



Exposé de position du SNDPI

Gestion de la cybermenace pour les membres du Cabinet

Préparé pour le compte du SNDPI avec la contribution des membres du Comité par

Martin Dinel, BSc, ISP-EATI, ITCP-PATI, CISSP/ALBERTA

09-11-2017

INTRODUCTION

En tant que représentants élus du gouvernement, les membres du Cabinet sont dans la mire du public et utilisent de plus en plus les réseaux sociaux et les médias d'information pour s'acquitter de leurs fonctions. Par conséquent, une grande partie de leurs renseignements personnels sont rendus publics, ce qui fait d'eux d'excellentes cibles pour les cybercriminels.

POSITION DU SNDPI

Les instances fédérales, provinciales et territoriales du Canada ont toutes un programme quelconque de sensibilisation à la cybersécurité à l'intention du personnel de leur organisation. Il s'agit souvent de ressources accessibles en ligne combinées à des exposés en classe. Ces programmes sont offerts aux employés, qui sont habituellement tenus de suivre des cours chaque année. Or, malgré le fait que les membres du Cabinet constituent une cible attrayante, ils sont rarement exposés aux mêmes programmes.

Les sujets abordés par les programmes de formation en cybersécurité comprennent, sans s'y limiter, les suivants :

- l'hameçonnage et le piratage psychologique;
- les pratiques générales de sécurité liées à l'utilisation d'ordinateurs et d'appareils mobiles;
- la classification de sécurité des renseignements et la gestion de l'information;
- l'accès à l'information et la protection des renseignements personnels.

Il est important de tenir compte du fait que les membres du Cabinet reçoivent des renseignements de nature très délicate qui sont essentiels aux opérations gouvernementales et, bien souvent, au bien-être de leurs électeurs. Une atteinte à ces renseignements aura **inévitablement** une incidence sur la réputation du gouvernement et sur la confiance des électeurs en la protection des renseignements détenus à leur sujet. Une atteinte **pourrait** aussi avoir des répercussions financières (perte d'emplois, occasions manquées, répercussions juridiques, etc.).

La cybermenace pour les membres du Cabinet pourrait se manifester de bien des façons lorsque des renseignements accessibles au public sur les réseaux sociaux ou dans les médias sont utilisés aux fins suivantes :

- deviner les mots de passe et les justificatifs d'identité ou les extorquer par la ruse;
- avoir accès à des renseignements de nature délicate, modifier des renseignements ou se faire passer pour le membre du Cabinet afin de convaincre quelqu'un d'exécuter une activité en son nom (p. ex. le personnel administratif de l'Université MacEwan en Alberta a reçu un faux courriel contenant suffisamment

Sous-comité national
des DPI sur la
protection de l'information



d'information pour le convaincre de modifier les renseignements relatifs aux comptes à payer à un entrepreneur, ce qui a entraîné une fraude de 11 millions de dollars);

- déterminer un lieu fréquenté par le membre du Cabinet, comme un café, afin de lancer une attaque d'interception permettant à l'auteur de la menace de lire des courriels ou d'effectuer des activités en ligne à l'insu de l'utilisateur.

Bien que toutes les instances conviennent que les membres du Cabinet doivent être informés de ces menaces et de la façon d'y réagir, seuls deux secteurs de compétence ont actuellement un accès direct aux membres de leur Cabinet :

- Le gouvernement du Canada – Les membres du Cabinet sont informés des questions de cybersécurité par divers moyens (déjeuners des sous-ministres, réunions sur les cybermenaces, réunions des organes décisionnels exécutifs), selon les besoins.
- La Colombie-Britannique – Le dirigeant principal de la sécurité de l'information est en mesure de se mettre directement en rapport avec les membres du Cabinet pour leur faire des présentations de sensibilisation générale.

RECOMMANDATION

Les membres du SNDPI conviennent qu'il est essentiel que les employés de tous les niveaux, en particulier les dirigeants clés comme les membres du Cabinet, soient mis au courant des cybermenaces qui peuvent les toucher et reçoivent des renseignements pertinents sur la façon de reconnaître ces menaces, de les prévenir et d'y réagir.

Nous recommandons que les mesures suivantes soient mises en œuvre dans tous les secteurs de compétence dès que possible :

- Donner des séances annuelles de sensibilisation à la cybersécurité de 15 à 20 minutes où l'on traite de la vigilance face aux cybermenaces et de la façon de les reconnaître et d'y réagir.
- Veiller à ce que les membres du Cabinet reçoivent la même formation de sensibilisation à la cybersécurité que celle dont bénéficient les employés internes.
- Obliger tous les membres du Cabinet qui voyagent à l'extérieur du pays à suivre une séance d'information sur la cybersécurité avant leur départ (voir l'exposé de position du SNDPI sur la gestion de la cybermenace résultant des voyages à l'étranger).

Le SNDPI demande l'aide du Conseil des dirigeants principaux de l'information du secteur public (CDPISP) pour mettre en œuvre ces recommandations.