e-Veille

À la rencontre des gouvernements en ligne du globe

Bulletin électronique
Volume 8 - Septembre 2004

Ce mois-ci :

La sécurité de l'information : enjeu majeur des gouvernements électroniques. Différents pays, différents défis!

SOMMAIRE

La loi antipourriels américaine CAN-SPAM ne suffira pas - Sophos, un des leaders mondiaux des logiciels antipourriels, a publié le 24 août dernier la liste des douze principaux pays émetteurs de pourriels (spam). En tête de lice, et loin devant, on retrouve les États-Unis, d'où proviennent 42,5 % des pourriels diffusés dans le monde. Malgré la loi fédérale adoptée par nos voisins, la quantité de courriels non sollicités diffusés par Internet n'a cessé de croître.

Authentification électronique: Coup d'oeil sur les principes mis de l'avant par les gouvernements canadien et américain - Toute personne qui s'intéresse au gouvernement électronique peut en témoigner, l'identification électronique des usagers est certainement l'un des enjeux majeurs du développement des services gouvernementaux en ligne. La mise en œuvre de tels services va en effet de pair avec celle de procédures d'identification des citoyens et des entreprises qui sachent répondre aux plus hauts standards en matière de sécurité des transactions et de protection des renseignements personnels. La confiance du public face aux mécanismes de sécurité implantés n'est ainsi rien de moins que la condition sine qua non du succès des initiatives reliées au gouvernement en ligne.

La sécurité informatique en chiffres

Utilisation des technologies de sécurité dans les entreprises privées et publiques canadiennes

Investissements dans la sécurité aux États-Unis : des disparités selon le palier de gouvernement

Secrétariat du Conseil du trésor Québec

En collaboration avec le cefrio

La sécurité de l'information: enjeu majeur des gouvernements électroniques. Différents pays, différents défis!

La loi antipourriels américaine CAN-SPAM ne suffira pas

Sophos, un des leaders mondiaux des logiciels antipourriels, a publié le 24 août dernier la liste des douze principaux pays émetteurs de pourriels (spam). En tête de lice, et loin devant, on retrouve les États-Unis, d'où proviennent 42,5 % des pourriels diffusés dans le monde. Malgré la loi fédérale adoptée par nos voisins, la quantité de courriels non sollicités diffusés par Internet n'a cessé de croître.

En décembre 2003, le président des États-Unis, Georges W. Bush, signait le CAN-SPAM Act, loi qui fut mise en vigueur le 1er janvier 2004. Cette loi visait à réglementer davantage le pollupostage en obligeant les auteurs de messages de marketing à indiquer, dans leur courriel, une adresse courriel de retour, une adresse postale valide, un mécanisme de retrait de la liste d'envoi ainsi qu'un titre pertinent dans le champ sujet. Si cette loi donne maintenant la possibilité de poursuivre les émetteurs de pourriels non conformes à la loi et de les condamner à une peine pouvant atteindre cinq ans de prison ou 6 millions de dollars, elle n'a eu que très peu d'impact jusqu'à présent sur le volume de pourriels reçus par les internautes. Malgré le fait que seulement 1 % des courriels non sollicités respecteraient la nouvelle loi peu de poursuites ont en effet été intentées, les moyens manquants pour investiguer et les polluposteurs s'avérant difficiles à retracer.

« La tentative des États-Unis d'adapter sa législation anti-spam n'a eu que peu d'effet. Le pays reste de loin le plus gros émetteur de spam dans le monde », commente Annie Gray, directrice générale de Sophos France. Selon une étude de Pew Internet & American Life Project, depuis l'entrée en vigueur de cette loi, 24 % des internautes américains possédant une adresse courriel personnelle déclarent avoir reçu plus de pourriels qu'avant le 1er janvier 2004 et 53 % n'ont noté aucun changement. L'enquête révèle par contre que 71 % des détenteurs d'adresses de courriel ont déjà reçu des pourriels à caractère pornographique, mais que, depuis la CAN-SPAM Act, 25 % ont remarqué une diminution du nombre de ce type de message alors que 53 % n'ont pas remarqué de variation.

D'après l'étude de Sophos, le Canada aurait de son côté fait quelques progrès en divisant par deux sa part du pourriel émis dans le monde, de 6,8 % il y a six mois à 2,9 % aujourd'hui. La guerre aux pourriels n'est pourtant pas gagnée : Selon les prévisions d'Industrie Canada, le pourriel représentera jusqu'à 70 % du courriel global d'ici la fin de 2004.

