La virtualisation relÃ¨ve dâ□□un vÃ©ritable choix stratÃ©gique des entreprises
Internet
PostÃ© par : JulieM
PubliÃ©e le : 23/10/2009 15:00:00

Avec la montÃ©e en puissance des rÃ©seaux virtuels, lâ□□adoption de la **nouvelle technologie de virtualisation devient incontestablement une rÃ©alitÃ© pour les entreprises.**

Mais les entreprises de type SME ou petites/moyennes structures ne peuvent encore aujourdâ□□hui bÃ©nÃ©ficier de cette innovation estimÃ©e Ã la fois trop complexe et coÃ»teuse.

Beaucoup de SME se montrent aujourdâ□□hui rÃ©ticentes Ã la migration vers cette nouvelle technologie pour 3 principales raisons : la complexitÃ© de management, le coÃ»t Ã©levÃ© et lâ□□installation peu compatible avec les infrastructures existantes.

Andreas Asander, VP Product Management de Clavister, dÃ©clare : â□□*En amont de la migration vers un environnement virtuel, les entreprises intÃ©ressÃ©es sont invitÃ©es Ã se former aux bonnes pratiques dâ□□usage propres Ã cette technologie, ceci pour en profiter dans les meilleures conditions. Les petites entreprises rÃ©alisent progressivement que la virtualisation nâ□□est pas exclusivement rÃ©servÃ©e aux grands comptes ayant les moyens financiers de dÃ©ployer cette technologie. Le choix de la virtualisation dÃ©pend du type dâ□□infrastructure informatique existante, pour ce faire la rÃ©alisation dâ□□un audit interne sâ□□avÃ¨re indispensable.* Â»

Andreas Asander ajoute : Â« *Les entreprises doivent impÃ©rativement prendre en compte le critÃ¨re majeur de la sÃ©curitÃ© IT dans un projet de dÃ©ploiement dâ□□infrastructure virtualisÃ©e. Nous avons rÃ©cemment fait le constat que les entreprises ayant installÃ© des serveurs virtuels avaient fait involontairement lâ□□impasse sur les aspects sÃ©curitÃ©, pensant Ã tort que ceux-ci ne nÃ©cessitaient*

aucune configuration. Â»

â□□*Dans lâ□□Ã©lan de pouvoir profiter des nombreux avantages offerts par la virtualisation, beaucoup dâ□□entreprises omettent de gÃ©rer comment ce nouvel environnement pourrait affecter leurs politiques de sÃ©curitÃ©. Souvent ces projets de dÃ©ploiement sont managÃ©s directement par le responsable serveur dÃ©signÃ© par lâ□□entreprise et le chef de la sÃ©curitÃ© est souvent mis dans la boucle longtemps aprÃ¨s, ou bien mÃªme Ã©cartÃ© !. Lorsque les entreprises implÃ©mentent une solution de virtualisation, il est trÃ¨s dangereux de penser que la sÃ©curitÃ© est induiteâ¦les menaces restant potentiellement prÃ©sentes.* Â»

Afin dâ□□accompagner les entreprises qui font le choix de dÃ©ployer une infrastructure virtualisÃ©e, **Clavister a mis en place un vÃ©ritable plan dâ□□actions qui sâ□□appuie sur 5 importantes Ã©tapes :**

Â· RedÃ©finir la politique sÃ©curitÃ© interne pour permettre lâ□□implÃ©mentation dâ□□un environnement virtuel,

Â· Recommander lâ□□utilisation de gateways sÃ©curisÃ©s au sein de lâ□□infrastructure virtualisÃ©e,

Â· Garantir la protection du centre dâ□□administration virtualisÃ© et autoriser lâ□□accÃ¨s via un rÃ©seau indÃ©pendant,

Â· Identifier et limiter le nombre dâ□□administrateurs rÃ©seaux, ayant accÃ¨s au rÃ©seau virtualisÃ©,

Â· Mesurer et tester rÃ©guliÃ¨rement le niveau de sÃ©curitÃ© du rÃ©seau de lâ□□entreprise.

Pour plus dâ□□informations pour dÃ©ployer une infrastructure virtualisÃ©e, Clavister a rÃ©alisÃ© un **whitepaper sur cette thÃ©matique disponible**