Extrait du Spyworld Actu

http://www.spyworld-actu.com/spip.php?article9148

La norme de sécurité ISO 27001 est-elle utile à l'entreprise ?

- Informatique - Sécurité Informatique -

Date de mise en ligne : lundi 3 novembre 2008

Spyworld Actu

C'est la question que s'est posé récemment le Club de la sécurité de l'information français au cours d'une conférence. Seules 11 entreprises françaises sont aujourd'hui certifiées ISO 27001.

Le Clusif (Club de la sécurité de l'information français) s'interrogeait fin octobre sur l'utilité de la certification ISO 27001. Cette norme est à la sécurité des systèmes d'information ce que l'ISO 9001 est à la qualité. Depuis 2005, elle donne aux entreprises un cadre de bonnes pratiques reconnues, et une démarche visant à la mise en place d'un Système de management de la sécurité de l'information (SMSI). Ce dernier établit une politique de sécurité, des objectifs, et les moyens mis en oeuvre pour les atteindre, voir encadré.

Toutes les entreprises sont concernées

Malgré l'aspect vertueux de la norme ISO 27001, elle est très peu utilisée en France. Sur les 4500 sociétés certifiées dans le monde, seulement 11 d'entre elles sont françaises. Difficile de dire à quoi est due cette frilosité. Toutes les entreprises sont concernées, surtout celles qui doivent démontrer à leurs clients et partenaires la mise en place de bonnes pratiques de sécurité.

La conférence du Clusif a en outre mis en avant les bénéfices de la 27001, et combattu les préjugés. Le coût ne saurait être un frein. « La certification permet d'éviter l'accumulation d'audits externes, très consommateurs en ressources », note ainsi Stéphane Duproz, directeur général de TelecityGroup. Selon l'entreprise et le périmètre de la certification, la durée d'un projet 27001 varie de 9 mois à plus d'un an. D'où un coût jours/hommes en fonction de la taille de l'entreprise et du périmètre choisi. Coût auquel il faut ajouter l'audit initial (entre 5 et 10 jours) puis le contrôle tous les 6 mois afin de conserver la certification. De fait, si nombre d'entreprises entreprennent la démarche, peu vont jusqu'au bout de la certification. La méthode, structurante pour la sécurité, suffit à beaucoup. Les coûts sont réduits en n'allant pas jusqu'à l'obtention du cachet. Cependant, cette approche semble risquée. « Un SMSI est entropique, et a tendance à partir dans tous les sens, prévient Alexandre Fernandez-Toro, auditeur de certification, et assistant dans la mise en oeuvre, du cabinet HSC, la certification sert d'objectif et de couperet afin de s'assurer de tenir les objectifs, et de lutter contre l'impopularité en interne conséquente des efforts mis en oeuvre ».

Zoom sur le SMSI et la démarche de certification

Le Système de management de la décurité de l'information, SMSI, vise à l'amélioration continue du niveau de sécurité, dans le contexte des risques métiers d'une entreprise. La démarche conduisant à la certification assure l'orchestration des mesures de sécurité selon un modèle dit PDCA : Plan, Do, Check, Act, soit respectivement Planifier, Mettre en oeuvre, Contrôler, Améliorer.

Le point de départ d'une démarche de certification est l'appréciation des risques. Ce qui implique de faire le point sur les pratiques internes en matière de sécurité, de vérifier que les mesures déjà en place sont en cohérence avec des objectifs.

Sont définies dans la norme 133 mesures de sécurité, classées dans 11 sections. La rédaction d'une documentation prend une place importante, selon le principe « écrire ce que l'on a fait et faire ce que l'on a écrit ». Ce canevas structure la conduite de la sécurité de l'entreprise en implémentant des contrôles et des indicateurs de mesure de la

performance et de l'efficacité du SMSI.

Post-scriptum :

http://www.01net.com/editorial/3948...