Les gouvernements de plusieurs pays mettent donc l'épaule à la roue pour réduire le nombre de pourriels reçus par leurs citoyens.

- **Pays de l'Organisation de coopération et de développement économiques (OCDE)**

Un Groupe de réflexion de l'OCDE pour coordonner la lutte contre les courriels non sollicités vient d'être mis en place afin de concerter les efforts des pouvoirs publics, des entreprises et de la société civile contre ce fléau. Il aura deux ans pour étudier les stratégies antipourriels en place ou sur le point de l'être dans l'ensemble des secteurs d'activités; développer et prévoir des outils antipourriels et enfin, à définir une stratégie de sensibilisation du public.

- **Canada**

Le 11 mai dernier, le ministre d'Industrie Canada a annoncé la mise sur pied d'un Groupe de travail spécial sur le pourriel pour coordonner la mise en œuvre d'un plan d'action visant à réduire le volume des messages électroniques commerciaux non sollicités. Ce plan vise à agir sur divers aspects et à mobiliser les acteurs de différents milieux à la lutte contre le pourriel. Le plan prévoit notamment l'utilisation des lois et réglementations existantes, telles que la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), qui traite les adresses de courrier électronique comme des renseignements personnels, ainsi que la Loi sur la concurrence et le Code criminel comme étant des outils pouvant servir au traitement du pourriel. Le Groupe souhaite néanmoins effectuer une révision des mesures législatives, réglementaires et coercitives actuelles. Le plan prévoit également établir des codes pour l'industrie et suggérer aux organisations canadiennes des pratiques de gestion des réseaux visant à amoindrir le volume de pourriel. Le Groupe aura aussi pour mandat de réfléchir sur la mise en place de systèmes servant à valider les communications commerciales légitimes ainsi qu'à des moyens de sensibilisation et d'éducation des consommateurs à un usage du courriel et d'Internet permettant d'éviter la réception de pourriels.

Le Canada souhaite également participer activement aux efforts internationaux de lutte contre le pourriel. Pour ce faire, il préside, au sein de l'OCDE, un groupe de travail conjoint qui élabore actuellement un plan d'action sur le pourriel. Il participe également aux travaux du Forum de coopération économique Asie-Pacifique (APEC) et du Dialogue mondial des entreprises sur le commerce électronique (GBDe), dirigé par le secteur privé.

- **Australie**

L'Australie s'est doté l'an dernier d'une loi anti-pourriel, la Spam Act 2003. Depuis son entrée en vigueur, tous les messages électroniques commerciaux non sollicités, qu'ils soient envoyés par courriel, par messagerie instantanée, par messagerie multimédia ou par messages courts envoyés par téléphones portables, sont considérés comme des pourriels (spams).

En regard de cette loi, il est maintenant de mise que tous les expéditeurs de messages électroniques commerciaux s'identifient clairement. Les destinataires doivent donc être en mesure de savoir précisément qui est l'entité responsable de l'envoi du message et comment il peut être contacté. Aussi, les expéditeurs doivent obtenir le consentement direct ou indirect du destinataire. Le consentement indirect est basé sur la présence de relations d'affaires, ou d'autres types de relations, entre l'expéditeur et le destinataire. Aussi, les expéditeurs doivent inclure dans leur message un mécanisme permettant aux destinataires de se retirer des listes de diffusion. Notons enfin que la loi interdit l'utilisation de logiciels conçus pour automatiser la collecte d'adresses dans le but de constituer une liste d'envoi ainsi que l'acquisition de listes ainsi constituées.

Nous verrons prochainement si les initiatives mises en place par les gouvernements auront un réel impact sur la proportion de pourriels que nous recevrons au cours des prochains mois. Selon madame Gray, « plusieurs mesures ont été suggérées pour venir à bout du spam (depuis la facturation de l'envoi des e-mails jusqu'à la création des mécanismes d'authentification de l'expéditeur), mais elles ne suffiront pas à résoudre le problème. Seule une combinaison de technologies, de législations internationales et de changements du comportement des usagers permettra d'arrêter le spam ».

Rédactrices : Isabelle Vachon et Caroline Jacob, analystes-conseils, Enquêtes et Veille stratégique, CEFRIO

Sources:

Australian Government. Department of Communications, Information Technology and the Arts, février 2004, *Spam Act 2003: An overview for business* , 6 pages.

Robyn Greenspan, 20 avril 2004, « E-Marketers Not Fully CAN-SPAM Compliant » , ClickZ news.

Grant Gross, 11 août 2004, « Most spam is domestic, study says : spammers aren't ducking antispam laws by operating offshore, they're just ignoring it » , PC World.

