CHRONIQUE DE SÉCURITÉ

NUMÉRO SPÉCIAL : LA POLITIQUE DE SÉCURITÉ DES ACTIFS INFORMATIONNELS

Octobre 2007, Volume 4 - Numéro 1

LA POLITIQUE DE SÉCURITÉ DES ACTIFS INFORMATIONNELS DÉMYSTIFIÉE

Lors de votre arrivée dans votre organisation ou au cours des dernières années, on vous a remis un important document à savoir la « Politique de sécurité des actifs informationnels ».

L'informatique est omniprésente et nous sommes constamment appelés à nous servir d'actifs informationnels dans l'exercice de nos fonctions. Leur utilisation doit être réglementée afin d'éviter des incidents qui pourraient avoir des conséquences fâcheuses, autant pour l'employé, son organisation que pour les gens qui bénéficient des services offerts par celle-ci.

Une politique de sécurité est un court texte signalant :

- que les actifs informationnels sont importants pour l'organisation;
- qu'il faut les protéger comme les autres actifs de l'entreprise;
- que la responsabilité de cette protection doit être partagée entre diverses personnes;
- que différents rôles doivent être confiés dans l'organisation quant à la manipulation de ces actifs;
- que l'organisation doit élaborer des normes afin de mettre en œuvre cette politique, l'une d'elles attestant que l'organisation s'engage à prendre des mesures pour assurer la sécurité;
- que le personnel qui sera trouvé coupable d'avoir porté atteinte à cette dernière en subira des conséquences.

Je vous propose donc une série de 5 chroniques expliquant l'importance d'un tel document en tenant compte des aspects humains, légaux, fonctionnels et techniques.

Bonne lecture.
Luis Lalancette, CISSP, conseiller régional en sécurité

À venir dans les prochains numéros

La politique de sécurité et

- L'aspect humain;
- La loi
- L'aspect fonctionnel
- L'aspect technique

LA POLITIQUE DE SÉCURITÉ — C'EST QUOI?

La sécurité des systèmes informatiques vise principalement à garantir les droits d'accès aux données et ressources d'un système à partir de mécanismes d'authentification et de contrôle définis. Elle permet à l'organisation d'attribuer des droits d'accès aux utilisateurs en fonction de ce qui est nécessaire à l'exercice de leurs fonctions, évitant ainsi les erreurs involontaires.

Agence de la santé et des services sociaux de Chaudière-Appalaches
Québec

LA POLITIQUE—C'EST QUOI …

Mais cette dernière va plus loin : elle permet aussi de garantir l'intégrité des données afin qu'elles soient exactes et conformes à ce qui a été saisi, la confidentialité des transactions pour que ne soient pas divulguées les informations à caractère personnel ou privé à la suite d'une perte ou d'une fuite d'informations et la disponibilité des systèmes ayant pour objectif que les informations soient présentes lorsque nécessaire, afin de répondre aux exigences et aux besoins d'affaires de l'établissement.

Nous pourrions associer ces objectifs à un seul mot : la confiance. En exerçant la sécurité des systèmes, l'établissement permet aux usagers d'espérer qu'aucun individu ne pourra usurper son identité pour commettre des actes de nature criminelle, que ses données ne seront pas perdues, qu'aucune personne non autorisée ne pourra avoir accès à ses documents personnels et qu'ils auront accès à des données correspondant à ce qui a été saisi en temps voulu.

Ce sentiment de confiance va encore plus loin : il s'étend aussi à l'usager du système de santé québécois qui s'attend à avoir des services de qualité afin de lui aider à conserver ce qu'il a de plus précieux … sa santé. On doit donc s'assurer que les systèmes soient disponibles en temps opportun et que les renseignements personnels qui y transitent soient protégés de façon adéquate.

Afin de se doter de lignes directrices claires en la matière, un établissement doit se doter d'une **politique de sécurité** dans laquelle seront inscrites l'ensemble des orientations qu'il entend suivre en matière de sécurité.

Cette politique a pour objectifs d'assurer :

- Le respect de la vie privée des individus, notamment la confidentialité des renseignements à caractère nominatif, relatifs aux usagers et au personnel du réseau sociosanitaire;
- La sécurité de l'information au regard de l'utilisation des réseaux informatiques, du RTSS et d'Internet;
- La sécurité de l'information au regard de l'utilisation des actifs informationnels et de télécommunication;
- La sécurité de données corporatives[1].

Elle permet aussi d'assurer le respect des lois à l'égard de l'usage et du traitement de l'information, plus particulièrement les renseignements nominatifs et les informations à caractère confidentiel transmises ou conservées à l'aide d'actifs informationnels et de télécommunication. Elle sert aussi d'outil pour sensibiliser les usagers aux risques visant les systèmes d'information et à la promotion de la collaboration entre les différents usagers des systèmes et, enfin, elle permet de susciter la confiance des usagers envers les systèmes d'information.

