60% des serveurs virtualisés moins sécurisés que les serveurs physiques

Le cabinet Gartner revient sur la problématique, ô combien sensible, de la sécurité des serveurs virtalisés. Sa dernière étude en la matière n'a rien d'encourageant.

Selon le cabinet d'analyses, 60 % des serveurs virtualisés seront moins sécurisés que les serveurs physiques qu'ils seront amenés à remplacer à partir de 2012. De quoi refroidir les velléités d'un DSI jeté corps et âme dans des opérations de consolidation de serveurs. Néanmoins, la prise de conscience est là puisque la situation évoluera dans le bon sens les années suivantes. En 2015, ce sont moins de 30 % des serveurs virtuels qui afficheront un niveau de sécurité inférieur à leurs prédécesseurs.

La raison de cette situation étonnante? Les projets de déploiements des technologies de virtualisation se décideraient sans impliquer les équipes liées à la sécurité des systèmes. Si *« la virtualisation n'est pas intrinsèquement insécurisé*, rassure Neil MacDonald, vice président au Gartner, *cependant, la plupart des charges de travail virtualisées sont déployées de manière non sécurisée. »* Une conséquence directe de *« l'immaturité des outils et des processus et la formation insuffisante des agents, des revendeurs et des consultants »*.

Six menaces sur le data center

Quelles menaces pèsent particulièrement sur un centre de données exploitant des technologies de virtualisation? L'analyste en dénombre pas moins de six. En premier lieu, l'absence de prise en compte de la problématique sécuritaire dans les projets de virtualisation autre que les mesures de protection habituelle. Une situation constatée dans 40 % des cas. Autre menace, les risques induits par les brèches de sécurités forcément présentes (comme toutes applications informatiques) dans les couches des logiciels de virtualisation. A la différence qu'une vulnérabilité exploitées dans un hyperviseur donnera accès à l'ensemble des machines virtualisés derrières. Quelques sueurs froides en perspectives face aux pirates qui ne manqueront pas de tenter d'exploiter ces éventuelles failles.

Les réseaux et commutateurs virtualisés afin de faciliter la communication entre les machines virtuelles au sein du data center mériteront également une surveillance soutenue puisque leur contrôle échappera aux périphériques en place dédié à la sécurité. Autre risque potentiel, l'hébergement d'applications hétéroclite en terme de niveau d'affectation de sécurité dans une même unité physique. *« Ce n'est pas vraiment un problème mais cela peut le devenir lorsque les charges de travail sont combinées avec d'autres charges issues des zones de confiance différentes sur le même serveur physique sans séparation adéquate »*, estime le gartner.

Qui va administrer et comment?

Se pose également la question de la fiabilité des outils et interfaces de contrôle des accès administrateur. Si les accès à l'hyperviseur doivent être surveillés de près, *« ceci est compliqué par le fait que la plupart des plates-formes de virtualisation fournissent de multiples moyens d'administration pour*

cette couche [de virtualisation] ». Enfin, le Gartner pointe aussi les risques que, dans un environnement de deux systèmes virtualisés, les administrateurs et utilisateurs accèdent à des données pourtant interdites selon leurs droits d'accès. Un risque induit par la complexité de gestion des système qui amène l'analyste à laisser l'équipe de l'infrastructure physique gérer également l'infrastructure virtuelle.

Ces annonces un brin alarmistes ne suffiront pas à freiner la lame de fond de la virtualisation des serveurs, voire des postes de travail, qui monte dans les projets d'entreprises. Si seulement 18 % des ressources se prétend à la virtualisation l'ont été effectivement, cette tendance devrait dépasser les 50 % à l'horizon 2012. Autant de thématiques qui seront développées à l'occasion des Gartner Security Summits du 21 au 23 juin à Washington et les 22 et 23 septembre à Londres.