Grant Gross, 13 janvier 2004, « Is the CAN-SPAM law working? : only a small percentage of unsolicited e-mail complies with the new law, studies show » , PC World.

Gregg Keiser, 5 août 2004, « Can-Spam isn't doing the job » , Information Week.

Industrie Canada, mai 2004, Un plan d'action anti-pourriel pour le Canada , 12 pages.

OCDE, 12 août 2004, « Un Groupe de réflexion de l'OCDE pour coordonner la lutte contre le spam » , communiqué de presse.

Pew Internet & American Life Project, mars 2004, “The CAN-SPAM Act has not Helped Most Email Users So Far” .

Sophos, 24 août 2004, « Sophos publie la nouvelle liste des douze principaux pays émetteurs de spam » , Communiqué de presse.

Authentification électronique: Coup d'oeil sur les principes mis de l'avant par les gouvernements canadien et américain

Toute personne qui s’intéresse au gouvernement électronique peut en témoigner, l’identification électronique des usagers est certainement l’un des enjeux majeurs du développement des services gouvernementaux en ligne. La mise en œuvre de tels services va en effet de pair avec celle de procédures d’identification des citoyens et des entreprises qui sachent répondre aux plus hauts standards en matière de sécurité des transactions et de protection des renseignements personnels. La confiance du public face aux mécanismes de sécurité implantés n’est ainsi rien de moins que la condition sine qua non du succès des initiatives reliées au gouvernement en ligne.

Éléments de définition

Mais encore, qu’entend-on par authentification de l’utilisateur? Il s’agit en fait d’un processus par lequel l’identité d’une personne est validée de façon électronique, processus qui peut s’appuyer sur les authentifiants suivants :

1. ce que la personne est seule à savoir, par exemple un mot de passe ou un algorithme;
2. un objet physique uniquement possédé par l’individu concerné et qu’il est donc seul à pouvoir fournir, soit un jeton (carte à microprocesseur ou clé de chiffrement) et
3. l’un des attributs biométriques de la personne, soit ces empreintes digitales, la forme de sa main, etc.

Puisque l'authentification électronique implique la transmission de renseignements personnels en ligne, elle présente, on le conçoit aisément, des défis technologiques de taille aux administrations publiques. Les standards entourant le processus doivent ainsi être établis en tenant compte des risques associés aux erreurs ainsi qu'aux utilisations illicites de l'information transmise par voie électronique.

Les cadres canadiens et américains

C'est dans le but de présenter les balises devant entourer l'élaboration et l'utilisation des services d'authentification que les gouvernements du Canada et des États-Unis se sont penchés sur la question et ont récemment publié (mai et juin 2004) deux documents destinés à leurs ministères, organismes et agences. Voici donc un aperçu des principes et recommandations formulés par chacune des deux administrations publiques.

- **Le Canada**

Élaborés par un Groupe de travail sur les principes d'authentification convoqué par Industrie Canada, les six grands principes présentés ici ont été développés pour servir de points de repère lors de la mise en œuvre de mesures d'identification électronique. Ils se veulent complémentaires à la structure de gouvernance existant au Canada pour l'authentification, structure constituée, entre autres, de la Politique du Canada en matière de cryptographie de 1998, de lois fédérales et provinciales, y compris la Loi sur la protection des renseignements personnels et les documents électroniques de 2000, les Principes régissant la protection des consommateurs dans le commerce électronique (2001) et le Code canadien de pratiques pour la protection des consommateurs dans le commerce électronique (2004).

Principe 1 : Responsabilités des parties prenantes

Les différentes parties impliquées dans un processus d'authentification devraient être conscientes des fonctions qu'elles accomplissent (administration de l'authentification, spécification et utilisation finale, élaboration de normes, etc.) ainsi que des responsabilités reliées à ces fonctions. Ces responsabilités sont en outre proportionnelles au niveau de connaissance que chacune des parties devrait posséder ainsi qu'au niveau de contrôle qu'elles devraient exercer.

Principe 2 : Gestion du risque

Les risques liés aux processus d'authentification devraient être déterminés, évalués et gérés d'une manière raisonnable, juste et efficace. À noter que ces risques peuvent être financiers, mais aussi plutôt reliés à la perte de confidentialité ou de renseignements personnels, à des dommages à la réputation ainsi qu'au vol d'identité.

Principe 3 : Sécurité

Toutes les parties impliquées dans un processus d'authentification devraient être responsables de la sécurité, en proportion des rôles qu'elles jouent dans ce processus. Chacune d'entre elles est ainsi appelée à atténuer les risques et ce, grâce à de saines pratiques en matière de sécurité.