LES PRINCIPES DIRECTEURS DE LA POLITIQUE

- Personne ne doit utiliser, modifier, détruire ou transmettre des données confidentielles à des fins autres que celles prévues par son travail. L'accès aux informations devra donc être contrôlé à partir de privilèges d'accès octroyés en fonction du rôle des usagers dans l'organisation et des tâches reliées à l'exercice de leurs fonctions.
- Le droit de l'utilisateur à la confidentialité de l'information qui le concerne ne couvre pas les cas où l'utilisation qu'il fait de cette information ou des actifs informationnels va à l'encontre de la politique ou ses directives. Soyons bien clair ici : cela ne veut pas dire que toutes vos communications sont vérifiées systématiquement. Cependant, *s'il y a un motif raisonnable*, par exemple une enquête de nature criminelle ou à la suite de plaintes répétées à l'endroit de l'usager, l'établissement, à la demande de son directeur, peut avoir accès aux courriels ou autres données de l'usager pour fins d'enquête. De toute façon, personne n'a le temps, l'intérêt ou les moyens de vérifier systématiquement ce que tout le monde fait. Ce serait abusif de la part de l'employeur. Cependant, l'employeur doit s'assurer que le matériel qu'il possède ne soit pas utilisé de façon illicite afin d'agir « en bon père de famille ».
- Chaque utilisateur convient que l'établissement peut procéder à la télésurveillance de l'utilisation qu'il fait de ses actifs et prendre connaissance du contenu des messages qu'il reçoit ou transmet à l'aide de ceux-ci pour les mêmes raisons que celles mentionnées dans le paragraphe précédent.

En termes clairs, l'utilisation des outils informatiques de l'établissement ne devrait se limiter que pour l'exercice des fonctions des usagers et devrait se faire dans le respect des lois en vigueur au Québec. Une simple question de bon sens.

EST-CE QUE JE SUIS CONCERNÉ(E) PAR CETTE POLITIQUE ?

Bien sûr ! La politique de sécurité s'adresse à :

- Tout employé de l'établissement et les professionnels qui y sont attachés administrativement, de façon permanente, temporaire ou ponctuelle;
- Toute personne pouvant utiliser ou ayant accès aux actifs informationnels détenus par l'établissement;
- Tout actif informationnel de l'établissement (système, équipement informatique, équipement de télécommunication, logiciel, base de données résidant dans un équipement informatique, support informatique (clef USB, CD-ROM, etc.), système de transmission de courriels ou de messagerie vocale), peu importe sa localisation;
- Toute information détenue, saisie, traitée ou emmagasinée à même ou à l'aide des actifs informationnels de l'établissement.

Y A-T-IL AUTRE CHOSE QUE CETTE POLITIQUE CONTIENT QUE JE DEVRAIS CONNAÎTRE ?

Certainement ! On y retrouve, entre autres :

- Un registre des responsabilités et autorités afin de connaître les rôles et responsabilités de chacun en matière de sécurité des actifs informationnels. Croyez-moi, vous en faites partie! La sécurité, c'est comme une chaîne : un seul maillon faible rend l'ensemble plus fragile. C'est donc l'affaire de tout le monde si l'on veut que cela fonctionne. Un seul individu qui n'applique pas les règles peut réduire à néant les efforts de tous. **Personne ne peut donc se soustraire à la politique;**
- Une directive spécifiant que l'usage des actifs informationnels est réservé exclusivement à la réalisation des activités de l'établissement. Les actifs entreposés, produits et utilisés par l'établissement en sont sa propriété exclusive;
- Une directive voulant que chaque individu est tenu par la Loi de respecter les droits d'auteur vis-à-vis les ressources qu'il utilise;
- Une directive spécifiant qu'il est interdit de partager ses mots de passe. N'oubliez pas qu'une fois votre mot de passe divulgué, vous ne pouvez pasêtre certains de l'usage que l'on en fera. Même si vous l'avez donné à une personne de confiance, il pourrait toujours se produire des incidents, parfois bien involontaires, sous votre identité;
- Une directive spécifiant qu'il est interdit d'apporter des modifications aux équipements de télécommunication, d'installer des logiciels ou des connexions à d'autres réseaux, par modem ou sans fil, sans l'autorisation du responsable de la sécurité de l'établissement;
- Une directive spécifiant que tout système informatique doit être muni d'un antivirus qui sera mis à jour régulièrement;
- Une directive spécifiant que la destruction de données confidentielles doit se faire selon des standards prévus à cette fin. Rappelez-vous qu'il est facile pour une personne, même sans expérience, de retrouver les données sur un disque même après une dizaine de formatages consécutifs;
- Une directive concernant l'utilisation des portables.

Contraignant tout ca? Pas du tout! La sécurité ne devrait jamais être vue comme une contrainte, mais bien comme un ensemble de règles consenties et appliquées par tous afin d'assurer le bon fonctionnement des systèmes et d'obtenir une utilisation plus harmonieuse des ressources mises à notre disposition. Il s'agit d'un outil pour vous venir en aide et non pour vous créer des difficultés. N'hésitez pas à en parler au personnel informatique en cas de problèmes : cela pourra vous aider à dissiper un grand nombre de malentendus et vous pourriez même échanger des trucs afin de vous faciliter mutuellement le travail.

Et n'oubliez pas l'essentiel : ce n'est qu'ensemble que nous réussirons!

Références :

1. ARMAND, Claude, Guide d'information et de sensibilisation de la Politique de sécurité des actifs informationnels de l'Hôtel-Dieu de Lévis, 2002, 32 p.

Source : Direction des ressources financières, matérielles et informationnelles
Courriel : Luis_Lalancette@ssss.gouv.qc.ca
ISSN : 1710-5692
Dépôt légal — Bibliothèque et archives nationales du Québec, 2007
Bibliothèque et archives Canada, 2007