Communications Security Establishment | Centre de la sécurité des télécommunications

Répercussions sur la sécurité de l'exposition de systèmes TI classifiés à des dispositifs mobiles et à des signaux sans fil

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

ITSB-104 **Octobre 2014**

1 Objet

De nombreux ministères du gouvernement du Canada (GC) et entreprises utilisent des technologies sans fil pour faciliter la collaboration, en raison de la commodité, de la souplesse et de la mobilité qu'elles offrent à leurs employés. Les dispositifs mobiles et signaux sans fil sont des éléments clés dans l'atteinte de cet objectif, mais ils peuvent constituer une menace pour le GC et ses biens d'information, puisque les auteurs de menaces ciblent fréquemment les ministères et leurs réseaux pour obtenir de l'information sur les employés, les projets et les systèmes du GC.

Le présent bulletin décrit les risques découlant de l'exposition de systèmes TI classifiés à des signaux sans fil et à des dispositifs mobiles non autorisés, de même que les mesures d'atténuation possibles. Il s'adresse aux responsables des activités de gestion des risques en matière de sécurité des TI et aux praticiens de la sécurité des systèmes d'information.

2 Répercussions

Les dispositifs mobiles sont dotés de capacités informatiques puissantes et peuvent communiquer avec des réseaux Wi-Fi®, des réseaux cellulaires et tout autre dispositif au moyen de protocoles comme Bluetooth. Les dispositifs mobiles sont aussi vulnérables aux mêmes types de cybermenaces que les ordinateurs traditionnels, dont les maliciels, les logiciels espions et les chevaux de Troie. Le fait de permettre la présence de dispositifs à capacité sans fil dans des zones où sont hébergés des renseignements sensibles ou classifiés peut entraîner une exfiltration (fuite) de données électroniques ou vocales. L'exfiltration peut être intentionnelle ou non, et être effectuée au moyen d'un implant installé dans le dispositif par un auteur de menace. L'auteur d'une menace peut utiliser divers moyens pour acquérir de l'information du GC : vidéo, photographie, enregistrement vocal, ou connexion d'un dispositif directement à une infrastructure câblée.

La menace d'exfiltration est amplifiée lorsqu'un signal sans fil provenant d'un réseau sans fil n'appartenant pas au GC (p. ex. accès Wi-Fi® gratuit dans un café local) se trouve dans le champ de portée d'un réseau sans fil du GC ou d'un dispositif mobile appartenant au GC. Un dispositif du GC peut être connecté par inadvertance ou intentionnellement à un réseau n'appartenant pas au GC ou servir de pont entre un réseau sans fil externe et un réseau du GC, fournissant ainsi une voie de transmission pour l'exfiltration.

L'installation de systèmes TI classifiés à proximité d'émetteurs radioélectriques peut aussi donner lieu à des fuites d'information non intentionnelles.

3 Stratégies d'atténuation

Pour atténuer les risques que posent les dispositifs mobiles et signaux sans fil à l'égard de l'information sensible ou classifiée, les ministères du GC doivent mettre en place des pratiques de sécurité rigoureuses et aviser leurs employés des répercussions en matière de sécurité. Lorsqu'elles sont mises en œuvre ensemble, les mesures présentées ci-dessous peuvent réduire le risque de compromission de l'information.

3.1 Politiques et procédures

Les ministères doivent élaborer des politiques et des règles internes claires sur l'utilisation de dispositifs sans fil dans les zones où sont traités des renseignements sensibles ou classifiés, ou près de ces zones. Le *Guide pour l'établissement des zones de sécurité matérielle (G1-026)* de la Gendarmerie royale du Canada (GRC) doit servir d'élément clé dans l'élaboration d'une stratégie globale de gestion des risques.

Les ministères qui utilisent une solution de gestion de dispositifs mobiles (MDM pour *Mobile Device Management*) doivent s'assurer que les configurations de sécurité sont clairement définies dans leurs politiques et procédures internes. La publication *ITSB 64 – Solutions de gestion de dispositifs mobiles (MDM)* du CST pourra les aider à choisir la solution MDM appropriée.

Des activités régulières portant sur la sensibilisation aux vulnérabilités et sur l'adoption d'habitudes d'utilisation appropriées devraient être proposées à tous les utilisateurs ayant accès aux systèmes ministériels.

3.2 Technologies

Les ministères et organismes du GC devraient envisager d'adopter les contrôles de sécurité suivants pour leurs dispositifs mobiles :

- utiliser une liste blanche pour imposer des restrictions dans l'ensemble de l'organisme;
- contrôler l'utilisation des caméras et des émetteurs sans fil;
- restreindre les connexions à un réseau Wi-Fi® aux points d'accès autorisés du GC.

4 Mise en application

Pour éviter toute fuite d'information non intentionnelle, il faut installer les systèmes TI classifiés le plus loin possible des émetteurs radioélectriques comme les points d'accès Wi-Fi®, les répéteurs de signaux, les dispositifs portables (p. ex. ordinateurs portatifs, tablettes, téléphones mobiles) et les technologies sans fil à l'appui (p. ex. Wi-Fi® ou cellulaire). À noter que les émetteurs radioélectriques fixes posent un plus grand risque que les dispositifs mobiles. Consultez la publication *ITSG-11 – Planification des installations COMSEC – Conseils et critères*, pour en savoir plus sur l'installation de systèmes TI classifiés à proximité d'émetteurs radioélectriques.

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. L'utilisation de dispositifs mobiles et de signaux sans fil à proximité des systèmes TI qui traitent de l'information sensible ou classifiée met à risque les renseignements et actifs du GC. Les ministères peuvent accroître la sécurité de leurs réseaux et prévenir l'exfiltration de données en mettant en place des politiques de sécurité solides, des programmes de formation et de sensibilisation, des contrôles de sécurité adaptés et un processus rigoureux de gestion des risques.

6 Aide et renseignements

Pour obtenir de plus amples renseignements, prière de communiquer par courriel ou par téléphone avec le Centre d'appel du

Centre pour la cybersécurité :
contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88