Principe 4 : Protection des renseignements personnels

Les organisations engagées dans la conception ou l'exécution des processus d'authentification devraient se conformer aux normes de protection des données énoncées dans les codes de pratique (codes en matière de protection des renseignements personnels) en plus de se conformer aux lois et à la

jurisprudence (lois en matière de protection des renseignements personnels) applicables.

Principe 5 : Obligations d'information

Les parties prenantes qui offrent des services d'authentification devraient divulguer de l'information aux autres parties impliquées afin de faire en sorte qu'elles soient toutes conscientes des risques et des responsabilités inhérents à leur participation.

Principe 6 : Traitement des plaintes

Les organisations qui mettent en œuvre un processus d'authentification devraient élaborer une méthode de traitement des plaintes permettant aux parties prenantes de répondre à ces plaintes de façon efficace.

- **Les États-Unis**

Les recommandations destinées aux agences fédérales américaines, mais pouvant aussi être utilisées par des organisations non gouvernementales, ont pour leur part été développées par le National Institute of Standards and Technology (NIST) des États-Unis.

Quatre niveaux d'authentification ont été établis par le NIST, ceux-ci ayant été définis selon l'importance des conséquences associées aux erreurs ainsi qu'aux mauvaises utilisations des données transmises en ligne :

Niveau 1 : peu ou pas d'assurance quant à la validité de l'identité de la personne requérante
Niveau 2 : une certaine assurance quant à la validité de l'identité du requérant
Niveau 3 : une forte assurance quant à la validité de l'identité du requérant
Niveau 4 : une très forte assurance quant à la validité de l'identité du requérant

Pour déterminer le niveau de sécurité approprié au processus d'authentification qu'elles souhaitent mettre en place, les agences peuvent en outre se référer, entre autres, au tableau récapitulatif suivant :

Impacts potentiels maximums selon chacun des niveaux d'assurance

Catégories d'impacts reliés à des erreurs d'authentification	**Niveau 1**	**Niveau 2**	**Niveau 3**	**Niveau 4**
Inconvénients, angoisse ou dommages à la réputation	Faible	Modéré	Modéré	Élevé
Pertes financières ou reliées à la responsabilité de l'agence concernée	Faible	Modéré	Modéré	Élevé
Tort aux programmes de l'agence ou à l'intérêt public	N/A	Faible	Modéré	Élevé
Divulgation non autorisée d'information « sensible »	N/A	Faible	Modéré	Élevé
Sécurité personnelle	N/A	N/A	Faible	Modéré-élevé
Infraction civile ou criminelle	N/A	Faible	Modéré	Élevé

Source : Joshua B. Bolten, 16 décembre 2003, E-Authentication Guidance for Federal Agencies , p. 7.

Par ailleurs, à l'intérieur de chacun de ces niveaux d'assurance, différents types d'authentifiants doivent être considérés soit, comme on l'a vu plus haut, des simples mots de passe aux attributs biométriques, en passant par l'utilisation de jetons.

Reste finalement à espérer que ces principes directeurs, et surtout la mise en œuvre des processus et d'initiatives qui les matérialisent, contribueront au renforcement de la confiance des citoyens canadiens et américains face au gouvernement en ligne.

Rédactrice : Catherine Lamy, directrice adjointe, Enquêtes et Veille stratégique, CEFRIO

Sources :

Canada, Industrie Canada, mai 2004, Principes d'authentification électronique : cadre canadien .

United States, Department of Commerce, Technology Administration, National Institute of Standards and Technology, juin 2004, Electronic authentification guideline : recommendations of the National Institute of Standards and Technology . (NIST special publication ; 800-63).

