

SafeNet : S curit  des donn es stock es dans les environnements virtuels
Internet

Post  par : JulieM

Publi e le : 28/11/2011 13:30:00

Le chiffrement appara t comme la solution privil gi e bien que 69 % des entreprises privil gient toujours la combinaison « nom d utilisateur - mot de passe » pour prot ger l acc s aux informations.

Alors que les f tes de fin d ann e approchent   grand pas, bon nombre d entre nous ont d j  entam  leurs courses sur Internet afin d acheter des cadeaux pour leurs proches.

Mais alors que la cybercriminalit  et les failles de s curit  sont devenues une r alit  quasi quotidienne, quelles sont les mesures mises en  uvre par les entreprises pour s assurer que les donn es personnelles et les informations de paiement ne sont pas d rob es de fa on frauduleuse ? Une r cente  tude men e par SafeNet, Inc., leader mondial de la protection des donn es, aupr s de 170 cadres de s curit  informatique dans l ensemble de la zone EMEA, confirme que la s curit  en environnement virtualis  constitue une priorit  absolue pour 46 % des personnes interrog es, juste apr s la s curit  du Cloud, cit e par 52 % d entre elles.



La virtualisation pose de s rieuses difficult s aux  quipes charg es de la s curit  au sein des entreprises, notamment pour celles qui doivent se conformer au standard PCI DSS qui porte sur la s curit  des donn es bancaires: 63 % des personnes interrog es ont d clar  que cela avait eu un impact sur la strat gie de mise en conformit  et de gestion du risque de leur entreprise, dans la mesure o ¹ les p nalit s encourues incitaient fortement   respecter ces consignes.

Fait impressionnant : 70 % des personnes interrog es ont indiqu  avoir d j  stock  des donn es sensibles dans des machines virtuelles (35 %), dans un Cloud priv  (26 %) ou public (9 %), tendance qui est non seulement irr versible mais qui  clipse de loin toutes les autres,   la fois en termes de rythme et d  chelle d adoption. Ce ph nom ne ne peut d ailleurs que s acc lerer et prendre de l ampleur. Les donn es h berg es dans un environnement multi-utilisateurs constituent par cons quent une pr occupation majeure pour 55 % des responsables de s curit  informatique.

En effet, 53 % d entre eux s inqui tent de ce que les administrateurs du Cloud disposent d un acc s illimit  aux donn es, tandis que 50 % des personnes interrog es se plaignent du manque de visibilit  sur les conditions de stockage des donn es dans le Cloud.

Et pourtant, lorsqu il s agit de mettre en place des politiques d entreprise pour g rer l acc s aux donn es, 69 % des entreprises indiquent s en tenir uniquement au nom

d utilisateur et au mot de passe pour prot ger l acc s aux informations.

Cependant, pour r pondre aux crit res PCI DSS et s curiser efficacement les donn es sensibles en environnements virtualis s, de nombreuses entreprises commencent   recourir   de solides contr les de s curit  proactifs par chiffrement. L tude r v le que le chiffrement est en fait la solution de protection des donn es privili e par la majorit  des personnes interrog es, avec la r partition suivante :

R partition des solutions de chiffrements :

  des e-mails 38 %

  de disque 36 %

  des fichiers 35 %

  des bases de donn es 33 %

  de bout en bout 34 %

  des donn es d application 21 %

  NAS 12 %

  SAN 19 %

  *De nos jours, les technologies et techniques d impl mentation ont consid rablement  volu  et les entreprises modifient leur strat gie de mise en conformit  afin d y inclure le chiffrement d s le d but du programme*  , d clare **Alexandre Pinto**, directeur technique senior et  valuateur de s curit  qualifi  chez Cipher Security.