Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Septembre 2013

Les risques à la cybersécurité associés à l'utilisation de médias sociaux

Conseils à l'intention du gouvernement du Canada

ITSB-66

Introduction

Les gens utilisent les sites Web de médias sociaux pour entrer en contact avec les autres et échanger de l'information avec eux. Cette interaction s'effectue tout autant sur les blogues et les wikis que par le biais des groupes de discussion comme Facebook, Twitter, LinkedIn, Google+ et Wikipédia. Ces sites Web peuvent toutefois représenter une menace pour le gouvernement du Canada (GC) puisque les ministères et les réseaux du GC sont souvent la cible de nombreux types d'auteurs de cybermenaces qui cherchent à recueillir des renseignements sur les employés, les projets et les systèmes du gouvernement canadien. Il est primordial que les ministères du GC mettent en place de saines pratiques en matière de sécurité et veillent à ce que les employés soient sensibilisés afin de réduire les risques associés à l'utilisation des plateformes de médias sociaux.

Public visé

Le présent bulletin est destiné aux utilisateurs de médias sociaux et aux praticiens de la sécurité des TI. Il a pour objectif de proposer des stratégies d'atténuation visant à protéger les réseaux du GC lors de l'utilisation de médias sociaux dans le cadre d'activités officielles. Comme les employés constituent une cible de choix, ce bulletin offre également d'importants conseils de sécurité à partager avec les employés qui utilisent les médias sociaux dans leur vie personnelle et professionnelle.

Cybermenaces et risques associés aux médias sociaux

Les risques à la sécurité suivants devraient être pris en considération :

- **Virus :** Les auteurs de menaces intègrent souvent des maliciels aux sites Web de médias sociaux ou aux applications tierces. Les utilisateurs infectés propagent alors le maliciel en partageant sans le savoir les liens et les fichiers malveillants avec leurs contacts.
- **Applications tierces :** On n'est pas sans savoir que les applications tierces disponibles sur les plateformes des médias sociaux, telles que les jeux en ligne, accèdent à l'information du profil à l'insu de l'utilisateur. Que ces applications contiennent ou non un programme malveillant, l'information recueillie peut servir à plusieurs fins, comme l'envoi de pourriels, l'accès non autorisé aux contacts ou des activités criminelles.
- **Compromission de comptes officiels :** Les auteurs de cybermenaces emploient des méthodes comme l'ingénierie sociale pour prendre contrôle d'un compte officiel en vue de divulguer de l'information sensible, compromettant par la même occasion la sécurité des réseaux du ministère.
- **Vol d'identité :** Les auteurs de cybermenaces sont en mesure de recueillir de l'information personnelle essentielle sur un employé dans l'intention d'usurper son identité ou d'obtenir ses mots de passe, ce qui peut éventuellement mener à la compromission de la sécurité des autres applications ou services en ligne.
- **Reconnaissance :** Les auteurs de cybermenaces peuvent recueillir de l'information sur une personne ou un groupe de personnes en les amenant à répondre à des courriels de harponnage ou des courriels bien conçus d'ingénierie sociale dont la livraison vise à compromettre l'ensemble d'un système ou d'un réseau. Pour en savoir plus sur le harponnage, téléchargez le bulletin Identification des courriels malveillants (ITSB-100).
- **Utilisation non appropriée des données :** Le plus grand risque que pose l'utilisation des médias sociaux à des fins officielles est la possibilité que des données soient utilisées dans un but malveillant à la suite d'une publication publique excessive ou non autorisée d'information par les employés.

