Les entreprises françaises plus concernées par leur sécurité informatique

- Informatique - Sécurité Informatique -

Date de mise en ligne : jeudi 29 juin 2006

Selon la dernière étude du Clusif sur les politiques de sécurité informatique, les sociétés françaises ont pris conscience, dans leur majorité, de la nécessité de protéger leur système d'information. Sans toujours prévoir d'augmenter leur budget.

Les entreprises françaises sont de plus en plus nombreuses à mettre en place une politique de protection de leur système d'information. Et pourtant, elles rechignent à dégager des budgets en conséquence. C'est la tendance qu'a observée le Club de la sécurité des systèmes d'information français (Clusif), dans son étude "Politiques de Sécurité Informatique & Sinistralité en 2005", présentée le 28 juin.

Dans ce document de 58 pages, l'organisme synthétise les témoignages d'un échantillon représentatif de 400 entreprises de plus de 200 salariés, tous secteurs confondus. Résultat : 56% des sociétés françaises étaient dotées en 2005 d'une politique de sécurité informatique (PSI) contre 41% il y a deux ans lors de la précédente étude.

« Il y a une prise de conscience des dirigeants sur la nécessité de mettre en place une politique de sécurité au sein de l'entreprise », commente pour ZDNet.fr Laurent Bellefin, directeur sécurité du cabinet de conseil SoluCom et coordinateur de l'étude.

« Cela s'explique notamment par la pression des auditeurs des comptes des entreprises qui étudient désormais les risques opérationnels liés à la sécurité informatique. Certains assureurs ajoutent également une clause excluant la couverture en cas de problèmes liés par exemple aux virus. »

Une forte volonté de contrôle des RSSI

Mais cette prise de conscience ne s'accompagne pas toujours d'un renforcement des budgets dédiés à la sécurité. Le Clusif note que seulement 38% des entreprises prévoient d'augmenter cette enveloppe, 46% préfèrent la garder constante, 4% le réduire et 12% n'ont pas pris de décision. « Les dirigeants sont difficiles à convaincre. Ils ne sont pas encore totalement rassurés quant à la bonne utilisation des budgets qui doivent être consentis pour la sécurité du système d'information », poursuit Laurent Bellefin.

Par ailleurs, l'étude met en avant une « forte volonté de contrôle » de la part des responsables de la sécurité du système d'information (RSSI). Bon nombre d'entre eux préfère bloquer l'usage de nouvelles techniques plutôt que de chercher une solution pour son déploiement dans l'entreprise. Ainsi 76% des entreprises interdisent l'accès aux webmail, 73% refusent l'utilisation de la VoIP, 56% prohibent le Wi-Fi et 43% les PDA et smartphones.

« Cette position de fermeté est difficile à ternir sur le long terme », estime l'étude. « Une opposition formelle et continue sera ressentie comme un frein à l'innovation ». Mieux vaut « s'efforcer de proposer des règles et solutions permettant de contenir les risques, et de sensibiliser les utilisateurs aux bonnes pratiques à adopter », conclut le Clusif.

Quant aux différents types d'incidents vécus par les entreprises : seuls 36% ont comme source des virus et 2% des intrusions sur le système d'information. La majeure partie, soit 56%, proviennent d'erreurs de conception ou de déploiement des logiciels, 47% de coupures d'électricité ou de télécoms, 46% d'erreurs d'utilisation.

Les mairies et hôpitaux en retard sur les entreprises

Le Clusif a également analysé les stratégies de sécurité des mairies de plus de 30.000 habitants et des hôpitaux publics. « D'une manière générale, les mairies et hôpitaux sont en retard sur les entreprises en matière de sécurité de leur système d'information. Le principal frein étant le budget, suivi du manque de compétences disponibles », résume Laurent Bellefin.

Ainsi seulement 50% des villes ont mis en place une politique de sécurité. Mais elles sont 72% à ne pas disposer de plan de continuité de service pour leur réseau interne, pointe l'étude. En cas de panne du système d'information, rien n'est prévu pour sa restauration. Du côté des centres hospitaliers, c'est pire puisque ils sont juste 40% a avoir intégré une politique de sécurité.

Mais d'autres chiffres font plus froid dans le dos : 70% s'estiment en complète conformité avec la Cnil (Commission nationale de l'informatique et des libertés) en matière de protection des données personnelles. Environ 20% indiquent avoir pris des dispositions uniquement pour « les traitements les plus sensibles », 5% ne savent pas et les 5% restants reconnaissent ne pas être en conformité avec la loi informatique et liberté.

Post-scriptum :

http://www.zdnet.fr/actualites/info...