Protection de lâ□□information : se former, Ã©vite les fuites d'informations stratÃ©giques
Internet
PostÃ© par : JulieM
PubliÃ©e le : 31/10/2011 11:30:00

Plus que jamais **la protection de lâ□□information est une donnÃ©e fondamentale** Ã prendre en compte. En effet, la fuite dâ□□une information peut avoir aujourdâ□□hui des consÃ©quences graves. Lâ□□entreprise doit donc nÃ©cessairement mettre en place un processus Ã©prouvÃ© lui permettant de se prÃ©munir de ce type de menace, nous dit **Mikael MASSON**, Directeur Risk Management et Cybercrime de SDN International

Ce travail de fond doit Ãªtre minutieusement prÃ©parÃ© au niveau du Top Management de lâ□□entreprise et prendre en compte un ensemble de donnÃ©es complÃ©mentaires. Il est utile de prendre de la hauteur et de raisonner de maniÃ¨re intÃ©grÃ©e pour que la dÃ©marche soit rÃ©ellement couronnÃ©e de succÃ¨s.

Cela passe nÃ©cessairement par la mise en place de dÃ©marche de formation et de sensibilisation multi facette . ConcrÃ¨tement, il est utile de sâ□□appuyer sur une mÃ©thodologie reposant sur un triptyque : gouvernance, architecture technique, ressources humaines.

Cette dÃ©marche est une nÃ©cessitÃ© et doit permettre dâ□□aborder tous les points stratÃ©giques Ã couvrir. Nâ□□oublions pas non plus que ces projets doivent Ãªtre partagÃ©s et compris par tous les collaborateurs de lâ□□entreprise.

Au niveau du sÃ©quencement, il est donc important de sâ□□appuyer sur trois grandes Ã©tapes :

- Audit

Il est tout dâ□□abord utile de bien connaÃ®tre le processus organisationnel de lâ□□entreprise, son mode de fonctionnement, la nature de ses activitÃ©s et donc lâ□□approche critique des informations dont elle dispose. Cet audit permet de comprendre les rÃ´les de chacun et de qualifier le type dâ□□information dont dispose la sociÃ©tÃ©, de connaÃ®tre son mode de circulation, les modalitÃ©s pratiques pour y accÃ©derâ□¦ Tous ces Ã©lÃ©ments ont pour objectifs de cartographier au plus prÃ©cis les modalitÃ©s organisationnelles liÃ©es Ã la gestion et Ã la diffusion de lâ□□information.

- PrÃ©conisation

A la suite de lâ□□audit, un travail de synthÃ¨se est rÃ©alisÃ©, mettant en avant les Ã©lÃ©ments recueillis. Ce travail doit Ãªtre factuel et prÃ©senter clairement la problÃ©matique. Il doit aussi permettre Ã lâ□□entreprise de mettre en place un plan dâ□□action et de formation qui mettra en avant tout le processus nÃ©cessaire pour se prÃ©munir de la fuite dâ□□informations sensibles. Cette recommandation constituera le chemin de fer Ã suivre et donnera des lignes directrices sur

les plans techniques, organisationnels et humains.

- Mise en Å□uvre

Ce dernier point concerne le dÃ©ploiement et lâ□□implÃ©mentation des mesures prÃ©sentÃ©es dans la prÃ©conisation.

Enfin, le volet Ressources Humaines est Ã©galement Ã prendre en compte. Il faut Ã©valuer le niveau de la Â« culture sÃ©curitÃ© Â» de lâ□□entreprise et sensibiliser les collaborateurs sur les sujets de protection de l'information et aussi sur la nÃ©cessitÃ© de dÃ©tecter les comportements dÃ©viants de leurs collÃ¨gues quand Ã§a arrive . La prÃ©servation de lâ□□information est donc un facteur Ã surveiller. Cela ne sâ□□improvise pas et combine de nombreuses donnÃ©es complÃ©mentaires. Les entreprises doivent prendre en compte ces derniÃ¨res et positionner la sÃ©curitÃ© au centre de leur modÃ¨le organisationnel.