Stratégies d'atténuation des risques à l'intention du praticien de la sécurité

Avant d'utiliser les médias sociaux à des fins officielles, les ministères doivent mener une évaluation en fonction des risques afin de déterminer quelles plateformes de médias sociaux il est préférable d'utiliser et quelles sont les limitations à imposer en matière d'accès et d'utilisation. Les mesures de sécurité suivantes doivent également être mises en œuvre :

- **Politique sur les médias sociaux :** Il est nécessaire d'élaborer une politique visant à établir clairement quels sites Web de médias sociaux peuvent être utilisés à des fins officielles ou personnelles à partir des réseaux du ministère.
- **Contrôle d'accès :** Tenez à jour une liste de contrôle d'accès indiquant qui est en mesure d'accéder au compte des médias sociaux et qui sont les administrateurs du compte.
- **Applications tierces :** Assurez-vous que les employés n'utilisent que des applications dignes de confiance et qu'ils limitent la quantité d'information sur les employés à laquelle une application tierce peut accéder.
- **Paramètres de sécurité :** Veillez à activer tous les paramètres de sécurité ou de confidentialité sur les sites Web de médias sociaux. Utilisez une authentification multifactorielle si une telle fonction est disponible. Servez-vous de mots de passe robustes uniques sur chaque site Web.
- **Surveillance :** Surveillez les comptes officiels de médias sociaux pour tout signe d'accès malveillant ou non autorisé et assurez-vous que la diffusion de l'information affichée a bien été approuvée.
- **Signalement d'incident :** Communiquez l'importance de signaler aux services des TI toute activité malveillante et prenez des mesures immédiates pour reprendre le contrôle positif du compte.
- **Sensibilisation des employés :** Veillez à ce que les utilisateurs soient au courant des politiques du ministère sur l'utilisation d'Internet et des médias sociaux. Tenez des séances d'information à intervalles réguliers pour rappeler aux utilisateurs les risques inhérents aux médias sociaux de même que les processus internes de signalement de courriels ou d'incidents suspects. Intégrez des conseils de sécurité aux politiques et documents de sensibilisation.

Conseils de sécurité à l'intention de l'employé

1. Lorsque vous utilisez les comptes des médias sociaux ministériels, assurez-vous d'avoir lu et compris la politique en matière d'usage Internet ainsi que les politiques additionnelles liées aux médias sociaux.
2. Veillez à ce que les renseignements administratifs affichés soient approuvés aux fins de diffusion et portez une attention particulière aux renseignements que vous fournissez à propos de vos activités professionnelles.
3. Faites preuve de prudence lorsque vous affichez des renseignements professionnels sur d'éventuelles promotions, votre participation à des conférences, vos déplacements, vos projets en cours, etc.
4. Dans la mesure du possible, ne publiez pas votre adresse électronique professionnelle dans les documents ou sur Internet, utilisez plutôt une adresse électronique générique ou un formulaire « Contactez-nous ».
5. Assurez-vous que les options de sécurité et de protection offertes ont bien été configurées.
6. Consultez régulièrement les politiques liées à la sécurité et la protection de la vie privée du site Web de votre compte pour prendre connaissance des plus récents changements.

La meilleure façon de protéger vos renseignements et d'atténuer les conséquences d'une compromission est d'utiliser un mot de passe unique pour chaque compte.

On qualifie de « paresseux du mot de passe » l'utilisateur qui se sert toujours des mêmes mots de passe.

7. Soyez vigilant lorsque vous cliquez sur les liens d'un site Web inconnu ou ouvrez des pièces jointes.
8. Signalez tout incident de sécurité suspect à la direction des TI de votre ministère.
9. Pour des raisons de confidentialité et de cybersécurité, faites preuve de jugement lorsque vous publiez des renseignements personnels sur les médias sociaux.

Conclusion

La décision d'utiliser les médias sociaux à des fins officielles doit être accompagnée d'une stratégie de gestion des risques et de politiques rigoureuses en matière d'utilisation d'Internet et des médias sociaux. Les utilisateurs finaux doivent également être informés des risques associés à l'utilisation des médias sociaux, ainsi que des politiques ministérielles quant à leur usage.

Autres renseignements

Pour les questions d'ordre général au sujet du présent document, veuillez envoyer un courriel à itsclientservices@cse-cst.gc.ca.

Références

Commissariat à la protection de la vie privée du Canada : http://www.priv.gc.ca

Sécurité publique Canada : http://www.publicsafety.gc.ca/