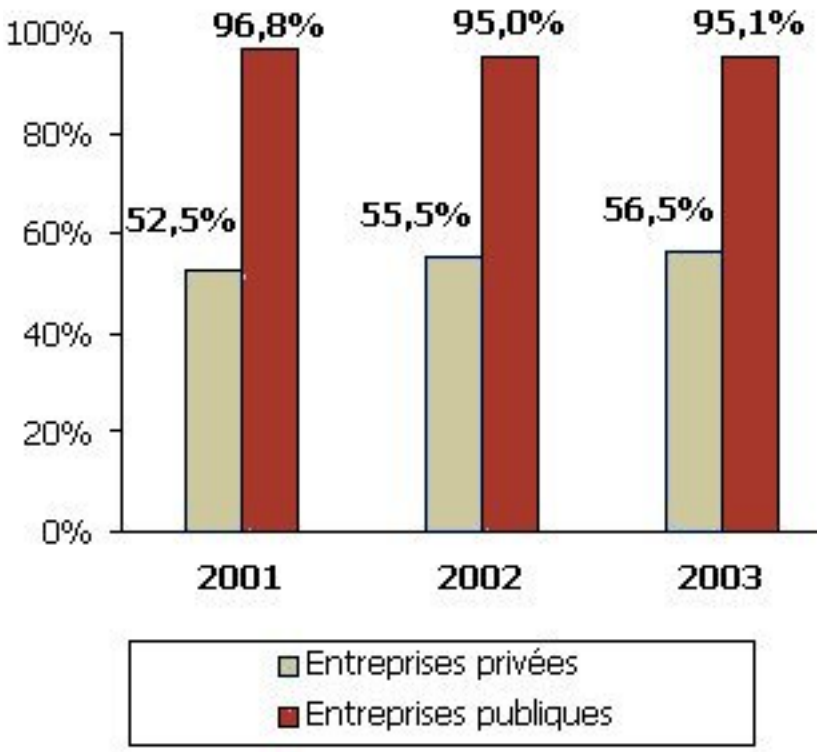
Joshua B. Bolten, 16 décembre 2003, E-Authentication Guidance for Federal Agencies .

La sécurité informatique en chiffres

Utilisation des technologies de sécurité dans les entreprises privées et publiques canadiennes

Statistique Canada, dans son Enquête sur le commerce électronique et la technologie, a interrogé les entreprises canadiennes privées et publiques à propos de leur utilisation de technologies de sécurité des réseaux et de l'information. Comme le présente le tableau ci-dessous, entre les années 2001 et 2003, le pourcentage d'entreprises utilisant ce type de technologies est demeuré relativement stable dans les entreprises publiques, alors qu'il a crû de 4 points de pourcentage chez les entreprises privées.

Utilisation de technologies de sécurité des réseaux et de l'information par les entreprises canadiennes (2001, 2002 et 2003)



Source: Statistique Canada, 2004, *Utilisation des technologies de sécurité des réseaux et de l'information par les entreprises privées et publiques, selon le Système de classification des industries de l'Amérique du Nord (SCIAN)*, données annuelles (pourcentage), 4 tableaux (Tableau 358-0007)

Investissements dans la sécurité aux États-Unis : des disparités selon le palier de gouvernement

S'il est vrai que l'argent est le nerf de la guerre, il convient alors de dire qu'en matière de lutte contre les attaques informatiques, les différents paliers de gouvernements aux États-Unis ne luttent pas tous à armes égales.

La neuvième édition de l'enquête Computer Crime and Security Survey réalisée en 2003 auprès de 494 professionnels de la sécurité informatique, dont des représentants d'agences gouvernementales, s'est intéressée à plusieurs aspects entourant la sécurité dans les organisations américaines, notamment les dépenses en capital et les investissements.

En combinant les dépenses et les investissements en sécurité informatique, c'est le gouvernement fédéral qui arrive en tête de lice (261 $ par employé). Viennent ensuite les gouvernements d'États ou State government (154 $) et les gouvernements locaux (17 $).

Rédactrice: Caroline Jacob, analyste-conseil, Enquêtes et Veille stratégique, CEFRIO

Source :

CSI/FBI, juin 2004, 2004 CSI/FBI computer crime and security survey ,

Accès au communiqué de presse : http://www.gocsi.com/press/20040609.jhtml

Le bulletin E-Veille est produit sous la coordination du Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles du Secrétariat du Conseil du trésor.

1500-H, rue Jean-Talon Nord
Sainte-Foy (Québec)
G1N 4T5
Téléphone : (418) 528-5505
Télécopieur : (418)528-5506

Gestion et supervision
Pascal Doucet , conseiller en ingénierie documentaire et veille stratégique, Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles, Secrétariat du Conseil du trésor
Éric Lacroix , directeur, Enquêtes et Veille stratégique, CEFRIO

Réalisation et rédaction
Isabelle Vachon , analyste-conseil, Enquêtes et Veille stratégique, CEFRIO

Recherche documentaire
Isabelle Poulin , documentaliste, Enquêtes et Veille stratégique, CEFRIO

Avec la collaboration de
Catherine Lamy , directrice adjointe, Enquêtes et Veille stratégique, CEFRIO
Caroline Jacob , analyste-conseil, Enquêtes et Veille stratégique, CEFRIO