la productivité et l'efficacité, ils peuvent aussi accroître le risque de compromission de l'information et des réseaux du GC. Ce risque accru découle du fait que les employés apportent les dispositifs à l'extérieur du bureau et les connectent à des réseaux inconnus qui ne sont peut-être pas sécurisés. Une compromission de l'information ou des réseaux du GC peut entraîner des problèmes tels que des baisses de rendement système, des pannes, des pertes de productivité, des mesures de reprise coûteuses et des dommages à la réputation du GC.

Les auteurs de menaces possèdent des capacités qui leur permettent :

- de transmettre un maliciel sur les réseaux du GC en repérant et en ciblant un dispositif mobile;
- d'accéder aux connexions réseau du dispositif (capacités cellulaires, WiFi et Bluetooth) et de s'en servir à des fins malintentionnées;
- d'utiliser le dispositif pour infiltrer d'autres réseaux du GC;
- d'accéder au dispositif pour y extraire l'information du GC qu'il contient;
- d'utiliser le téléphone comme dispositif d'écoute mobile.

Gestion des risques liés aux dispositifs mobiles

Bon nombre des menaces que les technologies mobiles font peser sur les réseaux du GC peuvent être attribuables au fait que les systèmes d'exploitation des dispositifs mobiles sont généralement beaucoup moins évolués que ceux des postes de travail et portables traditionnels. Par conséquent, il se pourrait que la robustesse et la granularité de contrôle propres au système d'exploitation d'un dispositif mobile ne permettent pas d'obtenir un niveau de protection approprié contre les auteurs de cybermenaces.

Les contrôles de sécurité des technologies mobiles devraient être déterminés en fonction du profil de menaces et de risques du ministère. Le guide *La gestion des risques liés à la sécurité des TI : une méthode axée sur le cycle de vie* du CST décrit un processus de gestion des risques de sécurité des TI en vertu duquel on peut adapter une série prédéfinie de contrôles de sécurité de base de manière à répondre aux besoins spécifiques d'un ministère en matière de sécurité.

Afin de sécuriser l'information et les réseaux du GC, les contrôles de sécurité doivent être déployés et vérifiés pour l'ensemble du système d'information, et ce, du dispositif mobile jusqu'aux services de réseau du ministère qui gèrent les processus opérationnels et l'accès à l'information.

Chaque jour, des dispositifs mobiles permettent d'accéder aux réseaux du GC.

Sécuriser les technologies mobiles

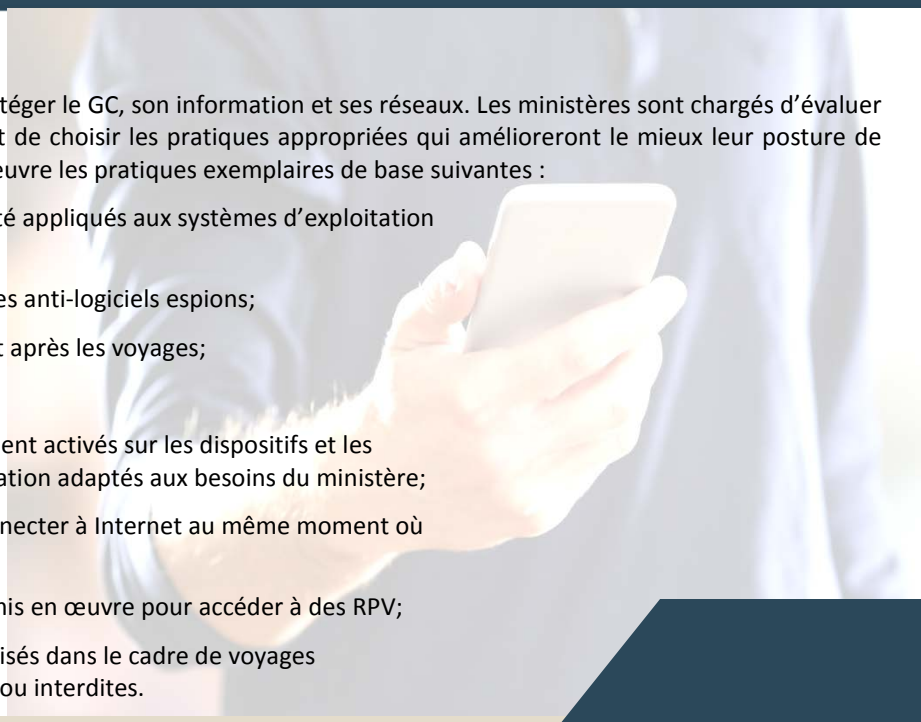
Les dispositifs mobiles se connectent à Internet au moyen de réseaux WiFi ou de réseaux cellulaires commerciaux. Comme le GC n'a aucune influence sur la sécurité de ces réseaux, on considère qu'ils sont vulnérables à des menaces accrues. Pour aider à atténuer les risques associés à l'utilisation de réseaux non fiables, les ministères devraient sécuriser leurs voies de communication en exigeant des connexions RPV sécurisées pour accéder aux réseaux et aux systèmes du GC, et en veillant à ce qu'on utilise uniquement des points d'accès WiFi fiables.

