

Insolite : Les salariés, principal risque pour les données des PME

Insolite

Posté par : JulieM

Publié le : 12/3/2010 0:00:00

La nouvelle étude annuelle commandée par Absolute Software montre que **les salariés ne tiennent pas compte des bonnes pratiques** destinées à sécuriser leurs ordinateurs portables et les données qui s'y trouvent

Absolute® Software Corporation, spécialiste des solutions de récupération d'ordinateurs volés, de protection des données et de gestion sécurisée des ordinateurs, et Ponemon Institute, un cabinet de recherche spécialisé dans la gestion de l'information, publie aujourd'hui les résultats de la deuxième étude annuelle « Human Factor in Laptop Encryption ». Cette étude porte sur l'impact du facteur humain sur la sécurisation des données en entreprise.

Selon les conclusions de l'étude, les managers d'entreprise feraient courir des risques importants aux données confidentielles comme les dossiers clients, les informations liées à la santé et toute autre sorte de données privées. Malgré les efforts des départements informatiques, beaucoup de managers désactivent trop souvent les solutions de cryptage qui se trouvent sur leurs ordinateurs. En cas de vol d'ordinateur, les données les plus sensibles de l'entreprise se retrouvent ainsi entre les mains du voleur ou de toute autre personne qui chercherait à nuire à l'entreprise.



Plus précisément, cette étude est dédiée à la façon dont sont perçues l'efficacité des solutions de cryptage et les actions menées par les responsables IT et managers d'entreprise pour sécuriser leurs ordinateurs portables. Cette année, en plus des Etats-Unis, l'étude couvre le Royaume-Uni, la Suède, le Canada, la France et l'Allemagne. Les résultats montrent que 15% des managers allemands et 13% des managers suédois ont désactivé leur solution de cryptage. En comparaison, 52% des canadiens, 53% des anglais et 50% des français ont fait de même alors que les américains arrivent en tête avec 60% des managers ayant trouvé un moyen de contourner la politique de sécurisation des données de leur entreprise.

Si les allemands et les suédois sont moins enclins à se passer de leur solution de cryptage, ils ne cherchent pas non plus à crypter toutes leurs données : 49% des responsables informatiques suédois ayant déclaré avoir perdu ou s'être fait voler un ordinateur portable ont admis que cela a conduit à une violation de données. C'est également le cas pour un peu moins de 46% des responsables informatiques allemands et 50% de responsables IT canadiens. Les Etats-Unis suivis de près par le Royaume-Uni, arrivent en tête avec respectivement 72% et 61%. Les

Français nous ont déclaré qu'à 28% que le vol ou la perte d'un ordinateur a donné lieu à une violation de données.

D'autres résultats marquants pour la France :

☛ **52%** des responsables IT pensent que le cryptage rend superflue l'application de toute autre mesure de sécurité et 49% des managers sont du même avis.

☛ **45%** des managers interrogés pensent que le cryptage empêche les cybercriminels d'accéder aux données d'un ordinateur et de les voler et 46% des responsables IT partagent la même opinion.

☛ **31%** des managers déclarent noter leur mot de passe sur un document comme un post-it par exemple afin de pouvoir s'en souvenir et 25% admettent le partager avec d'autres personnes. A l'inverse, aucun responsable IT français ne note son mot de passe et seulement 10% le partagent avec d'autres personnes au cas où ils l'oublieraient.

« Cette étude montre bien que les managers dépendent trop de leur solution de cryptage pour protéger et sécuriser les données confidentielles qui se trouvent sur leur ordinateur. Or, si le cryptage est un outil de sécurité nécessaire, certains comportements inappropriés comme la désactivation de la solution, le partage du mot de passe ou l'utilisation d'un réseau sans fil non sécurisé peuvent considérablement réduire son efficacité. » explique le **Dr. Larry Ponemon**.

« L'étude montre que les outils utilisés par les départements informatiques et les départements de conformité sont encore insuffisants pour renforcer les politiques de l'entreprise particulièrement en ce qui concerne la protection des données sensibles. Malgré de réels efforts comme le déploiement de la technologie de cryptage, ceux-ci sont souvent contrariés par des comportements inappropriés de la part des utilisateurs. Quel que soit le pays où se situe l'entreprise, il est important de savoir jusqu'à quel niveau les employés peuvent être à l'origine d'une potentielle violation de données. Le facteur humain doit réellement être pris en compte dans les plans de sécurité des ordinateurs » déclare **John Livingston**, chairman et CEO d'Absolute Software.

L'étude « Human Factor in Laptop Encryption » a été menée auprès d'informaticiens incluant les responsables sécurité informatique, et auprès de managers n'ayant pas de responsabilité informatique. Les personnes interrogées étaient réparties dans 20 entreprises situées aux Etats-Unis, au Canada, en France, en Allemagne et en Suède.

[Les résultats de l'étude](#)