Une "grappe" d'entreprises pour relever le défi de la sécurité de l'information

Le Centre de Recherche Public Henri Tudor poursuit ses travaux de recherche et de transfert sur la sécurité des systèmes d'information, notamment à destination des PME.

La loi du 2 aout 2002, relative à la protection des personnes à l'égard du traitement des données à caractère personnel, concerne la très grande majorité des entreprises luxembourgeoises. Elle traduit une exigence grandissante de toutes les parties prenantes de l'entreprise: clients, personnels, financeurs, fournisseurs… Face à cette demande, la norme ISO/IEC 27001 fournit un langage commun et un corpus d'exigences et de bonnes pratiques pour la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI). Son audience est grandissante dans les pays occidentaux, dans la continuité du très grand nombre de certifications constatées en Asie. Malheureusement, alors que le tissu économique grand-ducal est composé de plus de 90% de PME, celles-ci restent désavantagées par leur manque de ressources et de compétences et la crise n'a fait qu'accentuer ces difficultés.

En 2008 et 2009, le projet "Information Security Management System pour PME" (ISMS-PME), mené par le CRP Henri Tudor et cofinancé par le Ministère de l'Economie et du Commerce extérieur, a permis de faire un premier pas en direction des PME. Un guide méthodologique, des modèles de documents et des outils IT ont été développés et sont maintenant opérationnels. La méthode d'appréciation des risques, le choix des processus, la documentation et la gestion du projet, qui ont fait l'objet d'une approche spécifique aux PME, ont montré leur capacité à réduire les coûts et la durée de déploiement d'un SMSI.

En 2010, le CRP Henri Tudor fait un second pas en inaugurant un modèle de déploiement spécifiquement conçu pour les PME. Le modèle consiste en la création d'une "grappe" d'entreprises s'engageant tant dans le déploiement d'un SMSI que dans un processus commun d'implémentation. Partageant un même projet, les entreprises de la grappe suivent un cycle commun de formation comprenant 8 à 10 sessions réparties sur 5 mois. Entre chaque session, des coachings personnalisés permettent de mettre en pratique les connaissances acquises en formation et d'adapter les modèles et outils. L'objectif est le même pour tout le monde: la certification ISO/IEC 27001.

Le modèle en "grappe" d'entreprises permet:

- de diminuer très sensiblement les coûts de formation,
- de mutualiser les travaux et d'échanger les bonnes pratiques,
- de motiver les entreprises engagées à atteindre leurs objectifs.

Une des clés du modèle réside dans l'adhésion de toutes les entreprises au même calendrier de déploiement!

En fin d'expérimentation, les avantages du modèle développé seront confirmés par les premiers retours d'expérience. En février prochain, une grappe de 5 entreprises sera lancée: 3 entreprises ont déjà confirmé leur participation, mais il reste encore deux places sont disponibles! Toute entreprise intéressée à rejoindre la grappe, ou souhaitant plus d'informations sur l'expérimentation, est invitée à contacter Nicolas Mayer (nicolas.mayer@tudor.lu) avant le 15 janvier 2010.

Ainsi, le CRP Henri Tudor espère compléter son approche en ajoutant la méthode aux outils pour composer un dispositif complet pour les PME. D'autres modèles de transfert sont en cours d'étude et permettront d'adresser les PME via les réseaux de consultants labellisés. Les expérimentations menées et le panel des entreprises déjà certifiées dans les pays étrangers confirment que l'ISO/IEC 27001 est accessible et potentiellement adaptée aux PME. Il convient simplement de les y aider.

Sébastien Pineau, Product Manager, responsable du projet ISMS-PME et Nicolas Mayer, Product Manager Security & Continuity Management