En outre, on peut utiliser des technologies de gestion des dispositifs mobiles pour renforcer la sécurité. Un logiciel de gestion de dispositifs mobiles permet de sécuriser, surveiller, gérer et prendre en charge les dispositifs mobiles connectés à un réseau, en contrôlant les paramètres de configuration et l'utilisation des applications, en sécurisant les données, et en intégrant les services de communication.

En contrôlant les dispositifs et en s'assurant qu'ils ne contiennent pas de maliciels, les ministères peuvent renforcer considérablement la protection du GC contre les compromissions. Les ministères devraient mettre en œuvre des politiques rigoureuses sur les dispositifs mobiles, puisque l'utilisation non réglementée des dispositifs, à des fins personnelles, peut avoir des conséquences négatives importantes sur leur posture de sécurité.

Canada

Sécuriser les dispositifs mobiles



Il est primordial de sécuriser les dispositifs mobiles afin de protéger le GC, son information et ses réseaux. Les ministères sont chargés d'évaluer le niveau de risque lié à l'utilisation des dispositifs mobiles et de choisir les pratiques appropriées qui amélioreront le mieux leur posture de sécurité. À tout le moins, les ministères devraient mettre en œuvre les pratiques exemplaires de base suivantes :

- ✓ S'assurer que les derniers correctifs et mises à jour ont été appliqués aux systèmes d'exploitation et aux applications;
- ✓ Installer les dernières versions des logiciels antivirus et des anti-logiciels espions;
- ✓ Mettre souvent les mots de passe à jour, surtout avant et après les voyages;
- ✓ Limiter les privilèges administratifs;
- ✓ Veiller à ce que les paramètres de sécurité appropriés soient activés sur les dispositifs et les applications. Le CST peut offrir des conseils et une orientation adaptés aux besoins du ministère;
- ✓ Vérifier que les dispositifs mobiles ne peuvent pas se connecter à Internet au même moment où l'utilisateur accède au réseau interne de son ministère;
- ✓ S'assurer que les paramètres de sécurité adéquats sont mis en œuvre pour accéder à des RPV;
- ✓ Optimiser les capacités de surveillance des dispositifs utilisés dans le cadre de voyages internationaux, afin de repérer les activités inhabituelles ou interdites.

Série du CST sur la mobilité

Afin d'aider les ministères à atténuer les menaces, le CST a créé une série de publications sur la sécurité des dispositifs mobiles qui peuvent aider les ministères du GC à grandement réduire l'exposition des dispositifs mobiles aux menaces. Visitez la page Web Sans-fil et mobilité du CST pour télécharger les documents suivants :

- ❖ Technologies mobiles pour les voyages internationaux;
- ❖ Solutions de gestion de dispositifs mobiles;
- ❖ Exigences de sécurité liées aux réseaux locaux sans fil;
- ❖ Gestion des risques associés aux iPad;
- ❖ Sécurité des réseaux sans fil;
- ❖ Dispositifs mobiles et signaux sans fil.

Pour en apprendre plus, inscrivez-vous au cours du CST sur la sécurité du sans-fil (350).

En 2015, Symantec a découvert 430 millions de nouveaux maliciels uniques. Une augmentation de 36 % depuis 2014.

Rapport de Symantec sur la sécurité Internet, 2016

Pour en savoir plus sur la sécurité des dispositifs mobiles, visitez la page Web Sans-fil et mobilité du CST.

Questions?

Communiquez avec les Services à la clientèle de la STI
itsclientservices@cse-cst.gc.ca
613-991-7654

Les dispositifs mobiles et les 10 meilleures mesures de sécurité du CST

La liste des 10 meilleures mesures de sécurité du CST présente, en ordre de priorité, des mesures qu'on peut appliquer non seulement aux réseaux du GC, mais aussi aux dispositifs mobiles. Il s'agit de facteurs de sécurité des TI qu'il importe de prendre en considération lorsqu'on déploie des dispositifs mobiles connectés aux réseaux et aux systèmes du GC.