CENTRE FOR PUBLIC MANAGEMENT INC.
CENTRE DE GESTION PUBLIQUE INC.

Commission des relations de travail dans la fonction publique

Vérification de la sécurité sur Internet

31 mars 2006

Résumé

Suite /Pièce 1016,
130 rue Albert Street,
Ottawa, ON K1P 5G4

(T) 613-567-7752
(F) 613-567-7790
cpm.ca

Résumé

Contexte, objectifs et portée de la vérification

Le Centre de gestion publique Inc. a obtenu un contrat de la Commission des relations de travail dans la fonction publique (CRTFP) pour effectuer une vérification de l'utilisation et de la sécurité sur Internet. La CRTFP tient à rendre ses services et ses données facilement accessibles à tous et a mis en place une infrastructure sécurisée pour protéger son infrastructure technique. Or, Internet représente un point d'accès potentiel aux réseaux du gouvernement; c'est pourquoi cette vérification visait les objectifs suivants :

- Évaluer l'utilisation d'Internet à la CRTFP;
- Évaluer les mesures de sécurité en place pour empêcher tout accès non autorisé aux réseaux de la CRTFP à partir d'Internet, y compris la mise en œuvre et le respect des sections pertinentes de la Politique du gouvernement sur la sécurité et des normes en matière de gestion de la sécurité des TI.

Constatations

Utilisation d'Internet par les employés

Malgré l'absence d'une politique d'utilisation d'Internet, nous avons constaté que le temps consacré à l'utilisation d'Internet (87 %) par la majorité des employés était lié à leur travail. L'utilisation à des fins personnelles concernait l'accès à des fonctions fréquemment utilisées tels les groupes de nouvelles, les courriels personnels, l'achat en ligne, etc. Toutefois, on a noté des accès occasionnels à des sites dont la consultation est questionnable du point de vue d'un environnement de travail. Même si ces accès comptaient pour moins de 1/10^{e} de 1 % de tous les sites Web visités, ils augmentent néanmoins l'exposition de la CRTFP aux risques liés aux virus et au code informatique malveillant en plus de donner lieu à des plaintes de la part d'employés qui sont exposés par inadvertance à ces contenus par un collègue.

1. Nous recommandons l'élaboration d'un projet de politique d'utilisation d'Internet qui stipule clairement ce que l'on entend par utilisation acceptable d'Internet.

   Réponse de la direction : La CRTFP a déjà en place une politique sur l'utilisation des réseaux électroniques qui est affichée sur son site intranet. Dans la politique, les réseaux sont définis comme des groupes d'ordinateurs et de systèmes informatiques capables de communiquer les uns avec les autres, incluant Internet, les réseaux internes ainsi que les réseaux publiques et privés à l'extérieur de la CRTFP. L'objectif de la politique est le suivant :

   […] La Commission des relations de travail dans la fonction publique encourage les personnes autorisées à utiliser les réseaux électroniques pour mener les affaires de la Commission, pour communiquer avec d'autres personnes autorisées et avec le public, pour recueillir des renseignements pertinents pouvant les aider dans leurs fonctions et pour maîtriser les

techniques d'utilisation de ces réseaux. Étant donné que certaines personnes peuvent, par inadvertance ou délibérément, se servir des réseaux électroniques pour saper un milieu de travail sain, pour divulguer sans autorisation des renseignements classifiés ou désignés, pour engager des frais ou pour s'adonner à des activités illégales, la CRTFP a décidé d'instaurer la présente politique pour aider les personnes autorisées à exploiter les réseaux électroniques de façon optimale. Une liste des activités inacceptables liées à l'accès aux réseaux électroniques est annexée à la politique (Annexe C).

Malgré ce qui précède, la CRTFP prévoit élaborer et mettre en œuvre en 2006-2007 une nouvelle politique d'utilisation d'Internet qui satisfera aux exigences des normes de la Gestion de la sécurité des TI (GSTI) et répondra aux préoccupations constatées au cours de cette vérification interne. Effectivement, la nouvelle politique misera sur un environnement Internet plus contrôlé et mieux sécurisé.

2. Nous recommandons également de configurer le pare-feu de manière à bloquer l'accès à tout site Web suspect.

   Réponse de la direction : La CRTFP convient qu'il faut bloquer les sites Web suspects. Toutefois, au lieu de reconfigurer le pare-feu à cette fin, elle prévoit plutôt procéder à l'acquisition et à la mise en œuvre en 2006-2007 d'un système de détection d'intrusion (SDI) qui non seulement servira à repérer et à vérifier les preuves d'intrusions ou de tentatives d'intrusion externes, mais également à détecter et signaler l'existence d'autres vulnérabilités du réseau en matière de sécurité, telle la mauvaise utilisation des systèmes. Selon la capacité démontrée par le SDI, la CRTFP pourra également décider d'acquérir un logiciel de blocage, tel Websense, qui servira de complément à son infrastructure de sécurité.

Sécurité d'Internet

Nous avons constaté que la périphérie du réseau était raisonnablement sûre. Nous avons examiné la documentation, les politiques et les procédures liées au réseau, les niveaux du logiciel du système d'exploitation et les règles du pare-feu, et nous les avons jugés adéquats. Nous avons également effectué une analyse externe des réseaux de la CRTFP et n'avons noté aucune situation imprévue.

Afin d'accroître davantage la sécurité, nous recommandons ce qui suit à la CRTFP :

3. Mettre en place une politique de gestion des mots de passe.

   Réponse de la direction : Une nouvelle procédure d'attribution et de gestion des mots de passe a été présentée au Comité des TI de la CRTFP le 30 août 2005 dans le cadre de la stratégie de migration de l'environnement Novell à un environnement Windows. Cette procédure, qui vise le transfert de la responsabilité de la gestion des mots de passe des Services des TI à l'ensemble des utilisateurs, sera communiquée à tous les employés et mise en œuvre d'ici le 30 mai 2006.

4. Officialiser la planification, les essais et la diffusion de rustines pour les systèmes de la zone démilitarisée (DMZ).

   Réponse de la direction : La CRTFP souscrit à la recommandation d'officialiser la gestion des rustines des systèmes de la DMZ qui, en principe, concernent uniquement ses serveurs Web. Un calendrier sera élaboré et mis en application d'ici le 30 juin 2006.

5. Restreindre l'utilisation du serveur Microsoft Exchange aux seules activités propres à Microsoft Exchange.

   Réponse de la direction : La CRTFP reconnaît l'importance de restreindre les activités exécutées dans le serveur MS Exchange. À des fins fonctionnelles, nous avons installé dans le serveur MS Exchange une page initiale dans laquelle on demande aux utilisateurs internes, lors de leur connexion, d'accepter la politique sur le réseau. C'est là le seul contenu non MS Exchange dans le serveur. Cette approche a été adoptée à des fins de fonctionnalité et de respect des protocoles établis d'accès à l'intranet. La CRTFP s'engage à faire une utilisation stricte du serveur MS Exchange et à ne plus procéder à l'installation dans celui-ci d'applications non MS Exchange.