Les fiches de l'ISIQ – Des guides pratiques pour les entreprises et organisations qui veulent protéger leurs systèmes informatiques

Toutes les entreprises et organisations doivent un jour ou l'autre penser à la protection de ses systèmes informatique.

Mais, par ou commencer?

Par Luc Poulin *M.Sc. CISSP-ISSMP, CISA, ift.a.*
Chef de la sécurité du CRIM
Conseiller senior de sécurité de l'ISIQ

Article pour : Les Affaires.com
12 septembre 2006

Avec la collaboration de Jean-Guy Pelletier
Directeur du développement d'affaires, ISIQ.

La protection des systèmes informatiques

Aujourd'hui plus que jamais, chaque organisation doit protéger ses ressources informationnelles sensibles et critiques. Ce travail de protection peut être plus ou moins facile selon que l'entreprise a des moyens et de l'expertise en sécurité. Mais ce n'est pas le cas pour la majorité des PME québécoises, qui peuvent se sentir démunies devant l'ampleur de cette tâche. La première question qui se pose est : « Par où doit-on commencer ? »

En vue d'aider les entreprises à répondre à cette question, l'Institut de la sécurité de l'information du Québec (ISIQ) a développé et rend disponibles gratuitement sur son site Web 12 fiches thématiques. Les thèmes sont multiples : premières procédures à mettre en place, bonnes pratiques à adopter et solutions minimales à appliquer en vue de protéger les organisations contre les principales menaces et vulnérabilités, etc.

Les fiches, basées sur la norme ISO 17799:2005, indiquent les conditions à remplir pour implanter, maintenir et améliorer le système de gestion de la sécurité de l'information (SGSI). Le modèle suggéré utilise une démarche d'amélioration continue qui comprend quatre étapes récurrentes :

Planifier : Définir le périmètre du SGSI, bâtir la politique de sécurité de l'information, procéder à l'évaluation des risques et préparer le plan d'action de sécurité.

Réaliser : Mettre en place le plan d'action de sécurité, sensibiliser et former le personnel à la sécurité de l'information.

Vérifier : S'assurer que les mesures de sécurité mises en place sont efficaces; effectuer le contrôle des procédures; évaluer la fiabilité des données et réaliser périodiquement des audits du SGSI.

Agir : Mettre en place des mesures correctives et de prévention appropriées, implanter les améliorations du SGSI qui ont été identifiées.

Les fiches de l'ISIQ abordent les thèmes suivants :

- **Thème 0 – Comprendre la sécurité de l'information :** présente les 12 thèmes (fiches) de la sécurité informationnelle et indique leur ordre d'utilisation.
- **Thème 1 – Organiser la sécurité de l'information :** préciser les rôles, responsabilités et qualifications des gestionnaires, utilisateurs, contractuels et fournisseurs de services, propriétaires de ressources informationnelles. Réaliser une analyse de risque. Détailler également les mécanismes de sécurité à mettre en place pour assurer la sécurisation de l'accès des tiers aux informations et ressources de l'entreprise.
- **Thème 2 – Bâtir une politique de sécurité de l'information :** indiquer les éléments à considérer et le contenu de cette politique.
- **Thème 3 – Gérer les risques de sécurité :** analyser et évaluer les menaces, impacts et vulnérabilités auxquels les actifs sont exposés et la probabilité de leur survenance. Déterminer les mesures de sécurité à implanter pour réduire les risques et leur impact à un coût acceptable.
- **Thème 4 – Gérer l'actif informationnel :** procéder à l'inventaire des ressources informationnelles de l'organisation; leur désigner un propriétaire; les catégoriser; déterminer leur niveau de protection et établir les mesures de sécurité à mettre en place, selon la sensibilité des données et le contexte d'utilisation.
- **Thème 5 – Assurer la sécurité liée aux ressources humaines :** informer le personnel des bonnes pratiques à utiliser pour protéger les renseignements confidentiels et nominatifs. Faire un bon usage de leur équipement informatique selon les normes et les règles. Mettre en place un programme de sensibilisation à la sécurité de l'information, de même qu'une procédure d'accueil des nouveaux employés.
- **Thème 6 – Vérifier la conformité :** assurer du respect des lois, des réglementations et des exigences de sécurité, ainsi que de l'efficacité des procédures et des mesures de sécurité en place, en relation avec la politique de sécurité émise par votre entreprise.
- **Thème 7 – Assurer la sécurité physique et environnementale :** préciser les mesures à mettre en place pour sécuriser le matériel et éviter les accès non autorisés dans les locaux, de même que des dommages pouvant affecter les actifs et les opérations quotidiennes.

- **Thème 8 – Contrôler les accès :** gérer et contrôler les accès logiques et physiques aux informations et ressources; détecter les activités non autorisées; préciser les règles à observer concernant l'identifiant et le mot de passe, de même que les autorisations reliées à votre profil d'accès.
- **Thème 9 – Gérer l'exploitation et les télécommunications :** indiquer comment sécuriser les moyens de traitement de l'information, les réseaux de télécommunications et les informations échangées avec vos partenaires et clients.
- **Thème 10 – Gérer les systèmes d'information :** indiquer les règles de sécurité à observer ou à exiger dans l'acquisition, le développement, l'implantation et l'entretien des systèmes d'information.
- **Thème 11 – Gérer les incidents de sécurité :** mettre en place un processus de gestion des incidents et dysfonctionnements de sécurité, puis indiquer les comportements à adopter lors de la détection d'un incident ou d'un dysfonctionnement de sécurité.

Les fiches sont accessibles sur le site Web de l'ISIQ : https://www.isiq.ca/fr/outils/Guides/PME

Note de l'auteur : Plusieurs informations présentées dans cet article sont extraites de la fiche « Comprendre la sécurité de l'information ».