SafeNet : Sécurité des données stockées dans les environnements virtuels
Internet
Posté par : JulieM
Publiée le : 28/11/2011 13:30:00

Le chiffrement apparaît comme la solution privilégiée bien que 69 % des entreprises privilégient toujours la combinaison « nom d'utilisateur - mot de passe » pour protéger l'accès aux informations.

Alors que les fêtes de fin d'année approchent à grand pas, bon nombre d'entre nous ont déjà entamé leurs courses sur Internet afin d'acheter des cadeaux pour leurs proches.

Mais alors que la cybercriminalité et les failles de sécurité sont devenues une réalité quasi quotidienne, quelles sont les mesures mises en uvre par les entreprises pour s'assurer que les données personnelles et les informations de paiement ne sont pas dérobées de façon frauduleuse ? Une récente étude menée par SafeNet, Inc., leader mondial de la protection des données, auprès de 170 cadres de sécurité informatique dans l'ensemble de la zone EMEA, confirme que la sécurité en environnement virtualisé constitue une priorité absolue pour 46 % des personnes interrogées, juste après la sécurité du Cloud, citée par 52 % d'entre elles.

La virtualisation pose de sérieuses difficultés aux équipes chargées de la sécurité au sein des entreprises, notamment pour celles qui doivent se conformer au standard PCI DSS qui porte sur la sécurité des données bancaires: 63 % des personnes interrogées ont déclaré que cela avait eu un impact sur la stratégie de mise en conformité et de gestion du risque de leur entreprise, dans la mesure où les pénalités encourues incitaient fortement à respecter ces consignes.

Fait impressionnant : 70 % des personnes interrogées ont indiqué avoir déjà stocké des données sensibles dans des machines virtuelles (35 %), dans un Cloud privé (26 %) ou public (9 %), tendance qui est non seulement irréversible mais qui éclipse de loin toutes les autres, à la fois en termes de rythme et d'échelle d'adoption. Ce phénomène ne peut d'ailleurs que s'accélérer et prendre de l'ampleur. Les données hébergées dans un environnement multi-utilisateurs constituent par conséquent une préoccupation majeure pour 55 % des responsables de sécurité informatique.

En effet, 53 % d'entre eux s'inquiètent de ce que les administrateurs du Cloud disposent d'un accès illimité aux données, tandis que 50 % des personnes interrogées se plaignent du manque de visibilité sur les conditions de stockage des données dans le Cloud.

Et pourtant, lorsqu'il s'agit de mettre en place des politiques d'entreprise pour gérer l'accès aux données, 69 % des entreprises indiquent s'en tenir uniquement au nom d'utilisateur et au mot de passe pour protéger l'accès aux informations.

Cependant, pour répondre aux critères PCI DSS et sécuriser efficacement les données sensibles en

environnements virtualisés, de nombreuses entreprises commencent à recourir à de solides contrôles de sécurité proactifs par chiffrement. L'étude révèle que le chiffrement est en fait la solution de protection des données privilégiée par la majorité des personnes interrogées, avec la répartition suivante :

Répartition des solutions de chiffrements :

- des e-mails 38 %

- de disque 36 %

- des fichiers 35 %

- des bases de données 33 %

- de bout en bout 34 %

- des données d'application 21 %

- NAS 12 %

- SAN 19 %

« *De nos jours, les technologies et techniques d'implémentation ont considérablement évolué et les entreprises modifient leur stratégie de mise en conformité afin d'y inclure le chiffrement dès le début du programme* », déclare **Alexandre Pinto**, directeur technique senior et évaluateur de sécurité qualifié chez Cipher Security.