Le cryptage des donnÃ©es, une solution nÃ©cessaire mais insuffisante !
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 26/10/2009 0:00:00

Lâerreur humaine nâest pas toujours Ã lâorigine de toutes les violations de donnÃ©es, **Stephen Midgley** dâAbsolute Software revient sur **les piÃ¨ges du cryptage et sur les mesures de sÃ©curitÃ©** Ã appliquer pour la sÃ©curitÃ© des Ã©quipements mobiles.

Nâimporte quel chef dâentreprise vous dira quâil est impossible de contrer lâerreur humaine. Des erreurs peuvent toujours arriver et elles peuvent avoir un effet nÃ©gatif sur les donnÃ©es confidentielles des entreprises.

Le travail mobile ou nomade est en plein essor et le risque de se faire voler un ordinateur portable ou tout autre Ã©quipement mobile augmente avec. Les ordinateurs qui sont oubliÃ©s dans les bars, les trains ou encore les taxis sont souvent volÃ©s et les voleurs ont bien conscience que ce nâest pas tant le matÃ©riel qui reprÃ©sente une valeur marchande lâimportance mais bien les donnÃ©es qui se trouvent dessus.

Que faire pour protÃ©ger les donnÃ©es de lâinattention des utilisateurs ou face au personnes malveillantes ?

Le cryptage doit Ãªtre intÃ©grÃ© dans toute stratÃ©gie de sÃ©curitÃ©. GÃ©nÃ©ralement, câest une solution qui fonctionne bien et qui permet de protÃ©ger les donnÃ©es des regards indiscrets, cependant les entreprises ne prennent pas suffisamment la peine de le dÃ©ployer.

Les piÃ¨ges du cryptage

Une Ã©tude menÃ©e rÃ©cemment par lâinstitut Ponemon montre que 86% des experts sÃ©curitÃ© ont dÃ©jÃ dÃ» faire face Ã des vols dâordinateurs portables dans leur entreprise. Dans 56% de ces cas, la perte dâun ordinateur portable a engendrÃ© une violation des donnÃ©es confidentielles. Ce mÃªme rapport constate que 40% des responsables sÃ©curitÃ© nâont pas installÃ© de solution de cryptage sur leurs ordinateurs portables. Cela soulÃ¨ve une question : si mÃªme les experts en sÃ©curitÃ© nâutilisent pas les technologies Ã leur disposition sur qui peut-on compter dâautre au sein dâune entreprise ?

Une telle nÃ©gligence explique pourquoi la grande majoritÃ© des ordinateurs portables volÃ©s contiennent encore des donnÃ©es non protÃ©gÃ©es par le cryptage. Câest pour cette raison que les entreprises ont besoin dâun filet de sÃ©curitÃ© leur permettant de supprimer Ã distance des donnÃ©es contenues dans un ordinateur volÃ©.

Lâ□□Ã©tude de lâ□□**Institut Ponemon** prouve que les entreprises peuvent attendre longtemps avant que le personnel ne se dÃ©cide Ã utiliser tous les outils de sÃ©curitÃ©, comme le cryptage, mis Ã leur disposition. Pour que cela soit efficace, les utilisateurs doivent systÃ©matiquement suivre la politique de cryptage de lâ□□entreprise, ce qui fait porter une lourde responsabilitÃ© aux employÃ©s. Au lieu de cela, les responsables dâ□□entreprises doivent Ãªtre rÃ©alistes et avoir un plan imparable pour protÃ©ger les donnÃ©es en cas de vol.

Si le vol est ciblÃ©, que les voleurs sont expÃ©rimentÃ©s et que les informations sont intÃ©ressantes, alors les solutions de cryptage mises en place pourront Ãªtre vulnÃ©rables.

Et le risque ne sâ□□arrÃªte pas lÃ . **Selon lâ□□institut Gartner**, 70% des vols de donnÃ©es sont commis par les employÃ©s. Une fois de plus la fiabilitÃ© du cryptage est remise en question quand les employÃ©s quittent le bureau avec un ordinateur portable contenant lâ□□authentification requise pour accÃ©der aux donnÃ©es. De plus les conclusions dâ□□une lâ□□enquÃªte menÃ©e par Deloitte montrent que deux tiers des cadres sâ□□attendent Ã une augmentation des dÃ©lits internes dans les deux prochaines annÃ©es notamment avec la rÃ©cession actuelle qui entraÃ®ne des gels des salaires et des promotions dans de nombreuses entreprises. Par consÃ©quent, les employÃ©s mÃ©contents seront eux aussi de plus en plus nombreux.

ArmÃ©s de mots de passe et des clÃ©s de cryptage nÃ©cessaires pour accÃ©der aux donnÃ©es, les employÃ©s malhonnÃªtes reprÃ©sentent une menace qui ne peut Ãªtre contrÃ©e uniquement par le cryptage.

Chercher les alternatives

Le cryptage fait partie intÃ©grante de tout plan de sÃ©curitÃ© de donnÃ©es efficace. Mais pour renforcer la sÃ©curitÃ©, une autre option est possible comme les logiciels permettant de localiser et suivre les ordinateurs portables volÃ©s et dâ□□effacer les donnÃ©es dÃ¨s quâ□□une connexion rÃ©seau est Ã©tablie, afin que personne ne puisse avoir accÃ¨s aux donnÃ©es sensibles. Une fois que le voleur se connecte Ã Internet, le logiciel peut ensuite localiser lâ□□ordinateur portable et, dans certains cas, lâ□□Ã©quipe de rÃ©cupÃ©ration peut le ramener Ã son propriÃ©taire. En complÃ©ment des mesures standards comme les anti-vols ou cadenas, les anti-virus et les anti-spams, les entreprises ont une variÃ©tÃ© dâ□□outils disponibles pour lutter contre le vol dâ□□ordinateurs portables.

En rÃ©sumÃ©

Des accidents se produiront toujours, les vols en internes vont certainement augmenter et les ordinateurs portables continueront Ã Ãªtre volÃ©s. Comme nous lâ□□avons vu, le cryptage nâ□□est pas la seule mesure de prÃ©vention pour contrer les violations de donnÃ©es confidentielles. Il est vital que les entreprises aient un moyen pour accÃ©der Ã lâ□□ordinateur portable en cas de vol, soit pour la suppression des donnÃ©es Ã distance ou pour rÃ©cupÃ©rer lâ□□appareil. En anticipant le pire, les entreprises pourront sâ□□armer contre le vol de donnÃ©es.