Munich RE

10 façons d'aider à prévenir une violation de données

Leçons tirées de hackers éthiques

La Compagnie d'Inspection et d'Assurance Chaudière et Machinerie du Canada

390, rue Bay
Bureau 2000
Toronto (Ontario), M5H 2Y2
Tél. : (416) 363-5491
munichre.com/HSBBII

Branchez-vous

Quelle est la meilleure façon de protéger une entreprise contre une violation de données? « Pensez comme un pirate », disent les experts, et améliorez la sécurité de sorte que les cybercriminels s'attaqueront à une autre cible.

Les spécialistes de la sécurité du Groupe HSB ont travaillé en équipe avec un groupe de « chapeaux blancs » hackers (étiques) pour élaborer une liste de conseils en gestion de risques qui peuvent aider votre entreprise à protéger les renseignements personnels que vous conservez sur les clients, les employés et les tiers.

1. **Externalisez le processus de traitement des paiements.** Évitez de manipuler et/ou conserver vous-mêmes les renseignements personnels des cartes. Des fournisseurs réputés, que ce soit pour un paiement à un point de vente ou par Internet, possèdent du personnel de sécurité dédié qui peut protéger les données mieux que vous ne le puissiez.

2. **Séparez les réseaux sociaux des activités financières.** Utilisez un appareil dédié pour vos transactions bancaires en ligne. Servez-vous d'un appareil différent pour les courriers électroniques et les réseaux sociaux. Sinon, en visitant seulement un site de réseau social infecté, vous pourriez exposer l'appareil que vous utilisez pour vos transactions bancaires et vos comptes d'épargne.

3. **Pensez au-delà des mots de passe.** Ne les réutilisez jamais et ne faites confiance à aucun site Web pour les conserver sécuritairement. Vous ne pouvez jamais savoir lorsqu'un site Web a déjà été piraté et si votre mot de passe a été exposé. Configurez une authentification à deux facteurs : ceci envoie un code secret à votre téléphone confirmant votre identité.

4. **Éduquez et formez les employés.** Établissez une politique écrite à l'égard de la sécurité et communiquez-la à tous les employés. Informez les employés au sujet des types de renseignements qui sont sensibles ou confidentiels et quelles sont leurs responsabilités à l'égard de la protection de ces données. Aussi, la plupart des arnaques et attaques malicieuses proviennent de courriels; assurez-vous que les membres de votre équipe en soient avertis et qu'ils en informent les autres lorsqu'ils reçoivent de tels courriels.

1866

HSB BI&I

5. **Demeurez informé.** Évaluez l'ensemble de la chaîne d'événements d'une attaque potentielle. De l'évaluation de l'infrastructure de votre courrier électronique à votre responsabilité en tant qu'utilisateur, jusqu'à la vulnérabilité de votre navigateur, identifiez les endroits où votre organisation est le plus à risque. Par la suite interrogez-vous sur la politique en place, en matière de sécurité, à l'égard de vos lignes d'affaires, vendeurs, fournisseurs ou partenaires.

6. **Cessez la transmission de données qui ne sont pas cryptées.** Rendez obligatoire le cryptage de toutes les données. Ceci inclut les données « inactives » et « en mouvement ». Si des renseignements personnels sont transmis par courriels à l'intérieur de votre entreprise, considérez également le cryptage de ceux-ci. Évitez d'utiliser les réseaux Wi-Fi : ils peuvent autoriser l'interception de données.

7. **Sécurisez votre navigateur.** En raison de l'augmentation de la popularité des attaques de point d'eau – codes malicieux installés sur des sites Web fiables – comment savez-vous à quels sites Web vous pouvez vous fier? Oubliez les « patchs » individuels. Concentrez-vous plutôt sur la mise à jour de votre navigateur par la dernière version. Par la suite, effectuez des vérifications de configuration de votre navigateur afin de déceler ses points faibles.

8. **Sécurisez votre système d'exploitation.** Il est beaucoup plus facile de s'introduire dans les systèmes d'exploitation plus anciens tels que Windows XP ou OSX10.6. Tirez avantage des améliorations de sécurité majeures apportées aux systèmes d'exploitation plus récents.

9. **Sécurisez votre routeur.** Celui-ci connecte votre ordinateur à l'Internet. Assurez-vous que personne ne puisse intercepter les données qui sont transmises par celui-ci. Il est important de configurer un mot de passe d'administrateur fiable sur votre routeur et un mot de passe WPA2 sur votre Wi-Fi.

10. **Sécurisez vos données.** Que vous perdiez des données par accident ou en raison d'une attaque, vous serez toujours heureux d'avoir une copie de sauvegarde. Idéalement, en cas de feu ou de cambriolage, votre copie de sauvegarde doit être cryptée et conservée dans un endroit situé hors des lieux.

© 2015 La Compagnie d'Inspection et d'Assurance Chaudière et Machinerie du Canada. Tous droits réservés.